CISSP Study Notes 2024

CISSP - Certified Information Systems Security Professional | ISC2
This document was created and written from multiple internet resources.

Domain 1 Security and Risk Management

A **risk** is a calculation of the probability of occurrence and the level of damage that could be caused if an exposure is realized (i.e., actually occurs).

The presence of a vulnerability when a related threat exists is an exposure, not a **risk**.

Anything that removes a vulnerability or protects against one or more specific threats is considered a safeguard or a countermeasure, not a **risk**.

The primary goal of **risk** **management** is to reduce **risk** to an acceptable level. Determining this level depends on the organization, the value of its assets, and the size of its budget.

Risk analysis/assessment

Risk analysis/assessment is the process by which **risk** management is achieved and includes inventorying assets, analyzing an environment for threats, and evaluating each risk as to its likelihood of occurring and the cost of the resulting damage.
Risk response is the assessing of the cost of various countermeasures for each **risk** and creating a cost/benefit report for safeguards to present to upper management.

- Analyzing an environment for risks
- Creating a cost/benefit report for safeguards to present to upper management
- Evaluating each threat event as to its likelihood of occurring and cost of the resulting damage

Threat modelling concepts and processes
Compliance, legal, regulatory and privacy
Professional ethics - know the ISC2 code by heart
Security governance principles (ITIL, oversight)
Security policies, standards, procedures and guidelines (know suggested vs. mandatory)

Strong Executive support is the most critical factor for ensuring the success of a security governance program.

Security governance seeks to **compare** the security processes and infrastructure used within the organization with knowledge and insight obtained from **external sources**.

CIA TRIAD - 5 Pillars

Confidentiality
Integrity

Availability
Authenticity
Nonrepudiation

Confidentiality
Access **cont**rols help ensure that only **aut**horized subjects can access objects

Integrity
Ensure that data or **sys**tem **conf**igurations are not **mod**ified without authorization
If a security mechanism offers **integrity**, then it offers a high level of confidence that data, objects, and resources are unaltered from their original protected state.

Availability
Authorized **req**uests for objects must be granted to subjects within a **reas**onable amount of time

Scenario: An organisation wants to make sure its sensitive data is unreadable if it is intercepted during transmissions. Confidentiality principle is the organisation's most concern.

Following is considered violation of **confidentiality**:

- Stealing passwords using a keystroke logging tool
- Eavesdropping on wireless network communications
- Social engineering that tricks a user into providing personal information to a false website

Definition of Risk

Following are valid definitions for risk:

- An assessment of probability, possibility, or chance
- Every instance of exposure

RISK Calculated

Risk == **T**hreat ✖ **V**ulnerability ✖ **I**mpact

5 Pillars of Information Security

1. **Confidentiality** - prevent authorized disclosure of information
2. **Integrity** - prevent unauthorized or unexpected changes to information
3. **Availability** - Ensure access to resources (databases, networks, information, etc.) is available when required by the business
4. **Authenticity** - Proves assets are legitimate, verifies that they are trusted. Proves the source and origin AKA “proof of origin”

5. **Non-repudiation** - Cannot deny or dispute the validity of something; the inability to refute accountability or responsibility. Also inability to deny having done something. Cryptography context, verifying the origin of a message.

Tip
An internal employee transfer should not be used to move a problem employee into a different department rather than firing them.
Consider the overall 5 Pillars of Information Security and benefit to the organization; if a person is not acceptable as an employee in one department, is it realistic to assume they would be in another?
Rather than passing around the problem, the better option is to terminate the problematic employee, especially if direct training and coaching do not provide a resolution.

To defend the security of an organization, a **log of events** and activities must be created. Auditing is a required factor to sustain and enforce Accountability.
Accountability is maintained by **monitor**ing the activities of subjects and objects as well as monitoring core system functions that maintain the operating environment and the security mechanisms.

Ethics are simply rules of personal behavior. Many professional organizations establish formal codes of ethics to govern their members, but ethics are personal rules individuals use to guide their lives.

Canons of ISC^2 **co**de of **eth**ics

The ISC2 Code of Ethics applies only to information security professionals who are members of ISC2.

1. **Prot**ect society the commonwealth, and the infrastructure
2. **Act** honourably, honestly, justly, responsibly and legally
    a. Honorably, honestly, justly, responsibly, and legally
3. **Prov**ide **dil**igent and **com**petent **serv**ice to **prin**cipals
4. **Adv**ance and **prot**ect the **prof**ession

CISSP Example:
Gina recently took the CISSP® certification exam and then wrote a blog post that included the text of many of the exam questions that she experienced.
What aspect of the ISC2® Code of Ethics is most directly violated in this situation?

Answer. Advance and protect the profession.

The canon of the ISC^2 Code of Ethics above.

ISC^2 Code of Ethics complaints Canons:

- Canon I - Any member of general public may bring complaints
- Canon II - Any member of general public may bring complaints
- Canon III - Only an employer or contracted organization may bring complaints

- Canon IV - professionals, example a (CPA, Certified Public Accountant) with standing to bring a complaint

Uncovered evidence that may raise ethical issues, allow the file of a complaint.
According to the (ISC)² ethics policy, complaints must be submitted in writing.

The primary role of a steering committee is setting **strategic** security objectives and priorities.

Whether a person has standing to report a situation to ISC2 depends upon the canon(s) violated by the activity.
This behavior violates canon II, "Act honorably, honestly, justly, responsibly, and legally." Any member of the public may file a claim under canons I or II.
Only an employer or someone with a contracting relationship with the individual may file a complaint under canon III.
Anyone who is certified or licensed as a professional and subscribes to a code of ethics as part of that licensure or certification is eligible to file a canon IV complaint.

Domain 1 Security Documents

Security Documentation definitions:

- Security Policy
  - Document that defines the scope of security needed
  - Policy is promulgated by senior management and outlines the organization's strategic vision and goals
  - mandatory
- Security **proc**edures -
  - detailed **step**-by-step
- Security **Guide**lines -
  - offer **recom**mendations
  - A guideline would be the perfect place to document best practices for securing IoT devices.
  - Guidelines provide advice based on best practices developed throughout industry and organizations, but they are **not compulsory**.
  - Compliance with guidelines is **optional**.
- Security **base**lines
  - define **mini**mum levels
  - provide configuration information regarding the **minimum leve**l of security that every system in the organization must meet.
  - Baselines provide the **minimum level** of security that every system throughout the organization must meet.
- Security Standard -
  - **mandatory**
  - compulsory requirements for the homogenous use of hardware, software, technology, and security controls
- Acceptable use **pol**icy - Assign **role**s and **resp**onsibilities

Security Policy Roles

- The **security professional (CISSP)** has the functional responsibility for security, including writing the security policy and implementing it.
- Senior **management** is ultimately responsible for the security maintained by an organization and who should be most concerned about the protection of its assets.
    - security governance is based on the idea that senior management is responsible for the success or failure of a security endeavor
- The **custodian** role assigned to the user responsible for the tasks of implementing the prescribed protection defined by the security policy and senior management.
- An **auditor** is responsible for reviewing and verifying that the security policy is properly implemented and the derived security solutions are adequate.

Security Policy

Security policies provide direction for all levels of the organization's hierarchy.
Security policies typically provide guidance on acceptable employee behaviour and actions to maintain a secure environment.

Primary purpose of a **security policy** in an organisation is to provide high-level guidance and direction for security efforts.

A security policy is best described as a set of mandatory directives that employees must follow providing the basic framework upon which a company's security program is based.

While security policies may reference technical configurations, roles and responsibilities, and **incident resp**onse procedures. These details are typically found in supporting documents and procedures.

Domain 1 Risk Categories

- **Dam**age - results in physical loss of an asset or the inability to access the asset
- **Discl**osure - disclosing critical info regardless of where or how it was disclosed
- **Loss**es - these might be permanent or temporary, including **alt**ered **dat**a or **inac**cessible **da**ta (ransomware)

Domain 1 Risk Factors

- **Phy**sical damage - natural disaster, power loss or vandalism
- **Malf**unctions - failure of systems, networks or peripherals
- **Att**acks - purposeful acts whether from the inside or outside, such as unauthorized disclosure
- **Hum**an errors - usually considered accidental incidents, whereas attacks are purposeful incidents
- **App**lication **er**rors - failures of the application, including the operating system

Regardless of the specifics of a security solution, **humans** are often considered the weakest element. No matter what physical or logical controls are deployed, humans can discover ways to avoid them, circumvent or subvert them, or disable them.

Domain 1 Security Planning

- **Strategic** - long-term, stable plan that should include a risk assessment (**5 y**ear horizon, annual updates)
    - A strategic plan is a long-term plan that is fairly stable. It defines the organization's security purpose. It defines the security function and aligns it to the goals, mission, and objectives of the organization.
- **Tact**ical - **midterm** plan developed to provide more details on goals of the strategic plan (usually **1 y**ear)
- **Opera**tional - **short term** highly detailed plan based on the strategic and tactical plans (**monthl**y, quarterly).

Domain 1 Response to Risk

- Risk **Accept**ance -
    - **do not**hing and you must accept the risk and potential loss if threat occurs
    - if the safeguards or counter measures outweigh the potential loss in terms of their cost then just simply accepting a risk might make sense
    - A **risk acceptance documentation** should contain a thorough review of the risks facing the organization, including the determination as to which risks should be considered acceptable and unacceptable. For acceptable risks, the documentation should include a rationale for that decision and a list of potential future events that might warrant a reconsideration of that determination. The documentation should include a list of controls used to mitigate unacceptable risks, but it would not include controls used to mitigate acceptable risks,
- Risk **mitigation** -
    - you do this by implementing a **counter**measure and accepting the **resid**ual risk
    - implement countermeasure and we accept the residual risk that's the risk that's left over once our safeguards our security controls are in place now in risk assignment this is also called risk transference
- Risk **Assign**ment -
    - **transfer** assigns risk to **3rd** parties, like purchasing insurance against damage.
    - Insurance is a form of risk assignment or transference.
    - we're transferring or assigning that risk to a third party like in purchasing insurance against damage and outsourcing to companies with specific expertise is another way we commonly see risk assigned or transferred
- Risk **Avoid**ance
    - when **costs** of mitigating or **accept**ing are higher than benefits of the service.
    - Stop offering the service because of the risk, cost, or accepting
    - the cost of compliance would outweigh the additional revenue.

    - In the context of security risk management, risk avoidance is the most appropriate response for risks that are outside the organisation's risk appetite.
- Risk **Det**errence -
    - implementing de**terrent**s to would be violators of security and policy
    - Audit policy to employees
    - Security cameras or warning signs
- Risk **reje**ction -
    - an **unacc**eptable possible response to risk or **ign**ore risk

Risk Acceptance - When controls are not cost effective, they are not worth implementing. During a risk management project, an evaluation of several controls determines that none are cost-effective in reducing the risk related to a specific important asset.

In the context of risk management, the primary purpose of a risk treatment plan is to make sure risks do not take place in the organization.
From Risk management options, **avoidance** is preventing the risk all together!
mitigation lowers the likelihood, or impact, but risk may still happen.

Remember: Handling risk is not a one-time process!

Risk Mitigations

- **Third-party assessment** and monitoring
    - Evaluating and continuously monitoring the security practices and performance of third-party vendors or suppliers
    - Business partnerships
    - Cloud Services
    - Telecommuting
- **Minimum security requirements**
    - Predefined baseline security standards that vendors must meet
- **Service level requirements**
    - Specifications set in contracts that dictate the expected performance, availability, and responsiveness of a service provided by a vendor.
- Silicon root of trust
    - A secure cryptographic identity embedded in hardware, ensuring that the hardware starts in a trusted state and that the firmware loaded onto it is genuine.
- Physically unclonable function
    - A hardware feature that uses the unique physical characteristics of semiconductor devices to generate ***cryptographic*** keys, ensuring that each device has a unique and unclonable identity.
- Software bill of materials
    - Comprehensive list of components, libraries, and modules that are used to build a software product, often detailing versions, sources, and dependencies.

Purchasing insurance that covers the theft or loss of a computer best describes **transferring risk**. Risk transfer occurs when a company shifts the risk to another party, such as an

insurance company. Risk transfer should be performed whenever the cost of the insurance is less than the cost of the item being insured.

Installing antivirus software on a computer is not an example of transferring risk: it is an example of mitigating risk. Risk mitigation lowers the chance that a risk event occurs or lowers the damage that a risk event causes. Risk mitigation should be performed whenever the costs of mitigating a risk are lower than the benefits gained.

Teaching employees how to handle social engineering threats is not an example of transferring risk: it is an example of mitigating risk. It is important to note that teaching employees how to handle social engineering threats does not transfer the risk to the employees; you are merely transferring some of the responsibility of handling the risk to the employees.

Cybersecurity Insurance

Specialised insurance product designed to help organisations protect against financial losses resulting from cyber-related incidents.
Cybersecurty insurance does not transfer the risk, accountability is still with the company.
Cybersecurity insurance mitigates the cost and financial outlay.

Vendor Management System (VMS)

This scenario describes a situation that would benefit from a vendor management system (VMS). VMS is a software solution that assists with the management and procurement of staffing services, hardware, software, and other needed products and services. A VMS can offer ordering convenience, order distribution, order training, consolidated billing, and more.
VMS Scenario:
Your organization works with several third-party suppliers for a wide range of services, including accounting, payroll, benefits management, help desk, incident response, log analysis, and more. The CEO has recently complained that the organization is likely wasting money due to paying for the same services from multiple providers and not taking full advantage of the services from those providers and still performing some of those tasks in-house. In order to gain a better understanding of the outsourced services as well as improve ordering convenience, manage related training, and consolidated billing, Vendor Management System (VMS) should be implemented.

Domain 1 Risk Management Framework

Risk Maturity Model

RMM
The Risk Maturity Model (RMM) is specifically designed for the purpose of assessing enterprise risk management programs.

RMM is an industry-standard approach for assessing the processes his organization uses to manage risk.

Frameworks & Standards

- ISO - International Organization for Standardization
  - 15408 Evaluation Criteria
  - 22301 Security and Resilience
  - 27001 Information Security (Standard/Controls)
  - 27002 InfoSec Guidance (Implementation Guidance)
  - 27031 Business Continuity
- NIST - National Institute of standards and technology
  - NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments
  - 800-37 Risk Management Framework (**RMF**)
  - 800-47 Certification and Accreditation
  - 800-**53 Cybersecurity Framework**
    - NIST SP 800-53 description of controls mandatory for use on U.S. federal government systems
  - 800-53A
    - NIST SP 800-53A is titled Assessing Security and Privacy Controls in Information Systems and Organizations and would be the best guide for conducting an internal assessment of a U.S. federal government system to determine whether it has appropriate security and privacy controls.
    - Entitled Security and Privacy Controls for Information Systems and organisations
  - 800-63 Password policy
    - NIST SP 800-63B recommends users only be required to change their password if their current password is compromised. They do not recommend that users be required to change their password regularly at any interval.
  - NIST SP 800-88
    - guidelines for media sanitization.
  - 800-92 Log Management
  - 800-122
    - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
  - NIST SP 800-137, continuous security monitoring strategy
    - organizations should use the following factors to determine assessment and monitoring frequency: security control volatility, system categorizations/impact levels, security controls or specific assessment objects providing critical functions, security controls with identified weaknesses, organizational risk tolerance, threat information, vulnerability information, risk assessment results, the output of monitoring strategy reviews, and reporting requirements.
  - 800-171
    - Environments containing controlled **unclassified** information
  - 800-162 Guide to ABAC (Attribute Based Access Control)

- FIPS - Federal Information Processing Standards
    - 140-3 Security Requirements for Cryptographic Modules
- COBIT - Control Objectives for information and Related Technology
- SABSA - Sherwoord Applied Business Security Architecture
- PCI - Payment Card Industry
- FedRAMP - Federal Risk and Authorization Management Program

Primary goal of a security governance framework, aligning security with **business objectives.**

Security Control Frameworks

- COBIT - Assurance
    - Preferred choice by Business owners data role
- ITIL - IT Service Management
    - Security framework Information Technology Infrastructure Library (**ITIL**) was initially created by the British UK government for **domestic** use but is now an international standard, which is a set of recommended best practices for core IT security and operational processes, and is often used as a starting point for the crafting of a customized IT security solution.
    - British government for domestic use
    - ITIL, which originally stood for IT Infrastructure Library, is a set of practices for IT service management and is **not** typically used for auditing.
    - IT service management and includes topics such as change management, configuration management, and service-level agreements
- **NIST - Cybersecurity framework**
- PCI Credit card Processing
- HIPAA - Safeguarding medical information
    - involve criminal penalties if violated
    - Health Insurance Portability and Accountability Act (HIPAA) is a U.S. law governing the healthcare sector that does provide for criminal penalties
- SOX - Protect investors
    - may involve criminal penalties if violated
    - Sarbanes–Oxley (SOX) Act governs publicly traded corporations and also provides for criminal penalties.
- FedRAMP - Cloud security for US Government
- FISMA - Security requirements for US Government
    - places authority for classified systems in the hands of the National Security Agency (NSA) and authority for all other systems with the National Institute for Standards and Technology (NIST).

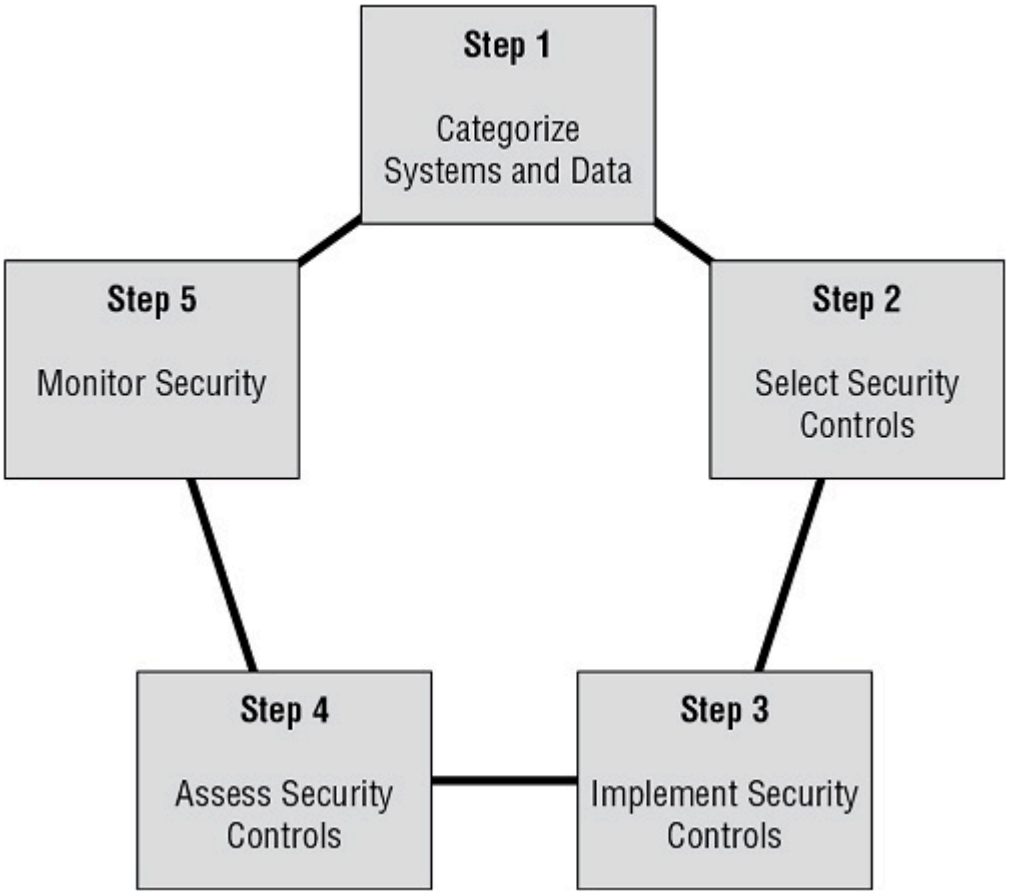
Primary purpose of a security control framework in an organization's information security program is to provide a baseline for secure configurations.

The primary risk management framework referenced in CISSP is NIST 800-37
Chapter 2 Personal Security and Risk Management Concepts - page 79 - Risk Frameworks

security life-cycle diagram

As shown in the following security life-cycle diagram (loosely based on the NIST reference architecture), NIST uses a five-step process for risk management. Using your knowledge of data roles and practices, answer the following questions based on the NIST framework process.

1. Step 1 - Categorize System and Data
2. Step 2 - Select Security Controls
3. Step 3 - Implement Security Controls
4. Step 4 - Assess Security Controls
5. Step 5 - Monitor Security



PCI-DSS Scenario:
If the systems that are being assessed all handle credit card information (and no other sensitive data), at what step would the PCI DSS first play an important role?
Step 2 - Select Security Controls
Reason:
PCI DSS provides a set of required security controls and standards. Step 2 would be guided by the requirements of PCI DSS. PCI DSS will not greatly influence step 1 because all of the systems handle credit card information, making PCI DSS apply to all systems covered. Steps 3 and 4 will be conducted after PCI DSS has guided the decisions in step 2.

Risk Management Framework

One of the first and most important security planning steps is to consider the overall security control framework or structure of the security solution desired by the organization. This framework establishes **mandatory** requirements for federal agencies.

Risk assessment or risk analysis is the examination of an environment for risks, evaluating each threat event as to its likelihood of occurring and the severity of the damage it would cause if it did occur, and assess the cost of various countermeasures for each risk. This results in a sorted criticality prioritisation of risks.

The primary purpose of a risk assessment is to identify and prioritize potential risks to the organization's information assets, not necessarily to eliminate them.

Risk Assessment is evaluating an asset to ascertain the amount of vulnerability it represents to a company.

Risk management is composed of two primary elements: risk assessment and risk response.

Risk assessment or risk analysis is the examination of an environment for risks, evaluating each threat event as to its likelihood of occurring and the severity of the damage it would cause if it did occur, and assessing the cost of various countermeasures for each risk.

Risk response is evaluation of countermeasures, safeguards, and security controls using a cost/benefit analysis; adjusting findings based on other conditions, concerns, priorities, and resources; and providing a proposal of response options in a report to senior management;

Risk awareness is the effort to increase the knowledge of risks within an organization.

Sherwood Applied Business Security Architecture (SABSA)

- Security control frameworks
  - Provide a prescriptive set of cybersecurity safeguards and best practices to protect an organizations valuable assets
  - Help in implementing the risk management strategy
  - **How** - providing specific controls to mitigate cybersecurity risks.
- Risk Frameworks
  - Provide a structure approach to identifying, assessing, prioritising, and managing risk to guide decision making
  - Provide the overarching structure for making risk-informed decisions
  - **Why** - they guide strategic decision making about risk

SABSA adds another “**how**” layer by focusing on the structure and design of the security architecture itself.

SABSA focuses on aligning security with **business goals** by providing a structured method for designing, implementing, and managing security architectures.
It can be used in conjunction with both risk frameworks and security control frameworks.
SABSA adds a layer focused on practical security architecture implementation.

NIST Risk Management Framework (RMF)

RMF's audience is federal government agencies
The RMF is mandatory for those to which it applies.
Address cybersecurity risk management

NIST Cybersecurity Framework (CSF)

CSF is aimed at private commercial business
The CSF is purely optional guidance from NIST
Address cybersecurity risk management

FedRAMP

Federal Risk and Authorization Management Program
A government wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for **cloud products and service**s.
The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government-wide program designed to standardize the security assessment, authorization, and continuous monitoring processes for cloud products and services used by federal agencies.

FedRAMP Goals:

- Accelerate secure cloud adoption
- Enhance trust in cloud solutions
- Promote a reusable approach for multiple agencies

FedRAMP Key Elements

- Security standardisation
- Authorization process
- Continuous monitoring
- Reuse of authorizations
- Collaboration
- Three impact levels (Low, Moderate, High)
- Compliance framework

ISO/IEC 27001:2022 Framework

Standard / Controls based on British standard 7799 (BS 7799)
ISO 27001 focuses more on the **WHAT** and **WHY**

Outlines a framework for implementing, maintaining, and continually improving an information security management system (ISMS)
An ISMS is a set of policies, processes and controls that helps organizations protect their information assets.

Guides organizations:

- Identifying information assets and assessing their value and information security risks AND
- Implementing mitigation security controls (based on ISO 27002)
- Regularly monitoring and measuring effectiveness of and continuously improving the ISMS

ISO/IEC 27002:2022 Frameworks

Implementation Guidance
ISO 27002 brings practical guidance on the **HOW**

ISO 27002 control objective framework that is widely accepted around the world and focuses specifically on information security controls.

Offers best practices and control objectives related to key aspects of cybersecurity in support of ISO/IEC 27001.
Focus areas include access control, cryptography, human resource security, operational security, and incident response.
Serves as a practical blueprint for organizations aiming to effectively safeguard their information assets against cyber threats.

Organizations can certify on ISO 27001 as an attestation to their implementation of information security best practices.

attestation = evidence or proof

Risk Documents

- Risk reporting involves the production of a risk report and a presentation of that report to the interested/relevant parties
- A risk register or risk log is a document that inventories all of the identified risks to an organization or system or within an individual project
- A risk matrix or risk heat map is a form of risk assessment that is performed on a basic graph or chart.
- A risk register can serve as a project management document to track completion of risk response activities as well as a historical record of risk management over time.

Security Risk Management Frameworks

- RMF defined by NIST 800-37

- ISO 31000
- COSO's ERM
    - Committee of Sponsoring Organizations (COSO) of the Treadway Commission's Enterprise Risk Management
- ISACA Risk IT - Information Systems Audit and Control Association
- OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation
- FAIR
- TARA
    - Threat Agent Risk Assessment
- **FedRAMP**
- **SABSA**
    - SABSA is a proven methodology for developing business-driven, risk and opportunity focused Security Architectures at both enterprise and solutions level

RMF 7 steps (NIST 800-37)

Risk Management Framework (RMF) Elements:

1. **Prep**are to execute the RMF (Risk management Framework)
    a. **Prep**are the organisation to manage its security and privacy risks using the RMF
2. **Categorize** info systems
    a. Determine the **adv**erse **imp**act to operations, assets, individuals, etc. with respect to the loss of CIA or organisational systems.
3. **Select** security **cont**rols
    a. Assigning different values for a control
    b. Select, **tail**or, and document the controls necessary to protect the information system and organisation commensurate with the risk.
    c. The tailoring process refers to modifying a list of controls to align with the organization's mission.
        i. Example is Scoping and tailoring using the Center for Internet Security (CIS) benchmarks
    d. Tailoring refers to modifying a list of security controls to align with the organization's mission.
4. **Implement** security **cont**rols
    a. Implement controls and to document in a **base**line configuration, the specific details of the control implementation
5. **Assess** the security controls
    a. **Deter**mine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome
6. **Authorize** the system
    a. Provide **account**ability by requiring a senior management official to determine if the security and privacy risk based on the controls is acceptable
    b. Phase of RMF focuses on determining whether system or common controls are based on a determination that the risk to organizational operations and

assets, individuals, other organizations, and the nation is acceptable/**reasonable**.

7. **Monitor** security controls
    a. Monitor security is the Custodians role, primarily responsible
    b. Maintain an **ong**oing situational awareness about the security and privacy posture of the information system and the organisation in support of risk management decisions.

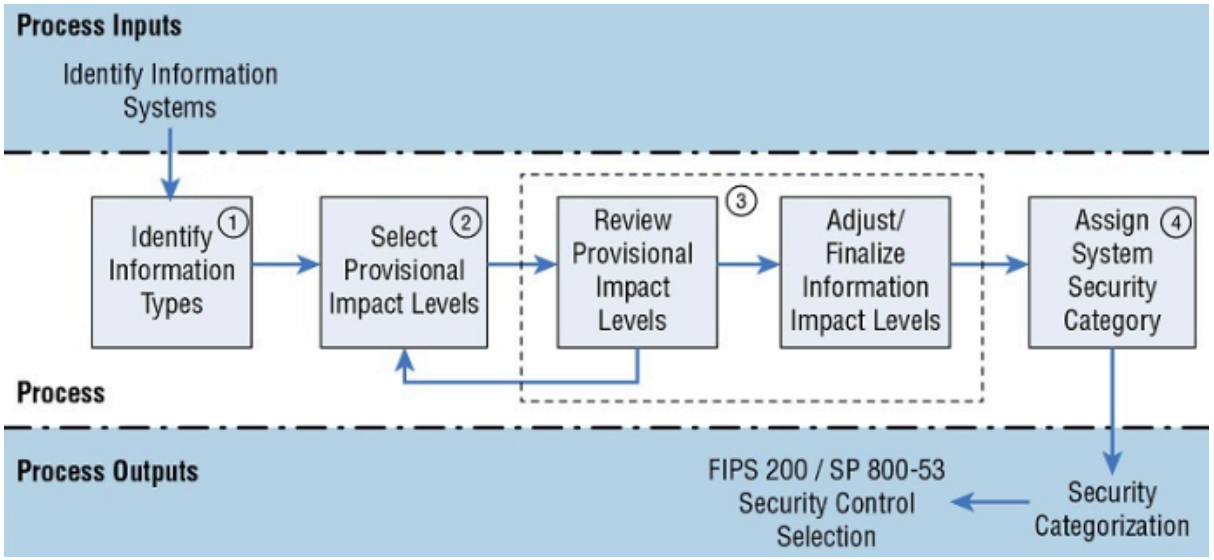
"People **C**an **S**ee **I** **A**m **A**lways **M**onitoring"

Categorize info systems

NIST Special Publication (SP) 800-60 has been developed to assist Federal government agencies to categorize information and information systems.
In the NIST SP 800-60 diagram, the process determines appropriate categorization levels resulting in security categorization and then uses that as an input to determine controls.
Steps

1. Process inputs, identify information systems
2. Identify information types
3. **Select** provisional impact levels
4. **Review** provisional impact levels
5. Adjust finalize information impact levels
6. Assign system security category
7. Security Configuration FIPS 200 / SP 800-53 Security Control Selection

Diagram process determines appropriate categorization levels



Standard selection would occur at an organizational level, while baselining occurs when systems are configured to meet a baseline. Sanitization would require the intentional removal of data from machines or media.

Exam Notes:

- Not every risk can be mitigated
- Management decide how that risk is handled
- Security professional is risk adviser
- When multiple priorities present, human safety is most important
- When a legal issues are involved, "call an attorney" is valid choice

Organisational Processes

A **divestiture** or any form of asset or employee reduction is another time period of increased risk and thus increased need for focused security governance.
Assets need to be sanitised to prevent data leakage.
Storage media should be removed and destroyed, because media sanitization techniques do not guarantee against data remnant recovery.
Employees released from duty need to be debriefed. This process is often called an **exit interview.**

Domain 1 Types of Risk

Residual Risk - The Risk that **rem**ains even with all **conc**eivable **safe**guards in place. The risk management has chosen to accept rather than mitigate.
Inherent Risk - Newly identified risk **not** yet **add**ressed with risk **man**agement **strat**egies, The amount of risk that exists in the absence of controls.
Total Risk - The amount of risk an organisation would face if **no safeguards** were implemented.

Residual AFTER
Inherent BEFORE
Total WITHOUT

Risk Management Program

Ultimate goal of a good risk management program is to minimize the residual risk.
Key risk indicators (KRIs) are often used to monitor risk for organizations that establish an ongoing risk management program.

Key Risk Indicators (KRIs) are metrics used by organizations to signal potential risks that could impact the achievement of key business objectives. They are forward-looking measures designed to provide early warnings about potential issues so that preventive actions can be taken. KRIs are an important component of a proactive risk management strategy.

Using automated data gathering and tools that allow data to be digested and summarised can provide predictive information about how organizational risks are changing.

KPIs are key performance indicators, which are used to assess how an organization is performing.
Key risk indicators (KRIs) are valuable for organizational risk planning and understanding risk perceptions but are ***not*** designed for real-time security incident response.

Example of Inherent Risk:
A new web application was installed onto the company's public web server last week. Over the weekend a malicious hacker was able to exploit the new code and gained access to data files hosted on the system.

Formulas

Total Risk:

Threats * vulnerabilities * asset value = total risk

Risks

Risks are the combination of a threat and a vulnerability.

Risk = threat * vulnerability

Risk Scenario:

Ryan is a security risk analyst for an insurance company. He is currently examining a scenario in which a malicious hacker might use a SQL injection attack to deface a web server due to a missing patch in the company's web application.
In this scenario, what is the threat?
Malicious hacker
Risks are the combination of a threat and a vulnerability.
Threats are the external forces seeking to undermine security, such as the malicious hacker in this case.
Vulnerabilities are the internal weaknesses that might allow a threat to succeed.
In this scenario the missing patch is the vulnerability, and the malicious hacker is the threat.
If the hacker (threat) attempts a SQL injection attack against the unpatched server (vulnerability), the result is website defacement.

Domain 1 Risk Analysis

Qua**lita**tive vs. Quan**titati**ve

Quan**titati**ve - Assigns a **doll**ar value to evaluate **eff**ectiveness of countermeasures

Quantitative Risk Analysis Steps

1. **Inv**entory **ass**ets and assign a value (asset value, or AV)
2. **Id**entify **thr**eats - **res**earch each asset and produce a list of all possible threats of each asset (and calculate EF and SLE)

3. **Perf**orm a threat **anal**ysis to calculate the likelihood of each threat being realised within a single **ye**ar (the ARO)
4. **Esti**mate the **pot**ential loss by calculating the **ann**ualised loss expectancy(**ALE**)
5. **Res**earch countermeasures for each **thr**eat, and then **calc**ulate the changes to ARO and ALE based on an applied countermeasure.
6. Perform a **cos**t/benefit **ana**lysis of each **counter**measure for each threat for each asset.

Quantitative risk assessment, describes the determination of asset value (**AV**) as well as the **exposure factor (EF)** and the annualized rate of occurrence (**ARO**) for each identified threat. These are the needed values to calculate the annualized loss expectancy (**ALE**), which is a quantitative factor.

The annual costs of safeguards should not exceed the expected annual cost of asset value loss. (ALE)

Qua**litati**ve - uses a **scor**ing system to **ran**k threats and **effe**ctiveness of countermeasures. It is difficult to put a dollar figure on the business lost because of **negative publicity**. Therefore, this type of concern is better evaluated through a **qualitative** analysis.

Delphi Technique - an anonymous feedback-and-response process used to arrive at a consensus.

Consider:

Loss **pot**ential - **what** would be **lost** if the threat agent is successful in exploiting a vulnerability.
Delayed **los**s - this is the amount of loss that can occur over time.

Threat **ag**ents are what **cau**se the threats by **exp**loiting vulnerabilities.

Domain 1 Calculating Risk

Terms and formulas:

- **Asset Value (AV)**
- **Exp**osure factor (EF) **%**
- **Sin**gle loss expectancy (SLE) - Impact Assessment
- **Ann**ualised rate of occurrence (ARO)
- **Ann**ualised loss expectancy (ALE)
- **Safe**guard evaluation (ACS)

CISSP Practice Questions and Answers | CISSP Exam 2024 | CISSP Questions and A…

AV (Asset Value)

The crown jewel asset of the business money value, containing sensitive information, systems or processes.

EF (Exposure factor)

Percentage of loss that an organisation would experience if a specific asset were violated by a realised risk

SLE (Single Loss Expectancy)

The single loss expectancy (SLE) is a quantitative measure of how much damage would occur each time a risk materializes.
Single ***item*** loss expectancy even if three of the same items fail.?
It is a measure of risk impact.
Represents the **cos**t associated with a **sing**le realised **ris**k against a specific **ass**et.

SLE	= Asset Value (AV)	X Exposure Factor (EF)
$30 000	= $100 000	X 0.3 (30%)

<u>Scenario / Example:</u>
concerned about the risk that an avalanche poses to your $3 million shipping facility. Based on expert **opinion**, you determine that there is a 5 percent chance that an avalanche will occur each year. Experts advise you that an avalanche would completely destroy your building and require you to rebuild on the same land. Ninety percent of the $3 million value of the facility is attributed to the building, and 10 percent is attributed to the land itself. What is the single loss expectancy (SLE) of your shipping facility to avalanches?

- (AV $3 000 000 x 0.90 EF 90 %) == $2,700,000

ARO (**Ann**ualised **ra**te of **Occ**urrence)

The expected frequency with which a specific threat or risk will occur within a **sing**le **ye**ar.

The annualized rate of occurrence (ARO) is the likelihood that the risk will materialise in any given year.
The fact that a power outage did not occur in any of the past three years does not change the probability that one will occur in the upcoming year.
Unless other circumstances have changed, the ARO should remain the same.

A **countermeasure** primarily affects the **annualized rate of occurrence (ARO)**, because the countermeasure is designed to prevent (or mitigate or reduce) the occurrence of the risk, thus reducing its frequency per year. It is possible that a countermeasure will also reduce the exposure factor (EF) or the amount of loss per incident, but this is not as common as ARO reduction.

The Annualized Rate of Occurrence (ARO) represents the expected frequency of a particular risk event occurring within a given timeframe. Given that the ARO of a power outage was assessed as 20% three years ago and no power outage has occurred since, Darren should continue to use this ARO in his current assessment if the circumstances underlying the analysis have not changed.

The lack of occurrence of the event in the past three years does not necessarily reduce the ARO unless there are specific changes in the environment or mitigating controls that reduce the likelihood of such an event.

ALE (Annualised loss expectancy)

The annualized loss expectancy (ALE) is the best metric to compare **relative risks** because it incorporates both the likelihood and the impact of those risks.
The possible yearly cost of all instances of a specific realised threat against a specific asset.

ALE = single loss expectancy (SLE) * annualised rate of occurrence (ARO)

ALE = AV × EF × ARO

The **annualized loss expectancy (ALE)** is computed as the product of the **asset value (AV)** times the **exposure factor (EF)** times the annualized rate of **occurrence (ARO).**
This is the longer form of the formula ALE = SLE × ARO, since SLE = AV × EF.

The annualized loss expectancy (ALE) is the product of the annualized rate of occurrence (ARO) and the single loss expectancy (SLE).
Example, we first calculate the ARO as once every 50 years equals 1 / 50, or 2 percent. The SLE is $8 million, giving an ALE of $160,000.

ACS (Annual Cost Safeguard Evaluation)

Good security controls mitigate risk, are transparent to users, difficult to bypass, and are cost effective.
If a security control's benefits cannot be quantified, evaluated, or compared, then it does not actually provide any security.

Cost Effective?

ALE before safeguard **-** ALE after safeguard **-** annual cost of safeguard (ACS) **=** value of safeguard

The **value of a safeguard** to an organization is calculated as following:
ALE before safeguard – **ALE** after implementing the safeguard – annual cost of safeguard
This is known as the cost-benefit equation for safeguards.

To determine the optimal allocation of resources in the context of risk management, is the primary purpose of conducting a cost-benefit analysis.

ACS Scenario

You are evaluating the benefit of a **safeguard** to a specific threat.
The asset is a customer database, which is estimated to be worth **$10 million**.
The threat is an intrusion that could cause a **50 percent value loss.**
The attack has already been attempted **three** times in the last **6 months**.
The best **countermeasure** would be to reduce the success rate to only **once per year**, but the cost of the protection is **$350,000**.

Calculating benefit:

- Asset Value (AV) =$10,000,000
- Exposure Factor (EF) = 50%
- ACS (Annual Cost **Safeguard**) = $350,000.

Single Loss Expectancy
SLE = AV x EF
= $10mil x 50%
= $ 5 000 000 (SLE) : Single Loss

Annual Rate Occurrence
ARO = 6 per year : Rate occurs

Annual Loss Expected
ALE.1 = SLE x ARO
= $5mil x 6
= $ 30 000 000 : Annual Loss Expect

Post Safeguard installed calculations:

Annual Rate Occurrence **with SafeGuard**
ARO = 1 per year

Annual Loss Expected **with SafeGuard**
ALE.2 = SLE x ARO
= $ 5mil x 1
= $ 5 000 000 : ALE **after installed safeguard**

Benefit = ALE.1 - ALE.2 - ACS
= $30 mil - $5 mil - $ 350 000
= $ 24 650 000

The benefit of this **countermeasure** is $24,650,000.

Countermeasure Definition:

- The result of the applied countermeasure should make the cost of an attack greater for the perpetrator than the derived benefit from an attack.

- The countermeasure should provide a solution to a real and identified problem.
- The benefit of the countermeasure should be testable and verifiable.

Scenario Buy vs. Lease

There is no cost difference between purchasing and leasing the printer.
The cost to purchase a printer plus the Annualized Loss Expectancy (ALE) of $300 equals $2,700 over the **five**-year contract, which is the same as the cost to lease the printer.

Your department's budget could be negatively affected if you make a decision based on inaccurate calculations.
For example, if you were to simply compare the cost of the printer to the cost of the lease over the five-year period, you might ***assume*** it would be $1,500 cheaper to purchase the printer. However, you must also add the cost to maintain or replace the printer, which is the ALE. To calculate the ALE, you must first determine the Annualized Rate of Occurrence (ARO) and the Single Loss Expectancy (SLE).
The ALE is the result of the calculation ARO × SLE = ALE.

Historical data or manufacturer data is used to calculate the ARO, which is the **frequency** at which equipment fails. For example, a printer that fails once every four years has an ARO of 0.25, or 25 percent, as shown in the following calculation:

1 failure ÷ 4 years = 0.25 failures per year (**ARO**)

The cost of one occurrence of a failure is known as the SLE, which includes the cost of materials, the technical service hours required, and lost productivity while the printer is unavailable to employees. In this scenario, the $1,200 cost of the printer represents the SLE. No costs must be added for lost productivity, because the scenario states that a failure will produce no significant effect on production or technical services.

When you know the value of the ARO and the SLE, you can calculate the ALE by multiplying the ARO by the SLE as shown below:

$1,200 (**SLE**) × 0.25 (**ARO**) = $300 (**ALE**)

To calculate the total cost of purchasing a new printer and using it over a five-year period, you should use the calculation shown below:

$1,200 (cost to purchase a printer) **+** $1,500 (ALE over the five-year contract period)
= $2,700
(total cost of purchasing and maintaining a printer for the five-year contract period)

To calculate the total cost of leasing the printer over a five-year period, you should use the calculation shown below:

$540 per year **×** 5 years = $2,700 (total cost to lease the printer for the five-year contract period)

It is important to note that although the cost of purchasing a printer versus leasing a printer is the same over a five-year period, the cost of purchasing a printer is less than the cost of leasing a printer over a longer period. Conversely, the cost of purchasing a printer is more than the cost of leasing a printer over a shorter period.
For example, the cost of purchasing and maintaining a printer for ***six*** years is $3,000, whereas the cost to lease the printer for ***six*** years is $3,240. Over a four-year period, the cost of purchasing and maintaining a printer is $2,400, whereas the cost to lease the printer for four years is $2,160.

Domain 1 Administrative Controls

The category of administrative access controls are the policies and procedures defined by an organization's security policy and other regulations or requirements. They are sometimes referred to as management controls, managerial controls, or procedural controls.
These controls focus on personnel oversight and business practices.

Administrative Access Controls Include:
- hiring and firing policies
- data classifications and labels
- security awareness and training

Scenario:
After attending a security conference, the CISO updates the security policy in regard to the use of smartcards. The new requirements are that cards are to be updated yearly and that both a PIN and a fingerprint scan must be used for system authentication. At the start of the next quarter, the CISO performs a compliance audit in regard to the changes of the smartcard authentication system.
Managerial control is this final activity.

A passport and a birth certificate **establish the identity** of the **new hire.**
Proofing requires users to answer questions to prove their identity.
Proofing when signing up for banking services, to ensure that users are who they claim to be.
In the context of banking applications, validate user identity using information that both the bank and the user have such as questions pulled from their credit report.

Examples of administrative controls include policies, procedures, hiring and firing practices, background checks, **data classif**ications and labelling, security awareness and training efforts, reports and reviews, work supervision, personnel controls, and testing.

A company's security policy states that user accounts should be disabled during the exit interview for any employee leaving the company.
To retain the decryption key is the most likely reason for this policy.

Firing/Termination process:
- Returning company property

- Having a witness for the exit interview
- Escorting off premises

Enrollment or Registration is the action of initial creation of user accounts for a batch of new employees.
Enrollment, or registration, is the initial creation of a user account in the provisioning process.
Provisioning processes to validate or verify process followed:

- Low Review
- Manual REview of permissions
- Review the audit trail

Domain 1 Controls Gap

Controls Gap formula

Total risk - controls gap = residual risk

Domain 1 Supply Chain

Supply Chain Evaluation

When evaluating 3rd parties in the chain, consider:

- **On-sit**e assessment -
    - visit organisation, interview personnel, and observe their operating habits
    - An on-site assessment is a third-party assessment tool where auditors visit the site of the organization to interview personnel and observe their operating habits.
- **Doc**ument exchange and **rev**iew -
    - investigate **dat**aset and doc exchange, review processes
    - Document exchange and review is a mechanism to investigate the means by which datasets and documentation are exchanged as well as the formal processes by which they perform assessments and reviews.
- **Proc**ess/Policy **Rev**iew -
    - request copies of their security policies, **proc**esses/procedures.
    - Process/policy review is a mechanism that requests copies of their security policies, processes/procedures, and documentation of incidents and responses for review.
- **Thir**d-party **Aud**it -
    - having an independent auditor provide an **unbi**ased review of an entities security infrastructure
    - A third-party audit is performed by a third party, such as defined by AICPA (American Institute of Certified Public Accountants), to provide an unbiased review of an entity's security infrastructure.

Supply Chain Risk Management SCRM

A means to ensure that all the vendors or links in the supply chain are reliable, trustworthy, reputable organizations that disclose their practices and security requirements to their business partners.
Supply chain risk management (SCRM) is a means to ensure that all the vendors or links in the supply chain are reliable, trustworthy, reputable organisations.
The following are **true SCRM statement**s:

- Each link in the supply chain should be responsible and accountable to the next link in the chain.
- Commodity vendors are unlikely to have mined their own metals or processed the oil for plastics or etched the silicon of their chips.
- Failing to properly secure a supply chain can result in flawed or less reliable products, or even embedded listing or remote control mechanisms.

Relying on a single vendor to provide vendor stability, **not** a common practice.

Concern about gray market suppliers that are importing the hardware from outside the country at a much lower price, is the security of the hardware and firmware

Gray market Supply chain risk examples:

- Product tampering
- Implants
- Counterfeits
- Adversary tampering with hardware prior to being shipped to the end customer
- Adversary using social engineering to compromise an employee of a SaaS vendor to gain access to customer accounts

<u>Scenario</u>
Mark's company has just signed a two-year SLA with a major cloud service provider. The company is developing a new line of product based on their own internally developed technology that has not been published or revealed to any external entity. A few months after the company has integrated the cloud service into their production processes, Mark receives an advertisement from a vendor claiming to sell a product based on new features never before seen. After further research, Mark realises that those new features are the exact technology their company developed and maintained as an internal trade secret. Mark is confident that he knows where the leak occurred.
Service-focused supply chain risk
service-focused supply chain risk based around the insecure services provided by the cloud company.

Risk Mitigations (SCRM)

Hardware Root of Trust
A line of defense against executing unauthorized firmware on a system
And when certificates are used in FDE, they use a hardware root of trust for key storage.
It verifies that the keys match before the secure boot process takes place.

Trusted platform module (TPM) and Silicon root of trust (SRoT) are both implementations of hardware root of trust.

Silicon Root of Trust (SRoT)

Silicon Root of Trust is a specialized chip or module embedded directly into the hardware of a device (server, IOT, etc.)
Contains a unique, unchangeable ***cryptographic*** identity that is established during manufacturing.
Acts as an anchor point for verifying the integrity of the system's firmware.
The unchangeable ***cryptographic*** identity is called its "immutable fingerprint".

If firmware is compromised, the SRoT will detect the change (because the signature will no longer match) and prevent the system from booting.

Physically Unclonable Function (PUF)

Hardware component that generates a digital fingerprint or signatures based on the unique physical characteristics of an integrated circuit or chip.
Typically a semiconductor device.
When a PUF is queried, or given a challenge, it responds with a unique output, based on the chip's inherent variations.
This response, like a fingerprint, is impossible to clone or recreate in another device.
PUFs are a unique hardware root of trust.
Multiple uses: in hardware security, including:

- Secure key generation
- Device Authentication
- Anti-tampering
- Secure boot

Software Bill of Materials (SBOM)

A list of all software components, libraries, and modules that go into a particular software build or product.
The SBOM functions as the inventory of all the building blocks that make up a software product.
Helps organizations better understand, manage, and secure their applications.

An attack in 2020 led to a U.S. Government requirement for **SBOM** in the 2021 Executive order on improving the nation's Cybersecurity.

EOS End-of-support

EOS identifies when a vendor will no longer support a product, and EOL identifies when a vendor will no longer offer a product for sale.

Systems with an EOS date that occurs in the following year should be a top priority for replacement.
The EOS date is the date that the vendor will stop supporting a product.
Protect End of supported (EOS) devices that cannot be patched from network attacks, by placing a hardware network security device in front of the devices.

EOL End-of-Life

The EOL date is the date that a vendor stops offering a product for sale, but the vendor continues to support the product until the EOS date.
The vendor will discontinue sales of the servers after the EOL date.
EOL date approach then Prepare to discontinue use of the device as part of the organization's normal planning cycle.

ATO - Authorization to Operate

Audit of a third-party supplier discovers several serious issues with the vendor, such as failing to require encryption for all communications and not requiring multi factor authentication on management interfaces.
Scenario requires the action to Void the ATO (authorization to operate) of the vendor.

ATO Examples:

- authorization to operate
- common control authorization
- authorization to use
- denial of authorization

Supply chain risk management (SCRM) processes should be applied. One of the common requirements is the establishment of minimum security requirements of the third party based on organisations **existing security policy**

The primary place where the minimum-security requirements for a third party should be documented is in the contract or service-level agreement (SLA) established with that vendor. A business partners agreement (BPA) and interconnection security agreement (ISA) could also be viable.

Domain 1 Threat Modelling

- Where is the application most vulnerable?
- What are the most relevant threats?
- What needs to be done to safeguard against threats?

The three common threat modelling approaches: focus on attackers, focus on assets, and focus on software.
3 approaches to threat modelling

- **Foc**used on **Ass**ets - uses asset valuation results to identify threats to the valuable assets

- **Foc**used on **Att**ackers - identify potential attackers and identify threats based on the attackers goals
- **Foc**used on **soft**ware - considers potential threats against the software the org develops.

SAMM - Domain 8
The activities of threat assessment, threat modelling, and security requirements are all part of the Design function under SAMM

Threat Definitions

- Threats—Any potential occurrence that may cause an undesirable or unwanted outcome for an organization or for a specific asset is a threat.
- Threat agents or threat actors—Entities that intentionally exploit vulnerabilities.
- Threat events—Accidental occurrences and intentional exploitations of vulnerabilities.
- Threat vector—The path or means by which an attack or attacker can gain access to a target in order to cause harm.

Threat modeling program

- To **reduce** the number of security-related design flaws
- To **reduce** the number of security-related coding flaws
- To **reduce** the severity of non-security-related flaws

Threat Vectors not in control of Risk assessor
The developer or evaluator of software has no control over the threat environment vectors, because it is external to the organization.

STRIDE

The STRIDE and MITRE ATT&CK models are used to classify the nature, not the severity, of threats.
developed my **micro**soft

- **Sp**oofing
  - Person successfully identifies as another by falsifying data
- **Tam**pering
  - URL parameters are changed without authorization
- **Repu**diation
  - subject unable to deny they did something and blame someone else
- **Infor**mation disclosure
  - When confidential documents are exposed to unauthorized entities
- **Denial** of service
- **Eleva**tion of privilege
  - A non-admin user gains access to make admin level changes.

STRIDE is often used in relation to assessing threats against applications or operating systems.

PASTA

The PASTA model is designed to help with countermeasure selection.
focus on developing countermeasures based on **ass**et **val**ue

- Stage I **def**inition of **obj**ective
- Stage II **Def**inition of **tech**nical **sco**pe
- Stage III app decomposition & analysis
- Stage IV threat analysis
- Stage V Weakness & vulnerability analysis
- Stage VI Attack Modeling & Simulation
- Stage VII Risk Analysis & Management

a risk-centric threat-modelling approach that aims at selecting or developing countermeasures in relation to the value of the assets to be protected.

Performing Reduction Analysis

The next step in threat modeling is to perform a reduction analysis.
Reduction analysis is also known as decomposing the application, system, or environment.
Decomposition process - five key concepts:

- **Trust Boundaries** Any location where the level of trust or
- security changes
- **Dataflow Paths** The movement of data between locations
- **Input Points** Locations where external input is received
- **Privileged Operations** Any activity that requires greater privileges than a standard user account or process typically required to make system changes or alter security
- **Details about Security Stance and Approach**

VAST

Based on Agile PM principles

- **V**isual
- **A**gile
- **S**imple
- **T**hreat

DREAD

Quantitative
Based on answer to 5 questions (**How**?)

- **Dam**age potential
- **Rep**roducibility
- **Exploit**ability
- **Aff**ected users
- **Discov**erability

The DREAD questions are about Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability.

DREAD Risk value calculated by giving value out of 10, adding 5 values, and divide by 5 to get risk value.

TRIKE

Focused on **acc**eptable risk **op**en **so**urce **mod**el
An open-source threat modelling process that implements a requirements model.
Ensure the assigned level of risk for each asset is "**acceptable**" to stakeholders.

COBIT

Control **Obj**ectives for **Info**rmation and **Rel**ated **Tec**hnologies principals.
COBIT is a documented set of **best IT security practice**s crafted by the Information Systems Audit and Control Association (**ISACA**) that prescribes goals and requirements for security controls and encourages the mapping of IT security ideals to business objectives.

IT management and governance framework
COBIT six key principles Security control framework

- Principle 1 - Provide **stakeholder values**
- Principle 2 - **Holistic** approach
- Principle 3 - **Dynami**c Governance System
- Principle 4 - **Governance Distinct** from Management
- Principle 5 - **Tailored** to enterprise Needs
- Principle 6 - **End-to-end** governance system

Control Objectives for Information and Related Technologies (COBIT) is a documented set of best IT security practices crafted by ISACA and the IT Governance Institute (ITGI).

Scenario:
An organization is implementing a preselected baseline of security controls but finds that some of the controls aren't relevant to their needs.
Tailor the baseline to their needs.

ATASM

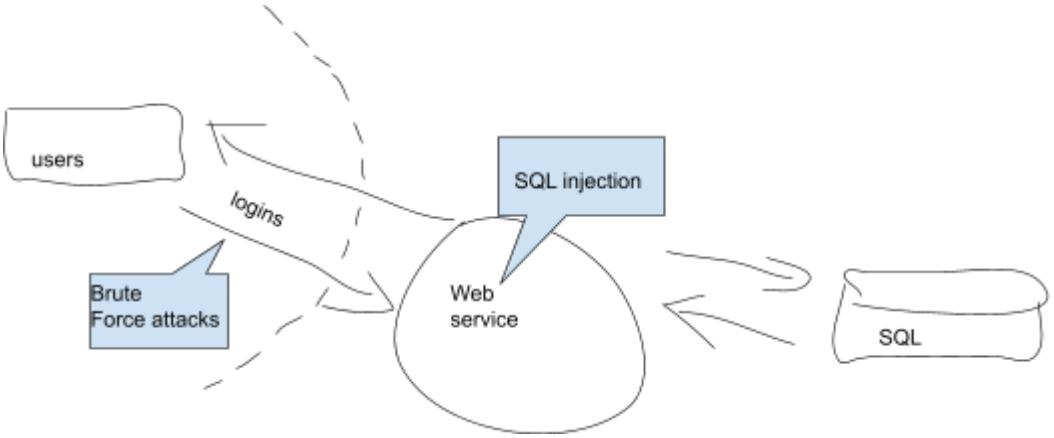
Architecture, Threats, Attack Surfaces, and Mitigations (ATASM) is a threat-modelling approach that highlights the importance of structural understanding of a system for the purpose of threat modelling (architecture).
The architecture is broken apart into its logical and functional components (decomposing and factoring) to discover all potential attackable surfaces (inputs and outputs of the system).
Decomposition is also used to define those points at which defences will be built (mitigations are placed at defensible boundaries).

- Architecture - components and flow

- Threats - agents, goals, attack methods objectives
- Attack Surfaces - decomposing and attack methods
- Mitigations - security controls, defense in depth

Diagramming Potential Attacks

Determining **pot**ential **att**ack **conc**epts is often achieved through **diagram**ming.



Reduction Analysis

Threat Modeling, Reduction analysis is also known as decomposing the application, system, or environment.

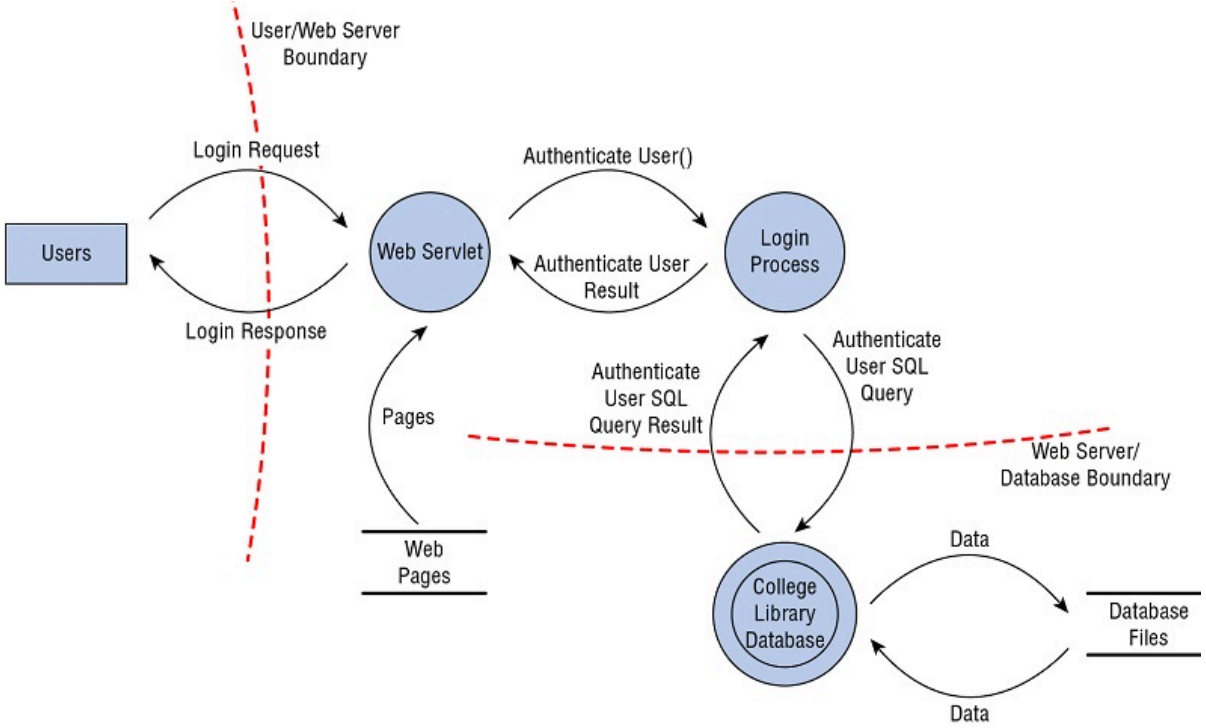
- **Tru**st Boundaries - any **loc**ation where the level of trust or security changes
- Data **Flo**w Paths - the **move**ment of **dat**a between locations
- **Inp**ut Points - locations where **ext**ernal input is **rec**eived
- **Priv**ilege **Oper**ations - Any **act**ivity that requires greater **priv**ileges than of a standard user account.
- **Det**ails about **sec**urity stance and **app**roach - declaration of security **poli**cy, security foundations and security **assum**ptions.

The next step after threat modelling is reduction analysis.

The purpose of this task is to gain a greater understanding of the logic of the product, its internal components, as well as its interactions with external elements.
In reduction analysis, the security professional breaks the system down into **five** core elements:

- trust boundaries,
- data flow paths,
- input points,
- privileged operations,
- details about security controls.

Example Diagram of Reduction Analysis



Prioritization and Response

Then threats are ranked or rated using **DREAD**, high/medium/low rating

Domain 1 Security Controls

Security **meas**ures for countering and minimising loss or unavailability of services or apps due to vulnerabilities
The terms safeguards and countermeasure may seem to be used interchangeably

- **Safeguard** are proactive
- **Countermeasure** are reactive

Domain 1 Control Categories

Three categories of security controls:

- **Tec**hnical - aka logical, involves the hardware or software mechanisms used to manage access
- **Adm**inistrative - policies and procedures defined by org security policy, other regulations and requirements.
- **Phys**ical - items you can physically **tou**ch

Control Types

- **Det**errent - deployed to **discou**rage violation of security policies
- **Prev**entative - deployed to thwart or **stop** unwanted or unauthorized activity from occurring - example is firewall

- **Detect**ive - deployed to discover or **det**ect **unw**anted or **unaut**horized activity, seeks to discover evidence of unwanted, unauthorized, or illicit behavior or activity.
- **Compen**sating -
    - provide **opti**ons to other existing controls to **aid** in enforcement of security policies
- **Corr**ective - modifies the **env**ironment to return **sys**tems to normal after an **unw**anted or **unau**thorized activity has occurred
- **Rec**overy - an extension of corrective controls but have more advanced or complex abilities
- **Direc**tive - direct **conf**ine control the actions of subjects to **forc**e or encourage **compl**iance with security **poli**cies

DPDCCRD

Security control assessment (SCA)

A security controls assessment (**SCA**) most often refers to a formal U.S. **government** process for assessing security controls.

A security control assessment (SCA) is the formal evaluation of a security infrastructure's individual mechanisms against a baseline or reliability expectation. The SCA can be performed in addition to or independently of a full security evaluation, such as a penetration test or vulnerability assessment.

SCA Goals:

- Ensure the **effectiveness** of the security **mechanisms.**
- Evaluate the **quality** and thoroughness of the **risk man**agement processes of the organization.
- **Produce** a **report** of the relative strengths and weaknesses of the deployed security infrastructure.

An SCA is the formal evaluation of a security infrastructure's individual mechanisms against a baseline or reliability expectation.

Domain 1 Legal & Regulatory

Legal and **regul**atory issues that pertain to information security in a **glob**al context

- ☐ Cyber crimes and data breaches
- ☐ Trans-border data flow
- ☐ Licensing and intellectual property requirements
- ☐ Privacy
- ☐ Import/export controls

In the context of cloud computing, the primary concern when it comes to **data** security and compliance is Data sovereignty and legal jurisdiction.

Privacy vs Confidentiality

- **Privacy**

    - The right of an individual to have some control over how their personal information (PII, PHI) is collected, used, and potentially disclosed.
    - Focus on rights of the individual person/customer
- **Confidentiality**
    - The duty to ensure private information is kept secret to the extent possible.
    - A legal obligation in regulatory scenarios, and a due care obligation in U.S. Law.
    - Focuses on data

Import/export control regulations tend to cover more technical items, such as high-performance computing, security software, and encryption technology. Governance, risk, and compliance (GRC) solutions are generally not covered by import/export control regulations.

The Bureau of Industry and Security (BIS) within the Department of Commerce sets regulations on the export of encryption products outside of the United States.

Type of Law

- **Crim**inal Law - contains prohibitions against acts such as murder, assault, **robb**ery and arson.
- **Civ**il Law - include contract disputes, real estate **transa**ctions, **employ**ment, estate, and probate.
    - Civil investigations typically follow the "preponderance of the evidence" standard.
- **Admin**istrative Law - government agencies have some leeway to **enact** administrative law.
    - Administrative laws do not require an act of the legislative branch to implement at the federal level. Administrative laws consist of the policies, procedures, and regulations promulgated by agencies of the executive branch of government.

Cissp exam focuses on security related generalities of law, regulations, investigations, and compliance.

Laws

- Computer Fraud and Abuse Act (**CFAA**)
    - first major piece of US cybercrime specific **legisl**ation
    - Example: passwords to systems and user accounts belonging to her organization were for sale on the dark web.
- **Fed**eral sentencing guidelines -
    - provide punishment guidelines to help federal judges interpret computer crime laws.
- Federal information security management act (**FISMA**) required a formal infosec operations for **fed**eral gov't
    - law governs information security operations at federal agencies
- **Copy**right and the digital millennium copyright act (DMCA)-

- Covers website content, literary, musical, software code and dramatic works
- Copyright protection generally lasts for 70 years after the death of the last surviving author of the work.

text of the law

Code of Federal Regulations (CFR) contains the text of all administrative laws promulgated by federal agencies.
Promulgate - promote or make widely known (an idea or cause).
The U.S. Code contains criminal and civil law.
Supreme Court rulings contain interpretations of law and are not laws themselves.

Intellectual Property (IP) and Licensing

- **Trade**marks ®
  - covers words, slogans, and logos used to identify a company and its products or services
  - product name should be protected under trademark law
  - Example: Brand name is a trademark, Brand Protection
- **Pat**ents
  - protect the intellectual property rights of **inve**ntors
  - Newly invented machine is patent
  - U.S. patent law provides for an exclusivity period of **20 years b**eginning at the time a utility patent application is **submitted** to the Patent and Trademark Office.
  - 20 years from the application date
  - Invention must be novel and non-obvious
- Copyright ©
  - Protect expressions of ideas not the ideas themself.
  - Content stolen
  - Work does not need to be published to be protected
  - covers literary, musical, software code and dramatic works
  - Copyright protection generally lasts for **70 y**ears after the death of the last surviving author of the work.
  - 95 years from publication or 120 years from creation if owned by a corporation.
  - Fair sale and fair use
  - Example: Music, drawing, movies are copyright.
- **Tra**de **Sec**rets
  - intellectual property that is absolutely critical to their business and must not be disclosed
  - The **Economic Espionage Act** imposes fines and jail sentences on anyone found guilty of stealing trade secrets from a U.S. corporation. It gives true teeth to the intellectual property rights of trade secret owners.
  - Example: Customer list or a oil formula is a trade secret
- **Lic**ensing - 4 types: **contractual**, **shrink**-wrap, **click**-through, and **cloud** services.

Symbols

The ® symbol is reserved for **trademarks** that have received official registration status by the U.S. Patent and Trademark Office.
The ™ symbol would be used before receiving USPTO approval.
The © symbol is used to represent a copyright.

The † symbol is ***not*** associated with intellectual property protections.

Licence Contracts

- **Contractual license** agreements use a written contract between the software vendor and the customer, outlining the responsibilities of each. These agreements are commonly found for high-priced and/or highly specialised software packages.
- **Shrink-wrap license** agreements are written on the outside of the software packaging. They commonly include a clause stating that you acknowledge agreement to the terms of the contract simply by breaking the shrink-wrap seal on the package.
- **Click-through** (also known as browser wrap) license agreements are becoming more commonplace than shrink-wrap agreements. In this type of agreement, the contract terms are either written on the software box or included in the software documentation.
    - During the installation process, you are required to click a button indicating that you have read the terms of the agreement and agree to abide by them. This adds an active consent to the process, ensuring that the individual is aware of the agreement's existence prior to installation.
- Cloud services license agreements take **click-through** agreements to the extreme.
    - Example: A user signed up for a cloud service storing corporate information. most likely agreed to a **click-through** license agreement binding the organization.
- Enterprise license agreement
    - It typically allows customization of terms, negotiation, discount and pricing, reflecting the negotiated details between the vendor and a corporate client.

<u>Scenario</u>:
A CISSP professional is purchasing the software, so it is not open source. It is used widely in her industry, so it is not custom developed for her organization. There is no indication in the question that the software is an enterprise resource planning (ERP) system.
The best answer here is commercial-off-the-shelf software (**COTS**).
COTS can immediately fulfill a business need at low cost.

Conflicting International Legislation

It is important to be aware of the various laws and regulations that govern cloud computing. Laws can introduce risks to a business, such as fines, penalties, or even a loss of the ability to do business in a certain place.
It is important to identify such risks and make recommendations to mitigate them just like any other risk.

Example of conflicting legislation:
GDPR forbids the transfer of data to countries that lack adequate privacy protections.
The clarifying lawful overseas use of data (CLOUD) act requires CSPs to hand over data to aid in investigation of serious crimes, even if stored in another country.
Answer: ***Call in an expert.***
As with many aspects of security, legal compliance requires collaboration.
Legal counsel should be part of the evaluation of any cloud-specific risks, legal requests, and the company's response to these.

The consuming organization is responsible for navigating these challenges where they use cloud resources.
Cannot transfer accountability.

Cloud practitioners must be aware of multiple sets of laws and regulations and the risks introduced by conflicting legislation across jurisdictions.

- Copyright and intellectual property law
  - Particularly the jurisdictions that companies need to deal with local versus international to protect and enforce their IP protections.
- Safeguards and security controls required for privacy compliance
  - Particularly details of data residency or the ability to move data between countries, as well as varying requirements of due care in different jurisdictions
- Data breaches and their aftermath, particularly breach notification
  - Data breach is the primary information security risk to data at rest.
- International import/export laws
  - Particularly technologies that may be sensitive or illegal under various international agreements

Cloud Practitioners must be aware of multiple sets of laws and regulations and the risks introduced by conflicting legislation access jurisdictions.

CISSP Exam Cram - 2024 Addendum

Laws are the legal rules. That are created by government entities, such as legislatures.
Regulations are the rules that are created by governmental agencies.
Laws and regulations must be followed or can result in **civil or criminal penalties** for the organization.
Standards dictate a reasonable level of performance.
They can be created by an organisation for its own purposes (**internal**) or come from industry bodies or trade groups (**external**).
Frameworks are a set of guidelines helping organizations improve their security posture.

Domain 1 Encryption and Privacy

- **Comp**uter **export** controls
  - US companies can**not** export to Cuba, Iran, North Korea, Sudan and Syria.
  - Bureau of Industry and Security (BIS)

    - Concern with AI-focused GPU-based computation nodes in China, Hardware and software can be subject to import and export controls.
    - Export controls may limit what hardware can be imported to China.
- Encryption Export Controls -
    - Dept of Commerce details limitations on export of encryption products outside the US.
- Privacy (US) - The basis for privacy rights is in the Fourth Amendment to the US Constitution.
    - The Fourth Amendment to the U.S. Constitution sets the "probable cause" standard that law enforcement officers must follow when conducting searches and/or seizures of private property. It also states that those officers must obtain a warrant before gaining involuntary access to such property.
- Privacy (EU) General Data Protection Regulation (**GDPR**) is not a US law.
    - Applies to any company with customers in the EU.
- The Privacy Act regulates what information government agencies may collect and maintain about individuals.
- The Second Amendment grants the right to keep and bear arms.
- The Gramm–Leach–Bliley Act regulates financial institutions.

US Privacy Laws

- **HIPAA** (Health Insurance Portability and Accountability Act)
    - protection and sharing of health records
    - **Scenario**: healthcare organization covered under HIPAA, would like to enter into a partnership with a vendor who will manage some of the organization's data. As part of the relationship, the vendor will have access to protected health information (PHI). Under ***business associate agreement*** circumstances this arrangement is permissible under HIPAA.
    - Organizations subject to HIPAA may enter into relationships with service providers as long as the provider's use of protected health information is regulated under a formal business associate agreement (**BAA**). The BAA makes the service provider liable under HIPAA.
    - HIPAA regulates three types of entities—
        - healthcare providers
        - health information clearinghouses
        - health insurance plans
    - Protected health information (PHI) is specifically defined by HIPAA to include information about an individual's medical bills.
- **HITECT** (Health Information Technology for Economic and Clinical Health)
- Gramm-Leach-Bliley Act - **GLBA**
    - **Fin**ancial **inst**itutions and private banks
    - financial institutions protect customer records
    - GLBA places strict privacy regulations on financial institutions, including providing written notice of privacy practices to customers
- Children's Online Privacy Protection Act (**COPPA**)
    - The Children's Online Privacy Protection Act (COPPA) provides severe penalties for companies that collect information from young children without **parental consent.** COPPA states that this consent must be obtained from the

parents of children younger than the **age of 13** before any information is collected (other than basic information required to obtain that consent).

- Privacy Act
  - 1974 law limits the ways government agencies may use information that private citizens disclose to them under certain circumstances
- Electronic Communications Privacy Act (**ECPA**)
  - safeguards against electronic *eavesdropping*
  - Electronic Communications Privacy Act (ECPA) makes it a crime to invade the electronic privacy of an individual.
- Communications Assistance for Law Enforcement Act (**CALEA**)
  - requires that all communications carriers make wiretaps possible for law enforcement officials who have an appropriate court order.
  - wiretapping one clients pursuant to a search warrant
  - The Communications Assistance for Law Enforcement Act (CALEA) required that communications carriers assist law enforcement with the implementation of wiretaps when done under an appropriate court order.
- Family Educational Rights and Privacy Act (**FERPA**) protects the rights of students and the parents of minor **students**.

Privacy Act

**OHASA The Occupational Health and Safety Act No. 85 of 1993 now includes the Code of Practice: Managing Exposure to SARS-COV-2 in the Workplace, 2022*

Other Privacy Laws

The following do not appear in the official study guide for the 2021 CISSP exam.
New to 2024 Exam syllabus.

- Personal Information Protection Law
  - Effective since late 2021, PIPL aims to establish a comprehensive framework for the protection of personal information in **China**
- Protection of Personal Information act (POPIA)
  - Enacted in 2013, establishes regulations for the responsible processing of personal information by both public and private entities in South Africa
- ATA - Australia Privacy Act

Both address data collection, security, usage and deletion.
CISSP Exam Cram - 2024 Addendum

Domain 1 Business continuity

You should strive to have the highest-ranking person possible sign the BCP statement of **importance**. Of the choices given, the chief executive officer (**CEO**) has the highest ranking.

As the first step of the process, the **business organization analysis** helps guide the remainder of the work.

Security Analyst and the infosec core team should conduct this analysis and use the results to aid in the selection of team members and the design of the **BCP** process.

Human life/People/***Personal Safety***/*Human Safety*
Developing a business continuity plan for your organization and want to document a set of guiding principles for the planning process. Personal safety should have the highest priority. People safety should always be your highest priority in business continuity planning. As life safety systems, fire suppression systems should always receive high prioritization.

Business continuity planning (**BCP**) issues that pertain to information security in:

1. **Strat**egy development
2. **Provi**sions and processes - design procedures and mechanisms to mitigate risks deemed unacceptable
3. **Plan** approval
4. Plan **impl**ementation
5. **Train**ing and education

SPPPT

BCP Definitions

Some **BCP** related definitions worth knowing

- BCP (Business Continuity Plan) the overall organisational plan for "**how-to**" continue business
- DRP (Disaster Recovery plan) the plan for recovering from a disaster impacting IT and **returni**ng the **IT** infrastructure **to oper**ation
- **COOP** (Continuity of Operations Plan) the plan for continuing to do business until the IT infrastructure can be restored.

BCP vs DRP

Difference?

BCP focuses on the **whole bus**iness
DRP **foc**uses more on the **tec**hnical aspects of **rec**overy
BCP will cover **comm**unications and **proc**ess more broadly

BCP is an umbrella policy and DRP is part of it.

BCP Motivation
The exercise is crucial to ensuring that the organization is prepared for emergencies and ensuring individuals remain familiar with their roles in BCP.

External Dependencies

Factors, entities or conditions outside the organisation upon which the organisation's continuity and operational resilience may depend.
E.g. Suppliers (supply chain) & vendors, utilities, transportation
Must assess these external dependencies, and devise strategies to mitigate potential disruptions.

Entities outside the organization that it depends on for business business continuity, disaster recovery, or operations.
Examples - ISPs, utility companies, providers of recovery sites, and fuel for backup generators.
The organization should **not** rely on a single vendor for a specific function during a disaster that may be **impacted** by the same event.

Domain 1 User Education / Awareness Training

Establish and maintain a security awareness, education, and training program:

- ➢ Methods and techniques to present awareness and training
- ➢ Periodic content reviews
- ➢ Program effectiveness evaluation

KPI Measure Security Awareness training:

- How many people took the training
- The level of security awareness before and after the training

The **safety of personnel** should be the highest priority when addressing safety and security in a **training and awareness program**. The value of both tangible and intangible assets is important, but not as important as human life.

Live Training is the security instruction option that offers the most potential for real-time feedback.

Often a **security champion** is a member of a group who decides (or is assigned) to take charge of leading the adoption and integration of security concepts into the group's work activities. Security champions are often non-security employees who take up the mantle to encourage others to support and adopt more security practices and behaviours.

Gamification

Security awareness and training can often be improved through gamification. Gamification is a means to encourage compliance and engagement by integrating common elements of game play into other activities, such as security compliance and behavior change.
This can include rewarding compliance behaviours and potentially punishing violating behaviours. Many aspects of game play can be integrated into security training and adoption, such as scoring points, earning achievements or badges.

Periodic Content Reviews

CISSP 2024 exam changes in DETAIL!

- Organisations and their threat environments are constantly changing
- Awareness, training & education materials must be updated accordingly

E.g. cryptocurrency, artificial intelligence (AI), blockchain

Return on Security Investment (ROSI)

establish proof of a positive ROSI,

- Administering a quiz immediately after the awareness event
- Have workers take a test 6 months after a training class
- Collect key security indicators that relate to insider security incidents over time

Domain 1 Privacy and Data Breaches

Although state data breach notification laws vary, they generally apply to Social Security numbers, driver's license numbers, state identification card numbers, credit/debit card numbers, and bank account numbers.

Data breach is the most comprehensive risk in terms of its potential to cause immediate and widespread reputational damage to an organization. A data breach directly impacts the public perception of an organization's ability to protect sensitive information, leading to a loss of trust, potential financial consequences, and lasting damage to the organization's reputation.

Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is designed to identify the privacy data being collected, processed , or stored by a system, and assess the effects of a data breach.

Several privacy laws explicitly require PIAs as a planning tool for identifying and implementing required privacy controls, including GDPR and HIPAA.
Conducting a PIA typically begins when a system or process is being evaluated.

However, evolving privacy regulation often necessitates assessment of existing systems.

To conduct a PIA you must define assessment scope, data collection methods and plan for data retention.
The international Association of Privacy professionals (IAPP) has published guides and resources related to privacy efforts including PIA.

Consequences of privacy data breaches

- **Repu**tational Damage -
  - effects may last for years, can result in loss of customer trust and loss of revenue
  - Data Breach, information security risk to data at rest would result in the greatest reputational impact on the organization
- **Ide**ntity **theft** - involves someone using a person's private information to impersonate that individual, usually for financial gain.
- **Intellec**tual **prop**erty (IP) theft - might quickly cost customers, credit ratings, and brand reputation. Brand Protection. Losing IP could mean forfeiture of first-to-market

advantage, loss of profitability, or even an entire lines of business to competitors or counterfeiters
- **Fines** -
    - and may lead to lawsuits, failing to report a breach can result in fines that can reach into the millions of dollars. **GDPR** outlines fines of up to **4%** of a company's annual global **rev**enues or **20 mil**lion **euros** for failing to report a breach. Any company with a **cust**omer in the **EU** is subject to GDPR.

Notifications of breaches

Data breach notifications laws
If a data breach occurs, failing to report a breach can result in fines that can reach into the millions of dollars.
The EU sets their standard GDPR, and **notific**ations of data breaches must be reported within **72 hours**.
Escalations to external sources, like law enforcement or outside experts to stop/investigate breach.

Typically, data breaches cause the greatest reputational damage as a result of threats to data at rest. Data at rest with a high level of sensitivity is often encrypted to help prevent this. Decryption is not as significant of a threat if strong encryption is used and encryption keys are well secured.
Insider threats are a risk, but the majority of insider threat issues are unintentional rather than intentional, making this risk less likely in most organizations.

Jurisdictional Differences in Data Privacy

Different laws and regulations may apply depending on the location of data residency:
- Data subject
    - Is the entity, individual human associated with a particular set of personally identifiable information (PII)
- Data collector
- Cloud service provider
- Subcontractors processing data
- Company headquarters of the entities involved

Legal concerns:
- Prevent the utilisation of a cloud services providers
- Add to costs and time to market
- Drive changes to technical architectures required to deliver services

Never replace compliance with convenience when evaluating services, as this increases risks.
Many privacy frameworks impose fines or other action for noncompliance.

Cyber Kill / Attack Chain

1. Reconnaissance
2. Weaponization

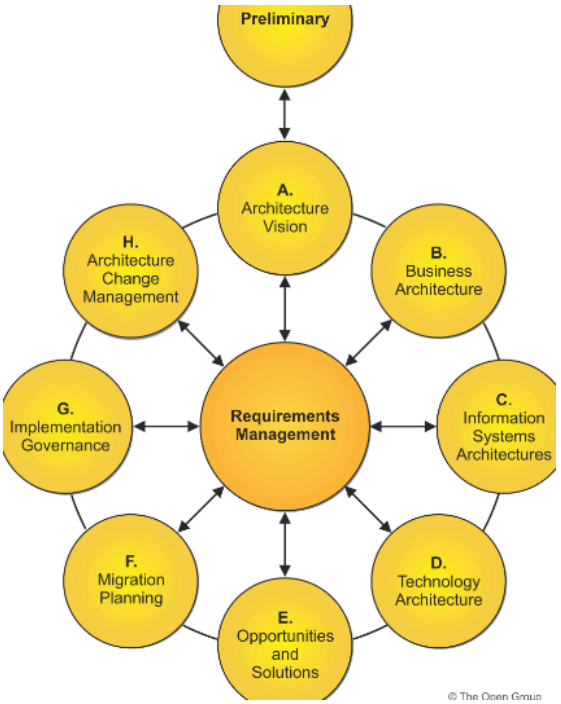
3. Delivery
4. Exploit (Malware is exploiting vulnerability, patching will break chain and stop attack)
5. Installation
6. C & C (C2)
7. Actions

3 Major Enterprise Security Architectures

- Zachman
    - The Zachman Framework is an enterprise ontology and is a fundamental structure for enterprise architecture which provides a formal and structured way of viewing and defining an enterprise. The ontology is a two dimensional classification schema that reflects the intersection between two historical classifications.
- SABSA - Sherwood Applied Business Security Architecture
- TOGAF
    - The Open Group Architecture Framework (TOGAF) focuses on IT architecture issues.

TOGAF

Central point reference is business requirements as a central point of comparison for every TOGAF phase of development architecture.



Zachman

	Why	How	What	Who	Where	When
Contextual	Goal List	Process List	Material List	Organisational Unit & Role List	Geographical Locations List	Event List
Conceptual	Goal Relationship	Process Model	Entity Relationship Model	Organisational Unit & Role Relationship Model	Locations Model	Event Model
Logical	Rules Diagram	Process Diagram	Data Model Diagram	Role Relationship Diagram	Locations Diagram	Event Diagram
Physical	Rules Specification	Process Function Specification	Data Entity Specification	Role Specification	Location Specification	Event Specification
Detailed	Rules Details	Process Details	Data Details	Role Details	Location Details	Event Details

Zachman framework for enterprise architecture is a matrix based methodology that enables the viewing of an architecture from ***six*** perspectives:

Why, How, What Who, Where, When

Contextual
Conceptual
Logical
Physical
Detailed

Risk Associated with Acquisition

Risk associated with the **acqui**sition of products and services

- **Product tampering**
  - Unauthorized alteration of modification of a product after its manufacture but before it reaches the end consumer.
  - Risks: malfunction, health hazards, compromised **integrity** & introduction of malicious code or vulnerabilities
- **Counterfeits**
  - Unauthorized replicas or imitations of genuine products, made to deceive consumers into thinking they are purchasing the real thing.
  - Risks: reduced performance, potential hazards, non-compliance with regulations, lack of proper security measures, increasing vulnerability
- **Implants**
  - Hardware or software components are stealthily inserted into products to perform unauthorized activities, often for espionage or data theft.
  - Risks: secretly transmit sensitive information to unauthorized entities, allow unauthorized access to systems, can remain undetected for extended periods.

Risks associated with mergers and acquisitions:

- Inappropriate information disclosure
- Data loss
- Downtime
- Failure to achieve sufficient return on investment (ROI)

Identity Management

A centralised identity management solution can *scale* up to handle additional traffic.
It can scale up to support additional traffic.

Scenario
An organization has merged with another organization. The two organisations are using different network operating systems. Management wants to implement a solution that will give them the most control while allowing both organisations to access resources in both networks.
Best choice is **On-premises identity** management.

Context:
A cloud-based solution is controlled by a third party. There's no need to have both an on-premises and a cloud-based solution in this situation, which would be a hybrid solution. Identity management solutions provide single sign-on (SSO)

Alternate Scenario:
An organization provides online training to employees of multiple organizations. Employees log on normally, and they can then access the training website without logging on again. Which of the following best identifies the system the training company is using?
Best Choice is The training company is most likely using a cloud-based identity management system.
Context:
On-premises identity management systems are used when users are from the same organization, not multiple different organizations. Hybrid solutions implement both an on-premises and a cloud-based solution, but both are not needed in this scenario. A credential management system provides storage space for credentials.

Risk perspectives, also known as risk management perspectives or approaches, are different lenses through which organizations and individuals can view and address risks.
Risk response involves evaluating countermeasures, safeguards, and security controls using a cost/benefit analysis; adjusting findings based on other conditions, concerns, priorities, and resources; and providing a proposal of response options in a report to senior management.
A risk register or risk log is a document that inventories all the identified risks to an organization or system or within an individual project. Risk acceptance occurs as a risk response when management has agreed to accept the consequences and the loss if a risk is realized.

Study Essentials

CIA Triad elements of confidentiality, integrity, and availability.
Confidentiality is the principle that objects are not disclosed to unauthorized subjects.
Integrity is the principle that objects retain their veracity and are intentionally modified only by authorized subjects.
Availability is the principle that authorized subjects are granted timely and uninterrupted access to objects.

AAA services focus on identification, authentication, authorization, auditing, and accounting.
Identification is when a subject professes an identity and accounting is initiated. A subject must provide an identity to a system to start the process of authentication, authorization, and accounting.
Authentication is the process of verifying or testing that a claimed identity is valid. Authentication requires information from the subject that must exactly correspond to the identity indicated.
Once a subject is authenticated, its access must be authorized.
The process of authorization ensures that the requested activity or object access is possible given the rights and privileges assigned to the authenticated identity.
Auditing is the programmatic means by which subjects are held accountable for their actions while authenticated on a system through the documentation or recording of subject activities.
Security can be maintained only if subjects are held accountable for their actions.
Effective accounting relies on the capability to prove a subject's identity and track their activities.
Abstraction is used to collect similar elements into groups, classes, or roles that are assigned security controls, restrictions, or permissions as a collective.
It adds efficiency to carrying out a security plan.
A security boundary is the line of intersection between any two areas, subnets, or environments that have different security requirements or needs.
Security governance is the collection of practices related to supporting, defining, and directing the security efforts of an organization.
Third-party governance is the system of external entity oversight that may be mandated by law, regulation, industry standards, contractual obligation, or licensing requirements. The actual method of governance may vary, but it generally involves an outside investigator or auditor.
Documentation review is the process of reading the exchanged materials and verifying them against standards and expectations. In many situations, especially those related to government or military agencies or contractors, failing to provide sufficient documentation to meet requirements of third-party governance can result in a loss of or a voiding of authorization to operate (ATO).
Understand the alignment of security function to business strategy, goals, mission, and objectives. Security management planning ensures the proper creation, implementation, and enforcement of a security policy. Security management planning aligns the security functions to the strategy, goals, mission, and objectives of the organization.
This includes designing and implementing security based on business cases, budget restrictions, or scarcity of resources.
A business case is usually a documented argument or stated position in order to define a need to make a decision or take some form of action.
To make a business case is to demonstrate a business-specific need to alter an existing process or choose an approach to a business task.
A business case is often made to justify the start of a new project, especially a project related to security.
Security management is based on three types of plans: strategic, tactical, and operational.

To create a comprehensive security plan, you need the following items in place:

- security policy,
- standards,
- baselines,
- guidelines,
- Procedures.

Threat modeling is the security process where potential threats are identified, categorized, and analyzed. Threat modeling can be performed as a proactive measure during design and development or as a reactive measure once a product has been deployed. Key concepts include assets/attackers/software, STRIDE, PASTA, VAST, diagramming, reduction/decomposing, and DREAD.
Understand supply chain risk management (SCRM) concepts. SCRM is a means to ensure that all the vendors or links in the supply chain are reliable, trustworthy, reputable organizations that disclose their practices and security requirements to their business partners. SCRM includes evaluating risks associated with hardware, software, and services; performing third-party assessment and monitoring; establishing minimum security requirements; and enforcing service-level requirements.

Domain 2 Asset Security

Provision Resource Securely
Manage Data Lifecycle
Determine data security controls and compliance requirements (DRM, CASB, DLP)

Examples of an intangible assets

- Company Reputation
- Files stored on servers
- Patents
- Databases
- Formulas

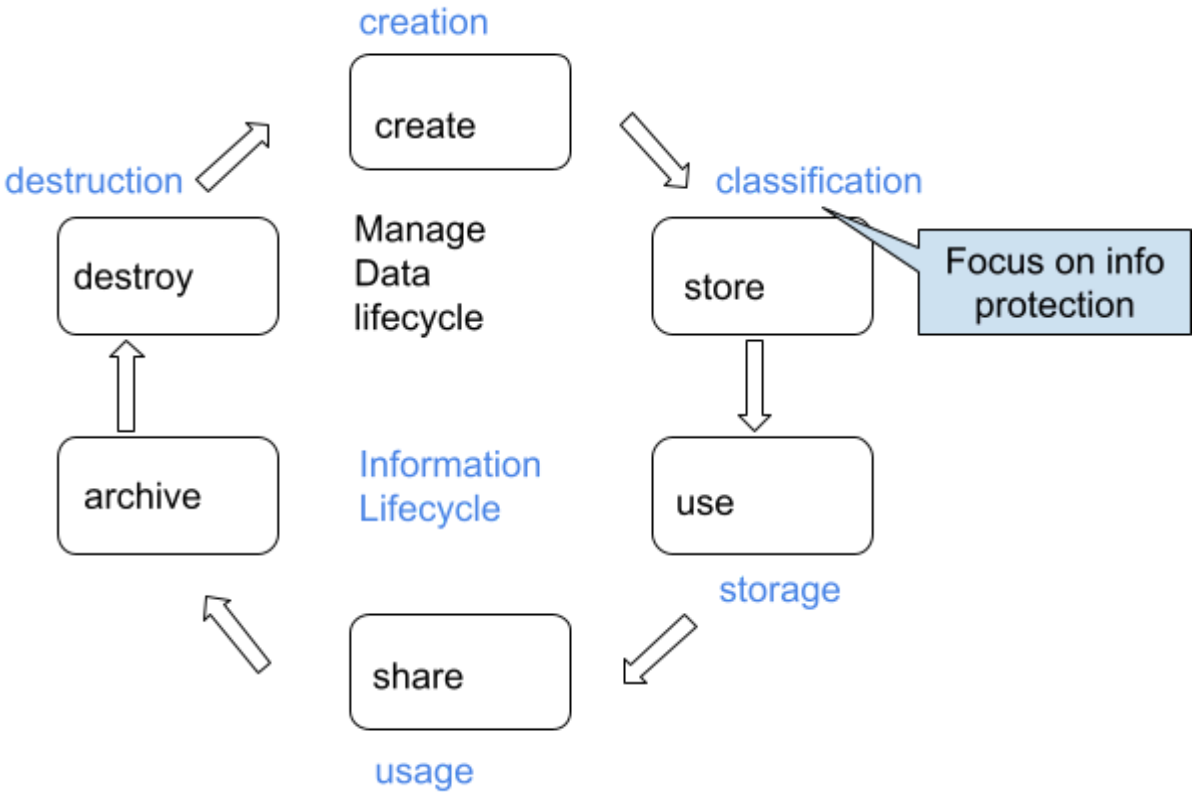
Example of tangible assets:

- Server hardware
- Desktop hardware
- mobile devices
- Employees - Personnel assets
- Cables
- Buildings

Domain 2 The Data Lifecycle

Information Lifecycle - conceptually understand the protection of data

Data Lifecycle -



Domain 2 Data Security Controls

Data security controls

Marking, labelling, handling, classification.
Marking and **labelling** practices protect the confidentiality of data held on storage media.
Classification is most important!

Minimum security requirements for email: Sensitive email should be encrypted and labeled
Encrypting and labeling sensitive email will ensure that it remains confidential and can be identified. Performing these actions only on sensitive email will reduce the cost and effort of encrypting all email, allowing only sensitive email to be the focus of the organization's efforts.

Scenario:
Administrators regularly back up sensitive data on servers within a data center. Security controls restrict access to the data center, and all systems that process sensitive information are marked. After backing up data, they send an unmarked copy to an unstaffed company warehouse for long-term storage. Recently, someone posted some of this data on the internet. Investigators determined much of the backup media is no longer in the warehouse.
Preventative Administrator action: Mark the tapes before sending them to the warehouse.

Encryption

Encryption protects data at rest and data in transit.

Network-level encryption protects *data in transit.*
Disk-level encryption and **column-level enc**ryption protects data at rest.
Purging memory buffers after data has been used protects **data in use.**

Scenario: Your organization recently suffered a data breach. You are reviewing your organization's data policy to see if it addresses protections that could have thwarted this attack.

Data handling. **Sh**ipping, **cha**in of **cus**tody. **Do** not open **box**es.

Data destruction. Erasing, clearing (overwriting w/ unclassified data)

Record retention. If the retention policy is 1 year, it should be destroyed when it ages out(>1 year)

Tape **bac**kup security Secure **faci**lity, tapes **lab**elled **ens**ures all understand the **class**ification of the data.

Scenario
Kaitlyn is concerned about the security of data users are retrieving from a website and would like to apply an appropriate ***cryptographic*** solution.
Kaitlyn is specifically concerned about information that users are retrieving. Therefore, she is considering a data in motion use case.

Domain 2 Destroying Data

Data Policy

Stress the problem that can result from incomplete sanitization:
Sanitization can be unreliable because **personnel** can perform the purging, degaussing, or other processes **improperly**. When done properly, purged data is not recoverable using any known methods.
Data cannot be retrieved from incinerated or burned media.
Physical destruction such as an incinerator to dispose of DVDs is the most secure method of deleting data on optical media such as a DVD.

Data Destruction Methods

- **Erasing** - **per**form a **del**ete operation against a file, files or media (**dat**a is **rec**overable)
    - Erasing data on a hard disk drive is likely to leave some data on a hard disk drive, also known as data remanence.
    - Data remnant destruction is a security concern related to storage technologies more so than an email solution.
    - Remnant data is data that is left after attempts have been made to remove or erase it
    - Erasing is the deletion of files or media and may not include all of the data on the device or media, making it the worst.

- **Clearing** (**over**writing)
  - preparing media for **reuse** and ensuring data **cannot** be **rec**overed using traditional recovery tools
  - Clearing describes preparing media for reuse. When media is cleared, unclassified data is written over all addressable locations on the media. Once that's completed, the media can be reused, although it may be possible to retrieve some of the original data using retrieval tools.
  - **clearing** is the process of preparing media for **reuse**
- **Purging**
  - a more **inte**nse form of **cle**aring that **prep**ares media for reuse in less secure environments.
  - If an organization allows media to be donated or downgraded, the purging process should be followed, and then the media should be relabeled.
    - Follow the organization's purging process, and then downgrade and replace labels.
  - **Data Purging** - Writing a series of 1s and 0s over media multiple times
  - **Zero fill** wipes a drive by replacing data with zeros
  - Example is SSD drives in computers donated to school - purging reliable methods to ensure data is removed.
- **Degaussing** create a **stro**ng **mag**netic field that erases data on some media
  - Degaussing and declassifying the tape is done if you plan to reuse it.
  - Degaussing the **disks** often damages the electronics but doesn't reliably remove the data.
  - Degaussing uses magnets to wipe magnetic media
  - Solid-state drives (SSDs) do not have magnetic flux, so degaussing an **SSD** doesn't destroy data.
- **Destruction**
  - is the **fin**al **sta**ge in the life cycle of tape media and is the most secure **meth**od of **sanit**ising media.
  - Destruction is the final stage in the lifecycle of backup media.
  - Due to problems with remnant data, the U.S. National Security Agency requires physical destruction of **SSDs**. This process, known as disintegration, results in very small fragments via a shredding process.
  - Data assets that can be safely shredded
    - Paper records
    - Credit cards
    - Removable media
    - SSD hard drives

- Sanitization
  - sanitization is a series of processes that removes data from a system or media while ensuring that the data is **unrecoverable** by any means.

*__Bitrot__ is a term used to describe aging media that decays over time.

Erase hard drives (HDD), desktops, laptops or servers free with a Darik's Boot and Nuke (DBAN), not SSDs.

sanitization Scenario
Organization allows downgrading of systems for reuse after projects have been finished and the systems have been purged.
Concern?
Downgrading systems and media is rare due to the difficulty of ensuring that sanitization is complete. The need to completely wipe (or destroy) the media that systems use means that the cost of reuse is often significant and may exceed the cost of purchasing a new system or media.
The goal of purging is to ensure that no data remains, so commingling data should not be a concern, nor should the exposure of the data; only staff with the proper clearance should handle the systems!
Result: The cost of the sanitization process may exceed the cost of new equipment.

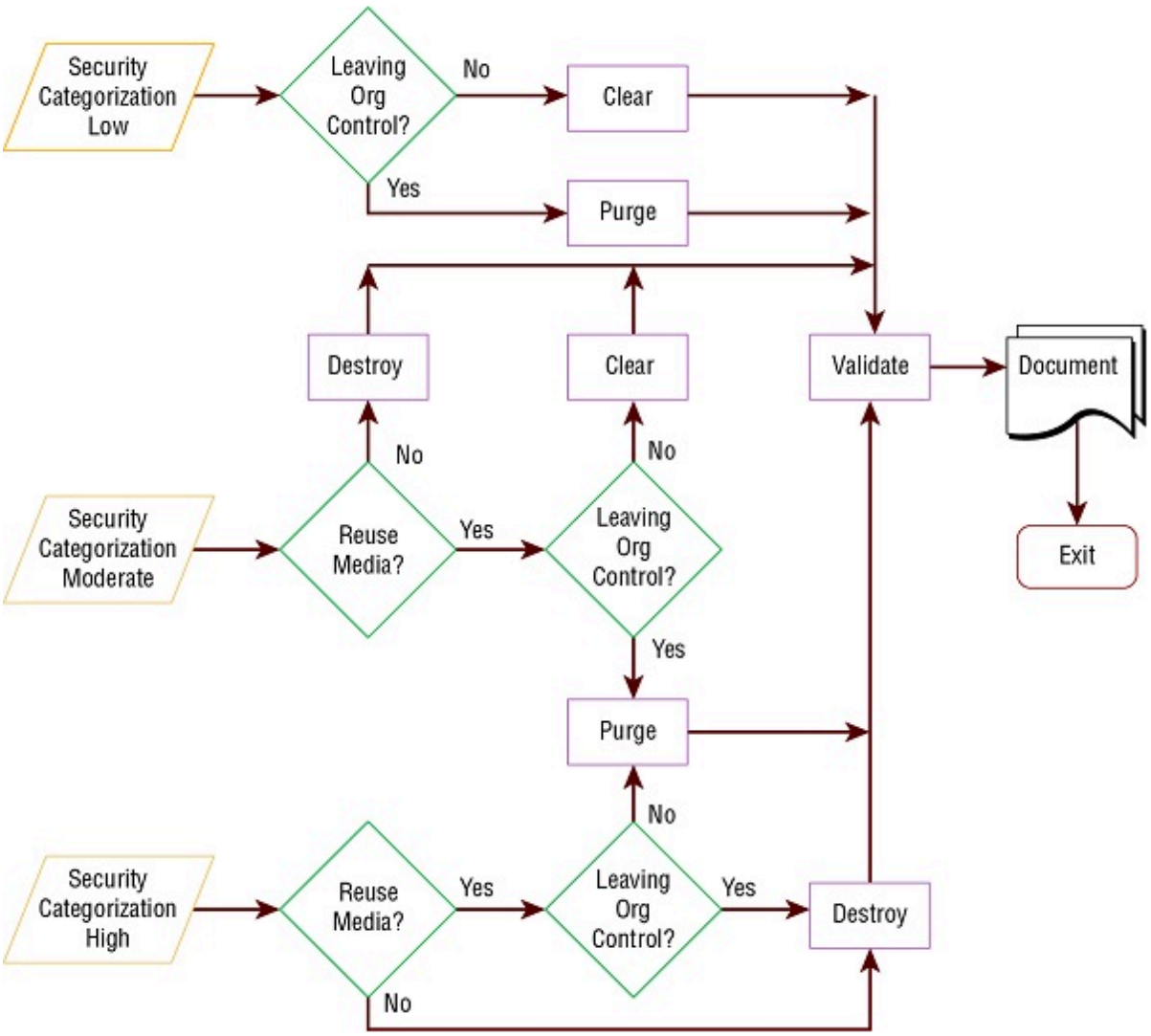
Degaussing involves using a strong magnetic field to erase data stored on magnetic media such as tapes. This method effectively destroys the data by randomizing the magnetic particles on the tape, making it virtually impossible to recover the original data. Degaussing ensures that sensitive information is securely erased before tapes are reused, maintaining data confidentiality and compliance with security policies.

Symmetric encryption uses the same key to **enc**rypt data and the same key to **dec**rypt the data.
Cryptographic shredding involves **destr**oying the encryption **key** used to encrypt data, making it **perm**anently **inacce**ssible.

Residual data might be **reco**verable after deletion or secure disk wipe and this data remanence is considered a security concern.
Mishandling of drives by the third party concerns.

Guidelines Sanitization NIST 800-88

NIST SP 800-88
Flow Diagram guidelines for media sanitization.



Example:
moderate security categorization in the NIST model. If the media is going to be sold as surplus (reuse).
Flow Path**: Purge, Validate, document, Exit**
The NIST SP 800-88 process for sanitization and disposition shows that media that will be reused and was classified at a moderate level should be purged and then that purge should be validated. Finally, it should be documented.

Slack Space

Slack space is the **unused space in a cluster.**
However, slack space can still contain data previously stored in memory. Clusters are groups of sectors. One way of eliminating data remanence is by overwriting clusters with random bits. However, overwriting a cluster with random bits does not create slack space.
Slack space is NOT directly related to files, even though files take up one or more clusters. Deleted files remain on the drive until the system overwrites them, but deleted files are not slack space.

Domain 2 Asset Classifications

End game is to protect data.
primary purpose of information classification processes: Define the requirements for protecting sensitive data.

Security Control Baseline

Provides a listing of controls that an organisation can apply as a baseline.

Security Baseline:

- A baseline defines a **minimum level of security that every system** throughout the organization must meet.
- A baseline is a more **operationally focused** form of a standard.
- All systems **not comply**ing with the baseline should be **taken out of prod**uction until they can be brought up to the baseline.
- Baselines are usually **system specific** and often refer to an industry or government standard.

After selecting a control baseline, organizations fine-tune it with tailoring and scoping processes. A big part of the tailoring process is aligning the controls with an organization's specific security requirements
The scoping process removes controls from a list of controls from a suggested baseline.
Removing Controls from a suggested baseline - scoping process.

These options are part of the **tailoring** process but not part of the scoping process:

- Selecting compensating controls
- Identifying common controls
- procedures match the specific systems
- Assigning different values for a control

Scoping is the process of reviewing and selecting security controls based on the system that they will be applied to.

See Domain 5
A **compensating control** is deployed to provide various options to other existing controls to aid in enforcement and support of security policies.
compensating control provides extended options to existing controls and is used in addition to, or in place of, another control
Compensating control can be any controls used in addition to, or in place of, another control. They can be a means to improve the effectiveness of a primary control or as the alternate or failover option in the event of a primary control failure.

Recovery controls are an extension of corrective controls but have more advanced or complex abilities. A recovery control attempts to repair or restore resources, functions, and capabilities after a security policy violation.

A **corrective control** modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred. It attempts to correct any problems that occurred as a result of a security incident. (

A **deterrent control** is deployed to discourage security policy violations.

Record retention

Record retention and data destruction - legal issues
Record retention policies define the amount of time to keep data, and laws or regulations often drive these policies.
Data retention policy reduces liabilities, By reducing the amount of data that may need to be produced for lawsuits.
Data retention policies can reduce the number of old logs and other files that may need to be produced during a legal case. That can reduce organizational risk, but retention policies need to be in place well before a legal hold is filed.

Data protection

Confidentiality is often protected through encryption (at rest and in transport)
See Domain 3!

When implementing security controls for **data at rest,** Full disk encryption is the most effective for ensuring confidentiality.

A security auditor is seeking evidence of how sensitive documents made their way out of the organization and onto a public document distribution site. It is suspected that an insider exfiltrated the data over a network connection to an external server. Investigation require following:

- DLP Alerts
- Log Analysis

Assign Asset Classifications

Asset classifications should match the data classifications.
Assign systems the classification of the highest level of information that they are ever expected to process.

Domain 2 Data Classification

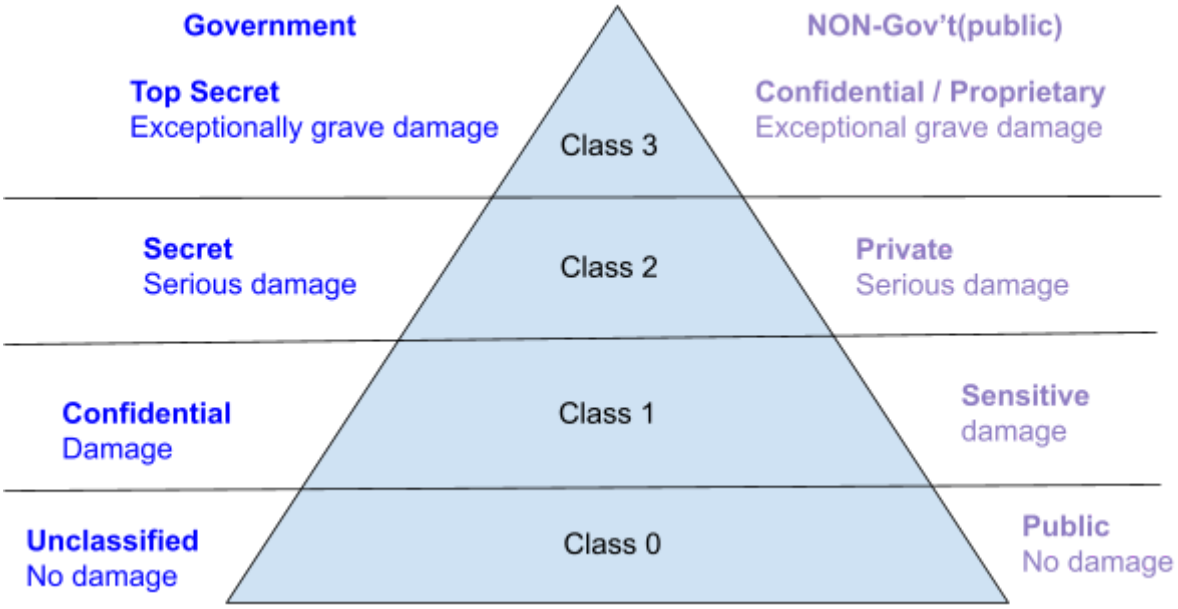
Integrity refers to the trustworthiness of the data.
Data classifications provide strong protection against the loss of confidentiality.
Data labels and proper data handling are based on first identifying data classifications.
Data degaussing methods apply only to magnetic media.

Data Classification Consideration

- Data is classified based on its value to the organization.
- Who can access the data
- What the impact would be if the data was lost or breached
- What Protection regulations may be required for the data

How much the data cost to create is not consideration for data classification.

Data Classes Drawing



Domain 3 will cover **Data Class**ification under **sens**itive but **uncl**assified in **crypto**graphy.

There are six standard data type classifications used in either a government/military or a private sector organization in this list of options:

1. Public
2. Private
3. Sensitive
4. *Proprietary*
5. ***Critical***
6. Confidential

The most **crit**ical factor to **cons**ider when s**ele**cting a **ven**dor in the context of information security is **Data Class**ification.
Data classification helps organisations identify and **categ**orize sensitive information, ensuring that the appropriate security measures are applied. Different types of data require varying levels of protection, and understanding data classification helps in making informed decisions.

Scenario:
Company ***proprietary*** data are discovered on a public social media posting by the CEO. While investigating, a significant number of similar emails were discovered to have been

sent to employees, which included links to malicious sites. Some employees report that they had received similar messages to their personal email accounts as well.
Security Improvements to implement:

- Block access to personal email from the company network
- Prohibit access to social networks on company equipment

Digital watermarking

method to embed unobtrusive labels in digital data. After they are embedded, other methods should be able to detect these labels.
Digital watermarking places labels or markings in files (digital data). Other methods, such as data loss prevention (DLP) and digital rights management (DRM), can detect the labels.

By labeling data, the DLP system can detect labels and apply appropriate protections.

Domain 2 Defining Sensitive Data

Defining Sensitive Data
Sensitive data is any information that is not public or **unclas**sified.

Personally Identifiable Information (**PII**) any **info**rmation that can identify an **indiv**idual (name, SSN, ID, Birthdate, place, biometric records,credit card, etc.)
PII Data

- Social Security number
- driver's license number
- state identification card number
- credit/debit card numbers
- bank account numbers (in conjunction with a PIN or password)
- ***Student ID number*** (PII under U.S. federal government regulations)

Model after California's data breach notification law.
These laws are separate and distinct from privacy laws, such as the California Consumer Privacy Act (CCPA), which regulates the handling of personal information more broadly.

A web service collects personal information from California residents. They must have a conspicuously posted privacy policy on the site as required by the California Online Privacy Protection Act requirement to be compliant.
conspicuously - in a clearly visible way.

Protected Health Information (**PHI**) and **heal**th related **infor**mation that can be **rela**ted to a specific person, covered by HIPAA in Domain 1.

Domain 2 Data Ownership

Data Security Roles:

- Data **Owner** -
    - Usually a member of senior management.
    - Establishes rules for appropriate use and protection of data

    - Can delegate some **day-to-day** duties. Cannot delegate total responsibility.
    - A data owner is the entity assigned specific responsibility for a data asset in order to ensure its protection **for use by the org**anization.
    - responsible for classifying data
    - A data owner is the person who has final corporate responsibility for the protection and storage of data.

- **Business**/Mission Owners -
    - Choose COBIT, Business owners have to balance the need to provide value with regulatory, security, and other requirements. This makes the adoption of a common framework like COBIT attractive.
    - Business owners might own processes that use systems managed by other entities.
    - As an example, the sales department could be the business owner, but the IT department and the software development department could be the system owners for systems used in sales Processes.
- System Owner
    - NIST SP 800-18 describes **system owner** responsibilities that include helping to develop system security plans, maintaining the plan, ensuring training, and identifying, implementing, and assessing security controls.
    - Develops a system security plan
    - Identifies and implements security controls
    - Ensures that system users receive appropriate security training
- **Data Custodian** -
    - usually someone in the IT department.
    - Custodians are trusted with day-to-day data handling tasks.
    - responsible for implementing the protections defined by the security policy
    - Does not decide what controls are needed, but does **impl**ement **contr**ols for **dat**a **own**ers.
    - Monitor Security
    - A data custodian protects the integrity and security of the data by performing day-to-day maintenance
    - A **data custodian** is the entity assigned or delegated the day-to-day responsibility for proper storage and transport as well as protecting data, assets, and other organizational objects.
    - implement data protection tasks based on the data classification
    - a data custodian is responsible for day-to-day tasks to protect data, such as **backing up data.**
- Data **Administrators**
    - Administrators have the rights to apply the permissions to access and handle data.
    - Responsible for **grant**ing appropriate **acc**ess to **person**nel (often via RBAC)
- **Data User** -
    - any person who accesses data via a computing system to **acco**mplish **work** tasks.
    - The user interacts with assets and is responsible for abiding by company security policy

- **Asset Owners**
    - Asset Owners own the asset or system that processes sensitive data and **associated security plans**.
    - ultimately responsible for **due diligence** in protecting a company's data
    - Asset owners are responsible for assets in an organization, including their procurement, management, and life cycle.
    - identifies the individual(s) responsible for protecting the asset
    - Owners may be liable for negligence if they fail to perform due diligence in establishing and enforcing security policy to protect and sustain sensitive data.
    - The asset owner is ultimately responsible for due diligence in protecting a company's data. The asset owner is accountable for the security and protection of the data or information under their control. This responsibility includes making decisions about how data should be classified, how it should be protected, and ensuring that appropriate security measures are implemented and maintained.
- Data Controller
    - A data controller decides what data to process and directs the **data processor** to process the data.
    - The small business is the data controller.
    - The data controller identifies what data to pass to the **data processor** and how that data should be processed.

Example:
A **data custodian** is responsible for securing resources after **the data owner** has assigned the resource a security label.

Domain 2 GDPR Terms and Concepts

California Consumer Privacy Act (**CCPA**) of 2018 was the first sweeping data privacy law enacted by a U.S. state. This follows California's passing of the first data breach notification law, which was modelled after the requirements of the European Union's General Data Protection Regulation (GDPR).

GDPR Requirements

- **Data Processor** - a natural or legal person, public authority, agency, or other body, which **processes** personal **data** solely on behalf of the data controller.
    - A **data processor** is the entity that performs operations on data.
    - Example: A small business is planning to outsource payroll. This requires the business to pass some data to the payroll company to handle payroll functions.
- **Data Controller** -
    - the person or entity that controls **processing** of the **data.**
    - A data controller is the entity that makes decisions about the data they are collecting.
- **Data Transfer** - GDPR restricts data transfers to countries outside the EU

The **right to erasure**, also known as the **right to be forgotten,** guarantees the data subject the ability to have their information removed from processing or use.
It may be tied to consent given for data processing; if a subject revokes consent for processing, the **data controller** may need to take additional steps, including **erasure**.

Providing consent, or agreeing to data collection and use, is important in many data collection scenarios and may be required by law. Consent ensures that data subject agree to the processing of their data.

Protecting the fundamental right to data privacy of EU residents best captures the primary intent of GDPR.
Organizations in the United States are not allowed to process EU citizen personal data.

"actions that compromise the privacy of users" are explicitly identified in RFC 1087.

Reducing GDPR Exposure

Steps to reduce or eliminate GDPR requirements/Compliance Problems:

- **Anony**mization -
  - Data de-identify
  - The process of **remov**ing all relevant **dat**a so that it is **imp**ossible to **iden**tify the original subject or person. If done effectively the GDPR is no longer relevant for the **anonymized** data.
- **Randomized** masking
  - one of many **anonymization** methods and is the best choice. When done correctly, it cannot be reversed to discover the original data.
  - Data masking is a method used to **anonymize** data and protect the privacy of individuals in a dataset. It replaces privacy data (such as names) with incorrect data, but the dataset still retains usable data.
  - The EU GDPR does not apply to effectively **anonymized** data.
  - **Anonymization** techniques remove all data so that it is difficult to identify the original identities. When done correctly, the GDPR no longer applies.
  - Tokenization replaces other data with a random string of characters. These tokens are then matched to the actual values for secure lookups as needed. Tokenization replaces data in a database field with a randomized string of characters that remains the same for each instance of that data.
  - In a tokenization system, the token on its own has no meaningful value or information and primarily distinguishes the token from the original sensitive data it represents.
- **Pseudonymization** -
  - However, if applying pseudonymization techniques, the GDPR still applies
  - The **proc**ess of using pseudonyms (**aliases**) to present other data.
  - Can result in **less string**ent requirements than would otherwise apply under the GDPR.
  - Like a health patient number without the name.
  - Pseudonymization is the process of replacing some data with an identifier, such as a pseudonym.

GDPR requires notification of breach in 72 hours.

Ensure subsidiaries that share information across EU boundaries, ensure sharing is consistent with GDPR:

- The European Union provides **standard contractual clauses** that may be used to facilitate data transfer. That would be the best choice in a case where two different companies are sharing data.
- If the data were being shared internally within a company, **binding corporate rules** would also be an option.

The EU/US ***Privacy Shield*** was a safe harbour agreement that would previously have allowed the transfer but that is ***no longer valid.***

Collection Limitation

The online e-commerce company selling digital products can implement a data collection policy of minimization to minimize the amount of data they collect and store.
If they are selling digital products, they don't need the physical address.
If they are reselling products to the same customers, they can use tokenization to save tokens that match the credit card data, instead of saving and storing credit card data.

A grocery store chain collects customer data used in a customer loyalty program. When registering, customers fill out a lengthy form about themselves. The chain uses this data to email customers and allows customers to claim discounts when checking out using their customer loyalty cards.
A best practice when collecting customer data is to l**imit the amount of data collected** to only what is needed. The company's lengthy form might include physical addresses, phone numbers, cell phone numbers, birthdates, social security numbers, and more.
A data breach can reveal all this personal data even though the company never planned to use it. If they do not collect the data, they eliminate the risk of losing it in a data breach.

Anonymization techniques remove all personal data and make the data unusable for reuse on the website.
Tokenization replaces other data with a random string of characters. These tokens are then matched to the actual values for secure lookups as needed. replaces data in a database field with a randomized string of characters that remains the same for each instance of that data.
Pseudonymization replaces data with pseudonyms. Although the process can be reversed, it is not necessary.

Domain 3 Security Architecture

Research, implement and manage engineering processes using secure design principles.
Primary purpose of security models is to define security requirements for systems.
Understand the fundamental concepts of **security models** (biba, star model, bell-lapadula)

Select controls based upon systems security requirements

Select and determine ***cryptographic*** solutions
Understand methods of cryptanalytic attacks
Apply security principles to site and facility design
Design site and facility security controls

Open Design security principles emphasise that security mechanisms should not rely on the secrecy of the design or implementation.

It's much easier to build security into a system during development than it is to add security to an existing system.

Information System Lifecycle

The entire lifespan of an information system, from its initial conceptualization to its eventual decommissioning.
SDLC Phases:

- Stakeholders needs and requirements
- Requirements analysis
- Architectural **design**
- Development / implement
- Integration
- Verification and validation (testing)
- Transition / deployment
- Operations and maintenance / sustainment
- Retirement / disposal

See Domain 8 Software development lifecycle.
Most critical step in the secure software development lifecycle (SDLC) for preventing security vulnerabilities is doing requirements gathering.
In SDLC the design phase is responsible for identifying and categorizing potential threats and vulnerabilities.

Domain 3 Information system LifeCycle

CISSP Exam Cram - 2024 Addendum
A Structured framework for managing an information system from its initial conception to its eventual retirement.
It outlines the key phases involved in:

- Planning, designing, and building
- Deploying, operating, maintaining
- Decommissioning a system

Security **Goal**:
Ensure a system is developed and managed in a way that meets business needs, remains secure and operates efficiently throughout its lifespan.

Info System Life-Cycle Steps

1. Stakeholders needs and requirements
    a. Identify the needs and requirements (problems the system needs to solve, goals it must achieve)
    b. Define functional and security features required
    c. Key Activities: Gather requirements, conduct stakeholder interviews and define project scope.
    d. Security **Goal**: Establish the baseline security expectations for the system. This includes understanding confidentiality, **integrity**, and availability needs as well as identifying compliance requirements.
2. Requirements analysis
    a. Analyse and refine the requirements gathered to ensure they are consistent, complete and unambiguous
    b. Key Activities: Prioritize requirements, create requirement specification documents, perform risk analysis
    c. Map requirements to security controls and conduct feasibility studies
    d. Security **Goal**: Translate high-level security expectations into detailed actionable security requirements and controls. These should address risks identified earlier.
3. Architecture design
    a. Develop a high-level blueprint of the overall architecture of the system, including hardware, software, and network components, with consideration to security and performance.
    b. Key activities: create system architecture diagrams, evaluate architectural options, interfaces, data flows and threat modelling.
    c. Security **Goal**: Incorporate security by design. Architectural decisions should address identified risks, support security principles (like least privilege), and aim for a defense-in-depth approach.
4. Development/Implementation
    a. Actual build, development, acquisition, or implementation of the system based on the architectural design, ensuring secure coding practices are followed.
    b. Key activities: Develop or procure software/hardware, conduct code reviews, and implement security configurations.
    c. Security **Goal**: Ensure secure implementation of the design. This includes secure coding practices, configuration hardening, and integrating necessary security tools.
5. Integration
    a. Ensure components function together and meet defined requirements by aligning with the overall system architecture.
    b. Key Activities: Perform integration testing and documentation of integration issues.
    c. Security **Goal**: Maintain integrity and security during integration, Identify and address potential security gaps or conflicts arising from how components interact.
6. Verification and validation

   a. Confirm the system meets intended requirements (verification) and addresses the overall business/stakeholder needs(validation)
   b. Key Activities: Employ various testing techniques (unit, functional, user acceptance, performance security), review test results, and obtain stakeholder feedback.
   c. Security **Goal**: Rigorously test that security requirements are met, vulnerabilities are minimised, and the system does not introduce unacceptable levels of risk.
7. Transition / Deployment
   a. Move the system from development into the production environment in a controlled and secure manner.
   b. **Key Activities:** Develop implementation plans, conduct user training, perform a pilot rollout (if applicable), execute a full system implementation.
   c. Security **Goal**: secure and controlled transition. Protect data during migration, apply security configurations for production environments, and ensure operational security processes are in place.
8. Operation and Maintenance sustainment
   a. Ongoing operation and management of the system to ensure availability and performance.
   b. This includes troubleshooting, applying updates, address vulnerabilities, and incident response.
   c. During the **data maintenance phase** of a typical data life cycle, activities like data scrubbing occur to remove unneeded, incorrect, or out-of-date data.
   d. **Key Activities:** Execute system monitoring, patch management, configuration management, incident response, and change control. *Care and feeding*.
   e. Security **Goal**: Continuous maintenance of security posture. This includes patch management, vulnerability scanning, incident response, and adapting controls to evolving threats.
9. Retirement / Disposal
   a. Secure decommissioning or disposal of the system when it reaches the end of its useful life or becomes obsolete.
   b. Focus on preventing data exposure and respecting data retention periods is critical.
   c. **Key Activities**: Data archival, system decommissioning and secure disposal of hardware and media.
   d. Security **Goal**: Prevent data exposure. Focus on security data sanitization, proper hardware disposal and ensuring compliance with data retention requirements.

CISSP Exam Cram - 2024 Addendum

Domain 3 Security Architecture & Engineering

Research implement and manage engineering processes using secure design principles.

- Threat modelling - keep it simple
- Least privilege - Zero Trust
- Defense in depth - Privacy by design (PbD)
- Secure defaults - Trust but verify
- Fail securely - Shared responsibility
- Separation of Duties

Understand **meth**ods of **cryptan**alytic **att**acks

- Brute force - Fault injection
- Ciphertext only - Timing
- Known plaintext - Man-in-the-Middle (MITM)
- Frequency analysis - Pass the hash
- Chosen ciphertext - Kerberos exploitation
- Implementation attacks
- Ransomware
- Side-channel
    - Side-channel attacks use information gathered about a system's use of resources, timing, or other characteristics to contribute to breaking the security of encryption.
    - attacker is measuring the electricity consumption of a cryptographic device deployed in the field to attempt to gain access to encrypted data.

Defense in depth

Defense in depth is simply the use of multiple controls in a **series**. No one control can protect against all possible threats. Using a multilayered solution allows for numerous, different controls to guard against whatever threats come to pass.
Layering is the deployment of multiple security mechanisms in a series. When security restrictions are performed in a series, they are performed one after the other in a linear fashion. Therefore, a single failure of a security control does not render the entire solution ineffective.

Terms that relate to or are based on defense in depth:

- Layering
- Classifications
- Zones
- Realms
- Compartments
- Silos
- Segmentations
- lattice structure - models are used to define the levels of security that an object may have and that a subject may have access to
- protection rings.

Domain 3 Common Cryptanalytic Attacks

Brute Force Attack

Attempts to randomly find the correct cryptographic key attempting all possible combinations (trial and error)
Rainbow tables and big hardware make this attack more effective.
Effective countermeasures include cryptographic salts, captcha, throttling rate of repeated logins and IP blocklists.
Strong password policies, physical access control, and two-factor authentication all improve the protection against brute-force and dictionary password attacks.

Password complexity is driven by length, and a longer password will be more effective against brute-force attacks than a shorter password with cp,[;exoty with at least three character classes.

Birthday Attack

An attempt to find collisions in hash functions.
Commonly target digital signatures.
Defeat with long hash output.
It is a collision attack that occurs when two different inputs produce the same hash value.

Replay Attack

An attempt to reuse authentication requests.
Commonly target authentication
Defeat with date/time stamps.
Lifetime limits prevent kerberos replay attacks.

Replay Attack can be used against **cryptog**raphic **algo**rithms that do not incorporate **temporal** protections.

Replay Attack Scenario
Jerry is investigating an attack where the attacker ***stole*** an authentication token from a user's web session and used it to impersonate the user on the site.
Answer:
Masquerading (or impersonation) attacks use stolen or falsified credentials to bypass authentication mechanisms. That term does describe this attack, but you should keep reading the answer choices even after finding a possible correct answer.
In this case, **replay** attacks are a more specific type of masquerading attack that **relies on captured authentication tokens**, and this is, therefore, a better answer.

Masquerading (or impersonation) attacks use stolen or falsified credentials to bypass authentication mechanisms. That term does describe this attack, but you should keep reading the answer choices even after finding a possible correct answer. In this case, replay attacks are a more specific type of masquerading attack that relies on captured authentication tokens, and this is, therefore, a better answer. Spoofing attacks rely on

falsifying an identity like an IP address or hostname without credentials. Modification attacks occur when captured packets are modified and replayed to a system to attempt to perform an action.

Meet-in-the-middle attack

The reason 2DES was retired.
Exploits protocols that use two rounds of encryption.

Man-in-the-middle attack

Fools both parties into communicating with the attacker (in between the two) instead of directly with each other.
Only use secure Wi-Fi, VPN, HTTPS, and use MFA.
Using a trusted channel and link encryption are both ways to prevent MITM attacks.
In a **man-in-the-middle attack**, attackers manage to insert themselves into a connection between a user and a legitimate website, relaying traffic between the two parties while eavesdropping on the connection.
Although similarly named, the **meet-in-the-middle attack** is a cryptographic attack that does not necessarily involve connection tampering.

Cryptographic Secret Attacks

- Known Plaintext = encrypted message + plaintext message
- Chosen Plaintext = choose the plaintext to be encrypted
- Chosen Ciphertext = algorithm + choose the ciphertext output.
- Brute-force = tries all possible key combinations

Known Plaintext

Attacker has a copy of both the encrypted message along with the plaintext message used to generate the ciphertext.

Chosen Ciphertext

Attacker has the ability to decrypt chosen portions of the ciphertext message and use the decrypted portion to discover the key.
Chosen ciphertext attacks require access to the algorithm and work by having the attacker perform encryption that results in an expected ciphertext.

Chosen Plaintext

Attackers can encrypt plaintext messages of their choosing and can then analyse the ciphertext output of the encryption algorithm.

Above “text” attacks are Stopped with good algorithm choices.
Symmetric AES256 example!

Ciphertext Only Attack

An attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts.
RC4 (symmetric algorithm) and **WEP** are susceptible to this type of attack.
An attacker without any special access to the system would only be able to perform ciphertext-only attacks.
A ciphertext-only attack (COA) is a type of cryptographic attack where the attacker has access only to a set of ciphertexts. The goal of the attacker is to deduce the plaintext (original message) or, ideally, the key used to encrypt the message. Here are the key points about ciphertext-only attacks:

Limited Information: The attacker does not have access to any corresponding plaintexts or the encryption algorithm. They only have the encrypted messages.
Feasibility: These attacks are generally more challenging to execute successfully because the attacker has very limited information. However, they are still a valid threat, especially if the encryption algorithm is weak or if patterns can be detected in the ciphertexts.
Methods: Attackers may use statistical analysis, ***frequency analysis***, or other methods to try and find patterns or weaknesses in the ciphertext.

Real-World Relevance: While difficult, ciphertext-only attacks can be practical in certain scenarios, particularly when large amounts of ciphertext are available for analysis.

Example Scenario
An attacker intercepts encrypted communications between two parties. They collect multiple ciphertexts but do not have access to the original plaintext messages or the encryption key. Through statistical analysis, the attacker identifies common patterns or anomalies in the ciphertexts. If the encryption scheme is not robust enough, these patterns could reveal information about the plaintext or the encryption key.

Known plaintext attack

Known plaintext and chosen plaintext attacks require the ability to encrypt data.
Linear cryptanalysis is a known plaintext attack. Cryptanalysis is the process of examining an info system in order to break its encryption.
Attack will use the plaintext and ciphertext to attempt to extract the encryption key.

Importance in CISSP Context
Understanding ciphertext-only attacks is crucial for the CISSP exam, as it emphasises the need for strong encryption algorithms and key management practices to protect sensitive data. The exam may test your knowledge on how to defend against such attacks by selecting appropriate encryption methods and implementing best practices in cryptographic systems.

Scenario Ciphertext-only

Alan intercepts an encrypted message and wants to determine what type of algorithm was used to create the message. He first performs a frequency analysis and notes that the frequency of letters in the message closely matches the distribution of letters in the English language.
What type of cipher was most likely used to create this message?

Transposition cipher.
The use of a substitution cipher, a category that includes AES and 3DES, would change the frequency distribution so that it did not mirror that of the English language.
This type of attack, where the attacker only has access to an encrypted message, is also known as a ciphertext-only attack.

Fault injection attack

Fault injection attacks require physical access to the facility.
Fault injection attacks compromise the **integrity** of a cryptographic device by causing some type of external fault, such as the application of high-voltage electricity.
Analyst believes that an attacker accessed a highly secure system in his data center and applied high-voltage electricity to it in an effort to compromise the cryptographic keys that it uses.

Example:
Ron is investigating a security incident that took place at a highly secure government facility. He believes that encryption keys were stolen during the attack and finds evidence that the attackers used dry ice to freeze an encryption component.
In a fault injection attack, the attacker attempts to compromise the integrity of a cryptographic device by causing some type of external fault. For example, they might use high-voltage electricity, high or low temperature, or other factors to cause a malfunction that undermines the security of the device.

Implementation attack

Implementation attacks rely on flaws in the cryptographic algorithm.

Timing attack

Timing attacks measure the length of time consumed by encryption operations.

Frequency Analysis

Counting the number of times each letter appears in the ciphertext. Based on the knowledge E, T, A, O, I, N are the most common in the English language.
If E,T,A,O,I,N most common = transposition cipher, Else if not, it is likely a substitution cipher.

Scenario:
An attacker has intercepted a large amount of data that was all encrypted with the same algorithm and encryption key. With no further information.
The attacker may attempt to perform **frequency analysis** or a brute-force attack against the large volume of encrypted ciphertext.

As the attacker does **not** have access to the plaintext information, a known plaintext attack is not possible. The attacker also **does not** have the ability to encrypt information, so they cannot use a chosen ciphertext attack.

Attacks and Countermeasures

Domain 3 Shared Responsibility

- Everyone in an organization has some level of security *responsibility*.
- Organizations are *responsible* to their stakeholders for making good security decisions in order to sustain the organization.
- When working with third parties, especially with cloud providers, each entity needs to understand their portion of the shared *responsibility* of performing work operations and maintaining security.
- As we become aware of new vulnerabilities and threats, we should consider it our responsibility (if not our duty) to *responsibly* disclose that information to the proper vendor or to an information sharing center.

Domain 3 Zero Trust Security

The primary driver behind the adoption of the **zero trust** model has been the **proliferation** of endpoint devices.
proliferation - rapid increase in the number or amount of something(threat)

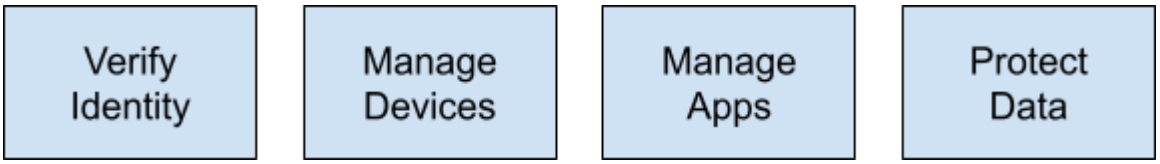
- Believe no one
- Assume no trust
- Check everything

Zero Trust 5 Steps

1. Inventory
    a. Identify the protect surface
2. Map data flows
3. Architect zero trust
    a. Just in time
    b. Just enough access
    c. Encryption / tokenization
    d. Microsegmentation
    e. Isolation
4. Dynamic policies / automation behaviour or conditional
    a. Automated rule based creation
5. Continuous monitoring
    a. SIEM and SOAR

An endpoint device could be a user's workstation, a tablet, a smartphone, an IoT device, an ICS system, an edge computing sensor, and any public-facing servers in a screened subnet or extranet.
Being able to control, much less trust, all of these devices has caused the loss of a clearly defined **security perim**eter between the outside untrusted world and the inside trusted organization.
This results in the "**assume breach**" stance, which requires organizations to "**never trust, always verify**."

Addresses the **limit**ations of the legacy network perimeter-based security model
Treats user identity as the control plane
Assumes **comp**romise / **brea**ch in **veri**fying every **req**uest
No entity is trusted by default



Secure Design Principles

- Least Privilege
  - The least privilege principle ensures that users (subjects) are granted only the most restrictive rights they need to perform their work tasks and job functions. Users don't execute system processes. The least privilege principle does not enforce the least restrictive rights but rather the most restrictive rights.
- **Sec**ure **Def**aults -
  - default configuration reflects a restrictive and conservative enforcement of security policy
- **Fai**l **Secu**rely -
  - Fail-secure - example is windows blue screen of death (BSoD)
  - indicates that components should fail in a state that **deni**es **rat**her than **grant**s access (NIST sp 800-160)
- **Trus**t but **veri**fy -
  - depended on an **init**ial **auth**entication process to gain **acc**ess to the internal secured environment then **rel**ied on generic access control methods.
- Threat Modelling
- Keep it simple
- Separation of duties
  - Role-based access control (RBAC)
  - User roles
- Zero Trust
- Privacy by design

System Development

- The idea that systems should be designed to operate in a secure manner if the user performs no other configuration is the secure defaults principle.
- The idea that systems should be designed to fall back to a secure state if they experience an error is the, fail securely principle.
- The idea that systems should be designed to incorporate security as a design feature is the security by design principle.
- The idea that systems should be designed in a manner that keeps their functionality as simple as possible is the keep it simple principle.

Privacy by design (PbD)

7 Privacy Principles from the IAPP

1. **Pro**active and not a reactive approach
2. **Priv**acy as the **def**ault settings
3. **Priv**acy **embed**ded in the design
4. **Priv**acy should be a **pos**itive-sum **app**roach and not a **zero-sum** approach
5. **End to end** full **life**cycle data protection
6. **Visib**ility and **transp**arency - keep it open
7. Respect for user privacy - Keep **user-centric** (GDPR be forget user data)

Transparency: Among the many aspects of a security solution, the most important is whether it addresses a specific need (i.e., a threat) for your assets. But there are many other aspects of security you should consider as well. A significant benefit of a security control is when it goes unnoticed by users.

Applying these principles in implementing a **laye**red **def**ense as part of a **zero** trust strategy ensures privacy.

Involving privacy **exp**erts from the **incep**tion of a project is the most **criti**cal **asp**ect of privacy by design.

Zero Trust

Zero trust verify everything

- Trust nothing, inside or outside
- Verify every transaction from any subject to any object
- Segmentation and granular security
- Policy drivers
    - User authentication
    - Device verification
    - Service authorization
    - Real-time monitoring

Trust but Verify

- Locking down architectures and focusing on prevention only is outdated

- Instead focus on complete controls (**preventative, detective, corrective**) based on detection and response as well
- Increased need to monitor, and trust through assurance mechanisms
    - Audits
    - Ongoing monitoring
    - SOC reporting
    - Contracts/agreements

Zero trust is the recommended replacement security approach for trust but verify.
A termination process often focuses on eliminating an employee who has become problematic, whether that employee is committing crimes or just violating company policy.
Once the worker is fired, the company has little direct control over that person.
So, the only remaining leverage is legal, which often relates to a nondisclosure agreement (NDA).
Hopefully, reviewing and reminding the ex-employee about their signed NDA will reduce future security issues, such as confidential data dissemination.

A memorandum of understanding (MOU) is not the optimal place to define minimum security requirements because it is only a statement of intentions and not a legal contract.

Cloud Audit Standards

CISSP Exam Cram - 2024 Addendum related to Domain 6
SSAE - Statements on Standards for Attestation Engagements
SSAE-18 does not assert specific controls.
Instead, SSAE-18 reviews the use and application of controls in an audited organization. It is an attestation standard, used for external audits, and forms part of the underlying framework for SOC 1, 2, and 3 reports.

	Report Content Detail	Audience
SOC 1	Financial	Users, auditors
SOC 2	Confidential. Full detail	Auditors, partners, customer
SOC 3	Public, but Limited info	Publicly available, third parties, external release

- SOC 1
    - Deals mainly with **financial controls** and are used primarily by CPAs auditing financial statements
- SOC 1 TYPE 1
    - A report that provides the **auditor's opinions of financial statements** about controls at the service organization and that includes a report on the **opinion** on the presentation of the service organization's system as well as suitability of the controls
- SOC 1 TYPE 2

    - A report that **provides an assessment of the risk of material misstatement** of financial statement assertions affected by the service organization's processing and that includes a description of the service auditor's tests of the controls and the results of the tests and their effectiveness
- SOC 2
    - A report that provides **predefined, standard benchmarks for controls** involving confidentiality, availability, integrity, and privacy of a system and the information it contains, generally for restricted use.
- SOC 2 Type I
    - Report that assesses the design of security processes and controls at a specific **point in time**
- SOC 2 Type II
    - Assesses how effective those controls are over time by observing operations for at least **six months**.
    - Often require an NDA due to sensitive contents, signed in the portal.
    - System and Organization Controls audit program includes business continuity controls in a SOC 2, but not SOC 1, audit. Although FISMA and PCI DSS may audit business continuity, they would not apply to an email service used by a hospital.
- SOC 3
    - A **general** use report that reports on controls related to compliance and/or operations
    - Containing only the auditors general **opinions** and non-sensitive data, is publicly shareable.

ISAE - International Standard on Assurance Engagements

- The international auditing and assurance standards board issues the ISAE
- This board and its ISAE standards are similar to the AICPA and it is SSAE standards
- The ISAE 3402 standard is roughly equivalent to the SOC 2 reports in the SSAE
- ISAE 3402 is mentioned briefly in the 2021 CISSP study guide

CSA - Cloud Security Alliance

- The **Security Trust Assurance and Risk (STAR)** certification program comes from CSA
- Can be used by cloud service providers, cloud customers, or auditors and consultants.
- Designed to demonstrate compliance to a desired level of assurance
- STAR consists of two levels of certification which provide increasing levels of assurance
    - Level 1: **Self- assessmen**t is a complimentary offering that documents the security controls provided by the CSP.
    - Level 2: **Third-party audi**t requires the CSP to engage an independent auditor to evaluate the CSPs controls against the CSA standard.
    - Stronger as Level 2 is a third party audit conducted by a trained, qualified auditor.
- CSA star is mentioned in 2021 CISSP study guide
- https://cloudsecurityalliance.org/star

SOC Reports

Service Organization Control (SOC) reports are not the appropriate place to define minimum security requirements for a third party, because an SOC is a review of the existing security of the entity.

<u>SOC Engagements (SSAE 18):</u>

SOC 1

- SOC 1 engagements assess the organization's controls that might impact the accuracy of financial reporting.

SOC 2

- IT & Security Professionals audience - 5 Trust principles AICPA
- Five AICPA Trust Services Criteria:
    - Security.
    - Availability.
    - Processing Integrity.
    - Confidentiality.
    - Privacy.
- SOC 2 and 3 engagements extend into controls protecting confidentiality, **integrity**, and availability more generally.
- SOC 2 audit results are **confidential** and are normally only shared outside the organization under an **NDA**.

SOC 3

- Public use, data removed from SOC 2 report before publish
- SOC 2 and 3 engagements extend into controls protecting confidentiality, **integrity**, and availability more generally.
- SOC 3 audit results are intended for **public** disclosure.

<u>SOC TYPE Reports:</u>

SSAE 18 engagements

Type I

- Type I SOC report is when no testing of the controls is performed.

Type II

- A vendor provides you with a **SOC 2 Type II** report.
- The **Type II** report also provides an **opinion** on the operating effectiveness of those controls over an extended period of time.
- The vendor's system controls have been audited over a specific period of time and were found to be operating effectively.
- A SOC 2 Type II report tests both the design and the operational effectiveness of controls over a period of time, typically 6-12 months.

SOC Bridge letter when there was no recent audit performance.

Keep it simple

Complexity is the worst enemy of security.

Best-in-suite over **best-in-breed** solutions are one approach used to simplify defense in-depth
Simplicity also helps to **avoid conf**iguration **mist**akes.

Keep it simple and small

- Economy of Mechanism
- Vulnerabilities increase as complexity increases
- Small and simple = less vulnerabilities, errors & easier to test

Fresh application of a classic ***'kiss'*** principle
Keep it simple and small - design principal

Security-AAS
A cloud provider concept in which security is provided to an organisation through or by an online entity.

Distributed Systems

A distributed system or a distributed computing environment (**DCE**) is a collection of individual systems that work together to support a resource or provide a service. Often a DCE is perceived by users as a single entity rather than numerous individual servers or components. DCEs are designed to support communication and coordination among their members in order to achieve a common function, **goal**, or operation
Example: blockchain
Use Case:
Your organization is considering the deployment of a DCE to support a massively multiplayer online role-playing game (MMORPG) based on the characters of a popular movie franchise. The **interconnectedness** of the components is the primary concern of a DCE that could allow for propagation of malware or making adversarial pivoting and lateral movement easy.

A DCE typically includes an **interface definition lang**uage (IDL). An IDL is a language used to define the interface between client and server processes or objects in a distributed system.
Following is examples of DCE IDL:

- RPC - remote procedure calls
- CORBA - Common Object Request Broker Architecture
- DCOM - Distributed Component Object Model

Internet of Things

A class of devices connected to the internet in order to provide automation, remote control, or AI processing in a home or business setting. IOT Devices

Smart devices

Mobile devices that offer customization options, typically through installing apps, and may use on-device or in-the-cloud artificial intelligence (AI) processing.

Mirai targeted “Internet of Things” devices, including routers, cameras, and DVRs.

Domain 3 SIEM and SOAR

Security orchestration, automation, and response (SOAR) technologies provide automated responses to common attacks, reducing an administrator’s workload. A security information and event management (SIEM) system is a centralised application that monitors log entries from multiple sources.

SIEM - Security Information Event Management
System that **coll**ects data from **man**y other **sourc**es within the network.
Provides **real-time mon**itoring, traffic **anal**ysis & notification of potential attacks.
Traffic analysis focuses more on the patterns and trends of data rather than the actual content.

SOAR - Security Orchestration Automation Response
Centralised alert and **resp**onse **auto**mation with **thre**at-specific **play**books.
Response may be fully automated or single-click.

A **playbook** is a document or checklist that defines steps taken to validate an incident and steps taken in response to an incident.
A **runbook** implements the checklists from a playbook.
An IPS attempts to prevent attacks, and SOAR technologies may use playbooks, but don't typically use checklists.

SIEM and SOAR often use AI, ML and threat intelligence to provide analysis.

Breach and attack simulation

Breach and attack simulation (**BAS**) systems are designed to inject threat indicators onto systems and networks in an effort to trigger other security controls, to verify that his organization’s intrusion prevention system is working properly.
Breach and attack simulation (BAS) platforms are intended to automate some aspects of penetration testing. These systems are designed to inject threat indicators onto systems and networks in an effort to trigger other security controls. White-box, grey-box, and black-box testing all involve more significant manual effort.

SOAR Benefits

Operations and functions that benefit from SOAR (Scripting and Automation):

- Configure a set of commands to occur based on a triggering event.
- Periodically perform vulnerability scans
- Run code at a specific time every day
- Performing fuzzing evaluation of deployed software

- Run code scanners to discover coding flaws
- Blocking communications based on invalid content

Automation and scripting can be essential elements of security management and software development.

Modern Compute & Security

Microservices and SOA
SOA is the creation of discrete services that may be accessed by users in a black box fashion.
Service-oriented architecture (SOA) constructs new applications or functions out of existing but separate and distinct software services. The resulting application is often new; thus, its security issues are unknown, untested, and unprotected.
Microservice is a direct extension of SOA that creates single-use functions that can be employed via an API by other software.

Service-oriented architecture (SOA) constructs new applications or functions out of existing but separate and distinct software services. The resulting application is often new; thus, its security issues are unknown, untested, and unprotected. Microservices is a direct extension of SOA that creates single-use functions that can be employed via an ***API*** by other software?

Microservices are **fine-g**rained services with a **discr**ete function. A modern **adapt**ation of SOA to cloud computing.

Microservices Principles:

- Supports purpose-specific business capabilities through services that are independently deployed
- Designed with few dependencies
- Based on fast short-term development cycles (similar to Agile)
- Commonly deployed based on immutable (unchanging over time or unable to be changed) architecture

Code-level vulnerabilities should be identified early in the development lifecycle.

Static code analysis and **dyna**mic testing incorporated early in the CI/CD process can identify deficiencies before release. ***See domain 8.***

Example:
CEO's plan to minimize his department and outsource code development to a foreign programming group. Consideration:

- Code from third parties will need to be manually reviewed for function and security.
- If the third party goes out of business, existing code may need to be abandoned.

Containerization

A **lightw**eight, granular, and portable way to **pack**age **app**lications for **multi**ple platforms.

Reduces overhead of server **virtu**alization by enabling **contain**erized apps to run on a **shared** OS kernel.
Containers do **not** have their **own OS**.
Share many **conc**erns of server **virtual**ization: isolation at host, process, network, and storage levels.
Crafted to host a single application, including only the OS resources needed, and sharing a common binaries and libraries

Focus on DevOps security (container-level) and application-level security (AuthN and AuthZ)

Capabilities of Containerization Solutions:
- Allow for multiple concurrent applications within a single container
- Offer customization of interaction between applications in separate containers

APIs (SOAP or REST)

Is a set of **expo**sed **interfa**ces that allow **program**matic **inter**action between **serv**ices.

REST uses the **HTTPS** protocol for **web com**munications to offer **API end**points

Best practice, public RESTful API for organization's data, limit its use to trusted partners by using API keys and limit request rates, rate limiting.
Unconstrained API calls can lead to denial-of-service conditions, one of the top 10 API security risks identified by OWASP in 2023. Attributing actions to an account requires proper authentication and logging, which are not tied to resource over-consumption.

All **commu**nications between client and server should be **encry**pted and **acce**ss limited with **API keys.**

API Keys: ensure that third-party users of API can be tracked to prevent abuse of the API.

Also ensure that storage, distribution, and transmission of **access keys** is done in a **sec**ure **fash**ion.

API Pentest Scenario:
Kevin is evaluating the security of a web service offered by his organization and wants to test that the interface used to interact with the service programmatically is secure.
API type of interface testing should Kevin perform.

Embedded Systems

The technology component of an **IOT** device is often referred to as an **emb**edded system.
A full computer system **emb**edded **insi**de of another **large**r **sys**tem.
Examples: hosts of embedded systems include printers, GPS, drones, semi-autonomous vehicles.

Embedded System concept of a computer implemented as part of a larger system that is typically designed around a limited set of **specific function**s (such as management, monitoring, and control) in relation to the larger product of which it's a component.

Control of a mechanism in the physical world is a security risk of an embedded system that is not commonly found in a standard PC.

An embedded system is a computer implemented as part of a larger system. The embedded system is typically designed around a limited set of specific functions in relation to the larger product of which it's a component. It may consist of the same components found in a typical computer system, or it may be a microcontroller.

High performance Computing

An Alternative to client-server computing model for compute-intensive operations with large data sets.
For problems that require the use of extremely large data sets and large *scale* **parallel** processing.SETI Project looking for aliens and spaceships.

High-performance computing (**HPC**) systems are computing platforms designed to perform complex calculations or data manipulations at extremely high speeds.
Super computers and MPP solutions are common examples of HPC systems.
HPC systems are used when real-time or near-real-time processing of massive data is necessary for a particular task or application.

Massive **parallel** processing (MPP) system is a type of large-*scale* **parallel** data system.
Large-scale parallel data management is likely a key tool in managing big data and will often involve cloud computing, grid computing, or peer-to-peer computing solutions.

The SETI project is a well-known example - looking for **aliens** on other planets.

Big Data

The variety V of Big Data describes how data is organized. **Big Data** is an umbrella term that is commonly used to describe the large amount of data that is processed by systems and networks in the modern age. Because scientific and technological advancements have not kept up with the amount of data in the modern age that is available for processing and analysis, most Big Data analysis occurs by using samples of data instead of the full range. One way to think about this form of Big Data analysis is in terms of surveys and polls, which attempt to calculate the majority of public opinion by taking information from a small sampling of the population.

There are four common Vs of Big Data as noted by the National Institute of Standards and Technology (NIST) Special Publication 1500-4:

- **Variety** describes organized data source types, such as whether the data is structured, unstructured, or partially structured.

- **Volume** describes how much data is inbound and processed.
- **Velocity** describes the speed at which data is inbound and processed.
- **Variability** is the process of correctly interpreting the meanings of raw data.

There are also other sub-characteristics that are also commonly described as Vs of Big Data; these include **veracity**, **validity**, and **volatility**. The total number of Vs of Big Data as well as their definitions can vary by source. NIST Special Publication 1500-4 is one instance of an attempt to define and organize information about Big Data as it pertains to privacy and security.

Grid Computing

Grid computing employs a **centralised controller** that makes computing assignments to grid members.
Key concerns

- include protecting grid controllers from takeover by bad actors or use of the grid for illicit activities.
- Isolation breach - allowing someone who compromises the controller to assume control of every grid computing device in the organization.
- Loss of data privacy due to use of Grid Computing.

In many grid computing implementations, grid members can access the contents of the distributed work segments or divisions. This grid computing over the Internet is not usually the best platform for sensitive operations. Grid computing is able to handle and compensate for latency of communications, duplicate work, and capacity fluctuation.

Edge Computing

Some computer operations require **processing activities** to **occur locally**, far from the cloud.

Common in various internet-of-things scenarios, like agricultural, science/space, military and retail.
This scenario is an example of edge computing. In edge computing, the intelligence and processing is contained within each device. Thus, rather than having to send data off to a master processing entity, each device can process its own data locally. The architecture of edge computing performs computations closer to the data source, which is at or near the edge of the network.

Fog Computing

Fog computing relies on sensors, IoT devices, or even edge computing devices to collect data and then transfer it back to a central location for processing.
Fog computing relies on sensors, IoT devices, or even edge computing devices to collect data and then transfer it back to a central location for processing.

Fog computing places **gate**way devices in the **field** to **coll**ect and **cor**relate data centrally at the **edge**.
With large **net**work-connected device counts in varied locations, data encryption, **spoof**ing **prot**ection, and **auth**entication are key.
Bot Army for DOS attacks?
Example Use Case:
A large manufacturer is deploying various sensors and devices throughout its operation to monitor and remotely control certain aspects of its operations. It is essential that all data collected by these devices be analyzed on a central server.

Domain 3 Compare Cloud Models & Services

Shared Responsibility model

Responsible
CSP
Customer

Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
OS	OS	OS	OS
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
On-Premises	**IaaS**	**PaaS**	**SaaS**

IaaS

- CSP provides building blocks, like network, storage, and compute
- CSP manages staff, HW, and datacenter
- The IaaS vendor will allow the user to set up infrastructure as quickly as she can deploy and pay for it. Allow to migrate her custom application quickly.
- Azure, Amazon, Google

PaaS
- Customer is responsible for deployment and management of apps
- CSP manages provisioning, configuration, hardware and OS
- Azure SQL databases, API management, Azure App Service
- **PaaS Example**: The company is moving from a self-hosted **Node.js** environment to one where code runs on application servers managed by a cloud vendor.

FaaS
- Server-less (Restaurant Menu App)
- Function As A Service - allow scale
- AWS Lambda

SaaS
- Customer just configures features
- CSP is responsible for management, operation, and service availability
- Office 365
- Service Now
- Salesforce
- Cymulate

IDaaS
- Identity as a service (IDaaS) - Azure EntraID
- cloud-based service that provides account provisioning, management, authentication, authorization, reporting, and monitoring capabilities
- provide the identity and access management functions

Serverless Architecture

Serverless architecture is a cloud computing concept where code is managed by the customer and the platform (i.e., supporting hardware and software) or server is managed by the **cloud service provider (CSP).** There is always a physical server running the code, but this execution model allows the software designer/architect/programmer/developer to focus on the logic of their code and not have to be concerned about the parameters or limitations of a specific server. This is also known as function as a service (**FaaS**).

Applications developed on serverless architecture are similar to microservices, and each function is crafted to operate independently and autonomously.

Data Segregation
How is your organization's information segregated from that of other clients?
The most significant concern regarding the use of cloud services for storing sensitive data, is segregated storage of data.

Cloud Models

- **Public** cloud -
  - advantages include **scal**ability, **agil**ity, **pay-as-y**ou-go, no **mainte**nance, and **low sk**ills.
  - Customer share computing infrastructure with other customers of the cloud vendor where one customer may not know the other's identity

    - shared tenancy
- **Private** cloud -
    - cloud environment in your **own** data**center** - vmware, advances include **leg**acy **supp**ort, **cont**rol, and **compl**iance.
    - In the private cloud computing model, the cloud computing environment is dedicated to a single organization and does not follow the shared tenancy model.
    - The environment may be built by the company in its own data center or built by a vendor at a co-location site.
- **Hybrid** cloud -
    - combines **pub**lic and **priv**ate cloud, **all**owing you to run your **app**s in the **righ**t **loc**ation. (VPN connection between cloud entities)

A community cloud deployment model provides cloud-based assets to two or more organizations.

Cloud Access Security Broker

CASB - **clo**ud **acc**ess **sec**urity **brok**er is a security **poli**cy **enforc**ement **sol**ution that may be **insta**lled on-premises or in the cloud.
A cloud access security broker (CASB) is software placed logically between users and cloud-based resources, and it can enforce security policies used in an internal network.
Data loss prevention (DLP) systems attempt to detect and block data exfiltration.
CASB systems typically include DLP capabilities.
Shadow IT

Solve shadow IT and data-based security policies.

Needs to apply security policies to both the activities her users engage in and to report on exceptions with her growing number of cloud services.

Domain 3 Post-quantum cryptography

CISSP Exam Cram - Cyber Attacks and Countermeasures (+ Quantum for CISSP 2021)

Chapter 7 - PKI and Cryptographic Applications

The **dev**elopment of **new** kinds of **crypto**graphic approaches that can be **imple**mented using today's **conve**ntional computers.
But will be **imp**ervious (**resistant**) to **att**acks from tomorrow's **quant**um computers.

Which **Algo**rithms are **suscep**tible and **resis**tant?

Symmetric (shared key) - **bulk** encryption (fast)
Asymmetric (Public **key** cryptography) - key exchange, digital signatures

Symmetric holds **fairly** well to quantum computing.
Asymmetric, quantum **poses** more immediate threats

Symmetric - **Grover's** algorithm shows that a quantum computer speeds up these attacks to effectively halve the key length.
The key length is a crucial factor when assessing the effectiveness of a cryptographic algorithm. Longer key lengths generally contribute to stronger security.
This would mean that a **256-bit** key is as strong against a **quantum** computer as a **128 bit** key is against a conventional computer.

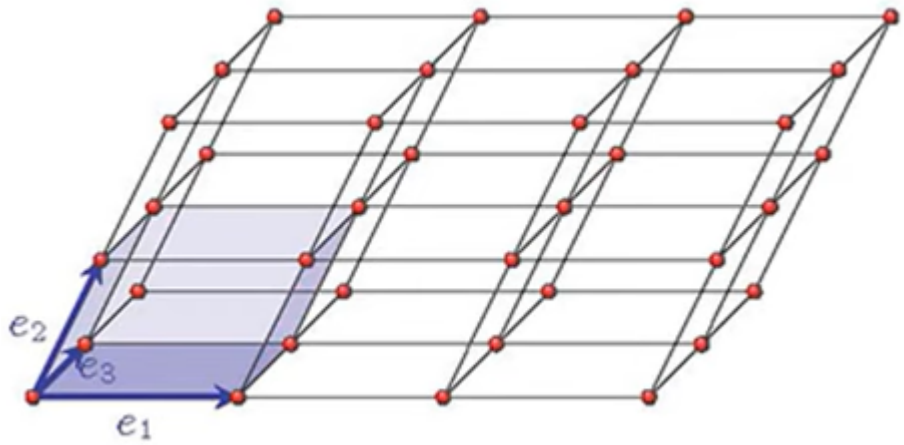
Asymmetric - **Shor's** algorithm can easily break all of the commonly used public-key algorithms based on both factoring and the discrete logarithm problem.

- RSA is vulnerable - large prime numbers
- Elliptic Curve is vulnerable
- **Lattice** offers **quant**um resistance

Lattice

Based on different type of problems: the **short**est **vec**tor problem and the **close**st **vec**tor problem
Potentially enables us to **repl**ace essentially all of our currently **endang**ered schemes
Lattice-based cryptographic schemes make up the **lion's** share of scientific publications on the post-quantum cryptography world.

Lattice is three dimensional array:



Domain 3 Cryptography

Code
Cryptographic **sys**tems of **sym**bols that **oper**ate on words or **phras**es and are sometimes **secr**et but do not **alw**ays provide **confid**entiality.

Cipher
Ciphers are always meant to **hide** the true meaning of a message. Cipher is secret.

Cryptography types of ciphers

- **Stream** cipher - is a **symm**etric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream.
- **Block** cipher -
    - is a method of encrypting text (to produce **ciphertext**) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time.
    - Block ciphers operate on message “chunks” rather than on individual characters or bits.
- **Substitution** - use the encryption algorithm to replace each character or bit of the plaintext message with a different character. **Julius Caesar** developed one of the earliest ciphers of this type now known as the Ceaser cipher”
- **Transposition** - uses an encryption algorithm to rearrange the letters of a plaintext message, forming the ciphertext message.
- **Initialization vector** (IV)
    - a cryptographic version of a random number, is a random bit string (a nonce) that is **XORed** with the message, reducing predictability and repeatability.
    - Size of the IV varies by algorithm but is normally the same length as the block size of the cipher or as large as the encryption key.
    - An initialization vector (IV) is used to create a unique ciphertext every time the same message is encrypted with the same key.
- Caesar, **Vigenere**
    - One-time Pad -
        - three very similar stream ciphers. The main difference between these ciphers is key length.
        - Assuming that it is used properly, the one-time pad is the only known cryptosystem that is not vulnerable to attacks.
    - **Caesar** shift cipher uses a key of length one
    - **Vigenere** cipher uses a longer key, usually a word or sentence
    - **One-time pad** uses a key that is as long as the message itself.

Vigenere cipher uses a square matrix to encrypt text:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

One-time Pad

For a one-time pad to be successful

- the key must be **generated randomly** without any known pattern.
- At least as long as the message is encrypted.
- The pads must be **protected against physical disclosure**
- Each pad must be used **only one time** and then discarded.

Assuming that it is used properly, the one-time pad is the only known cryptosystem that is not vulnerable to attacks.
A synchronous token generates and displays onetime passwords that are synchronised with an authentication server.

Smartcards

X.509 defines standards for public key certificates like those used with many smartcards authentication.
Smart Cards do not generate one time passwords, and common access cards are a version of a smartcard that includes a picture of the user.

Token Devices

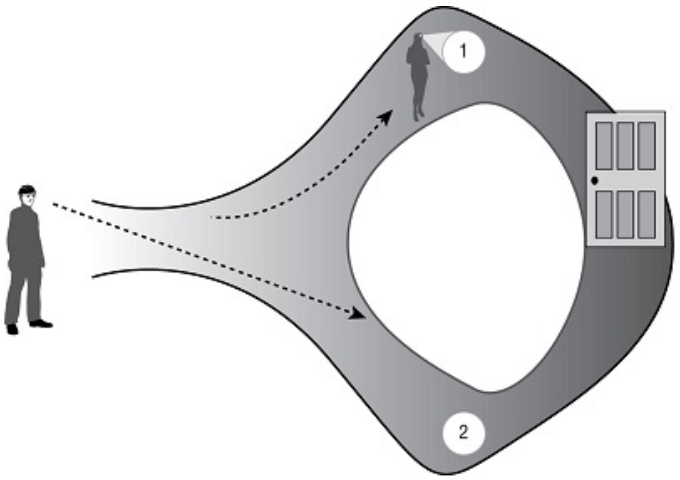
- TOTP - Time-based one-time password tokens or synchronous dynamic password tokens are devices or applications that generate passwords at fixed time intervals, such as every 60 seconds. Thus, TOTP produces new time-derived passwords on a specific time interval that can be used only a single time when attempting to authenticate.
- HOTP - HMAC-based one-time password tokens or asynchronous dynamic password tokens are devices or applications that generate passwords not based on fixed time intervals but instead based on a nonrepeating one-way function, such as a hash or hash message authentication code (HMAC—a type of hash that uses a symmetric key in the hashing process) operation.

Zero-knowledge proof

Zero-Knowledge Proof is a **comm**unication **conc**ept.
A specific type of information is exchanged, but no real data is transferred, as with digital signatures and digital certificates.

Simple definition:
It enables one to prove knowledge of a fact to another individual without revealing the fact itself.

Subject engages in an electronic version of the “magic door” scenario shown here.



In a zero-knowledge proof, one individual demonstrates to another that they can achieve a result that requires sensitive information without actually disclosing the sensitive information.

Split Knowledge

Split Knowledge means that the information or privilege required to perform an operation is divided among **multi**ple **user**s.
This ensures that no single person has **suffi**cient **privi**leges to compromise the security of the **enviro**nment.

Work Function / Work Factor

Work function or **work fac**tor, is a way to measure the strength of a cryptography system by measuring the effort in terms of **cost and or time to decrypt mes**sages.

Usually the **time and effort req**uired to perform a complete **brute-force** attack against an **encryp**tion system is what a work function rating represents.
The security and protection offered by a cryptosystem is directly proportional to the value of its work function/factor.

The time and effort required to break a protective measure.

Domain 3 Key Security

Cryptographic keys provide the necessary element of secrecy to a cryptosystem.
The purpose of key management in the design of cryptographic systems is to manage the lifecycle of cryptographic keys.

- Keys should be sufficiently long to protect against future attacks if the data is expected to remain sensitive.
- Longer keys provide greater levels of security
- Cryptographic keys should be randomly generated.
- Keys should be securely destroyed when they are no longer needed and not indefinitely retained.
- Longer keys do indeed provide greater security against brute-force attacks.

Confusion and diffusion are two principles underlying most cryptosystems.
Confusion occurs when the relationship between the plaintext and the key is so complicated that an attacker ***cannot*** merely continue altering the plaintext and analyzing the resulting ciphertext to determine the key.
Diffusion occurs when a change in the plaintext results in multiple changes spread throughout the ciphertext.

Modern cryptosystems utilise **keys** that are at least **128 bits** long to provide **adequate security**.

- **Symmetric** -
  - relies on the use of a **shared** secret **key**.
  - Lacks support for scalability, easy key distribution, and nonrepudiation.
  - Faster.
- **Asymmetric** -
  - public-private **key pairs** for communication between parties.
  - Supports scalability, **easy** key **distribution**, and **nonrepudiation**.
  - Stronger

Symmetric encryption depends on **cryptographic shredding** techniques **predominantly**.
Cryptographic shredding involves destroying the encryption key used to encrypt data, making it permanently inaccessible. Losing the key means losing access to the data.

Domain 3 Key Distribution

- Out-of-band - traditional method
- Hybrid / asymmetric
- Quantum key distribution - Quantum unconditional security (NEW)

CISSP 2024 exam changes in DETAIL!

Offline key distribution requires a side channel of trusted communication, such as in-person contact.
This can be difficult to arrange when users are geographically separated.
Alternatively, the individuals could use the Diffie–Hellman algorithm or other asymmetric/public key encryption technique to exchange a secret key.
The Diffie–Hellman algorithm allows the exchange of symmetric encryption keys between two parties over an insecure channel.

Key escrow is a method for managing the recovery of lost keys and is not used for key distribution.
M of N Control requires that a minimum number of agents (M) out of the total number of agents (N) work together to perform high-security tasks.
M of N Control is an example of a split knowledge technique, but not all split knowledge techniques are used for key **escrow**.

Quantum Key Distribution

Quantum Key Distribution (QKD) **NOT** the same as quantum cryptography!

CISSP Exam Cram - 2024 Addendum
A secure communication method that involves components of quantum mechanics.
Enables two parties to generate a shared random secret key known only to them.
Secret key can then be used to encrypt and decrypt messages securely.

An essential property of QKD is the ability to detect *eavesdropping* by any third party trying to gain knowledge of the key.
Eavesdropper interception introduces detectable anomalies.

The main drawback of quantum-key distribution is that it usually relies on having an authenticated classical channel of communication.
That means parties have already exchanged either a symmetric key of sufficient length or public keys of sufficient security level.
In practice one can achieve authenticated and sufficiently secure communication without using QKD, at much less expense.

QKD is used only to produce and distribute a key, not to transmit any message data.

Where is QKD used?
Commercial solutions currently target high security scenarios that use key distribution by courier, where key distribution schemes are considered inadequate.

Domain 3 Confidentiality, Integrity & nonrepudiation

- **Confidentiality** - is one of the major **goals** of cryptography. It protects the secrecy of data while it is both at rest and in transit.
- **Integrity** - provides the recipient of a message with the assurance that data was not altered (intentionally or unintentionally) between the time it was created and the time it was accessed.
- **Nonrepudiation** - provides undeniable proof that the sender of a message actually authored it. It prevents the sender from subsequently denying that they sent the original message.
    - Scenario: cryptographic **goal** needed to be met to convince John that Bill was actually the sender of the message - Non-repudiation

Video Index - Domain 3 - DES Modes

Nonrepudiation prevents the sender of a message from later denying that they sent it.
Confidentiality protects the contents of encrypted data from unauthorized disclosure.
Integrity protects data from unauthorized modification.
Availability is not a goal of cryptography.

Counter Mode

Counter mode allows you to break an encryption or decryption operation into multiple independent steps. This makes Counter mode well suited for use in **parallel** computing.

Symmetric cryptosystem

Galois/Counter Mode (**GCM**) and Counter with Cipher Block Chaining Message Authentication Code mode (**CCM**) are the only two modes that provide both **confiden**tiality and **data auth**enticity.
Galois/Counter mode allows you to break an encryption or decryption operation into multiple independent steps.
The Galois/Counter mode cryptographic algorithm will be used in a parallelized environment to distribute the workload of encryption and decryption among multiple processors.

Scenario - Symmetric Cryptosystem Admin:
Brian administers a symmetric cryptosystem used by 20 users, each of whom has the ability to communicate privately with any other user. One of those users lost control of their account and Brian believes that the user's keys were compromised.
19 keys must change.
In a symmetric cryptosystem, a unique key exists for each pair of users. In this case, every key involving the compromised user must be changed, meaning that the key that the user shared with each of the other 19 users must be changed.

Domain 3 DES [and 3DES] Modes

DES modes, including Electronic Code Book (ECB), Output Feedback (OFB), and Counter (CTR) modes, only provide **confidentiality**.
CISSP Exam Cram Full Course (All 8 Domains) - Good for 2024 exam!

- **Electronic** Codebook Mode (**ECB**) - simplest & least secure mode. Processes 64-bit blocks, encrypts blocks with the chosen key. If the same block is encountered multiple times, the same encrypted block is produced, making it easy to break.
- Cipher block **chaining** (CBC) -
    - Each block of unencrypted text is **XORed** with the block of ciphertext immediately preceding.
    - Decryption process simply decrypts ciphertext and **reverses** the XOR operation.
    - One important consideration when using CBC mode is that errors propagate
    - CBC encryption algorithm mode suffers from the undesirable characteristic of errors propagating between blocks
- Cipher **Feedback** (CFB) -
    - is the streaming version of CBC.
    - CFB Works on **data in real** time, using memory buffers of the same block size.
    - When the buffer is full, data is encrypted and transmitted.
    - Uses chaining, so **errors** propagate.

- **Output** Feedback (OFB) -
    - Operates similar to CFB, **but XORs** the plain text with a **seed** value. No chaining function, so **no errors or errors** do not propagate.
- **Counter** (CTR) - uses an incrementing counter instead of a **seed**.
    - Errors do not propagate.

Domain 3 XOR Cipher

The exclusive-OR option (XOR, also known as binary addition) is used heavily in cryptology, a function of flipping bits in a simple,systematic fashion.

Original Value	Key Value	Cipher Value
1	1	0
1	0	1
0	1	1
0	0	0

Binary values match = 0, otherwise binary values do not match cipher value is 1.

The ⊕ symbol represents the **XOR** function and returns a true value when only one of the input values is true. If both values are false or both values are true, the output of the XOR function is false.
Result of two values were combined using the **AND** (the ∧ symbol) function, which returns a value of true if the two values are both true.
If two values were combined using the **OR** (the ∨ symbol) function, which returns a value of true if either input values is true.
Result if only the X value was subjected to the **NOR** (the **~** symbol) function, which reverses the value of an input.

Key Clustering
A Weakness in cryptography where a plain-text message generates identical ciphertext messages using the same algorithm but using different keys.
Collisions - is same results

Domain 3 Asymmetric Keys

Public keys are shared among communicating parties.
Private keys are kept secret.

Data

To encrypt a message: use the recipient's **public** key.
To decrypt a message: use your own **private** key

Digital Signature

To sign a message: use your own **private** key
To validate a signature: use sender's **public** key
Encrypting the email content can provide confidentiality;
digital signatures can provide nonrepudiation.

Domain 3 Asymmetric Cryptosystem Communication

SMTP protocol does not guarantee confidentiality
Encrypt the email content - Confidentiality
digital signatures can provide nonrepudiation

Encrypt message Recipient Pub Key

Scenario: key to use to encrypt private message
Mike and Renee would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

Mike would like to send Renee a private message using the information gained during this exchange. What key should he use to encrypt the message?

Answer:
Renee's public key
Mike uses the public key that he extracted from Renee's digital certificate to encrypt the message that he would like to send to Renee.

Encrypt message Recipient Pub Key

Scenario: encrypt the message.
Matthew and Richard are friends located in different physical locations who would like to begin communicating with each other using cryptography to protect the confidentiality of their communications. They exchange digital certificates to begin this process and plan to use an asymmetric encryption algorithm for the secure exchange of email messages.

When Matthew sends Richard a message, what key should he use to encrypt the message?

Answer:
Richard's public key (Recipient)
Sender of a message encrypts the message using the public key of the message recipient.

Encrypt message Recipient Pub Key

Scenario: encrypt the message, confidentiality

Alice and Bob would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

If Alice wants to send Bob a message that is encrypted for confidentiality, what key does she use to encrypt the message?
Alice >>> Bob == Encrypt Message
CISSP Domain 3 | Security Architecture and Engineering | Practice Questions Explained

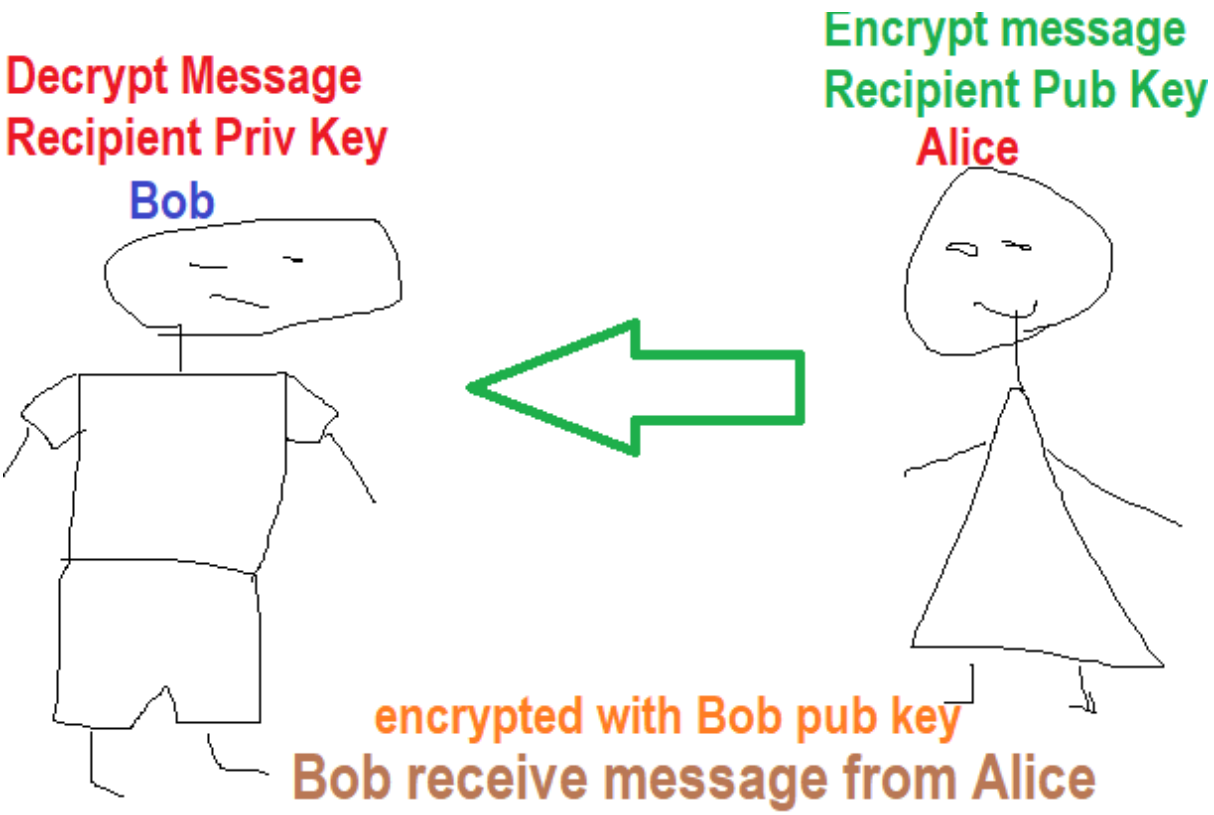
Answer
In an asymmetric cryptosystem, the sender of a message encrypts the message using the ***recipient's public key.***
The recipient may then decrypt that message using their own private key, which only they should possess.
Bob's **public key** to encrypt the message!

Decrypt Message Recipient Priv Key

Scenario: key use to decrypt message
Alice and Bob would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

When Bob receives the encrypted message from Alice, what key does he use to decrypt the message's plaintext content?

Answer:
Bob's private key (Recipient)
When Bob receives the message, he uses his **own private key to decrypt it.** Since he is the only one with his private key, he is the only one who should be able to decrypt it, thus preserving **confidentiality**.



Decrypt Message Recipient Priv Key

Scenario: key use to decrypt message
Matthew and Richard are friends located in different physical locations who would like to begin communicating with each other using cryptography to protect the confidentiality of their communications.
They exchange digital certificates to begin this process and plan to use an asymmetric encryption algorithm for the secure exchange of email messages.

When Richard receives the message from Matthew, what key should he use to decrypt the message?

Answer
Richards private key (Recipient)
The recipient of a message uses their own private key to decrypt messages that were encrypted with the recipient's public key.
This ensures that nobody other than the intended recipient can decrypt the message.

Sign message Sender Priv Key

Scenario: digital signature create the message
Matthew and Richard are friends located in different physical locations who would like to begin communicating with each other using cryptography to protect the confidentiality of their

communications. They exchange digital certificates to begin this process and plan to use an asymmetric encryption algorithm for the secure exchange of email messages.

When Matthew adds a digital signature to the message, what encryption key does he use to create the digital signature?

Answer:
Matthew's private key (Sender)
An individual creates a digital signature by encrypting the message digest with their own private key.

Sign message Sender Priv Key

Scenario: encrypt the message.
Richard wants to digitally **sign a** message he's sending to Sue so that Sue can be sure the message came from him without modification while in transit.
Richard >>> Sue = Sign Message

Answer:
Richard's private key, (sender) should he use to encrypt the message digest

Nonrepudiation - prove to a third party that the message did indeed come from the purported originator

Priv key

Scenario: keys would Bob *NOT* possess
Alice and Bob would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

Which one of the following keys would Bob not possess in this scenario?

Answer:
Alice's private key
Each user retains their **own private key** as secret information. In this scenario, Bob would only have access to his own private key and would not have access to the private key of Alice or any other user.

Verify authenticity of cert

Scenario: Verify the authenticity of the certificate

Mike and Renee would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

When Mike receives Renee's digital certificate, what key does he use to verify the authenticity of the certificate?

Answer:
CA's public key
When an individual receives a copy of a digital certificate, the person verifies the authenticity of that certificate by using the CA's public key to validate the digital signature contained on the certificate.

CA digital certificate body

Scenario: Certificate authority (CA) create digital certificate body
Mike and Renee would like to use an asymmetric cryptosystem to communicate with each other.
They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

When the certificate authority (CA) created Renee's digital certificate, what key was contained within the body of the certificate?
CA >>> Create Digital Certificate === Users Public Key

Answer:
Renee's public key
The purpose of a digital certificate is to provide the general public with an authenticated copy of the certificate subject's public key.

Domain 3 Hash Function Requirements

Hash functions do not include any element of secrecy and, therefore, do not require a cryptographic key.

Good hash function have **five** requirements:

1. They must allow input of **any len**gth.
2. Provide **fix**ed-length **out**put
3. Make it relatively **easy** to **comp**ute the hash function for any input
4. Provide **one-way** functionality
5. Must be **collision free**.

Hashing functions do not include any element of secrecy and, therefore, do not require a cryptographic key.

Domain 3 Cryptographic Salts

Salts
Attackers may use **rain**bow **table**s of precomputed values to identify commonly used passwords.
A salt is **rand**om data that is used as an additional input, a **one-way** function that hashes data, a password or **passph**rase.
A passphrase is a long string of characters that is easy to remember, such as ***IP@$$edTheCISSPEx@m***. = I Passed the CISSP Exam.
Passphrase is not short and typically includes at least three sets of character types. It is strong and complex, making it difficult to crack.
Adding salts to the passwords before hashing them reduces the **effectiveness** of rainbow table attacks.
The best practice for storing passwords is by using salted hashes for password storage.

If a password is encrypted using AES then a key is needed to decrypt and thus not used to store passwords.

ElGamal

The major disadvantage of the ElGamal cryptosystem is that it doubles the length of any message it encrypts. Therefore, a 2,048-bit plaintext message would yield a 4,096-bit ciphertext message when ElGamal is used for the encryption process.

Domain 3 Digital Signature Standard

Confidentiality is NOT achieved by digital signatures as the original message is not encrypted.

DSS
The digital signature standard uses the SHA-1, SHA-2, and SHA-3 **message digest** functions.
Works in conjunction with one of **three** encryption algorithms:

- Digital Signature Algorithm (**DSA**)
- Rivest, Shamir, Adleman (**RSA**) algorithm
- Elliptic Curve DSA (**ECDSA**) algorithm

The **Digital Signature Standard** allows federal government use of the Digital Signature Algorithm, RSA, or the Elliptic Curve DSA in conjunction with the SHA-1 hashing function to produce secure digital signatures.

When verifying a digital signature, the following is most critical for ensuring the signatures authenticity:

- Comparing the hash value of the received data with the decrypted hash in the signature.

This process ensures that the data has not been tampered with during transmission and that the signature matches the content it claims to authenticate.

Using server public key cryptography, verify that the digital signature of the CA is authentic, that the certificate has not expired, and that the certificate has not been revoked.

512 bits is a valid SHA-2 hash length

Domain 3 Public Key Infrastructure

PKI

Certificate **Auth**orities (**CAs**) generate digital certificates containing the public keys of system users.
Users then distribute certificates to people with whom they want to communicate.
Certificate **recipients** verify a certificate using the CA's public key.
DNSSEC uses certificates to perform mutual authentication between DNS servers, and thus public key infrastructure (PKI) is needed to provide and support those certificates.

Certificate revocation lists (CRLs) introduce an inherent latency to the certificate expiration process due to the time lag between CRL distributions.
The certificate revocation list (CRL) contains the serial numbers of digital certificates issued by a certificate authority that have later been revoked.

OCSP & CRL

The Online Certificate Status Protocol (OCSP) provides real-time query/response services to digital certificate users. This overcomes the latency inherent in the traditional certificate revocation list download and cross-check process.

a CRL is most likely to contain a list of PKI certificates that have been revoked. A CRL is a list by serial number of revoked certificates that should no longer be trusted. CRLs are typically maintained by CAs.

PKI enables encrypted communication by using a combination of a public and a private key pair. A certificate is bound to a user's public key, which is the key that is made available to anyone who wishes to send a message to the owner of the key pair. The private key is a secret key that is not shared. If a private key becomes compromised or is no longer needed, the associated CA should be notified immediately so that the CRL can be updated.
Certificates typically contain information, such as the owner's name and contact information, the public key, the key validity period, the digital signature of the certificate, and the location where the CRL can be retrieved.

A CSR does not contain a list of PKI certificates that have been revoked. A CSR is submitted to a CA in order to generate a new certificate. CSRs contain an entity's public key and other identifying information. CSRs are signed by the entity's private key.

The OCSP does not contain a list of PKI certificates that have been revoked. OCSP typically operates over Hypertext Transfer Protocol (HTTP) and is used to retrieve CRL information from CAs. For example, OCSP will typically return a status of "revoked" for a certificate that appears on a CRL. Other responses include "good" if the certificate is still trustworthy or "unknown" if OCSP cannot verify whether the certificate is either good or revoked.

An RA does not contain a list of PKI certificates that have been revoked. To obtain a certificate, an applicant sends a request to an RA. After an applicant's credentials are verified by the RA, certificates are generated by the CA.

X.509 governs digital certificates and the public key infrastructure (PKI). It defines the appropriate content for a digital certificate and the processes used by certificate authorities to generate and revoke certificates.
X.509 ITU-T standard is expected when using smartcards to provide a certificate to an upstream authentication service.
X.509 defines standards for public key certificates like those used with many smartcards.

Certificate Formats

The PFX format is most closely associated with Microsoft Windows systems that store certificates in binary key format
The P7B format is used for Windows systems storing files in text format.
The PEM format is another text format

Cryptography & Key Management

Level of protection
Encryption keys must be secured at the same level of control or higher as the data they protect.
Sensitivity of the data dictates this level of protection, as defined in the organizations data security policies.
Key Recovery
Circumstances where you need to recover a key for a particular user, without that users cooperation, such as in termination or key loss.
Key Escrow
Copies of keys are held by a trusted third party in a secure environment, which can aid in many of the other areas of key management.

Domain 3 Securing Traffic

Email

Standards for encrypted messages include **S/MIME** protocol and **Pretty Good Privacy** (**PGP**)

Domain Message Authentication Reporting and Conformance (DMARC) DMARC is a DNS-based email authentication system. It is intended to protect against business email compromise (BEC), phishing, and other email scams. Email servers can verify if a received message is valid by following the DNS-based instructions; if invalid, the email can be discarded, quarantined, or delivered anyway.
Email retention policy discussed with users include the privacy, length of retainer, and auditor review. Backup methods for email are not discussed.

designing a security system for internet-delivered email:

- Nonrepudiation
- Message **integrity**
- Access restrictions

DKIM & SPF

SPF helps prevent email spoofing by allowing the receiving mail server to verify incoming mail from a domain is sent from the host IP address authorized.
DKIM ensures the integrity and authenticity of the content of emails by enabling the sender to sign email digitally. A public key placed in DNS allows the recipient to verify the signature.
DKIM is effective against tampering and affirms email not be altered.
DKIM verifies the legitimacy of incoming email sources.
DMARC checks DKIM and SPF.

Web

The de facto standard for secure web traffic is the use of HTTP over Transport layer Security (**TLS**), largely replacing the older **SSL**.
TLS is widely used to ensure data confidentiality during transmission over the internet, providing encryption and authentication. While other options are secure, TLS is commonly used for web-based communication.
Encryption is the technical control for ensuring data confidentiality.

TLS - Transport Layer Security

- Allows for use of TCP port 443
- Prevents tampering, spoofing, and eavesdropping
- Ephemeral session key is used to encrypt the actual content of communications between a web server and a client
- Can be used as a VPN solution
- Handshake - negotiated and establish connection, exchange encryption algorithm
- Record - actual secure communication and data integrity
- TLS supports both one-way and two-way authentication.

TLS and SSL are **not** interoperable or backward compatible.

The Secure Sockets Layer (**SSL**) protocol is **deprecated** and no longer considered secure. It should never be used.

The Secure Hash Algorithm 3 (SHA-3), Transport Layer Security (**TLS**) 1.2, and IPsec are all ***modern***, secure protocols and standards.

Domain 3 IPSEC Basics

IPsec
A Security architecture framework that supports **sec**ure **commu**nication over IP.
IPsec is a security protocol that automatically performs reauthentication of the client system throughout the connected session in order to detect session hijacking.

IPsec can provide encryption, access control, nonrepudiation, and message authentication using public key cryptography.

Establishes a **sec**ure channel in either **trans**port mode or tunnel mode.

- **Tunnel mode**
    - VPNs are used to connect networks to networks or hosts to networks.
    - When IPsec is used in tunnel mode, entire packets, rather than just the payload, are encrypted.
    - Tunnel mode encrypts the entire packet and adds a new header to support transmission through the tunnel.
    - In tunnel mode, ESP encrypts the entire packet, including the IP headers and data.
    -
- **Transport** mode
    - is used to connect hosts to hosts.
    - **Transport mode** only encrypts the original payload, not the original header.
    - ESP's Transport mode encrypts IP packet data but leaves the packet header unencrypted.
    - AH is typically used with ESP in transport mode.
    - In transport mode, ESP encrypts only the packet data, leaving the Internet Protocol (IP) headers unencrypted.
    -

ESP provides confidentiality for IP Security (IPSec) virtual private network (VPN) tunnels; AH provides authentication and integrity for IPSec VPN tunnels.
IPSec operates in transport mode or tunnel mode.
AH uses the IP headers to authenticate packets. Therefore, AH is typically used with ESP in transport mode.
However, AH is not typically used with ESP in tunnel mode, because the IP headers are encrypted.

AH can be used with ESP, but it is not a requirement that they be used together. When they are used together, the Internet Security Association and Key Management Protocol (ISAKMP) must establish separate SAs for each protocol. In addition, because ISAKMP SAs are unidirectional, separate SAs must be established in each direction. Therefore, when both AH and ESP are used, ISAKMP must establish four SAs. An SA is a collection of security configuration parameters that each endpoint agrees to use, thus enabling the construction of

a secure channel of communication. To identify each unidirectional SA, a 32-bit number called a Security Parameter Index (SPI) is generated by the sending device.

Can be used to establish direct communication between computers or over a VPN **conn**ection.
IPsec is a **VPN** protocol that can be implemented as the payload encryption mechanism when **L2TP** is used to craft the VPN connection for an IP communication. Specifically, the ESP element of IPsec is used by L2TP rather than the entire IPsec protocol suite.
Uses two protocols: Authentication Header (**AH**) and Encapsulating Security Payload (**ESP**)

The Authentication Header of IPsec component provides assurances of message **integrity** and nonrepudiation.

Internet Security Association and Key Management Protocol (ISAKMP), an element of Internet Key Exchange (IKE), is used to organise and manage the encryption keys that have been generated and exchanged by OAKLEY and SKEME.
A security association is the agreed-on method of authentication and encryption used by two entities (a bit like a digital keyring).
ISAKMPs' use of security associations is what enables IPsec to **support multiple** simultaneous **VPNs** from each host.

Encapsulating Security Payload (ESP) provides confidentiality and **integrity** of packet contents.
The Encapsulating Security Payload (ESP) protocol provides confidentiality and integrity for packet contents. It encrypts packet payloads and provides limited authentication and protection against replay attacks.

ESP provides encryption and limited authentication, and prevents replay attacks.
Secure Key Exchange Mechanism (SKEME), an element of Internet Key Exchange (IKE), is a means of exchanging keys securely.
Authentication Header (AH) provides assurances of message **integrity** and nonrepudiation.
AH also provides authentication and access control, and prevents replay attacks.

Work-From-Home WFH - Telecommute

Protected encryption using Secure protocols with a VPN:

- IPsec
- SSH
- TLS

IPSEC VPN protocol has always offered native data encryption.

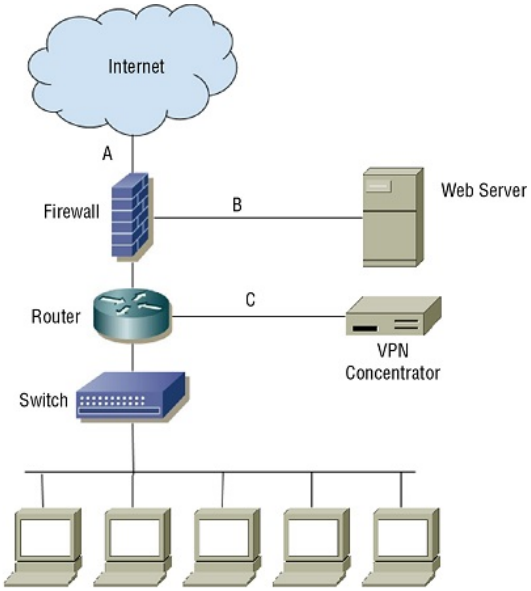
PPTP, L2F, L2TP, and IPsec are the most common VPN protocols.

WFH, shift to remote work. Each staff member needs access to specific applications, and due to the quick shift, staff members are working from systems that may be home systems or borrowed laptops.

An HTML5-based VPN will provide staff with access to the applications they need without requiring the installation of a client that might be challenging or impossible without managed machines.
A client-based IPsec VPN provides additional opportunities for control that a broadly deployed base of directly accessed machines via RDP does not, making it the second-best choice here.
Deploying fiber for direct connections for end users is not viable for most organizations based on cost and complexity.

Buried fiber-optic cable is best suited to long distances, particularly when there are trees or other obstacles blocking line of sight that may interfere with Wi-Fi or LiFi deployments.

VPN Concentrator Placement Diagram



The firewall in the diagram has two protected zones behind it, making it a two-tier firewall design.
VPN users should only connect from managed PCs.
Segmentation is a critical concept for network designers.
Remote PCs that connect to a protected network need to comply with security settings and standards that match those required for the internal network.
The VPN concentrator logically places remote users in the protected zone behind the firewall, but that means user workstations (and users) must be trusted in the same way that local workstations are.

Domain 3 Common Cryptographic Attacks

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

- **Brute-force** attacks are attempts to randomly find the correct cryptographic key. Known plaintext, chosen ciphertext, and chosen plaintext attacks require the attacker to have some extra information in addition to the ciphertext.
- **Meet-in-the-middle** attack exploits protocol that use two rounds of encryption

- **Man-in-the-middle** attack fools both parties into communicating with the attacker instead of directly with each other.
- **Birthday** attack is an attempt to find collisions in hash functions
- **Replay** attack is an attempt to reuse authentication requests.

In the context of cryptography, a collision attack that occurs when two different inputs produce the same hash value is the birthday attack.

Domain 3 Digital Rights Management

DRM
Digital rights management (DRM) methods attempt to provide copyright protection for copyrighted works.
DRM methods attempt to provide copyright protection for copyrighted works, including intellectual property.
Example: is writing and publishing a book on passing CISSP.

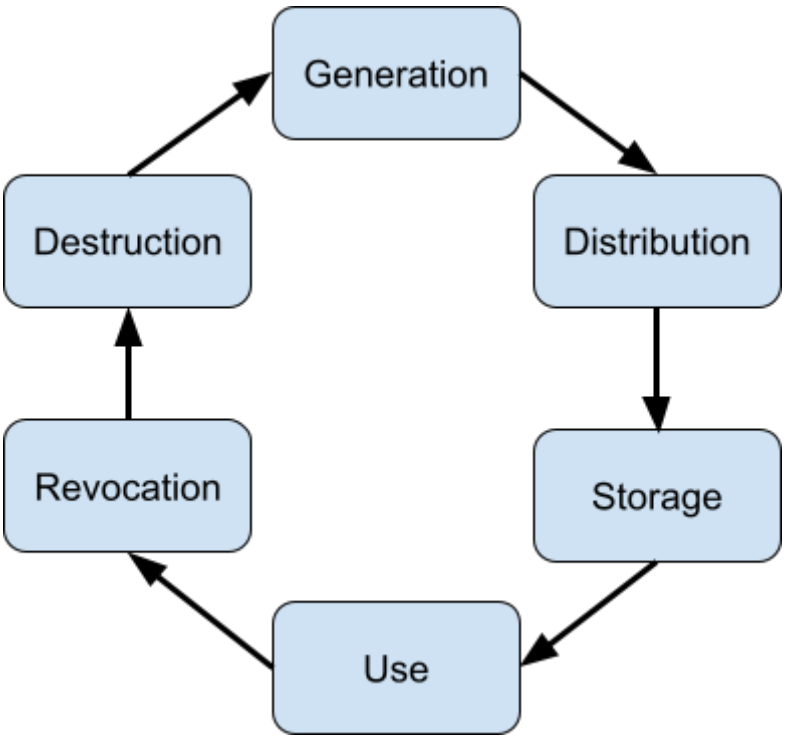
Allow content owners to **enf**orce restrictions on the use of their **cont**ent by others.
Commonly protect **entert**aining content, such as **music**, **mov**ies, and e-books.
Occasionally found in the enterprise, **prot**ecting sensitive information stored in documents.
Digital rights management (**DRM**) methods attempt to provide copyright protection for copyrighted works.

Scenario:
A software developer created an application and wants to protect it with DRM technologies.
Methods included:
- Persistent online authentication
- automatic expiration
- continuous audit trail

DRM, digital rights management technology can be used to limit use of the PDFs to paying customers.

Domain 3 CryptoGraphic Life Cycle

FIPS 140-2 Federal Information Processing Standard
Established to aid in the protection of digitally stored unclassified yet sensitive information.



Key Management Strategy for encryption key lifecycle

- Encryption keys should be generated within a trusted, secure cryptographic module. FIPS 140-⅔ validated modules provide tamper resistance and key **integrity**.
- Encryption keys should be distributed securely to prevent theft compromise during transit. Encrypt keys with a separate encryption key while distributing to other parties
- Encryption keys must be protected at rest and should never be stored in plaintext. This includes keys in volatile and persistent memory.
- Clients (users + trusted devices) will use keys for resource access as access controls allow. Acceptable use policy sets guardrails for data usage
- A process for revoking access at separation, policy breach, device or key compromise. In PKI you would revoke the certificate on the issuing Certificate Authority (CA)
- Key destruction is the removal of an encryption key from its operational location. Key deletion goes further and removes any info that could be used to reconstruct that key. MDM systems remove certificates from a device during device wipe or retirement. (Microsoft Intune or Airwatch)

CISSP Exam Cram - 2024 Addendum

Developed by NIST, for use in computer systems by non-military American government agencies and government contractors.

FIPS Security Levels:

- Level 1: Lowest level of security
- Level 2: Specifies the security requirements for cryptographic modules that protect sensitive information

- Level 3: Requires physical protections to ensure a high degree of confidence that any attempts to tamper are evident and detectable

FIPS 140-3 Security Levels (1 April 2022, supersedes FIPS 140-2)
- Level 1: Requires production grade equipment and externally tested algorithms
- Level 2: Adds requirements for physical tamper-evidence and role-based authentication.
- Level 3: Adds requirements for physical tamper-resistance, identity-based authentication, and separation between interfaces.
- Level 4: Makes the physical security requirements more stringent, requiring the ability to be tamper-active, erasing the contents of the device if it detects various forms of environmental attack.

FIPS 140-3 Cryptographic Modules

Example where FIPS used is in MS Teams: [Security guide for Microsoft Teams overview - Microsoft Teams | Microsoft Learn]

Cryptographic modules can be divided into 3 types:

Type	Examples
Hardware	Safenet Luna HSM (Thales) Gemalto SafeNet HSM (Thales) nShield HSM (Entrust) Utimaco CryptoServer HSM
Software	OpenSSL FIPS Object Module Microsoft Windows Crypto Modules Bouncy Castle FIPS Module
Cloud	Microsoft Azure Key Vault Amazon Key Management Service (KMS) Google Cloud Key Management Service (KMS)

Domain 3 Cryptography Symmetric Algorithms

CISSP Exam Cram Full Course (All 8 Domains) - Good for 2024 exam!

Name	Type	Algorithm Type	Block Size (bits)	Key Size (bits)	Strength
AES	Symmetric	Block cipher	128	128,192,256	Strong ***Modern***
Blowfish	Symmetric		64	32-448 key bit	
DES	Symmetric	Block cipher	64	56 bit	Very weak

3DES	Symmetric	Block cipher	64	112 / 168 bit	Moderate *Outdated*
IDEA	Symmetric		64	128	encryption algorithm
RC2	Symmetric		64	128	
RC4	Symmetric	Stream cipher	Streaming	128	*Outdated*
RC5	Symmetric	RSA Block mode cipher	32,64,128	0-2040 bit	Very strong
Skipjack	Symmetric		64	80	*Outdated*
Twofish	Symmetric		128	1-256	
IDEA	Symmetric		64-bit blocks	128-bit key	

AES

The Advanced Encryption Standard (AES) and Rivest Cipher 6 (RC6) are modern, secure algorithms.
AES is symmetric, meaning using the same key to encrypt and the same key to decrypt.
AES protects Data Confidentiality in the cloud.

AES provides **confi**dentiality, **integrity**, and **authen**tication when implemented properly.
Nonrepudiation requires the use of a public key cryptosystem to prevent users from falsely denying that they originated a message and cannot be achieved with a symmetric cryptosystem, such as AES.
AES-256 algorithm is a modern, secure cryptographic algorithm.

The RSA encryption algorithm is considered the **least** computationally efficient but provides the highest level of security, between the alternatives from question listing, AES, ECC and Blowfish.

In cryptography, CAST-256 is a symmetric-key block cipher published in June 1998. It was submitted as a candidate for the Advanced Encryption Standard; however, it was not among the five AES finalists.

Symmetric Keys

In a symmetric key network of 100 nodes where each node securely communicates with every other node using unique keys, 4950 symmetric keys are needed.

n x (n-1) / 2
((n*(n − 1))/2)

A separate key is required for each pair of users who want to communicate privately. In a group of six users, this would require a total of 15 secret keys. You can calculate this value by using the formula (n × (n – 1) / 2). In a case, n = 6, resulting in (6 × 5) / 2 = 15 keys.

Domain 3 Cryptography Hash Algorithms

Name	Type	Hash Value Length	Still in use	Replaced By
HMAC	Hash	Variable	Very strong	-
HAVAL	Hash	128,160,192,224,256		
MD2	Hash	128	No	MD6, et. al
MD4	Hash	128	No	MD6, et. al
MD5	Hash	128	No	MD6, et. al
SHA-1	Hash	160	NO	SHA-2
SHA-224	Hash	224	Yes	-
SHA-256	Hash	256	Yes	-
SHA-384	Hash	384	Yes	-
SHA-512	Hash	512	Yes	-

SHA-256 is best suited for ensuring the **integrity** of large files or messages.
SHA-256 is specifically designed for data integrity checks.

SHA 256 hashing tool should be used if it is believed that technically sophisticated attackers may have replaced the software package with a version containing a backdoor.
SHA-256 **integrity** algorithm

The MD5 hashing algorithm has known collisions and, as of **2005**, is no longer considered secure for use in modern environments.
A real-world collision attack against SHA 1 was announced in early **2017**.
In **2024**, AES, PGP, and WPA3 algorithms are all still considered secure.
Symmetric encryption like AES is typically used for data at rest.

The Merkle–Hellman Knapsack algorithm, which relies on the difficulty of factoring super-increasing sets, has been **broken** by cryptanalysts and is now considered insecure.

Domain 3 Major Public Key Cryptosystems

RSA

Is the most famous public key cryptosystem; it was developed by **Riv**est, **Sha**mir, and **Adle**man in 1977. It depends on the difficulty of factoring the product of prime numbers. Nonrepudiation is possible only with an asymmetric encryption algorithm. RSA is an asymmetric algorithm.

El Gamal
Is an extension of the **Diffie-H**ellman key exchange algorithm that depends on modular arithmetic. Less common than RSA in recent years.
Elliptic Curve
Algorithm depends on the **elliptic curve discrete** logarithm problem and provides more security than other algorithms when both are used with keys of the same length.

Domain 3 Digital Signatures

Rely on public key cryptography and hashing functions
DS algorithms suitable for use in FIPS 186-4 (the digital signature standard) must use SHA-2 hashing functions.

The FIPS 186-5 Digital Signature Standard allows federal government use of the:

- Rivest, Shamir, Adleman (RSA) algorithm;
- Elliptic Curve DSA (ECDSA) algorithm,
- Edwards Curve Digital Signature Algorithm (EdDSA)

in conjunction with the SHA-3 hashing function to produce secure digital signatures.

*note: HAVAL is a hash function, not an encryption algorithm.
While hash functions are used as part of the digital signature process, they do not provide encryption.

The Digital Signature Standard allows federal government use of the Digital Signature Algorithm, RSA, or the Elliptic Curve DSA in conjunction with the SHA-1 hashing function to produce secure digital signatures.
ElGamal DSA is not supported under FIPS 186-5.

Three currently approved encryption algorithms:

- ➢ Digital Signature Algorithm (DSA), as specified in FIPS 186-4
- ➢ Rivest, Shamir, Adleman (RSA), specified in ANSI X9.31
- ➢ Elliptic Curve DSA (ECDSA), specified in ANSI X9.62

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the only one of the algorithms listed in a scenario question that supports true digital signatures, providing **integrity** verification and nonrepudiation.

Domain 3 Cryptography Asymmetric Algorithms

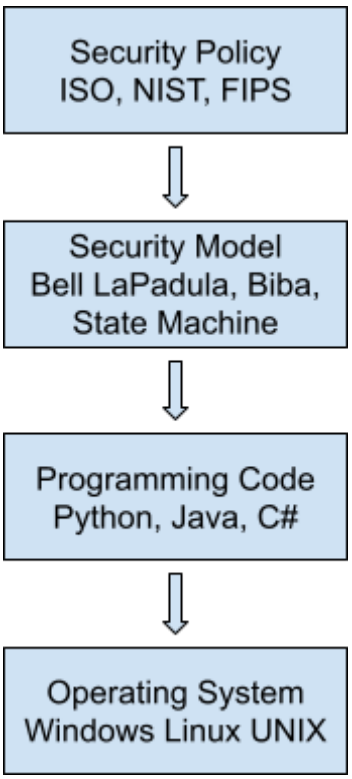
Name	Type	Algorithm Type	Size	Strength	Replaced By
RSA	Asymmetric	Key transport encryption algorithms	512	Strong	-
Diffie-Hellman	Asymmetric	Key transport	-	Moderate	El Gamal
El Gamal	Asymmetric	Key transport	-	Very Strong	-
ECC	Asymmetric	Elliptic Curve	Variable (smaller key size due to EC, 160-bit EC key = 1025 RSA)	Very Strong	-

ECC - Elliptic Curve Cryptosystem

The elliptic curve cryptosystem requires significantly shorter keys to achieve encryption that would be the same strength as encryption achieved with the RSA encryption algorithm.
A 3,072-bit RSA key is cryptographically equivalent to a 256-bit elliptic curve cryptosystem key.

Domain 3 Security Model

A security model provides a framework to implement a security policy.



Security models are used to determine how security will be implemented,
What subjects can access the system, and what objects they will have access to.

They are a way to formalise security policy.

Typically implemented by enforcing integrity, confidentiality, or other controls.

Each of these models lays out broad guidelines and is not specific in nature.

It is up to the developer to decide how these modals will be used and integrated into specific designs.

Security Models provide a way for designers to map abstract statements into a security policy.
Determines how security will be implemented, what subjects can access the system, and what objects they will have access to.

Access control matrix

An access control matrix assembles ACLs from multiple objects into a single table. The rows of that table are the ACEs of a subject across those objects, thus a capabilities list.

A table includes multiple objects and subjects, and the access control matrix identifies the specific access each subject has to different objects.

An access control matrix security method, mechanism, model reveals a capabilities list of a subject across multiple objects

State Machine Model

State Machine Model
Describes a system that is **alw**ays **secu**re no matter what **state** it is in.
Based on the computer science definition of a **fin**ite **sta**te **mac**hine (FSM)
A state is a snapshot of a system at a specific moment in time. All state transitions must be evaluated.
If each possible state transition results in another secure state, the system can be called a secure state machine.
The **state machine model** describes a system that is always secure no matter what state it is in. A secure state machine model system always boots into a secure state, maintains a secure state across all transitions, and allows subjects to access resources only in a secure manner compliant with the security policy.
Bell–LaPadula and **Biba** security models are built on a state machine model.

Information Flow Model

Focuses on the **flo**w of information
Information flow models are based on a state machine model
Biba and **Bell-Lapadula** are both **info**rmation **flow** models.
Bell-Lapadula **prevents** information flow from a **high** security level **to** a **low** security level.
Biba focuses on flow from **low** to **high** security level. integrity

Non-Interference Model

Is loosely based on the information flow model.
Is concerned with how actions of a subject at a higher security level affect the system state or the actions of a subject at a lower security level.
Ensures that the actions of different objects and subjects are not seen by and do not interfere with other objects and subjects on the same system.

Lattice-based model

Based on the interaction between any combination of:

- Objects (such as resources, computers, and applications) and
- Subjects (such as individuals, groups or organisations)

Lattice-based models are used to define the levels of security that an object may have and that a subject may have access to.

Security Models Properties

- **Simple** security property - describe rules for read
- **Star** * security property - describe rules for write
- **Invocation** property - rules around invocations (calls), such as to subjects.

Integrity	**Confidentiality**
Biba No read down, Star integrity property = no write up * Integrity	Bell-LaPadula No read up, Star Confidential Property = no write down Government (DoD)
Clark-Wilson Access control **triple**	Brewer and Nash Aka “Chinese Wall”
Goguen-Meseguer THE **noninterference** model	Take Grant Employs a direct graph
Sutherland Preventing interference (Information flow and State Machine Model)	-

Noninterference

Noninterference is the concept of limiting the actions of a subject at a higher security level so that they do not affect the system state or the actions of a subject at a lower security level.
If noninterference was being enforced, the writing of a file to a lower level would be prohibited, not allowed and supported.
Noninterference security architecture is implemented to avoid covert channel attacks.

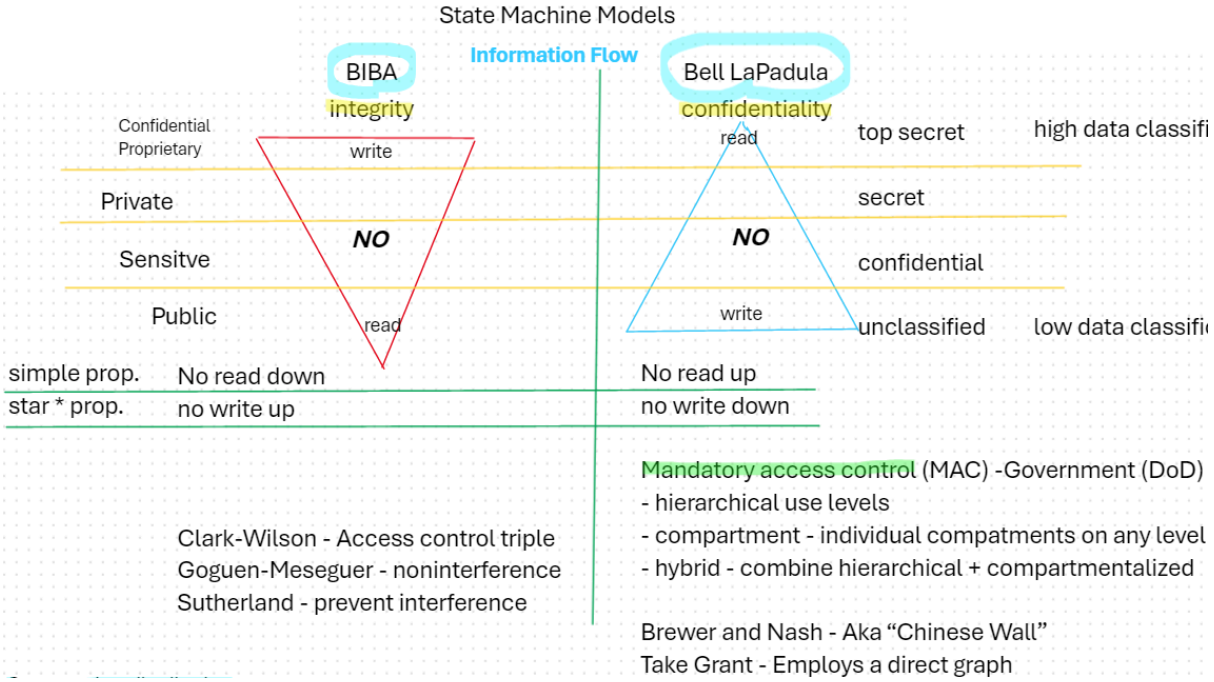
Bell-LaPadula

Only the Bell–LaPadula model addresses data confidentiality.
State machine model enforces confidentiality
Uses mandatory access control (MAC) to enforce the DoD multilevel security policy (Government)
Simple security property
Subject cannot read data at a higher level of classification. “No read up”
Star * security property
Subject **cannot** write info to lower level of classification “no write down”

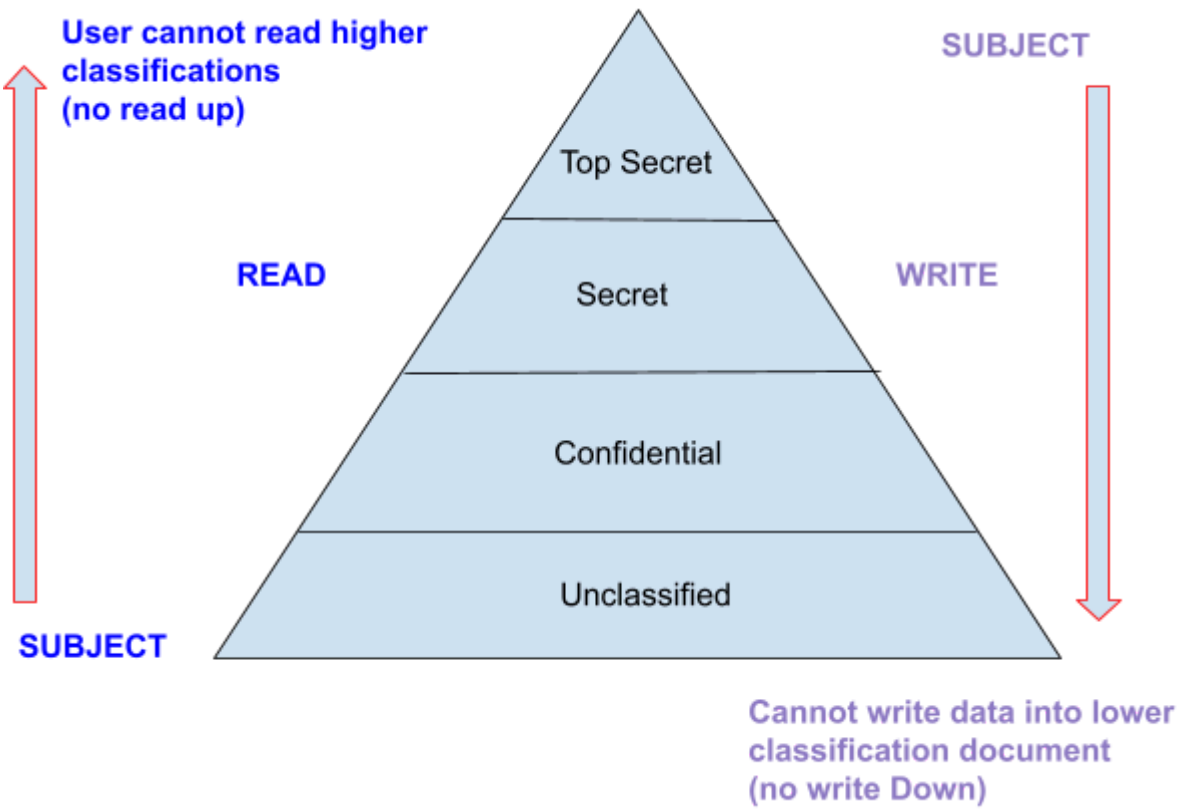
Declassification

When a trusted subject violates the star property of Bell–LaPadula in order to write an object into a lower level, ***declassification*** operation could be taking place
Declassification is the process of moving an object into a lower level of classification once it is determined that it no longer justifies being placed at a higher level. Only a trusted subject can perform **declassification** because this action is a violation of the verbiage of the star property of Bell–LaPadula, but not the spirit or intent, which is to prevent unauthorized disclosure.
Declassification is rarely chosen as an option for media reuse, as It is more expensive than new media and may still fail.

Bell-Lapadula used in a highly classified government agency where data confidentiality is of utmost importance. Encryption technical control for ensuring data confidentiality.

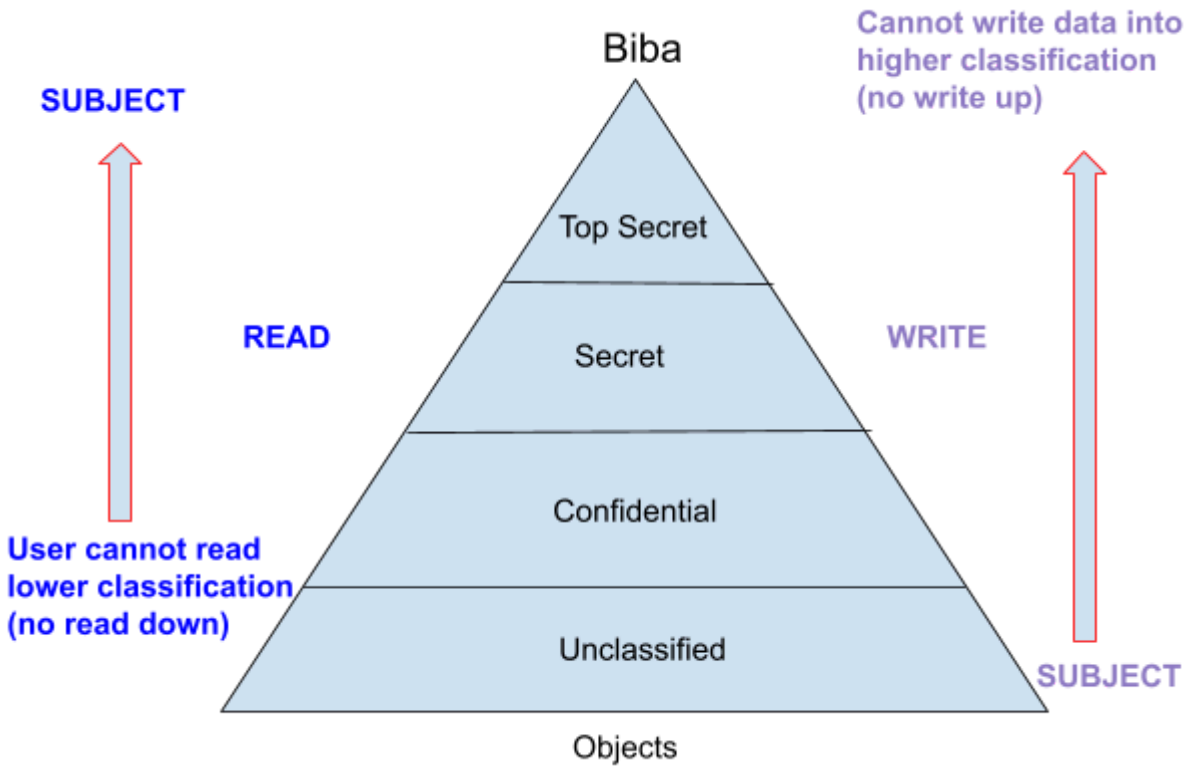


Bell LaPadula Pyramid Diagram



Biba

A Lattice-based model developed to address concerns of **integrity**.
Simple integrity property - subject at one level of **integrity** is not permitted to read an object of lower integrity. "**No read down**"
Star * integrity property - an object at one level of **integrity** is not allowed to write to an object of higher integrity. "**No write up**"
Invocation property - prohibits a subject at one level of **integrity** from invoking a subject at a **higher level of integrity**.



The **Biba** model was designed after the Bell–LaPadula model.
Whereas the **Bell–LaPadula** model addresses confidentiality, the Biba model addresses **integrity**.
The Biba model is also built on a **state machine** concept, is based on information flow, and is a multilevel model.
Read Up, is the implied meaning of the simple property of Biba.

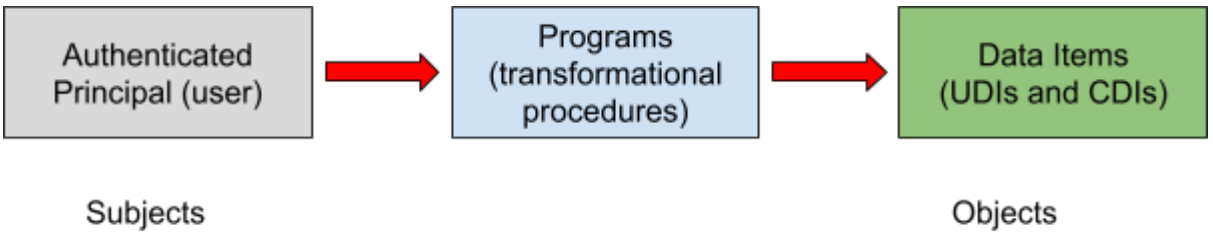
Clark-Wilson

The Biba and Clark–Wilson models address data **integrity**.
Uses security labels to grant access to objects

- **Constrained** data item (CDI) is any data item whose **integrity** is **protected** by the security model.
- **Unconstrained** data item (UDI) is any data item that is **not controlled** by the security model.
- **Integrity** verification procedure (IVP) is a procedure that **scans** data items and confirms their integrity.
- **Transformation** procedures (TPs) are the only procedures that are allowed to **modify** a CDI.

Clark-Wilson model Access control Triple(Triplet)

- Subject
- Object
- Interface (Program)



The relationship between an authenticated principal (i.e. user) and a set of programs (i.e. TPs) that operate on a set of data items (e.g. UDIs and CDIs).

A constrained interface or restricted interface can be used to protect **integrity** (such as the focus of the Clark–Wilson model) or confidentiality

Take Grant Model

Another confidentiality-based model that supports four basic operations: **take**, **grant**, **create** and **revoke.**

- The **grant rule** allows a subject to grant rights that it possesses on an object to another subject.
- The **create rule** allows a subject to create new objects and also creates an edge from the subject to that object, granting rights to the new object.
    - add another object to a security model and grant herself rights to that object.
- **Take rule** in the Take-Grant protection model allows a subject to take rights from another object if the subject has the **take** right over that object.

Brewer and Nash Model

The Brewer and Nash model prevents conflicts of interest.
Also called the "Chinese Wall" model. It was developed to prevent conflict of interest (**COI**) problems. (Confidentiality-based)
Brewer-Nash model allows access controls to change dynamically based upon a user's actions. It is often used in environments such as following example;
a consultant accesses data belonging to Acme Cola, a consulting client, they may then no longer access data belonging to any of Acme Cola competitors.
This is an implementation of a "**Chinese wall**" between data belonging to different clients.

Graham-Denning model

This model uses a formal set of protection rules for which each object has an owner and a controller.
It is focused on the secure creation and deletion of both subjects and objects.
A collection of eight primary protection rules or actions that define the boundaries of certain secure actions.
Rules:

1. Securely **create** an **object**
2. Securely **create** a **subject**
3. Securely **delete** an **object**
4. Securely **delete** a **subject**
5. Securely provide the **read** access right

6. Securely provide the **grant** access right
7. Securely provide the **delete** access right
8. Securely provide the **transfer** access right.

Domain 3 Security Modes

Dedicated Mode

Security clearance that permits access to ALL info processed by system, approval for ALL info processed by system, valid need-to-know for ALL info processed by system.

Multilevel Mode

Can process information at **different levels** even when all system users do not have the required security clearance to access all information processed by the system.

System High Mode

Each user must have **valid security clearance**, access approval for **ALL** info processed by the system, and valid **need-to-know** for at least **SOME** info on the system. Offers most granular control over resources and users of these models.

Users must have a security clearance and access approval in system high mode.

System High Mode clearance requirements

- Must have a clearance for the highest level of classification processed by the system, regardless of his access.
- Must have access approval for **all** information processed by the system.
- valid need to know for some information processed by the system.
- Must have a valid security clearance.

For systems running in System High mode, the user must have a valid security clearance for all information processed by the system, access approval for all information processed by the system, and a valid need to know for some, but not necessarily all, information processed by the system.

Compartmented Mode

Goes one step further than system high. Each user must have valid security clearance, access approval for **ALL INFO** processed by the system, but requires valid need-to-know for ALL INFO they will have access to on the system.

State machine model

Repeating Models - State Machine Model & Information Flow Model
CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Domain 3 Trusted Computing Base

TCB is a combination of hardware, software and controls that work together to form a "**trusted base**" to **enf**orce your **sec**urity policy.
Is a subset of the complete information system. Is the only portion that can be trusted to adhere to and enforce your security policy.

- **Sec**urity **peri**meter is an imaginary boundary that separates **TCB** from the rest of the system.
- The boundary of the physically secure area surrounding your system - context of physical security.

TCB must **cre**ate **sec**ure **chan**nels (aka "**trusted paths**") to communicate with the rest of the system.
Protects users (aka subjects) from compromise as a result of TCB interchange.
The trusted computing base (TCB) has a component known as the reference monitor in theory, which becomes the security kernel in implementation.

Reference Monitor & Security kernel

- **Reference monitor** is the logical part of the ***TCB*** that confirms whether a subject has the right to use a resource prior to granting access. **Enfor**ces access control.
- **Security kernel** is the collection of the TCB components that implement the functionality of the reference monitor.

The primary goal of a security reference monitor in a computer system is to enforce access controls based on user roles.

Domain 3 TCSEC, ITSEC and Common Criteria

Common Criteria (ISO-IEC 15408)

The **common Criteria** enable an object evaluation to validate that a particular product or system satisfies a defined set of security requirements.

TCSEC (Trusted Computer System Evaluation Criteria)

A structured set of criteria for evaluating computer security within products and systems.
Orange Book = TCSEC
ITSEC (Information Technology Security Evaluation Criteria)
The ITSEC represents an initial attempt to create security evaluation criteria in Europe.
ITSEC uses two scales to rate functionality and assurance.

CC has replaced ITSEC and TCSEC.

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Domain 3 Common Criteria

The primary distinction of the current Common Criteria (CC) from the previous security evaluation criteria systems it replaced is that the CC is a dynamic and subjective evaluation of security mechanisms and functions via the protection profiles (PPs) and security targets (STs) comparison mechanism.
Most previous systems were static in their evaluation of security protection mechanisms.
CC is not limited to confidentiality assessment, is not limited to evaluate standalone systems, and is not based only on mandatory access controls. These are characteristics of prior evaluation criteria systems, which were replaced by CC.

The Common Criteria defines various levels of testing and confirmation of systems' security capabilities, and the **number of the level** indicates what **kind of test**ing and confirmation has been **perform**ed.
Security Target is part of the Common Criteria specifying the claims of security from the vendor that are built into a target of evaluation.
Security targets (STs) specify the claims of security from the vendor that are built into a target of evaluation (TOE). STs are considered the implemented security measures or the "I will provide" from the vendor.

Steps Common Criteria (ISO-IEC 154080)

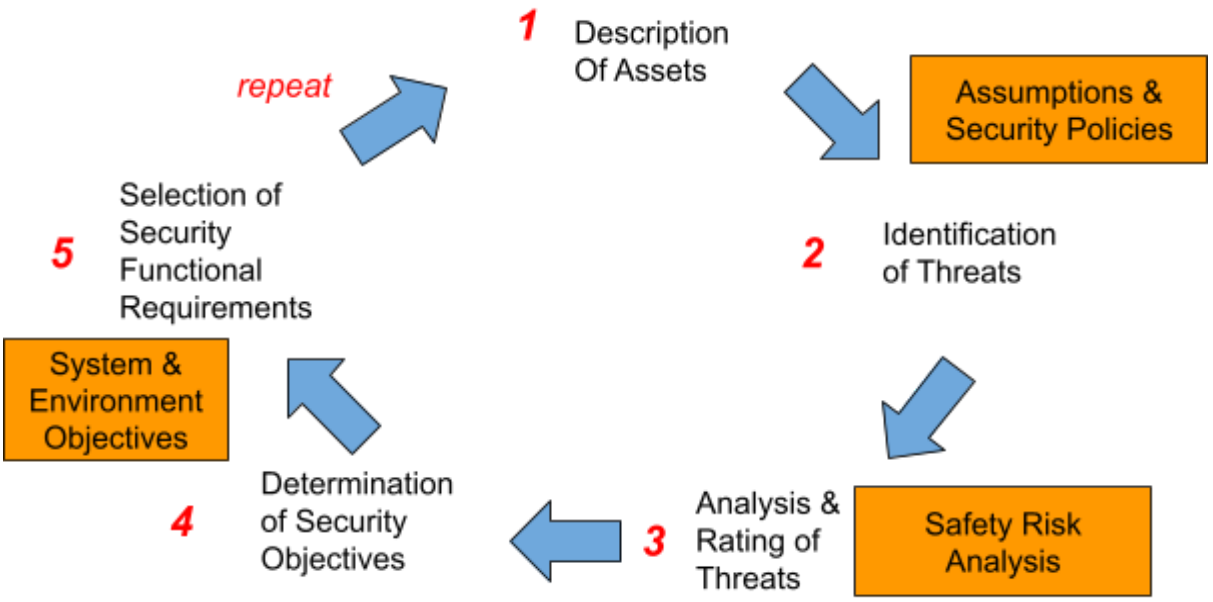


Table - Comparison of security **eval**uation **stan**dards

TCSEC	ITSEC	Common Criteria CC Level	Description
D	F-D+E0	EAL0, EAL1	Minimal no protection Functionally Tested
C1	F-C1+E1	EAL2	Discretionary security mechanisms Structurally Tested
C2	F-C2+E2	EAL3	Controlled access protection Methodically Tested & Checked
B1	F-B1+E3	EAL4	Labelled security protection Methodically Designed, Tested and Reviewed
B2	F-B2+E4	EAL5	Structured security protection Semi-Formally Designed and Tested
B3	F-B3+E5	EAL6	Security Domains Semi-Formally Verified Design and Tested
A1	F-B4+E6	EAL7	Verified security Design Formally Verified Design and Tested

Domain 3 Covert Channels

Covert Channels
A method that is used to pass information over a path that is not normally used for communication.
Because it's not normally used, it may not be protected by the system's normal security controls.
Two types: covert **timing** channing and covert **storage** channel.

Hard to detect because it's outside normal communication channels.

James Bond Top Secret Covert Channel
Covert channels use surreptitious communications' paths. Covert timing channels alter the use of a resource in a measurable fashion to exfiltrate information. If a user types using a specific rhythm of Morse code, this is an example of a covert timing channel. Someone watching or listening to the keystrokes could receive a secret message with no trace of the message left in logs.

Trusted Platform Module

A **chip** that resides on the **motherboard** of the device. (**TPM**)
Multi-purpose, like storage and management of keys used for full disk encryption (**FDE**) solutions.
Provides the operating system with access to keys, but prevents drive removal and data access.
The files on a windows drive are at their most secure when the system is off and the drive is encrypted and not in a readable state. Microsoft BitLocker decrypts files as needed when in use, meaning that any time after the system is booted files may be accessed, particularly if the user is logged in and access to the system can be gained or if malware is running.
TPM Features:

- Remote attestation creates a hash summary value from the system configuration to confirm the integrity of the configuration.
- Binding and sealing are techniques used by the TPM to encrypt data.
- The random number generator (RNG) function of the TPM is used to support cryptographic operations.

The **endorsement key (EK)** is a crucial part of a TPM and is created during the manufacturing process. The EK is a unique RSA key pair (composed of a public and private key) embedded into the TPM. It is used to establish trust in the TPM by allowing the TPM to prove its identity to external entities. The EK is never exposed outside the TPM, and its public part is used to verify the TPM's authenticity.
The **storage root key (SRK)** is created later when the TPM is initialized (or "provisioned") for use, not during the manufacturing process.

Domain 3 Types of Access Control

- **Mandatory** Access Control -
    - The MAC model uses labels to assign access.
    - In a mandatory access control system, all subjects and objects have a label.
    - enforces an access policy that is determined by the system, not the object owner.
    - Relies on **classification labels** that are representative of security domains and realms.
    - identifies the upper and lower bounds of access for subjects with labels
    - Hierarchical environment, the various classification labels are assigned in an ordered structure from low security to high security, using predefined labels for subjects and objects
- **Discretionary** Access Control
    - permits the owner or creator of an object to control and define its accessibility, because the **owner has full control** by default.
    - In a DAC model, the creator of a file is the owner, and the owner can grant access to others.
    - Discretionary access control (DAC) can provide greater **scalability** by leveraging many administrators, and those administrators can add **flexibility** by making decisions about access to their objects without fitting into an inflexible mandatory access control system (MAC)

    - DAC, allow individual administrators to make choices about the objects they control provides scalability and flexibility
- Attribute-based access control (ABAC)
    - An ABAC model gives access based on attributes.
    - Software-defined networks (SDNs) often use an ABAC model.
- Risk-based Access Control
    - A risk-based access control model evaluates the environment and the situation to determine access.
- **Non-discretionary** access control -
    - Enables the enforcement of **system-wide** restrictions that override object-specific access control.
- **Rule-based** access control
    - defines **specific functions** for access to requested objects.
    - Commonly found in **firewall** systems or Azure cloud **roles** such as security reader.
- **Role-based Access Control**
    - Uses a well defined collection of named job roles to endow each one with specific permissions.
    - Seeking to ensure that users who occupy such roles can access what they need to get their jobs done.

Domain 3 Access Control

Protection of sensitive and critical assets with access controls:

- Information
- Systems
- Devices

The primary goal when controlling access to assets is to Preserve confidentiality, **integrity**, and availability of systems and data.

Role-based Access Control
Uses a well-defined collection of named job roles to endow each one with specific permissions, thereby seeking to ensure that users who occupy such roles can access what they need to get their jobs done.

Domain 3 MAC Model Classifications

Mandatory access control (MAC) models rely on the use of labels for subjects and objects. They look similar to a lattice when drawn, so the MAC model is often referred to as a lattice-based model.

Mandatory Access Control - MAC
The MAC Model defines every object and every subject has one or more **labels**. These labels are **predefined**, and the system determines access based on assigned labels.

Mandatory access control (MAC) models rely on the use of labels for subjects and objects.

Hierarchical environment

Various classification labels are assigned in an ordered structure from low security to medium security to high security.
The hierarchical environment uses levels to assign access, using predefined labels for subjects and objects.

Compartmentalised environment

Requires specific security clearances over compartments or domains instead of objects.
A compartmentalised environment ignores the levels and only allows access for individual compartments on any level.

Hybrid environment

Contains levels with compartments that are isolated from the rest of the security domain.
Combines both **hierarchical** and **compartm**entalised environments so that security levels have subcompartments.

Domain 3 Security Models Design and Capabilities

Verification
The verification process is similar to the certification process in that it validates security controls. Verification may go a step further by involving a third-party testing service and compiling results that may be trusted by many different organizations.
Verification systems assurance process provide an independent third party evaluation of a system's controls that may be trusted by many different organizations.

Certification
The technical evaluation of each part of a computer system to assess its **concordance (agreement/alignment)** with security standards.

Accreditation
The process of **formal accept**ance of a certified configuration from a designated authority.
Accreditation is the act of management formally accepting a system, not evaluating the system itself.

Open System
Designed using industry standards and are usually easy to integrate with other open systems
Closed System
Generally proprietary hardware and or software. Their specifications are not normally published and they are usually harder to integrate with other systems. Black-Box.

Domain 3 Ensure Confidentiality Integrity Availability

- **Confinement** restricts a process to reading from and writing to certain memory locations
- **Bounds** are the limits of memory a process cannot exceed when reading or writing.
- **Isolation** is the mode a process runs in when it is confined through the use of memory bounds.

Domain 3 Factors of Authentication

Authentication Factors Overview

- Something you **know** (Pin or password)
- Something you **have** (Trusted device, token, key card) (***More Secure***)
- Some**thing** you **are** (biometric)
- Some**where** you **are (location)**

Among the authentication factors, possession-based factors (something you have) are generally considered more secure than knowledge-based (something you know) or biometric (something you are) factors.

Knowledge-based authentication (KBA) processes ask a user a series of questions based on their history that is recorded in authoritative sources.
Example where to use Knowledge-based authentication is for new customers online.

Cognitive authentication

A cognitive password asks a series of questions, but these are questions that the user previously answered, such as your favourite color.
A cognitive password authenticates users based on a series of facts or answers to questions that they know. Preset questions for cognitive passwords typically rely on common information about a user like their mother's maiden name or the name of their pet, and that information can frequently be found on the Internet. The best cognitive password systems let users make up their own questions.

Authentication & Authorization

- Authentication (**AuthN**) is the process of **proving** that you are who you say you are.
    - Identity
- Authorization (**AUTHZ**) is the act of **granting** an authenticated party permission to do something.
    - Access

Permissions, rights and privileges are then granted to users based on their proven identity.
If a user has rights to a resource they are granted authorization.

Domain 3 Multitasking & Multithreading

Multi**task**ing

Simultaneous execution of more than one application on a computer and is managed by the operating system.
Many PC OSs provide functionality that enables them to support the simultaneous execution of multiple applications on single-processor systems.

Multi**thread**ing

Multithreading permits multiple concurrent tasks (i.e., threads) to be performed within a single process.

Example:
A dual-core single-processor system can operate on two threads at a time (one by each core). There would be a total of four application threads in this scenario (ignoring any threads created by the OS), but the OS would be responsible for deciding which single thread is running on the processor at any given time.
A single-core single processor system would be limited to one thread executing at a time.

Affinity or preference is the assignment of the cores of a CPU to perform different tasks.

Domain 3 Multiprocessing & Multiprogramming

Multi**process**ing

The use of more than one processor to increase computing power.
In a multiprocessing environment, a multiprocessor computing system (that is, one with more than one CPU) harnesses the power of more than one processor to complete the execution of a multithreaded application.
In asymmetric multiprocessing (AMP), the processors are often operating independently of one another. Usually, each processor has its own OS and/or task instruction set.

Multi**program**ming

Similar to multitasking but takes place on **mainframe** systems and requires specific programming.

Domain 3 Single-state and multistate processing

Single-state processors are capable of operating at only one security level at a time
Multistate can simultaneously operate at multiple security levels.

Example of Multistate:
working with a Department of Defense (DoD) system that is authorized to simultaneously handle information classified at the Secret and Top Secret levels.

Domain 3 Processor Operating Modes

User
Applications operate in a **limited** instruction set environment known as user mode
Privileged
Controlled operations are performed in privileged mode, also known as **system** mode, **kernel** mode and **supervisory** mode.

Domain 3 Memory

Memory protection is a core security component that must be designed and implemented into an operating system. It must be enforced regardless of the programs executing in the system. Otherwise, instability, violation of **integrity**, denial of service, and disclosure are likely results.

Read-only Memory (**ROM**)

Read only contents burned in at the factory.

RAM

Static RAM (**SRAM**) uses flip-flops, dynamic RAM (**DRAM**) uses capacitors.
PROM
Programmable chip similar to ROM, with several subtypes.
EPROM
Erasing, Clearing (overwriting with unclassified data)

Ultraviolet EPROM (**UVEPROM**)

Chips have a small window that, when illuminated with a special ultraviolet light, erases contents.

Electronically Erasable PROM (**EEPROM**)

Uses Electric Voltages delivered to the pins of the chip to force erasure. A more flexible alternative to UV EPROM.

Flash Memory

Derivative concept from **EEPROM**.
Nonvolatile, can be electronically erased and rewritten.

Domain 3 Security Issues with Storage

Primary storage is the same as memory, .

Secondary storage (2nd Storage) consists of magnetic, flash, and optical media (CD-R) that must be first read into primary memory before the CPU can use the data.

Secondary memory is a term used to describe magnetic, optical, or flash media (i.e., typical storage devices like HDD, SSD, CD, DVD, and thumb drives). These devices will retain their contents after being removed from the computer and may later be read by another user.

Wear leveling on an SSD
Wear leveling is about writing to the disk evenly. **Encrypting** the data would protect against the disclosure of data on portions of the disk that have remnants due to too much wear and having been set aside as no longer usable.

Spare sectors, bad sectors, and space provided for wear leveling on SSDs (overprovisioned space) may all contain data that was written to the space that will not be cleared when the drive is wiped.
This is a form of data remanence and is a concern for organizations that do not want data to potentially be accessible. Many wiping utilities deal only with currently addressable space on the drive. SSDs cannot be degaussed, and wear leveling space cannot be reliably used to hide data. These spaces are still addressable by the drive, although they may not be seen by the operating system.

Random access storage devices can be read at any point.

Sequential access storage devices require scanning through all the data physically stored before the desired location.

Security Issues with secondary storage devices:
1. Removable media can be used to **steal** data
2. Access controls and encryption must be applied to **protect** data
3. Data can remain on the media even **after file deletion** or media formatting.

In a cloud computing environment, the most critical factor for ensuring data security and privacy is strong access controls and authentication.

Domain 3 Security risks of input & output devices

Subject to *eavesdropping* and tapping, used to smuggle data out of an organisation, or used to create unauthorized, insecure points of entry into an organisation's systems and networks.

Implementing Secure Real-time Transport Protocol (SRTP) is the best option to secure VoIP and prevent the recurrence of the *eavesdropping* attack.

Domain 3 Firmware

Software stored on a **ROM chip**, containing basic instructions needed to start a computer.
Also used to provide operating instructions in peripheral devices such as printers.
Gray imported hardware concern is whether the hardware and firmware can be trusted or may have been modified.

Domain 3 Vulnerabilities, Threats & Countermeasures

Process isolation
Ensures that individual **proc**esses can access only their own data.

Layering
Creates different realms of security within a process and limits communication between them.

Abstraction

Creates "**black-box**" interfaces for programmers to use without requiring knowledge of an algorithm or device's inner workings.

Data hiding
Prevents information from being read from a different security level. Hardware segmentation enforces process isolation with physical controls.

Domain 3 Security Policy

The role is to inform and **guid**e the design, development, implementation, testing, and maintenance of some particular system.

Cloud computing
The concept of computing where processing and storage are **perform**ed **else**where over a network connection rather than locally. (Azure, Amazon & GCP)

Sensitive & **confi**dential data can be at risk ***IF*** the cloud provider and their personnel might not adhere to the same security standards as your organisation.

When assessing the risk to **PHI** (protected health information) in a cloud environment, data access and control agreements with the cloud provider should be of primary concern.

Hypervisors

Type **I** hypervisor
A native or **bare-metal** hypervisor. In this configuration,there is no host OS, instead the hypervisor is installed directly onto the hardware where the host OS would normally reside. VMware ESXi

Type **II** hypervisor
A **hosted** hypervisor. In this configuration a standard regular OS is present on the hardware and the hypervisor is then installed as another software application. Oracle VirtualBox/Microsoft Hyper-V/VMWare Workstatrion Applications running on OS.

Domain 3 CASB

Cloud Access Security Broker
A cloud access security broker (CASB) is a security policy enforcement solution that may be installed on-premises or in the cloud.
Shadow IT

Domain 3 Security-AAS

A cloud provider concept in which security is provided to an organisation through or by an **online entity**. Outsourcing security function.

Smart Devices
Mobile devices that offer customization options, typically through installing apps, and may use on-device or in-the-cloud artificial intelligence (AI) processing.

Internet-of-Things
IOT
A class of devices connected to the internet in order to provide automation, remote control, or AI processing in a home or business setting. Google, Alexa, Tesla & Seri

Most Critical factor of IoT deployments:
The long-term support and patching model for the IoT devices may create security and operational risks for the organization.

Domain 3 Mobile device and Mobile app Security

Mobile device security

The range of potential security options or features that may be available for a mobile device. Security features include full device **encryption**, remote **wiping**, lockout, screen **locks**, **GPS**, application control, etc.
Understand mobile application security
The applications and functions used on a mobile device need to be secured.
Related concepts include key management, credential management, authentication, **geotag**ging, encryption, application **whitelist**ing, and **trans**itive trust/authentication.

Mobile Authentication that depend on users physical attributes:

- Fingerprint
- Voice
- Retina
- Facial recognition

Most effective means of reducing the risk of losing the data on a mobile device, Minimising sensitive data stored on the mobile device.

Bring your own device (BYOD)

Is a policy that allows employees to use their own personal mobile devices to work to access business information and resources. May improve employee morale and job satisfaction, but it increases security risks to the organisation.
Primary concern for a security manager in bring-your-own-device (BYOD) policy, is securing company data on personal devices.

Microsoft Azure Intune, Airwatch, and MobileIron samples of UEM platforms.

Key consideration when implementing a secure mobile device management (**MDM**) solution is to be able to perform **Remote wipe** capabilities.

Unified endpoint management (UEM) is a type of software tool that provides a single management platform to control mobile, PC, IoT, wearables, ICS, and other devices. UEM is intended to replace MDM and enterprise mobility management (EMM) products, by combining the features of numerous products into one solution. Microsoft Intune

Application **whitelisting** security control is most effective in **preventing** the executing of malicious code from untrusted sources.

Scenario:
Most effective in preventing unauthorised access to sensitive data stored on a mobile device that may be lost or stolen: Strong encryption of the data.
Confidentiality, cryptographic goal protects against the risks posed when a device is lost or stolen.

In the context of mobile application development, ensuring that application components are not exposed to others on the same device refers to: Application **sand**boxing.
Using a sandbox is an example of confinement, where the system restricts the access of a particular process to limit its ability to affect other processes running on the same system.

Choose Your Own Device

CYOD policy allows employees to use their own devices to connect to the company network.

Corporate-owned Mobile Strategy

Scenario
The CISO has asked you to propose an update to the company's mobile device security strategy. The main concerns are the intermingling of personal information with business data and complexities of assigning responsibility over device security, management, updates, and repairs.
The best option in this scenario is corporate-owned. A corporate-owned mobile strategy is when the company purchases mobile devices that can support compliance with the security policy. These devices are to be used exclusively for company purposes, and users should not perform any personal tasks on them. This option often requires workers to carry a

second device for personal use. Corporate-owned clearly assigns responsibility for device oversight to the organization.

Mobile device management

iPads used throughout retail organization as point-of-sale terminals.
Using an enterprise authentication system like Active Directory that requires individuals to log in with their credentials provides the ability to determine who was logged in if a problem occurs and also allows Greg to quickly and easily remove users who are terminated or switch roles.
Use Active Directory and user accounts for logins to the iPads using the AD user ID and password.
MDM, **context-aware** authentication is When a user attempts to authenticate to her organization's services, she knows that the organization uses a mobile device management MDM tool to check her location and whether she's logging in from her company-issued mobile device.
Authentication that takes attributes such as location, device, and **time of day** into account is **context-aware** authentication. - ABAC (Attribute Based Access Control)
This allows organizations to make choices about whether the authentication is appropriate and allowed in addition to the use of credentials. The decision is based on contextual information, not user knowledge or identity factors, which are used only to authenticate.

Domain 3 Embedded Systems & Static Environments

Embedded system
Is typically designed around a limited set of specific functions in relation to the larger product of which it is a component.
Scenario:
Arduino is an open source hardware and software organization that creates single-board 8-bit microcontrollers for building digital devices. An Arduino device has limited RAM, a single USB port, and I/O pins for controlling additional electronics (such as servo motors or LED lights), and does not include an OS or support networking. Instead, Arduino can execute C++ programs specifically written to its limited instruction set.

Static Environments
Are applications, OSs, hardware sets, or networks that are configured for a specific need, capability, or function, and then set to remain unaltered.

Managing Embedded and static systems
These techniques may include network segmentation, security layers, application firewalls, manual updates, firmware version control, TCP wrappers, and control redundancy and diversity.

A Raspberry Pi, another microcontroller option, has significantly more processing power than Arduino, is not limited to executing C++ programs, supports networking, and is more expensive than Arduino.

Domain 3 Privilege & Accountability

Principle of least privilege
Ensures that only a minimum number of processes are authorized to run in supervisory mode.
Separation of privilege
Increases the granularity of secure operations.
Accountability ensures that an audit trail exists to trace operations back to their source. Who or what did it?

?? Principle of least functionality ??

Separating the privileged operations any one entity can perform be that a system or a person so we sometimes call that in the world of people, we call that role separation.
Establish permissions who then administers the system somebody else grants permissions they grant they are the access administrator and then somebody else performs the technical functions of the system administrator, this ensures accountability.

Domain 3 Common Flaws & Vulnerabilities

Architecture security concepts to prevent attacks or exploits:

- Time of Check - The time at which the subject checks whether an object is available
- Covert Channel - A method used to pass information over a path not normally used for communication
- Time of use - The time at which a subject can access an object
- Maintenance hook - An access method known only to the developer of the system
- Parameter Checking - A method that can help prevent buffer overflow attacks
- Race condition -
    - The exploitation of the reliance of a system's behavior on the sequence of events that occur externally
    - Unlikely to be found by a web vulnerability scanner - burp suite pro

Buffer overflow

Occurs when the programmer fails to check the size of input data prior to writing the data into a specific memory location.
In addition to buffer overflows, programmers can leave **back doors** and privileged programs on a system after it is deployed.
Buffer overflow prevented with input validation.
Backdoor countermeasures: firewalls, anti-malware, network monitoring, code review.

Parameter checking (i.e., confirming input is within reasonable boundaries) is used to prevent the possibility of buffer overflow attacks.

Backdoor

Backdoors are undocumented command sequences that allow individuals with knowledge of the backdoor to bypass normal access restrictions.
Scenario:
Ben's system was infected by malicious code that modified the operating system to allow the malicious code author to gain access to his files.
Maintenance hooks, otherwise known as backdoors, provide developers with easy access to a system, bypassing normal security controls.

Backdoor in Javascript code can be identified as it is in human-readable form.
JavaScript is an interpreted language so the code is not compiled prior to execution, allowing Roger to inspect the contents of the code.
C, C++, and Java are all compiled languages, a compiler produces an executable file that is not human-readable, and thus the program may contain backdoor..

Time-of-check to time-of-use (TOCTTOU)

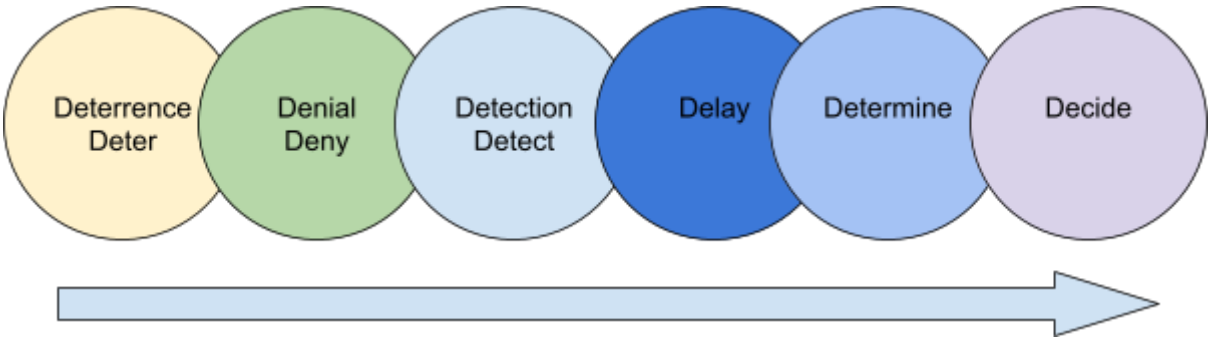
Time-of-check to time-of-use (TOCTTOU) attacks are not directly addressed by parameter checking or input filtering; defensive coding practices are needed to eliminate or reduce this issue.
A **proactive approach** to threat modelling, which is also known as the defensive approach.
Threat hunting takes place after a product has been created and deployed (this may be referred to as an adversarial approach or even reactive threat management).
Qualitative is typically associated with a form of risk assessment.

A development team is working on a new project. During the early stages of systems development, the team considers the vulnerabilities, threats, and risks of their solution and integrates protections against unwanted outcomes.
This scenario describes a proactive approach to threat modeling, which is also known as the defensive approach.

Even well-written systems can be susceptible to **time-of-check-to-time-of-use** (TOCTTOU) attacks.
Any state change presents an opportunity for an attacker to compromise a system.
Replay attack can be considered a TOCTTOU attack type. *back-to-the-future*

Domain 3 Functional order of Security Controls

Order of Steps:
Deter - Deny - Detect - Delay - Determine - Decide



Additional controls are **Determine**(cause of the attack) and **Decide** (on remedial or investigation action)

Domain 3 Physical Security Controls

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Physical **secu**rity **cont**rols can be divided into three groups:

- **Administrative**
  - also known as management controls and include policies and procedures, like site management, personnel controls, awareness training, and emergency response and emergency procedures.
  - emergency response guidelines should include the immediate steps an organization should follow in response to an emergency situation. These include immediate response procedures, a list of individuals who should be notified of the emergency, and secondary response procedures for incident responders.
    - Secondary response procedures for incident responders
- **Logical** - also known as technical controls and are implemented through technology like access controls, intrusion detection, alarms, CCTV, monitoring, HVAC, power supplies and fire detection and suppression.
- **Physical** - use physical means to protect objects and includes fencing, lighting, locks, construction materials, mantraps, bollards, dogs and guards.
  - An access control vestibule (also known as a **mantrap**)
  - Access control vestibules use two sets of doors to control access to a facility. This may be used to prevent piggybacking by monitoring use of the vestibule to allow only a single individual to enter a facility at a time. They may also be used to allow manual inspection of individuals or perform other security screening. Access control vestibules are also commonly known as mantraps.

Emergency response guidelines

- immediate response procedures
- a list of individuals who should be notified of the emergency
- secondary response procedures for incident responders.

Data Centers

Data centers should be located in the core of a building. Locating it on lower floors makes it susceptible to flooding and physical break-ins. Locating it on the top floor makes it vulnerable to wind and roof damage.

Key locks are the most common and inexpensive form of physical access control device for both interior and exterior use, if budget was reduced.
Lighting, security guards, and fences are all much more costly.
Fences are also mostly used outdoors.

Best Choice for Physical Access with multifactor authentication:
The combination of an ID card (something you have) and a PIN (something you know) is a reasonable way to control access to a physical facility.
The use of a password is not a user-friendly way to control access to a physical facility.

Cost effective physical access and still identifying individuals admitted:
either RFID or magstripe readers and PIN pads.

- RFID badges and readers with PIN pads
- Magstripe badges and readers with PIN pads

Lighting is often claimed to be the most commonly deployed physical security mechanism.
However, lighting is only a deterrent and not a strong deterrent

Domain 3 Physical Security Requirements

Access controls and perimeter security when evaluating the security of a physical facility, is a primary concern.

Technical controls for physical security include:

- Access controls
- Intrusion detection
- Alarms
- CCTV and monitoring
- HVAC
- Power supplies
- Fire detection and suppression

Administrative controls for physical security include:

- Facility construction
- Facility selection
- Site management
- Personnel controls
- Awareness training

- Emergency response
- Emergency procedure

Physical controls for physical security include:

- Fencing
- Lighting
- Locks
- Construction materials
- Mantraps
- Dogs
- Guards
- Bollards

There is **no security without physical sec**urity.
Without control over the physical environment, no amount of administrative or technical/logical access controls can provide adequate security.

If a malicious person can gain physical access to your facility or equipment they can do just about anything they want, from destruction to disclosure and alteration.

Alarms

There is **no** such thing as a preventive alarm.
Alarms are triggered in response to a **detected** intrusion or attack.
Whenever a motion detector registers a significant or meaningful change in the environment, it triggers an alarm.
Common types of alarms include deterrent, repellent, and notification.

Fence

- 3-4 feet deters casual trespasser
- 6-7 feet too hard to climb easily (1.8 metre)
- 8 feet with barbed wire will deter intruders (2.4 metre)

Physical Security to improve the prevention:
A PIDAS (perimeter intrusion detection and assessment system) is a fence system that has two or three fences used in concert to optimise security. The space between the fences can serve as a corridor for guard patrols or wandering guard dogs. One or more fences can support touch detection technologies.
An exterior fence is used to keep animals and casual trespassers from accessing the main fence.
This reduces the nuisance alarm rate (NAR) or false positives.

Crime Prevention Through Environmental Design (CPTED)

Crime Prevention Through Environmental Design (CPTED) is the concept to structure the physical environment and surroundings to influence individual decisions that potential offenders make before committing any criminal acts.

Crime Prevention Through Environmental Design (CPTED) has three main strategies:

- natural access control,
- natural surveillance,
- natural territorial reinforcement.

Natural access control is the subtle guidance of those entering and leaving a building through placement of entrance ways, use of fences and bollards, and placement of lights.
Natural surveillance is any means to make criminals feel uneasy through the increasing opportunities for them to be observed.
Natural territorial reinforcement is the attempt to make the area feel like an inclusive, caring community.

PIDAS is too direct and obvious of a security mechanism to be an element of CPTED.
A sensitive compartmented information facility (SCIF) is often used by government and military agencies, divisions, and contractors to provide a secure environment for highly sensitive data storage and computation.
An SCIF is typically located within a structure, although an entire structure can be implemented as an SCIF.
A main distribution frame (MDF) is a primary wiring closet of a facility.

Temperature

- **Hum**idity: 20-80% ideal
- Temps: for computers 60-75F / 15-23 C, damage at 175F. (Fahrenheit)
- Manage storage devices damaged at 100F

Electrical Impacts

- **Black**out: prolonged loss of power
- **Brown**out: prolonged low voltage
- **Fault**: short loss of power
- **Sur**ge: prolonged high voltage
- **Spi**ke: temporary high voltage
- **Sag**: temporary low voltage

Lights

- 8 Feet high with 2 feet candle power

Most effective in preventing unauthorised physical access to a data centre is a mantrap (Person trap) access control at the data centre entrance.

Vestibule

An access control vestibule is a double set of doors that is often protected by a guard and used to contain a subject until their identity and authentication is verified. **Mantrap**

Office Physical Access

Since physical access to the workstations is part of the problem, setting application timeouts and password-protected screensavers with relatively short inactivity timeouts can help prevent unauthorized access.
Set session timeouts for applications and use password-protected screensavers with inactivity timeouts on workstations.

Domain 3 Humidity and static electricity

Too much humidity can cause corrosion.
Too little humidity causes static electricity. Even on non static carpet, low humidity can generate 20,000 volt static discharge.
Electrostatic discharge can damage most computing components.
Static discharge from a person to a metal object can be over 1,000 volts.
Static electricity is not managed by the deployment of a UPS.

Domain 3 Fire and Suppression agents

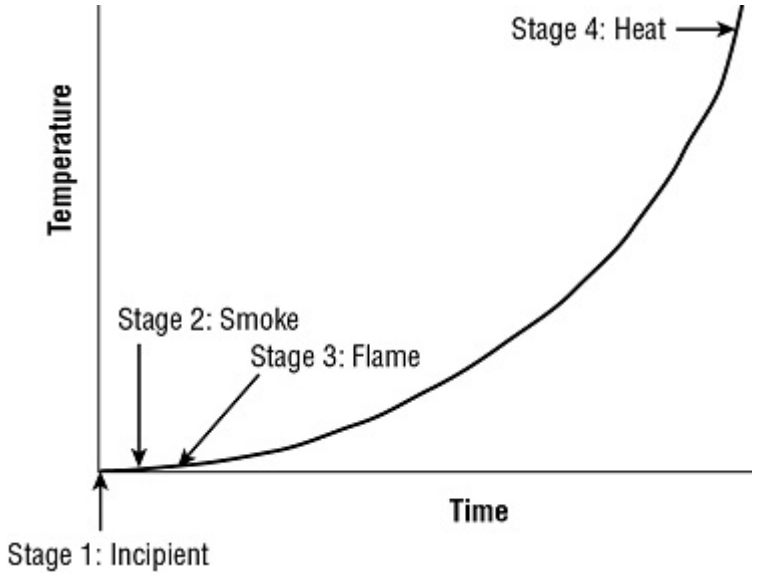
- Class A (ASH) fires are common combustibles such as wood, paper, etc. This type of fire is the most common and should be extinguished with water or soda acid.
- Class B (BOIL) fires are burning alcohol, oil and other petroleum products such as gasoline. They are extinguished with gas or soda acid. You should never use water to extinguish a class B fire.
    - Water is never the suppression medium in Type B fire extinguishers because they are used on liquid fires.
- Class C (Conductive) - fires are electrical fires which are fed by electricity and may occur in equipment or wiring. Electrical fires are conductive fires, and the extinguishing agent must be non-conductive, such as any type of gas.
- Class D (Dilithium) - fires are burning metals and are extinguished with dry powder.
- Class K (Kitchen) - fires are kitchen fires, such as burning oil or grease. Wet chemicals are used to extinguish Class K fires.

FM-200 is a chemical suppressant commonly used in place of water in data centers.
FM-200 is the best gas-based fire suppression system to install in a data center.

The three categories of fire **detection** systems include **smoke** sensing, **flame** sensing and **heat** sensing.

Diagram Earliest stage of a fire where it is possible to use detection technology to identify

1. Incipient



Fires may be detected as early as the incipient stage. During this stage, air ionization takes place, and specialized incipient fire detection systems can identify these changes to provide early warning of a fire.

Class	Type	Suppression Material
A	Common combustibles	Water, Soda acid (dry powder or liquid chemical)
B	Liquids	CO2, Halon, soda acid
C	Electrical	CO2, Halon
D	Metal	Dry power
K	Kitchen	Wet Chemicals

Domain 3 Voltage and Noise

- Electromagnetic Interference
  - Common mode noise - generated by the difference in power between the hot and ground wires of a power source operating electrical equipment
  - Traverse mode noise - generated by a difference in power in the hot and neutral wires of a power source operating electrical equipment
- Radio frequency interference (**RFI**) is the source of interference that is generated by electrical appliances, light sources, electrical cables and circuits, and more.

Static Voltage	Possible Damage

40	Destruction of sensitive circuits and other components
1000	Scrambling of monitor displays
1500	Destruction of hard drive data
2000	Abrupt system shutdown
4000	Printer jam or component damage
17000	Permanent circuit damage

Domain 3 Damage From fire and fire suppression

The destructive elements of a fire include smoke and heat but also the suppression medium, such as water or soda acid.

- **Smoke** is damaging to most storage devices
- **Heat** can damage any electronic or computer component
- **Suppression mediums** can cause short circuits, initiate corrosion, or otherwise render equipment useless.

All of these issues must be addressed when designing a fire response system.

People should always be your highest priority in business continuity planning. As **life safety** systems, **fire suppres**sion systems should always receive high prioritisation. Human Safety.

Domain 3 Water Suppression Systems

- **Preaction** systems
  - fills with water after a valve opens when the initial stages of a fire are detected and then requires a sprinkler head heat activation before dispensing water
  - use closed sprinkler heads and the pipe is charged with compressed air instead of **water**.
  - The **water** is held in check by an electrically-operated sprinkler valve and the compressed air.
  - A preaction system is the best type of **water**-based fire suppression system for a computer facility because it provides the opportunity to prevent the release of water in the event of a false alarm or false initial trigger.
  - Good for areas with people and computers
- **Wet pipe** systems are filled with **water**.
- **Dry pipe**
  - Dry pipe systems contain compressed air until fire suppression systems are triggered, and then the pipe is filled with water, and flame activated sprinklers trigger when a predefined temperature is reached.

    - systems also have closed sprinkler heads: the difference is the pipes are filled with compressed air. The **water** is held back by a valve that remains closed as long as sufficient air pressure remains in the pipes. Often used in areas where **water** may freeze, such as parking garages.
- **Deluge systems** are similar to dry pipes, except the sprinkler heads are open and larger than dry pipe heads. The pipes are empty at normal air pressure; the **water** is held back by a deluge valve.

Wet pipe suppression systems have water present in the pipes at all times, posing an unacceptable level of risk for a data center containing electronics that might be damaged if a pipe leaks. Dry pipe and pre-action systems only contain water when triggered in the event of a possible fire. FM-200 is a chemical suppressant commonly used in place of water in data centers.

The most common cause of a false positive for a **water**-based system is human/people error.

If you turn off the **water** source after a fire and forget to turn it back on, you'll be in trouble for the future. Also, pulling an alarm when there is no fire will trigger damaging **water** release throughout the office.
Water shortage would be a problem, but it is not a cause for a false positive event.

Domain 3 Gas Discharge Systems

Usually more effective than **water** discharge systems, but should not be used in environments where people are located, because they work by removing oxygen from the air.
Halon is effective, but **bad** for the environment (ozone-depleting), turns to toxic gas at **900F**.

Suitable replacements include:
- FM-200 (HFC-227ea)
- CEA-410 or CEA-308
- NAF-S-II (HCFC Blend A)
- FE-13 (HCFC-23)
- Argon (IG55) or Aragonite (IG01)
- Inergen (IG541)
- Aero-K

Domain 3 Lock Types

- Cipher lock/Electronic Combination Locks - something you **know**
    - Cipher locks can be programmed with more than one code. One code can open the door, and another code can open the door and also raise a silent alarm. allowing employees to raise a silent duress alarm as they enter.

    - ***Duress***, or being under threat of violence or other constraints, is a concern for organizations such as banks, jewelry stores, or other organizations where an attacker may attempt to force an employee to perform actions.
- Key Card Systems - something you **have**
- **Token - Something You Have**
- Biometric System - something you **are**
- Conventional Locks - easily picked / bumped & keys easily duplicated
- Pick-and-Bump Resistant locks - expensive, harder to pick & keys not easily duplicated.

Protecting physical servers housed in a server room using following:
- Cipher lock
- heating, ventilation, and air-conditioning (HVAC) systems

A cipher lock can limit physical access to a server room and is a physical security control.

Domain 3 Site Selection & Facility Design

Key elements in site selection and facility design.

- **Site** selection - **visibili**ty, composition of the surrounding area, area **accessib**ility, and the effects of **natur**al **dis**asters.
- **Facility** design - understanding the level of security needed by your organisation and planning for it before **construct**ion begins.

Technology convergence is the tendency for various technologies, solutions, utilities, and systems to evolve and merge over time. Often this results in multiple systems performing similar or redundant tasks or one system taking over the feature and abilities of another. Though in some instances this can result in improved efficiency and cost savings, it can also represent a single point of failure and become a more valuable target for hackers and intruders.

Domain 3 Secure Work area design and configuration

There should not be **equal access** to all locations within a facility. Areas with high-value assets require restricted access.
Valuable and confidential assets should be located in the heart of the centre of protection provided by a facility.
Centralised server or computer rooms need **not be human** compatible.

Domain 3 Threats to Physical Access Controls

No matter which physical access control is used, a security guard or other monitoring system must be deployed to prevent:

- **Abuse** of physical access control include propping open secured doors and bypassing locks or access controls
- **Masquerading** is using someone else's security ID to gain entry to a facility.
- **Piggy**backing is following someone through a secured gate or doorway without being identified or authorized personally. (**tailgating**)

Masquerading / Impersonation

Usually implies that authentication credentials have been stolen or **falsified** in order to bypass authentication mechanisms.
Countermeasures: one-time pads, token authentication systems (e.g. Kerberos), encrypt traffic, employee awareness training.

Domain 3 Securing a wiring closet

This is where the networking cables for **a floor or even a whole building** are connected to essential equipment such as patch panels, switches, routers, and backbone channels.

Most security focuses on preventing physical unauthorized access. If an unauthorized intruder gains access, they may steal equipment, pull cut cables, or plant a listening device. Though not explicitly stating hardware, integrated listening mechanism scenario describes a typical and potential risk of a supply chain, that a hardware risk results in the presence of a listening mechanism in the final product.

Wiring closet physical security network patch cabling room cabinet room.

Critical Path Analysis

Critical path analysis is a systematic effort to identify relationships between mission-critical applications, processes, and operations and all the necessary supporting elements when evaluating the security of a facility or designing a new facility.

Labelling and mapping out the critical paths of network cables throughout the building need the following information indicated:

- Entrance facility
- Equipment room
- Backbone distribution system
- Telecommunications room
- Horizontal distribution system

Domain 3 Physical Security Requirements

If a facility employs restricted areas to control physical security, then a mechanism to handle **visitors** is required.

Often an **escort** is assigned to **visitors**, and their access and activities are monitored closely.
Tracking actions of outsiders when they are granted access to prevent malicious activity against the most protected assets.
Understand the needs for **media storage.**
Media storage facilities should be designed to securely **store** blank reusable and installation media.
Media storage facilities used to store backup tapes.

Concerns include theft, corruption, data remnant recovery.
Media storage facility protections include:

- Locked cabinets
- Using a librarian custodian
- Implementing a **check-in/check-out** process
- Using media sanitization - shredding

Domain 3 Evidence Storage

Understand the concerns for evidence storage - **integrity**
Used to retain logs, drive images, virtual machine snapshots, and other datasets for recovery, internal investigations, and **forensic investiga**tions.
The most reasonable course of action would be to take a snapshot of the compromised system and use the snapshot for the investigation, restoring the website to operation as quickly as possible while using the results of the investigation to improve the security of the site.

Protect the chain of custody.
chain of custody is way To demonstrate the integrity and authenticity of the evidence.

Protections for evidence storage include:

- Locked cabinets or safes
- dedicated/isolated storage facilities
- Offline storage
- Access restrictions and activity tracking
- Hash management and encryption

Domain 3 Audit Trails and Access Logs

Audit trails and **access logs** are useful tools for managing **physical access cont**rol.
Creation may need to be created manually by security guards or may generated automatically with the right equipment (smartcards and certain proximity readers)
Monitoring should also consider monitoring entry points with **CCTV**. Through CCTV, you can compare the **audit trails** and access logs with a visually recorded history of the events.
Divergence

Audit trails provide documentation on what happened, when it happened, and who did it.

Audit trails provide a record of events in audit logs. They include what happened and who did it.
Users can be held accountable for their actions when the logs show what they did.

Log information is critical to reconstructing the events of an intrusion, breach or attack.

Log Scenario:
A file server in your network recently crashed. An investigation showed that logs grew so much that they filled the disk drive. You decide to enable rollover logging to prevent this from happening again.
First action: Copy existing logs to a different drive, so that valuable data is not deleted and evidence of possible attack lost.

Domain 3 Need for Clean Power

Load Shedding in South Africa !!!
Power supplied by electric companies is not always consistent and clean.
Most electronic equipment requires clean power in order to function properly and avoid damage.

A **UPS** is a type of **self-charging batt**ery that can be used to:

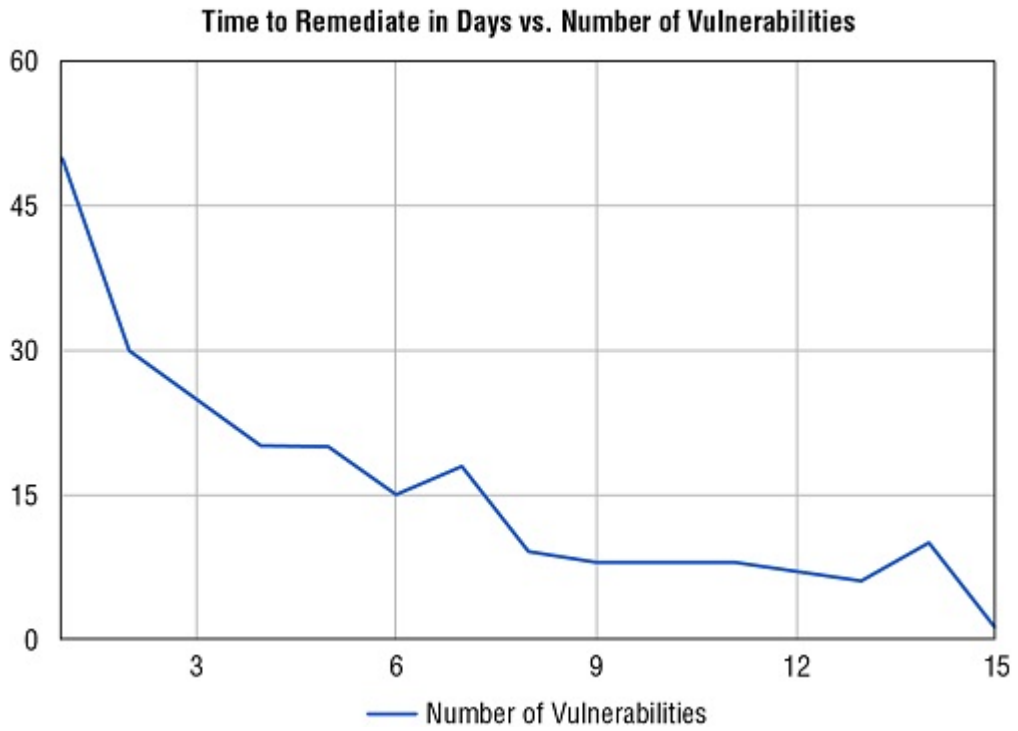
- Supply **consistent, clean power** to sensitive equipment.
- Supply power for minutes or hours (depending on its size) in the event of **power failure.**

Domain 3 Key Performance Indicators of Physical Security

Relevant KPI for physical security to track how well the security efforts are performing through the organization:

- Number of successful intrusions
- Number of successful disruptions
- Number of unsuccessful incidents
- Time to detect incidents
- Time to respond to incidents
- Level of organizational impact of incidents
- Number of false positives (i.e., false detection alerts/alarms)

Example KPI Graph



Time to remediate a vulnerability is a commonly used key performance indicator for security teams.

Domain 4 Communication and Network Security

- Implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design
- Assess and implement secure design principles in network architectures
- Micro-segmentation
    - Software Defined networks (SDN)
    - Virtual extensible Local area network (VXLAN)
    - Encapsulation
    - Software-defined Wide area network (SD-WAN)
- Wireless networks
    - Li-Fi - Bluetooth
    - Zigbee
    - Satelite
- Cellular networks
    - 4G and 5G
- Content Distribution Networks (CDN)

CISSP Exam Cram Full Course (All 8 Domains) - Good for 2024 exam!

It is important to verify that multimedia collaboration connections are **encrypted**, that robust **multifactor auth**entication is in use, and that tracking and **logging** of events and activities is available for the hosting organization to review. MS Teams/Zoom/Google Talk

Encapsulation

TCP/IP is a multilayer protocol.
The ability to operate at higher OSI layer levels is normally considered a benefit of multilayer protocols.
It is primarily based on IPv4, but the organization is planning on deploying IPv6 within the next year.
Benefit and a potentially harmful implication of multilayer protocols:

- Encapsulation is both a benefit and a potentially harmful implication of multilayer protocols.
- Encapsulation allows for encryption, flexibility, and resiliency, while also enabling covert channels, filter bypass, and overstepping network segmentation boundaries.
- Encapsulation is adding a header and possibly a footer to data as it moves down the OSI stack.

Adding a header and possibly a footer to data as it moves down the OSI stack.
De-encapsulation, process that occurs when the Session layer removes the header from data sent by the Transport layer in the OSI model
The process of removing a header (and possibly a footer) from the data received from a previous layer in the OSI model is known as de-encapsulation.

Implications of multilayer protocols

- VLAN hopping
- Multiple encapsulation
- Static IP addressing

<u>Scenario Bypass a filter:</u>

[Ethernet [IP [TCP [HTTP [FTP [Payload]]]]]

In this instance, the filter is likely related to blocking FTP, so the user is employing a utility that is taking advantage of the multilayer protocol feature of encapsulation to enclose the blocked protocol in an allowed protocol, namely HTTP. There is no indication of data being encrypted, since there is no listing of an encryption mechanism (such as TLS) or protocol (such as SSH or IPsec) (i.e., VPN).
Result: Bypassing a filter

SSH2
SSH2 adds support for simultaneous shell sessions over a single SSH connection. Both SSH1 and SSH2 are capable of supporting multifactor authentication.

IPv4

- Uses 32-bit addresses allowing for around 4 billion unique addresses
- Large portions of the address space are reserved or unused contributing to shortage of addresses

- Example IPv4 192.168.1.1

IPv6 Benefits

- IPv6 uses 16-byte (128-bit) addresses, 340 undecillion unique addresses
- supports auto configuration without DHCP
- supports Quality of Service (QoS) priority values
- Example ipv6 - 2001:0db8:85a3:0000:0000:8a2e:0370:7334

IPv6 and IPv4 coexist:

- Gateway
  - network that supports IPv6 but needs to connect it to an IPv4, best option is to install an IPv6 to IPv4 gateway that can translate traffic between the networks.
- Dual Stack
  - Dual stack is to have most systems operate both IPv4 and IPv6 and use the appropriate protocol for each conversation
- Tunnelling
  - Tunnelling allows most systems to operate a single stack of either IPv4 or IPv6 and use an encapsulation tunnel to access systems of the other protocol.
- NAT-PT
  - Network Address Translation-Protocol Translation (NAT-PT) (RFC-2766) can be used to convert between IPv4 and IPv6 network segments similar to how NAT converts between internal and external addresses

Multicast

- Supported by both IPv4 and IPv6
- A one-to-**many** communication method where a single packets is sent to multiple specific recipients

Broadcast

- Not supported by IPv6 (but workarounds exist)
- A one-to-**all** communication method where packets are sent from a single source to all recipients on the network segment.
- Install a router to create multiple broadcast domains on the network.

Unicast

- Supported by both IPv4 and IPv6
- A one-to-one transmission from one point to another point.
- The most common use of IPv4 and IPv6

Anycast

- Supported natively by IPv6
- From a single source to the nearest or most optimal recipient
- From a group of potential recipients
- Nearest or Best , Used with CDNs

Domain 4 Network Architectures

Designing a secure network architecture, the principle “Defense in depth” emphasises the separation of critical network segments to limit the impact of a security breach.

Backhaul Networks

For long-term connections like backhaul networks, a point-to-point VPN that is connected at all times is the most common choice to ensure all traffic is secured.
Use point-to-point VPN, to ensure that traffic sent via his backhaul networks provided by third-party telecom providers is secure.

VXLAN - Virtual Extensible LAN

Network virtualization enabling network segmentation a high scale
VXLAN tunnels layer 2 connections over a layer 3 network, stretching them across the underlying layer 3 network.

Overcomes VLAN scale limitations - limit is **4096** VLANs versus **millions** of VXLANs
Tunnelling protocol that encapsulates an Ethernet frame (layer 2) in a UDP packet.
Layer 2 can generally only be attacked from within (eg. MAC spoofing, or flooding to cause DOS), such as by a rogue host.

MAC spoofing

MAC spoofing is used to falsify the physical address of a system to impersonate that of another authorized device.
ARP poisoning associates an IP address with the wrong MAC address.
MAC Spoofing: Changing the physical address of a network interface to masquerade as a different device.
MAC spoofing relies on plaintext Ethernet headers to initially gather valid MAC addresses of legitimate network devices.
enables port security on the switches on her network, trying to prevent content addressable memory (CAM) table or MAC address table flooding by preventing large numbers of MAC addresses from being used on a single port.

Mitigation against MAC Spoofing

- Port security - CAM table flooding
- MAC Filtering
- NAC (network access control)
- DHCP Snooping
- Encryption
- Network Monitoring
- Security Awareness Education

CAM table flooding attack, overwhelm switches, resulting in switches broadcasting every message they see.

Mail-bombing is the use of email as an attack mechanism by flooding a system with messages, causing a denial of service.

VXLAN Scenario:
Your CISO is implementing a new technology to enable the various satellite offices to be connected to the central headquarters. This will increase business operations efficiency as well as allow for a more consistent application of company security policy. The technology is based on an encapsulation protocol that enables switch-created network segments to be stretched across subnets and geographic distances.

MUX

A multiplexer, often abbreviated as MUX, is a digital electronic device that combines multiple input signals into a single output signal for transmission over a shared medium.

SDN - Software Defined Networks

A network architecture approach that enables the network to be intelligently and centrally controlled, or 'programmed', using software.
SDN technology that will allow them to separate the routing process for the network from the packet switching process while increasing centralization
Software-defined networking provides a network architecture that can be defined and configured as code or software and separates routing processes from packet switching while centralizing control.

Has capacity to reprogram the data plane at any time.
Use cases include **SD-LAN** and **SD-WAN**
Separating the control plane from the data plane opens up a number of security challenges.
The control plane is centralized on an SDN network.

A software-defined network (**SDN**) typically uses an **Attribute-Based Access Contr**ol (ABAC) model.
A software-defined network (SDN) typically uses an attribute-based access control (ABAC) model.
The ABAC model is commonly used in SDNs.

Software-defined networking (SDN) uses code to configure and control the network. This allows for agile, programmatic control and configuration as needed from a central control point. SD-WAN provides the same sort of control for wide area network links, which aren't mentioned in this question.

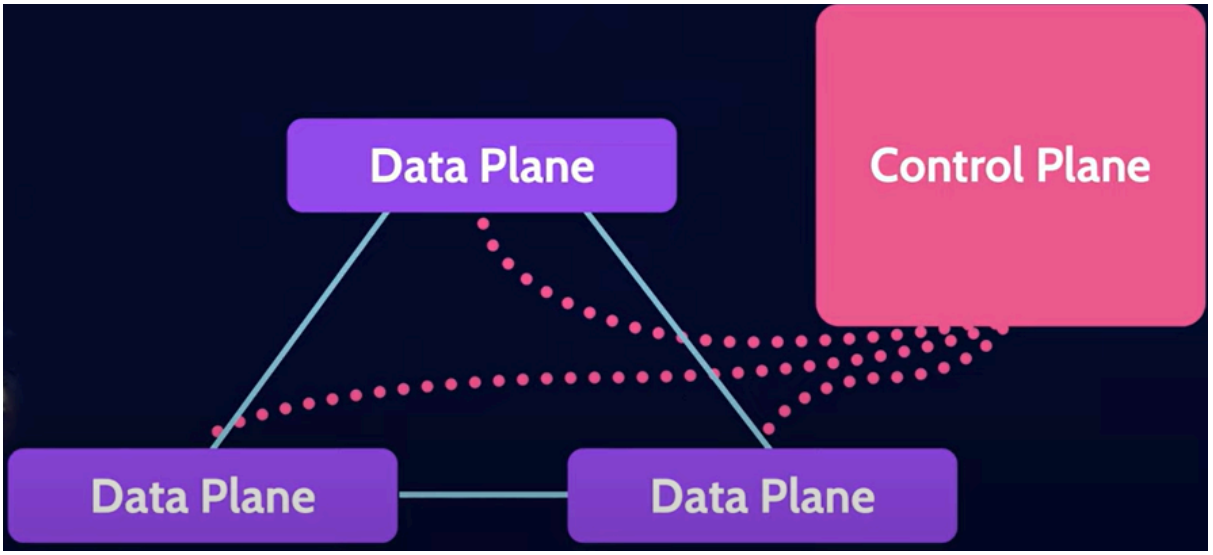
The separation of network infrastructure from the control layer, combined with the ability to centrally program a network design in a vendor-neutral, standards-based implementation, is an example of SDN.

SDN vulnerabilities can include man-in-the-middle attack (MITM) and a service denial(DOS) **Secure with TLS.**

SDN - Planes

Cloud fundamentally works because of SDN.
Software Defined Networks (SDN) provide abstraction from underlying physical networks to enable rapid reconfiguration with centralised control.

Control Plane - Functions and processes which determine paths.
Data Plane - Functions and processes that forward packets based on the direction of the Control Plane.



The **application plane** of a software-defined network (SDN) is where applications run that use application programming interfaces (APIs) to communicate with the SDN about needed resources.

Virtual Private Cloud (VPC)

VPC, or virtual private cloud, is the environment many organizations operate inside of public clouds.
Provides a logically isolated and customizable portion of a public cloud provider's infrastructure to a customer.
Virtual network that consists of cloud resources, where the VMs for one company are isolated from the resources of another company.
Separate VPCs can be isolated from the resources of another company.
Separate VPC can be isolated using public and private networks or segmentation.
Term in cloud providers:

- Amazon Web Services (AWS) - VPC
- Microsoft Azure - Virtual network (VNET)
- Google Cloud Platform (GCP) - VPC

SD-WAN - Software defined Wide Area Networks

Enables users in **branch offices** to remotely connect to an enterprise network
Enables use of many network services - MPLS, LTE, and broadband internet, etc. - to securely connect users to applications.
SD-WAN uses multiple Internet service providers (ISPs) to connect to its cloud VPC to ensure reliable access and bandwidth.

Security is based largely on IP security (IPSec), VPN tunnels, next-gen firewalls (NGFWs), and the micro-segmentation of application traffic.

Uses a **centralised control function** for intelligent routing and secure access service edge (SASE) to decentralise connectivity.

MPLS (Multiprotocol Label Switching) is a high-throughput, high-performance network technology that directs data across a network based on short path labels rather than longer network addresses. It uses encapsulation to handle a wide range of protocols. This technique saves significant time over traditional IP-based routing processes, which can be quite complex.

Secure Access Service Edge (SASE)

"Sassy" Secure Access Service Edge (SASE)
A Design philosophy closely related to zero trust network architecture.

A network model that merges traditional WAN management and security capabilities into a unified whole.
SASE is built, implemented and managed using cloud-native architectures.
SASE is a response to the edge-centric trends in mobility, cloud, SD-WAN and the internet of things.
Still considered an emerging / evolving cybersecurity concept.

Future of WAN
Combines network security and wide-area networking (WAN) capabilities into a cloud-based service.

LiFi Light Fidelity

Uses the modulation of light intensity to transmit data (**uses LED**)
Can safely function in areas otherwise susceptible to electromagnetic interference
Can theoretically transmit at speeds of up to **100 Gbit/s**
Li-Fi only requires working LED lights (Bluetooth is on new exam)
Visible light is that it **cannot** penetrate **opaque walls.**

LiFi (light fidelity) is a technology for wireless communications using light. LiFi does not require a network cable connection, is not affected by EMI, supports throughput rates of up to 100 Gbps, and can provide a modest level of communications even when the signal is interfered with (by bouncing off of reflective services).

Zigbee - Personal Area Network

A short-range wireless **PAN** (**Personal Area network**) technology developed to support automation, machine-to-machine communication, remote control and monitoring of **IoT** devices.
Supports both **centralised** and distributed security models, and **mesh** topology
Assumes that **symmetric keys** used are transmitted securely (encrypted in-transit)

Zigbee uses AES to protect network traffic, providing integrity and confidentiality controls.

Scenario:
A new startup company is designing a sensor that needs to connect wirelessly to a PC or IoT hub in order to transmit its gathered data to a local application or cloud service for data analysis. The company wants to ensure that all transferred data from the device cannot be disclosed to unauthorized entities. The device is also intended to be located within 1 metre of the PC or IoT hub it communicates with.

During pre-configuration of a new device, in which a single key might be sent unprotected, create a brief vulnerability.
IOT home devices use Zigbee ready.

5G Generation Cellular

Faster speeds and lower latency
Unlike 4G, 5G does not identify each user through their SIM card. Can Assign identities to each device.
Some air interface threats, such as **session hijacki**ng, are dealt with in 5G.
Standalone (SA) version of 5G will be more secure than the non standalone (**NSA**) version.

NSA anchors the control signalling of 5G networks to the 4G core.

5G technology includes both a new mutual authentication capability and additional protections for subscriber identities.

Concern sending sensitive data over the cellular network!
Cellular networks have the same issues that any public network does. Encryption requirements should match those that the organization selects for other public networks like hotels, conference Wi-Fi, and similar scenarios. Encrypting all data is difficult and adds overhead, so it should not be the default answer unless the company specifically requires it.

A common risk that cellular phone hotspots create for business networks is they can provide attackers with an unsecured network path into your network.

4G connectivity solutions

- Encryption
- device-based authentication (for example, using certificates)
- SIM-based authentication

4G connectivity solutions do NOT include security capabilities relating to Dedicated towers and antennas for secure service subscribers.

DIAMETER

Upgrade to Diameter from RADIUS and TACACS which present multiple security and operational challenges.
Diameter provides enhanced security features, better error handling, and supports more flexible transport protocols.
Diameter protocol, which provides authentication, authorization, and accounting (**AAA**), will be a target.
Because 5G has to work alongside older tech (3G/4G), old vulnerabilities may be targeted.
Because the scale of IOT endpoint counts on 5G is exponentially greater, **DDOS** is a concern.

Concerns when using 4g and 5G Cellular roaming data service capability:

- *Eavesdropping*
- Rogue Towers
- Reliability of establishing a connection

Cellular services, such as 4G and 5G, raise numerous security and operational concerns. Although cellular service is encrypted from device to tower, there is a risk of being fooled by a false or rogue tower. A rogue tower could offer only plain text connections, but even if it supported encrypted transactions, the encryption only applied to the radio transmissions between the device and the tower. Once the communication is on the tower, it will be decrypted, allowing for *eavesdropping* and content manipulation. Even without a rogue tower, *eavesdropping* can occur across the cellular carrier's interior network as well as across the internet, unless a VPN link is established between the remote mobile device and the network of the organization.

LEO

Low Earth orbit (LEO) satellite internet service will be the best option in this scenario.
LEO offers high-speed communications with minimal latency when compared to other satellite offerings. Geostationary orbit (GEO) satellite internet service would offer slower throughput with higher latency compared to LEO.
Most existing satellite Internet systems have relatively high latency. Newer low Earth orbit satellites like *Starlink* appear to provide better latency than higher orbits, but latency and susceptibility to interference from weather are both common concerns for satellite-based systems.

Content Delivery Network (CDN)

Content Distribution network (CDN)
A **Geo**graphically **distr**ibuted network of **prox**y servers and their **data** centres.
Goal is fast and highly available content delivery by distributing content spatially relative (**close to**) users.
CDN networks serving **JavaScript** have been targeted to inject malicious content into pages.

Example: Video and audio streaming, software downloads, etc.

STRP stands for Secure Real-time Transport Protocol. An extension of Real-time Transport Protocol (RTP) that features enhanced security measures. The protocol provides encryption, confidentiality, message authentication, and replay protection to your transmitted audio and video traffic.

Vendors in CDN space offer DDOS protection and web application firewalls (WAF)

CDN Properties:

- A CDN is able to maintain customer demand levels of multimedia performance quality.
- Using a CDN avoids straining individual servers.
- Data is stored close to customers.
- Client-based CDN (aka P2P) can support high-speed file exchange (BitTorrent).

Network access control

Network access control (NAC) is the concept of controlling access to an environment through strict adherence to and enforcement of security policy. NAC is meant to be an automated detection and response system that can react in real time to ensure that all monitored systems are current on patches and updates and are in compliance with the latest security configurations, as well as keep unauthorized devices out of the network.

IEEE 802.1X provides port-based access control and is useful both on wired and wireless connections to block access to systems and users that are unknown or that fail authentication. It is a common companion to NAC implementations.

NAC Functions:

- Agent-based
  - Agent-based NACs can quarantine noncompliant devices and implement updates automatically.
- Pre Admission-based
  - Pre Admission-based NAC requires a system to meet all current security requirements (such as patch application and malware scanner updates) before it is allowed to communicate with the network.
- post-admission
  - Post-admission philosophy allows or denies access based on user activity after connection based on a predefined authorization matrix.
  - Since this doesn't check the status of a machine before it connects, it can't prevent the exploit of the system immediately after connection.
- dissolvable NAC agen
  - A dissolvable NAC agent can be set to run once and then terminate.
- agentless NAC
  - An agentless NAC performs port scans, service queries, and vulnerability scans against networked systems to determine whether devices are authorized and baseline compliant.

NAC Goals

- detect/block rogue devices
- prevent or reduce zero-day attacks
- confirm compliance with updates and security settings
- enforce security policy throughout the network
- use identities to perform access control.

Port security

Port security can refer to several concepts:

- network access control (NAC)
- Transport layer ports
- RJ-45 jack ports

NAC requires authentication before devices can communicate on the network.
Transport-layer port security involves using firewalls to grant or deny communications to TCP and UDP ports. RJ-45 jacks should be managed so that unused ports are disabled and that when a cable is disconnected, the port is disabled.

NAC Scenario
Admin wants to ensure that systems are compliant with her network security settings before they are allowed on the network and wants to ensure that she can test and validate system settings as soon as possible.
A pre-admit, client-based NAC system will test systems before they are allowed on the network using a client that can determine more about a system than a clientless model can.

OT vs ICS

Industrial Control Systems (ICS) - old term
Operational Technology (OT) - new term

A real-time operating system (**RTOS**) is designed to process or handle data as it arrives on the system with minimal latency or delay. An RTOS is usually stored on read-only memory (ROM) and is designed to operate in a hard real-time or soft real-time condition.

Developing a new product that is intended to process data to trigger real-world adjustments with minimal latency or delay.
A scenario is describing a product that requires a real-time operating system (***RTOS***) solution, since it mentions the need to minimise latency and delay, storing code in ROM, and optimising for mission-critical operations.

OT refers to the hardware and software technology used to monitor and control physical processes, devices, and industrial systems. (broader term)

ICS is a subset of OT and specifically focuses on the control and automation of industrial processes. (subset of OT)
The availability of real-time control signals is a primary concern when implementing security measures for industrial control systems (ICSs).

SCADA

Administrative access via a second, physically separate Ethernet network with access controlled via VPN and multifactor authentication.

Types of ICS:

- Supervisory Control and Data Acquisition (SCADA)
    - A large utility company is very likely to be using supervisory control and data acquisition (SCADA) to manage and operate their equipment; example city municipality
    - That is the system that the APT (advanced persistent threat) group would have attempt to compromise
- Distributed Control Systems (DCS)
- Programmable Logic Controllers (PLC)

Distributed Network Protocol 3 (DNP3) is a set of communications protocols used between components in process automation systems managed by SCADA.
Distributed Network Protocol (DNP3) allows SCADA and other systems to use TCP/IP-based networks to communicate.
SCADA devices that are now connected to the network can be attacked over the network.
Many SCADA devices were never designed to be exposed to a network, and adding them to a potentially insecure network can create significant risks

DNP3 main use is in utilities such as electric and water companies communication between SCADA and the PLC devices.

Separate, physically isolated Ethernet networks that require strong authentication are a commonly used out-of-band (OOB) option.
While direct physical access is also an acceptable out-of-band option, it does not work well in a complex, production-oriented environment where devices may not be safe or easy to access.

Scenario:
How to secure types of ICS above!
An industrial processing facility has implemented SCADA systems to monitor and manage the mission-critical production lines. These ICSs cannot adhere to the company's 14-day patch application policy.
Answer: Prohibit nonauthorized nonessential software from executing.

Domain 4 OSI MODEL

Away	7 Application	All	SSH HTTP FTP

Pizza	6 Presentation	People	ASCII
Sausage	5 Session	Seem	**No hardware* SMB, SQL,*
Throw	4 Transport	To	Firewalls & Proxies - TLS segment
Not	3 Network	Need	Routers IPSEC packet gateways
Do	2 Data Link	Data	Frame switches - MAC Addresses
Please	1 Physical	Processing	Hubs & Repeaters

All People seem to need data processing.

In a multi-tier application architecture, which of the following layers is most vulnerable to injection attacks such as SQL injection and command injection is at ISO Model Application Layer.

DoD Model or TCP/IP Model

- Layer 4 - Application
- Layer 3 - Transport
- Layer 2 - Internetworking / Internet layer
- Layer 1 - Link

OSI Protocols

NAT operates at layers 3 and 4
VLAN exists at layer 2

7 Application	SSH, HTTP, FTP, LPD, SMTP, Telnet, TFTP, EDI, POP3, IMAP,SNMP
6 Presentation	Encryption protocols and format types ASCII, EBCDICM, TIFF, JPEG, MPEG, MIDI
5 Session	SMB, RPC, NFS, and SQL
4 Transport	SPX, SSL, TLS, TCP, UDP (Datagrams)
3 Network	**VRF,** ICMP, RIP, OSPF, BGP, IGMP, TFTP, IP, **IPSec**, IPX, **NAT**, SKIP
2 Data Link	ARP, RARP, SLIP, PPP, L2F, L2TP, PPTP, FDDI, ISDN, **VLAN**
1 Physical	EIA/TIA-232, X.21, HSSI, Bluetooth, 802.11 Wifi and Ethernet

OSI Functionality

7 Application	**Interfacing** user applications, network services, or the operating system with the protocol stack.

6 Presentation	Transforming data received from the application layer into a format that any system following the model can **understand**. Data reformatting
5 Session	establishing , maintaining and terminating communication **sessions** between two computers
4 Transport	Managing the **integrity** of a connection and controlling the session [**segment or datagram**] UDP is a simplex protocol
3 Network	Adding routing and addressing information (source and destination) to the data [**packet**] Logical addressing
2 Data Link	Formatting the packet from the network layer into the proper format for transmission. [**frame**] Mac Addresses
1 Physical	Contains the device drivers that tell the protocol how to use the **hardware** for the transmission and reception of **bits**

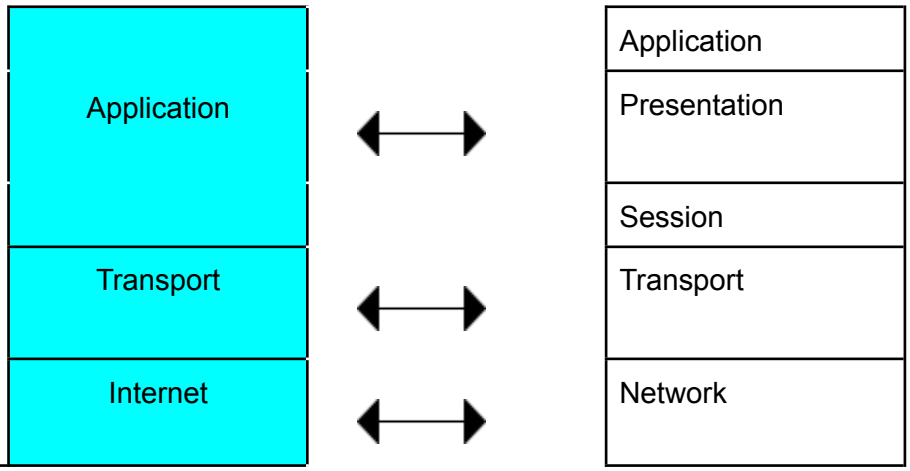
Network-layer traffic routing decisions prevent infinite transmission scenarios using hop limit and time to live.
The hop limit IPv6 header value and the time to live (TTL) IPv4 header values are both used to prevent infinite transmission.

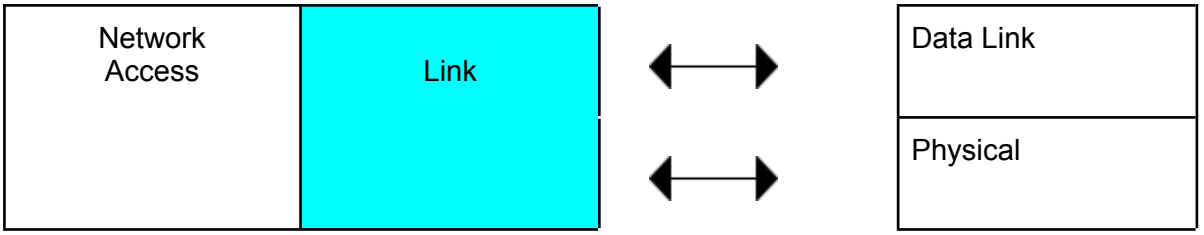
Common TCP UDP Ports

Protocol	TCP/UDP	Port
CHARGEN Character Generator Protocol	UDP	19
FTP Data Transfer	TCP	20
FTP Control Commands	TCP	21
SSH	TCP	22
Telnet	TCP	23
SMTP	TCP	25
TACACS+	TCP	49
DNS	TCP/UDP	53
DHCP	UDP	67,68
TFTP	UDP	69
HTTP	TCP	80

POP3	TCP	110
NTP	UDP	123
NetBIOS	TCP/UDP	137,138,139
IMAP	TCP	143
SNMP	TCP/UDP	161,162
BGP Border Gateway	TCP	179
LDAP	TCP/UDP	389
HTTPs	TCP	443
SMB	TCP	445
Syslog	UDP	514
Printer LPD	TCP	515
LDAP over TLS	TCP/UDP	636
FTP over TLS	TCP	989,990
RADIUS	UDP	1812
SQL	TCP	1433 database port , never expose to public networks.
RDP	TCP	3389
Diameter	TCP	3868
Printer LPD	TCP	9100

TCP/IP Stack





PSH is a TCP flag used to clear the buffer, resulting in immediately sending data, and URG is the TCP urgent flag. These flags are not present in UDP headers.

A TCP packet; PSH and URG are used to clear the buffer and indicate that the data is urgent

TCP/IP Scenario:

In Scenario is that a **private IP address** from RFC 1918 is assigned to the web server. RFC 1918 addresses are not internet routable or accessible because they are reserved for private or internal use only.
Example Private IP Addresses:

- 10.0.0.18
- 172.31.8.204
- 192.168.6.43

The web server has been positioned in the screened subnet and assigned an IP address of 172.31.201.17, and the issue in this scenario is that a private IP address from RFC 1918 is assigned to the web server. RFC 1918 addresses are not internet routable or accessible because they are reserved for private or internal use only.

Automatic Private IP Addressing (APIPA) = 169.254.1.119

So, even with the domain name linked to the address, any attempt to access it from an internet location will fail. Local access via jumpbox or LAN system likely uses an address in the same private IP address range and has no issues locally.
The **issue** of the scenario (i.e., being unable to access a website using its FQDN) could be resolved by either using a **public IP address** or implementing static NAT on the screened subnet's boundary firewall.
The **jumpbox** would not prevent access to the website regardless of whether it was rebooted, in active use, or turned off. That would only affect Michael's use of it from his desktop workstation.
Split-DNS does support internet-based domain name resolution; it separates internal-only domain information from external domain information.

Domain 4 TCP vs UDP

No.	**TCP**	**UDP**

1	Connection oriented	Connection-less protocol
2	Byte stream	Message Stream
3	**No** support for multicasting/broadcasting	**Supports** multicasting / **broadcast**ing
4	Supports **full duplex** transmission	No support for full duplex transmission
5	Reliable service of data transmission (error check)	Unreliable service of data transmission
6	TCP packet is called a **segment**	UDP packet is called a **datagram**
7	Provides **error detec**tion and flow control	**No** support for error detection and flow control

The three media management or control modes:

- simplex (one-direction)
- half-duplex (two-way, but only one direction can send data at a time)
- full-duplex (two-way, in which data can be sent in both directions simultaneously) communications.

UDP
UDP is a connectionless protocol that operates at the **Transport layer** of the OSI model and uses ports to manage simultaneous connections.
UDP is a simplex protocol at the Transport layer (layer 4 of the OSI model).

802.1X is the IEEE standard for port authentication.
Multiplexing is the mechanism of combining or integrating numerous signals into a single communication over a transmission media.

Domain 4 Cabling Types & Throughput

Network Cable distance, length range.

UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1 Mbps	-	Twisted Pair	Old Telephone cable

CAT2	Up to 4 Mbps	-	Twisted Pair	Token Ring Network
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Ring & 10Base-T
CAT4	Up to 16 Mbps	100m	Twisted Pair	Token Ring Network
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit
CAT6	Up to 10 Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 metres)
CAT6a	Up to 10 Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 metres)
CAT7	Up to 10 Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 metres)

A repeater, switch, or concentrator will amplify the signal, ensuring that the 100-meter distance limitation of 1000BaseT is not an issue.
Category 5e (cat 5e) and Category 6 (cat 6) UTP cables are both rated to 1000Mbps. Cat 5 (not Cat 5e) is only rated to 100Mbps, whereas Cat 7 is rated to 10Gbps.

Domain 4 Throughput & Cabling

Network cable speeds

Type	Max Speed	Distance	Difficulty to install	Susceptibility to EMI
10Base2	10 Mbps	185 m	Medium	Medium
10Base5	10 Mbps	500 m	High	Low
10BaseT (**UTP**)	10 Mbps	100 m	Low	**High**
STP	155 Mbps	100 m	Medium	Medium
100BaseT/100BaseTX	100 Mbps	100 m	Low	High
1000BaseT	1 Gbps	100 m	Low	**High**
Fiber-optic	2+ Gbps 100 Gbps	2+ Km	High to medium	None Fiber optic hardest to tap without specialized equipment

UTP = unshielded twisted pair

Domain 4 Standard Network Topologies

- **Star** -
  - employs a centralised connection device. Can be a simple hub or switch. Each system is connected to the central hub by a dedicated segment.
  - In network topology terms ethernet network is star BUT it is bus technology
- **Mesh** -
  - connects systems to all other systems using numerous paths.
  - Provides redundant connections to systems allowing multiple segment failures without seriously affecting connectivity.
  - Mesh topologies provide redundant connections to systems, allowing multiple segment failures without seriously affecting connectivity.
- **Ring** - Connects each system as points on a circle. The connection medium acts as a unidirectional transmission loop. Only one system can transmit data at a time. Traffic management is performed by a token.
- **Bus** -
  - A logical bus can be implemented as a physical star.
  - **Ethernet network is a bus-based technology.** It can be deployed as a physical star, but the hub or switch device is actually internally a logical bus connection
  - Device.
  - connects each system to a trunk or backbone cable. All systems on the bus can transmit data simultaneously, which can result in collisions.
  - A collision occurs when two systems transmit data at the same time. Ethernet.

Domain 4 Analog vs Digital

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Analog

Communications occur with continuous signals that vary in frequency, amplitude, phase, voltage and so on.
The variances in the continuous signal produce a wave shape as opposed to the square shape of a digital signal.
The actual communication becomes altered and corrupted because of the attenuation over long distances and interference.

Digital

Communications occur through the use of a discontinuous electrical signal and a state change or on-off pulses.
More reliable than analog signals over **long distances** or when interference is present because of a digital signals definitive information storage method.

Uses current voltage where voltage on represents a value of 1 and voltage off represents a value of 0. These **on-off pulses** create a stream of binary data.

Domain 4 Synchronous vs Asynchronous

Some communications are synchronised with some sort of clock or timing activity, and are synchronous or asynchronous.

Synchronous

Communications rely on a **timing** or clocking mechanism based on either an independent clock or a timestamp embedded in the data stream.
Are typically able to support very high rates of data transfer. Example: networking

Asynchronous

Communications rely on a stop and **start delimiter bit** to manage the transmission of data.
Best suited for smaller amounts of data.
Example: public switched telephone network (PSTN) modems.

Domain 4 Baseband & Broadband

Baseband

Can support only a **single comm**unication channel
It uses a direct current applied to the cable. A current that is at a higher level represents the binary **signal of 1,** and a lower level is a binary signal of 0.
Is a form of digital signal. Example **Ethernet**

Broadband

Can support multiple simultaneous signals. Uses **freq**uency **modula**tion to support numerous channels.
Each supporting a distinct communication session. Suitable for high throughput rates, especially when several channels are multiplexed.
Analog signal, Example is TV, cable modem, ISDN, DSL, T1, T3

Domain 4 Broadcast, Multicast, Unicast

Broadcast, multicast, and unicast technologies determine how many destinations a single transmission can reach.

- **Broadcast** technology supports communication to **all** possible recipients.
- **Multi**cast technology supports communications to **multiple specific recipi**ents. Such as Windows TFTP deploy new OS to multiple computers.

- **Unicast** a **single** communication to a specific recipient.

Multicasting is the transmission of data to multiple specific recipients.
Internet Group Management Protocol (**IGMP**) is used to register a host's dynamic multicast group membership in order to receive a copy of the data stream.
TFTP systems can be used to host or cache multicast datasets that are to be sent to the multiple recipients.

IP Addressing

UNICAST IP Addresses:

- Class A
    - Usage: Class A addresses are often used in large organizations with many devices. The private range (10.x.x.x) is commonly found in intranets.
- IP addresses with an initial octet of 128–191 (Class B)
    - Private IP Range: 172.16.0.0 to 172.31.255.255
- IP addresses with initial binary bits of 100 (Class C)
    - Private IP Range: 192.168.0.0 to 192.168.255.255

IP address groups expect to find in the intranet:

- Class A addresses start with a binary 0 and a first octet in dotted-decimal notation of 1–126.
- Class B addresses start with binary 10 and a first octet in dotted-decimal notation of 128–191.
- Class C addresses start with binary 110 and a first octet in dotted-decimal notation of 192–223.

The below will ***not*** be seen on intranet:

- Class D addresses, which are used for multicasting, start with binary 1110 and a first octet in dotted-decimal notation of 224–239.
- Class E addresses, which are reserved for experimentation, start with binary 1111 and a first octet in dotted-decimal notation of 240–255.
- IPv6 does not use class groupings.

Transmission methods

- Unicast (1 to 1)
- Multicast (1 to Many)
- Broadcast (1 to All)
- Anycast (nearest or Best, used with CDNs)

Transport Architecture

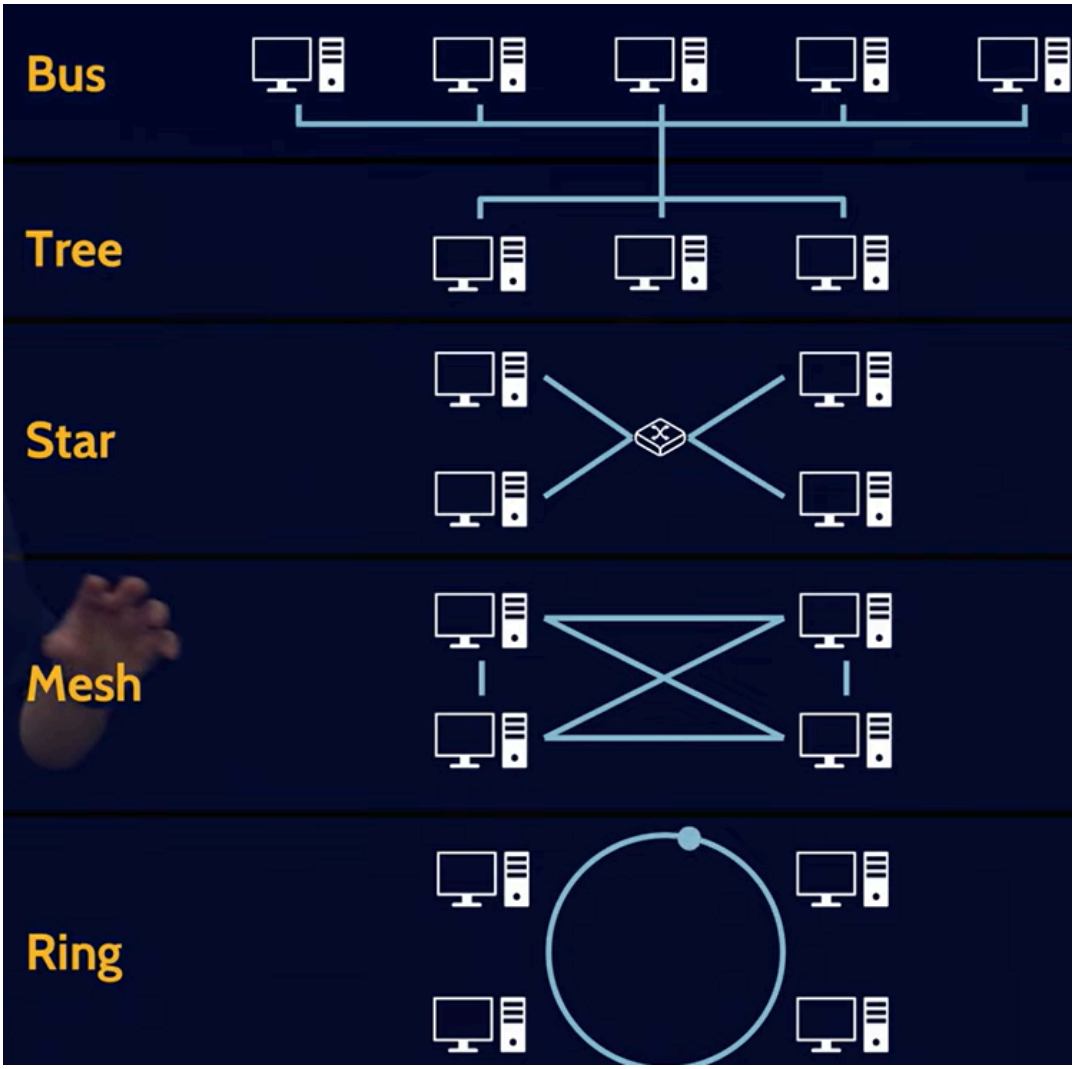
- Topology
    - Physical topology

        - Dicates how devices are physically linked and how they communicate over these physical connections
    - Logical topology
        - Defines how data actually flows within the network, regardless of its physical layout.
        - E.g. In a physically star-shaped network, the logical topology might be a bus if all communications are being broadcast to all nodes.

Domain 4 Transport Architecture - Planes

- Data Plane
    - Responsible for **forwarding** data packets between devices in the network
    - Transfers packets across the network based on direction from the Control Plane
    - Forward packets based on direction of the control plane
    - **Cut-through**
        - Switch starts forwarding the packet as soon as it reads the destination address, without waiting for the entire packet to be received.
        - Reduces latency but does not allow for error checking of the entire packet.
        - Switch makes a forwarding decision as soon as it receives the first part of the frame.
        - When ultra-low latency is important, and cost/simplicity a high priority
        - best suited to low-latency, high-throughput data transfer
    - **Store-and-forward**
        - Switch receives the entire packet, checks it for errors, and then forwards it to the destination.
        - Introduces more latency but ensures that the packet is error-free before forwarding.
        - The switch waits to receive the entire frame before making a forwarding decision.
        - When reliability is essential, or the network less reliable.
- Control Plane
    - Responsible for **managing** network routing protocols that facilitate communication between devices on the network
    - Determines the optimal path for data packets
    - Functions and processes which determine paths, route calculation / determination, OSPF, BGP (border gateway protocol)
    - Border Gateway Protocol (BGP) is the primary example of an exterior routing protocol.
    - Relevant protocols include Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP)
- Management Plane
    - Handles the **configuration**, monitoring, software updates and security management.

- Relevant protocols include Simple Network Management Protocol (SNMP) and Network Configuration Protocol (NETCONF). **SNMPv3** offers encryption security features to protect the confidentiality and integrity of data during transmission.
- Configure, manage, & maintain network performance.
- Manages and monitors the networks operations



Domain 4 Network Performance metrics

- Bandwidth
  - Maximum amount of data that can be transmitted over a network or internet connection in a given amount of time
  - Maximum capacity of a network channel to transmit data (Theoretical max)
- Throughput
  - Actual rate of successful data transfer achieved, measured over a period of time
  - Consider factors like latency, packet loss and network congestion.

- Latency
  - Latency is a delay in the delivery of packets from their source to their destination.
  - Time it takes for a signal to travel from its source to its destination and back (round-trip time)
  - Time delay between sending a data packet from the source to its arrival at the destination.
  - Latency has an inverse relationship to throughput (low latency = high throughput)
- **Jitter**
  - Variation in time delay in milliseconds between data packets over a network. Inconsistency of latency over time.
  - Affects quality of service (QoS) for real-time applications
  - Jitter is a variation in the latency for different packets.
  - variance of the delay between packets of data that are sent between two of his sites
- Packet loss
  - Packet loss is the disappearance of packets in transit that requires retransmission.
- Signal-to-noise ratio (SNR)
  - Measure of the level of the desired signal to the level of background noise. A higher **SNR** can allow for higher data rates.
  - Measures the quality of a signal relative to background noise. It is commonly used in wireless communication.
  - Higher SNR indicates better signal quality and less interference.
  - Interference is electrical noise or other disruptions that corrupt the contents of packets.

Domain 4 Traffic Flows

North-south and east-west traffic patterns
Crucial considerations when designing network architecture, as they impact the choice of network topologies, routing protocols and security strategies.

North-South

The flows of data in and out of the data centre.
Traffic between clients on the internet and servers within the data centre (northbound) or vice versa (southbound)

Traffic moves to/from endpoints on internal networks to nodes on the public cloud/internet.
Brings security concerns like data compromise, DDoS attacks, inadequate authentication.

East-West

The flows of traffic within the data centre itself.
The data that moves laterally between servers, storage systems, and applications within the data centre or across data centres.

East-west traffic is the traffic flow that occurs within a specific network, data center, or cloud environment.
North-south traffic is the traffic flow that occurs inbound or outbound between internal systems and external systems.
Access controls, micro-segmentation and isolation policies raise security.

BGP

Border Gateway Protocol (BGP) is the primary example of an exterior routing protocol.
This scenario describes a situation where network device updates caused problems with external communications.
If the device was a border router, maybe the update corrupted its BGP table, which is preventing proper routing to external systems.
The other options are all interior routing protocols: Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Interior Gateway Routing Protocol (IGRP), which were seemingly not affected since internal communications are taking place without issue.

Interior Gateway Routing Protocol (IGRP)
IGP / IGRP is a routing protocol that handles routing between the routers within an enterprise.

Domain 4 Carrier Sense Multiple access (CSMA)

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Carrier Sense Multiple Access (CSMA)

A **collision domain** is the set of systems that could cause a collision if they transmitted at the same time.
Systems outside a collision domain cannot cause a collision if they send at the same time.
This is important, as the number of systems in a collision domain increases the likelihood of network congestion due to an increase in collisions.

Developed to decrease the chances of collisions when two or more stations start sending their signals over the datalink layer. Requires that each **station first check the state** of the medium before sending.

- CSMA does not directly address collisions
- CSMA/CA (Collision **avoidance**) attempts to avoid collisions by granting only a single permission to communicate at any given time.
    - Example: Install a new wireless access point to extend your company's network into a newly opened portion of the building, someone raises the concern of interference between the existing Wi-Fi network and the new extension. CSMA/CA media access technology is used by 802.11 networks to manage collisions.

- CSMA/CD (Collision detection) responds to collisions by having each member of the collision domain wait for a short but random period of time before starting the process over.

No	CSMA/CD detection	CSMA/CA avoidance
1	CSMA/**CD** effective after a collision	CSMA/**CA** effective before collision
2	CSMA/**CD** is used in wired networks	CSMA/**CA** commonly used in wireless
3	Only **reduces** the recovery time	CSMA/**CA minimises** the possibility of collision
4	CSMA/**CD resends** the data frame whenever a conflict occurs	CSMA/**CA** first transmit the **intent** to send for data transmission
5	CSMA/**CD** used in **802.3** standard	CSMA/**CA** used in **802.11**
6	More efficient than simple CSMA.	Similar to simple CSMA in terms of efficiency

Domain 4 Token Passing Polling

- **Token** passing - Performs communications using a digital token. Once its transmission is complete, it **releases** the token to the next system.
    - Prevents collisions in ring networks
- **Polling** - performs communications using a **master-slave** configuration. The primary system polls each secondary system in turn whether they have a need to transmit data.
    - Used by **SDLC** (**synchronous** data link control)

SDLC - **Sync**hronous **Data Link Cont**rol by IBM

Domain 4 Network Segmentation

examples of network segmentation:

- **Intranet** - a private network that is designed to host the same information services found on the internet.
- **Extranet** - a section of an organisation's network that has been sectioned off to act as an intranet for the private network but also serves information to the public internet. A cross between internet and intranet
- **DMZ** - an extranet for public consumption is typically labelled a **demilitarised** zone (DMZ) or perimeter network. Used to control traffic and isolate static/sensitive environments. DMZ purpose is to host publicly accessible services.
- Subnet

- VLAN
  - hardware-imposed network segmentation that requires a routing function to support intersegment communications
  - A VLAN (virtual LAN) is a hardware-imposed network segmentation created by switches that requires a routing function to support communication between different segments.

CISSP Exam Cram Full Course (All 8 Domains) - Good for 2024 exam!

Microsegmentation

Microsegmentation is dividing up an internal network in numerous subzones, potentially as small as a single device, such as a high-value server or even a client or endpoint device.

- It can be implemented using ISFW's (internal segmentation firewalls).
- Transactions between zones are filtered.
- It can be implemented with virtual systems and virtual networks.

Static NAT can be appropriately and securely used to grant external entities access to resources positioned in a screened subnet or an extranet, especially when those resource hosts are using private IP addresses.

VLANs are typically not relevant to NAT because NAT operates at layers 3 and 4 and a VLAN exists at layer 2.
A VLAN (virtual LAN) is a hardware-imposed network segmentation created by switches that requires a routing function to support communication between different segments.

Reasons for Network Segmentation

- **Boosting perform**ance can improve performance through an organisational scheme in which systems that often communicate are located in the same segment, while systems that rarely or never communicate are located in other segments.
- **Reducing comm**unication problems reduces congestion and contains communication problems, such as broadcast storms, to individual subsections of the network
- **Providing security** can also improve security by **isolating** traffic and user access to those segments where they are authorized.

Network Segmentation Definitions

- Intranet
  - Private network that is designed to host the same information services found on the internet.
- Extranet
  - Section of an organization network that has been sectioned off to act as an intranet for the private network but also serves information to the public internet.
  - Cross between internet and intranet
- DMZ
  - Extranet for public consumption is typically labelled a demilitarised zone (**DMZ**) or perimeter network.

Physical Segmentation

- In-band management
  - Managing network devices through the same network that they are used to transmit user or application data
  - No physical segmentation - Less Secure
  - Subnets and VLANs
- Out-of-band management
  - Managing network devices using a dedicated network that is separate from the main network - More Secure
- Air-gapped
  - Extreme form of segmentation where one segment of the network is completely isolated from all others physically and logically.
  - Most Secure like utilities/municipalities.

Logical Segmentation

- Virtual Local Area Networks (VLANs)
  - A **switch** is a networking device that can be used to create digital virtual network segments (i.e., VLANs) that can be altered as needed by adjusting the settings internal to the device.
  - Allows a single physical network to be partitioned into multiple smaller logical networks
  - VLANs do not impose encryption on data or traffic. Encrypted traffic can occur within a VLAN, but encryption is not imposed by the VLAN.
  - VLANs do provide traffic isolation, traffic management and control, and a reduced vulnerability to sniffers.
  - VLAN hopping is a switch security issue
    - Prevent VLAN hopping; use physically separate switches.
- Virtual Private Networks (**VPNs**)
  - Create a private network network across public network infrastructure. Used to connect remote users or separate branches of a business to the main offices network. VPN Encrypts data in transit between two endpoints.
  - **Mutual auth**entication ensures that a server provides authentication before the client provides authentication. This prevents employees from revealing their credentials to rogue VPN servers.
- Virtual Routing & Forwarding (VRF)
  - Allows multiple instances of a routing table to coexist within the same router at the same time.
  - segmentation approach, also segment network routes
  - Virtual routing and forwarding (VRF) is used to allow multiple routing tables to exist in a virtual router, all working simultaneously as defined by network traffic rules.
- Virtual domain

- Ability to create multiple separate security domains within a single physical device (e.g. Firewall). Allows multiple virtual firewall instances within a single device.

Micro Segmentation

CISSP 2024 exam changes in DETAIL!

- segmenting the DMZ

Enhances security by minimising the lateral movement of attackers within a network, effectively creating a segmented. Compartmentalised architecture where each segment can have its own security policies and controls down to the workload level.

- Network overlays / Encapsulation
  - Creation of a virtual network that is abstracted or overlaid on top of the physical network.
- Distributed Firewalls
  - Instead of routing traffic through a central firewall, security policies are enforced at the virtual network interface level for each virtual machine (**VM**) or container
- Distributed routers
  - Similar to distributed firewalls, distributed routers operate at the workload level to control the flow of traffic between segments.
- IDS / IPS
  - Deployed strategically within the network to monitor and protect individual workloads or network segments rather than just at the perimeter.
- Zero Trust
  - Each micro-segment is treated as its own secure zone. Access to each zone is given only after the identity and context of the request have been thoroughly verified.

Domain 4 Edge Networks

Distributed networks that bring compute and storage resources physically closer to end users and devices on the "edge" of a network.

- **Ingress**
  - Traffic that **enters** a network. Typically generated by users accessing services hosted at the edge
- **Egress**
  - Traffic that **exits** a network. Data sent from the services at the edge back to the users or to another network
  - All packets leaving the ORG's network should have a source address from their public IP address block.
  - All packets leaving company's network should have a source address from her public IP address block.
  - Traffic shaping
- **Peering**

    - Direct **interconnection** of separate networks for the purpose of exchanging traffic. Instead of routing traffic through the broader internet (e.g. many ISP & content providers peer.)
    - Provide a direct path from her on-premises network to the cloud provider's services.
    - Peering allows you to connect directly to a cloud provider's network at a peering location where they provide edge facilities. This can reduce ingress/egress costs as well as provide direct paths to their networks and services.
    - connected servers they have hosted in a third-party data center to vendor-owned systems using fiber-optic cables for a direct connection to them.
    - Between edge network locations
    - Reduces latency costs and central bottlenecks
    - Peering can be either public peering, a connection through an Internet Exchange Point via a network connection, or private peering done directly with another entity in a colocation facility.
- east/west
    - refers to network traffic in the same zone or layer of a network.
- Caching
    - Caching popular content like video, audio and web pages.
    - Provides a better user experience in SaaS subscriber scenarios
- Compute
    - Granular compute functions, containerized, to provide low latency processing near end users and devices.
    - Known as edge computing
- Storage
    - Storage at multiple edge locations reduces latency for access and updates.
    - File shares synchronise

Egress Filtering
Block following traffic types on egress filtering policy (Outbound traffic):
- Traffic rapidly scanning many IP addresses on port 22
- Traffic with a broadcast destination
- Traffic with a source address from an external network

Domain 4 Bluetooth

Bluetooth (**IEEE 802.15**)
Bluetooth or IEEE 802.15 personal area networks (PAN) are another area of wireless security concern.
Connects headsets for cell phones, mice, keyboards, GPS and other devices.
Connections are set up using pairing where the primary device scans the 2.4 GHz radio frequencies for available devices.
Raspberry Pi
Pairing uses a 4-digit **code** often 0000 to reduce accidental pairings but is not actually secure.

Domain 4 Mobile System Attacks

- **Bluejacking** (annoyance) - high tech version of ding-dong-ditch, where savvy pranksters push unsolicited messages to engage or annoy other nearby bluetooth users by taking advantage of a loophole in the technology's messaging options.
- **Bluesnarfing** (**data theft**) - with bluesnarfing, thieves wirelessly connect to some early Bluetooth-enabled mobile devices without the owner's knowledge to download and alter phonebooks, calendars or worse.
- **Bluebugging** - attack that grants hackers **remote control** over the features and functions of a bluetooth device. This could include the ability to turn on the microphone to use the phone as an audio bug. Backdoor attack before returning control of the phone.

Mobile and wireless attacks to prevent use of long pin, 2FA, and disable discovery mode.
2FA fatigue, which relates to the weariness or complacency in using two-factor authentication

Bluejacking

Pranksters push unsolicited messages to engage or annoy other nearby Bluetooth through a loophole in Bluetooth messaging options.

Bluesnarfing

Data theft using bluetooth. Vulnerable devices are those using bluetooth in public places with devices in discoverable mode.

Bluebugging

Developed a year after bluejacking, creates a backdoor attack before returning control of the phone to its owner.
Eavesdropping or hacking

Domain 4 Wireless Technologies

Wifi wireless network speeds.

Version	Speed	Frequency
802.11	2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	200 - 600 Mbps	2.4 GHz

802.11ac	1 - 5.9 Gbps	5 GHz
802.11ax	9.6 Gbps	
802.11i		

802.11ax, which supports theoretical speeds up to 9.6 Gbps. 802.11ac (ad hoc mode) supports up to 5.9 Gbps, 802.11n supports up to 600 Mbps, and 802.11g is only capable up to 54 Mbps.
802.11ac operates in the 5 GHz range. The 900 MHz range has frequently been used for phones and non-Wi-Fi wireless networks as well as other amateur radio uses.
2.4 GHz is used by 802.11n.

802.11 technologies part of Wireless:

- WEP - uses a weak 24-bit initialization vector (IV)
- WPA3
- SAE
- 802.11i
- WPS

Enterprise extensions enable Wi-Fi networks to use a single SSID across multiple access points.

Scenario: Separate SSID
Use case of coffee shop with a single consumer-grade wireless router and a cable modem connected via a commercial cable data contract.
Ben intends to run an open (unencrypted) wireless network for his customers.
How should he connect his wireless business devices?
Solution
Set up a separate SSID using WPA3.
Many modern wireless routers can provide multiple SSIDs. Ben can create a private, secure network for his business operations, but he will need to make sure that the customer and business networks are firewalled or otherwise logically separated from each other.

Wireless Frequency

Orthogonal Frequency-Division Multiplexing (OFDM) offers high throughput with the least interference. OFDM employs a digital multicarrier modulation scheme that allows for a more tightly compacted transmission.
The modulated signals are perpendicular (orthogonal) and thus do not cause interference with each other.
This makes OFDM superior to FHSS and DSSS in throughput and interference.
OSPF is a routing protocol

Domain 4 SSID Broadcast

SSID
Wireless networks traditionally **announce** their SSID on a regular basis with a **beacon** frame.

When the SSID broadcasts, any device will automatically detect and connect to the network. Hiding the SSID is considered "**security through obscurity**" ; it is detectable through client traffic.
SSID = service set identifier

Domain 4 TKIP

TKIP

Temporal **Key Integrity prot**ocol was designed as the replacement for WEP without the need to replace legacy hardware.
Implemented into 802.11 wireless networking under the name WPA (Wi-Fi Protected Access)

Simultaneous authentication of equals (SAE)

A new Wireless Access Point (WAP) is being installed to add wireless connectivity to the company network. The configuration policy indicates that WPA3 is to be used and thus only newer or updated endpoint devices can connect. The policy also states that ENT authentication will not be implemented.
Simultaneous authentication of equals (SAE) mechanisms can be implemented.
WPA3 supports ENT (Enterprise Wi-Fi authentication, aka IEEE 802.1X) and SAE authentication.
WPA3's simultaneous authentication of equals (SAE) mode improves on WPA2's pre-shared key (PSK) mode by allowing for secure authentication between clients and the wireless network without enterprise user accounts.

Simultaneous Authentication of Equals (SAE) was introduced with WPA3 as an alternative to **preshared** keys. TKIP was introduced with the original version of WPA and was replaced with the AES-based CCMP in WPA2.

WPA3 uses SAE, or simultaneous authentication of equals, and does not send the password over the air. Traditional cracking methods used against previous versions of WPA and WPA2 no longer work. This is not because of complex passwords or MFA, but because of how the handshake's elements are created to avoid sending the password.

Domain 4 CCMP

CCMP
Counter Mode with **Ciph**er Block Chaining **Messa**ge Authentication Code **Prot**ocol
Created to replace WEP and TKIP/WPA
Uses AES (**Adva**nced **Encry**ption **Stan**dard) with a 128 bit key.
CCMP in wireless standard is the integrity method.
Used with WPA2, which replaced WEP and WPA

Domain 4 WPA2

WPA2
A New encryption scheme known as the counter mode with cipher block chaining message authentication code protocol (CCMP)
CCMP is based on the AES encryption scheme.

Domain 4 Converged Protocols

FCoE
iSCSI
VoIP
InfiniBand (remote direct memory access)
Compute Express Link (CPU to device / memory)

Fibre Channel & FCoE

Fibre Channel
A form of network data storage solution (IE. SAN (Storage area network) or NAS (Network attached storage) that allows for high speed file transfers
Understand FCoE
FCoE (Fibre Channel over Ethernet) is used to encapsulate Fibre channel communications over Ethernet networks

iSCSI

iSCSI is used for storage.
iSCSI (**Intern**et **sma**ll **comp**uter **sys**tem **inter**face) is a networking storage standard based on IP.

Infiniband over Ethernet

A Network protocol that allows remote direct memory access (RDMA) over an ethernet network
Provides lower latency and higher throughput than vs Ethernet alone.
InfiniBand engages in advanced scientific computations (HPC), demands of high-performance computing environments where rapid data processing and efficient data handling are crucial.

Infiniband over Ethernet is commonly used for purposes like building a high-performance computing cluster that requires **very high** bandwidth and very low latency, allowing direct memory access over Ethernet while providing high bandwidth and low latency.

Compute Express Link

Compute Express Link (CXL) is used for CPU to device and CPU to memory connections.

An open standard for high-speed, high-capacity CPU-to-device and CPU-to-memory connections.
CXL is the way Data-intensive AI research facilities meet demands of increasingly complex computational tasks, to improve the efficiency of connections between CPUs and high-speed peripherals, supporting the rapid processing requirements.
VoIP, iSCSI and CXL are converged protocols, which provide for SAN, voice, and AI/ML communication services.

Domain 4 Site Survey

The process of investigating the **prese**nce, strength and reach of **wireless** access points deployed in an environment.
Involves walking around with a portable wireless device, taking note of the wireless signal strength and mapping this on a plot or schematic of the building.

Domain 4 EAP PEAP LEAP

Extensible Authentication Protocol (EAP) is one of the three authentication options provided by Point-to-Point Protocol (PPP). EAP allows customized authentication security solutions.
EAP Methods

- **LEAP** (lightweight) is a **Cisco** proprietary alternative to TKIP for WPA. Developed to address deficiencies in TKIP before the 802.11i/WPA2 system was ratified as a standard.
- **PEAP** (Protected) encapsulates EAP methods **within a TLS tunnel** that provides authentication and potentially encryption.
- EAP-SIM
- EAP-FAST
- EAP-MD5
- EAP-POTP
- EAP-TLS
- EAP-TTLS
- **EAP** (extensible authentication protocol) an **auth**entication **framework**. Allows for new authentication technology to be compatible with existing wireless or point-to-point connections technologies.

RADIUS

EAP solutions support diverse authentication (VPN,Wifi, Dialup, RADIUS) methods across its network due to varying security requirements and device capabilities.

Domain 4 MAC Filtering

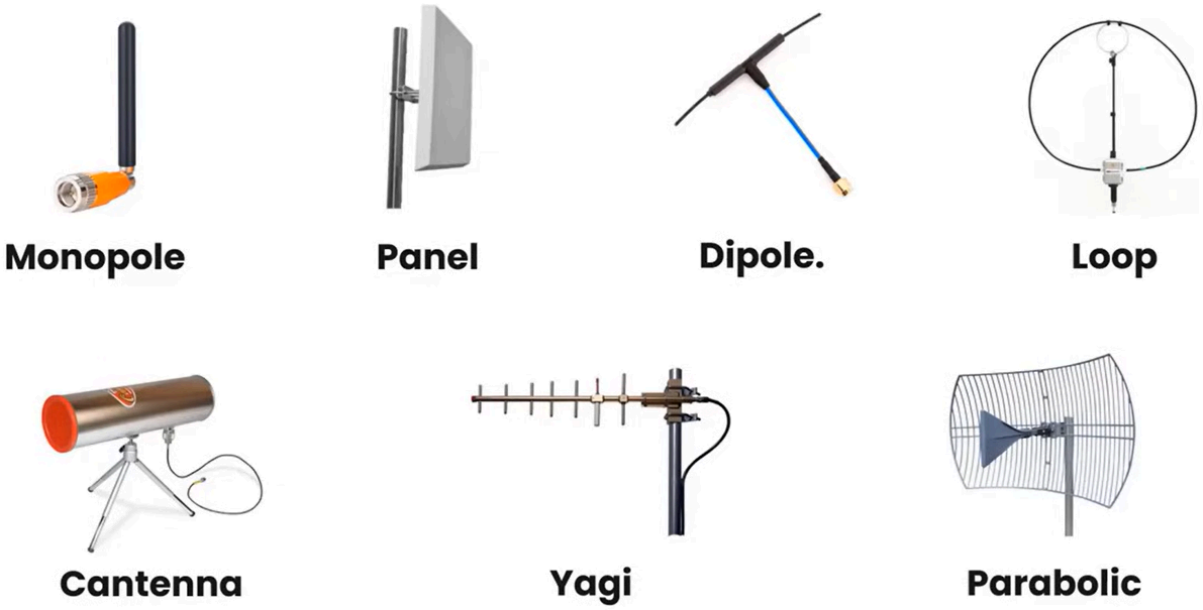
MAC Filtering a list of authorized wireless client interface MAC addresses.
Used by wireless access point to block access to all non authorized devices.

Domain 4 Captive Portals

Captive portals is an authentication technique that redirects a newly connected wireless web client to a portal access control page. Hotel wireless portal access web authentication redirect.
Farming Attack - Fake login on rogue wireless access point in public to farm login information credentials.
War walking detecting rogue wireless access point.

Example of Captive Portal
Susan knows that she will need to implement a Wi-Fi network for her customers and wants to gather information about the customers, such as their email address, without having to provide them with a wireless network password or key.
A captive portal is a popular solution that you may be familiar with from hotels and coffee shops. They combine the ability to gather data from customers with an open network, so customer data will not be encrypted. This avoids the need to distribute network passwords but means that customers must ensure their own traffic is encrypted if they are worried about security.

Domain 4 Antenna Types



- Loop - Omnidirectional if horizontally mounted
- Monopole - Omnidirectional perpendicular
- Dipole - Omnidirectional powerful
- Panel - focus one directional
- Parabolic - focus signals directional or weak signal sources
- Yagi - direction specific radio frequencies
- Cantenna - along direction focus

Domain 4 Network devices

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

- **Firewalls** are essential tools in managing and **controlling network traffic**. A firewall is a network device used to filter traffic.
- **Switch** repeats traffic only out of the port on which the destination is known to exist. Switches offer greater efficiency for traffic delivery, create separate **collision domains,** and improve the overall throughput of data. Usually **layer 2**, sometimes **layer 3.**
- **Routers** used to control traffic **flow** on networks and are often used to connect similar networks and control traffic flow between the two. They can function using statically defined routing tables, or they can employ a dynamic routing system **layer 3.**
- **Gateways** connect networks that are using **different network protocols**, also known as protocol translators, can be stand-alone hardware devices or a software service. Work at **layer 3.**
- **Repeaters**, concentrators and amplifiers used to strengthen the communication signal over a cable segment as well as connect network segments that use the same protocol **layer 1.**
- **Bridges** used to connect two networks (even networks of different topologies, cabling types, and speeds in order to connect network segments that use the same protocol **layer 2**
    - Organizations are most often concerned about **hotspots** creating an unsecured network connection into their secure network via laptops or other devices that are connected to them. **Bridging** a cellular connection to a network connection to the business's network creates a path that bypasses security controls. **Hotspots** could be used as rogue access points, but this is a less common scenario.
- **Hubs** used to connect multiple systems and connect network segments that use the same protocol. A hub is a multiport repeater. Hubs operate on **layer 1**
- **LAN extenders**, multilayer switches used to connect distant networks over WAN links.

Domain 4 LAN & WAN

WAN connections and communication links can include **private** circuit technologies and **packet** switching technologies.

Private circuit technologies use dedicated **physical circuits**.

- Dedicated or leased lines
- PPP point-to-point protocol
- SLIP serial line internet protocol
- ISDN integrated services digital network
- DSL digital subscriber line

PVC

A permanent virtual circuit (**PVC**) can be described as a **logical circuit** that always exists and is waiting for the customer to send data.
A PVC reestablishes a link using the same basic parameters or virtual pathway each time it connects.
PVC packet-switching networking system reuses the same basic parameters or virtual pathway each time it connects

Packet switching technologies use **virtual circuits** instead of dedicated physical circuits, efficient and cost effective.

- X.25 frame relay
- Asynchronous transfer mode (ATM)
- **Sync**hronous **Data Li**nk **Contr**ol (SDLC)
- High level data link control (HDLC)

Domain 4 Firewall Types

- **Static** packet filtering firewalls operate at **layer 3** and up filter traffic by examining data from a message header.
    - do not consider the context when applying filtering rules.
    - Static packet-filtering firewalls filter traffic by examining data from a message header. Usually, the rules are concerned with source and destination IP address (layer 3) and port numbers (layer 4).
    - Static packet filtering and circuit-level firewalls are both **stateless** and thus do not consider the context when applying filtering rules.
- **Applic**ation level firewalls operate at **layer 7** filters traffic based on single internet service protocol or application
    - An application-level firewall is able to make access control decisions based on the content of communications as well as the parameters of the associated protocol and software.
    - Stateful inspection firewalls (aka dynamic packet-filtering firewalls) enable the real-time modification of the filtering rules based on traffic content and context. An application-level gateway is a type of stateful firewall.
- **Circuit** level firewalls used to establish communication sessions between trusted partners. They operate at the session **layer 5**, example is **SOCKS**
    - Circuit-level firewalls are able to make permit and deny decisions in regard to circuit establishment either based on simple rules for IP and port, using captive portals, requiring port authentication via 802.1X, or more complex elements such as context- or attribute-based access control.
- **Stateful** inspection firewalls evaluate the state, session, or the context of network traffic.
    - **Stateful** inspection firewalls (aka **dynamic packet-filtering firewall**) enable the **real-time** modification of the filtering rules based on traffic content and context.
    - **Stateful** can watch traffic streams from end to end. **Aware** of communication paths and can implement various IP security functions such as tunnels and encryption.

    - Identifying unauthorized and forged communications.
    - Stateful inspection firewalls are able to grant a broader range of access for authorized users and activities and actively watch for and block unauthorized users and activities.
    - Stateful inspection firewalls make access control decisions based on the content and context of communications, but are not typically limited to a single application-layer protocol.

- **Deep packet inspection** firewalls are a filtering mechanism that operates typically at the application layer in order to filter the payload contents of a communication rather than only on the header values.
    - **Deep packet insp**ection firewall inspects and filters both the header and payload of a packet that is transmitted through an inspection point.
- **Stateless** watch network traffic and restrict or block packets **based on source** and destination addresses or other static values.
    - Not aware of traffic patterns of data flows.
    - Faster and perform better under heavier traffic loads
- **WAF**, web application firewall, filtering and monitoring HTTP traffic between a web application and the internet.
    - Protects web apps from **common attacks**, XSS, CSRF, SQL injection, etc.
    - Come with pre-configured with OWASP rulesets
- **NGFW**, deep packet inspection firewall that moves beyond port protocol inspection and blocking.
    - Adds application level inspection, intrusion prevention and brings **intelligence** from outside the firewall.
- **Unified Threat Mana**gement (**UTM**) composed of several security features in addition to a firewall.
    - **Multifunction device (MFD)**
    - **Includes** IDS, IPS, a TLS/SSL proxy, web filtering, QoS management, bandwidth throttling, NAT VPN anchoring and antivirus.
    - Common SMB **small medium busi**nesses.
    - QOS is the oversight and management of the efficiency and performance of network communications. Items to measure include throughput rate, bit rate, packet loss, latency, jitter, transmission delay, and availability.
    - Common in small and medium businesses (SMB)
- NAT **network address translation**
    - gateway allows private subnets to communicate with other cloud services and the internet but hides the internal network from internet users. NAT gateway has the network access control list (**NACL**) for the private subnets.
    - NAT hides the internal IP addressing scheme and enables the sharing of a few public internet addresses with a large number of internal clients.
    - NAT supports the use of the private IP addresses from RFC 1918 on an internal network.
    - Double NATing is not possible using the same IP range.
    - Double NATing isn't possible with the same IP range; the same IP addresses cannot appear inside and outside a NAT router. RFC 1918 addresses are reserved, but only so they are not used and routable on the Internet
- **Port address translation** (PAT)

    - Port address translation (PAT) is used to allow a network to use any IP address set inside without causing a conflict with the public Internet. PAT is often confused with network address translation (NAT), which maps one internal address to one external address.
- **Content URL filter** looks at the content on the requested web page and blocks requests depending on filters.
    - Used to block inappropriate content in the context of the situation.
    - Deep packet inspection
- **Open Source** licence freely available and allows access to the source code.
    - No vendor support.
    - Example is **pfsense**.
- **Proprietary** are more expensive but tend to provide more protection and more functionality and support at cost.
    - Example: **Cisco**, **Checkpoint**, **Palo Alto**, **Barracuda**
- **Hardware** purpose built network hardware, superior throughput versus software
- **Software** installed on your own hardware, flexibility to place firewalls anywhere.
    - Host based software is more vulnerable in some aspects.
- **Application** catered specifically application communications
    - example **NGFW**
    - **HTTP or Web traffic**
- **Host based** on a host OS such as Windows or Linux
    - Application installed on a host OS
- **Virtual as virtual network appliances** (VNA)
    - available from CSP (Azure, Google, AWS) and third party partners.
- TCP Wrapper, is an application that can serve as a basic firewall by restricting access based on user IDs or system IDs.

Host based Firewall Scenario:
A worker reports that they are unable to access an internal web application from their workstation. After you confirm that the worker has been assigned correct authorization, you review the logs from the workstation for clues.
Log shows drop TCP and UDP entries
Adjust the Host-based firewall to address this situation.

True Positive - Firewall blocks unpermitted traffic.
False Positive - Firewall blocks permitted traffic
False Negative - Firewall allows unpermitted traffic
True Negative - Firewall allows permitted Traffic

Example of a true positive report because the scan detected the vulnerability, and the vulnerability actually existed.

Fail open and Fail close
The Sample Case Scenario
Kim is troubleshooting an application firewall that serves as a supplement to the organization's network and host firewalls and intrusion prevention system, providing added protection against web-based attacks. The issue the organization is experiencing is that the

firewall technology suffers somewhat frequent restarts that render it unavailable for 10 minutes at a time.

A fail open configuration may be appropriate in the sample case. In the sample case configuration, the firewall would continue to pass traffic without inspection while it is restarting. This would minimize downtime, and the traffic would still be protected by the other security controls described in the scenario.

The **fail closed** approach prevents any activity from taking place during a system security failure and is the most **conservative** approach to failure management.
Fail open takes the opposite philosophy, allowing all activity in the event of a security control failure.

Domain 4 IDS & IPS

- Intrusion Detection System (**IDS**) - analyses whole packets both header and payload, looking for **known events**. When a known event is detected, a log message is **generated**.
    - Reports and alerts
    - Intrusion detection systems (IDSs) provide only passive responses, such as alerting administrators to a suspected attack.
- Intrusion Prevention System (**IPS**) - analyses whole packets, both header and payload, look for **known events**. When a known event is detected, the packet is **rejected**.
    - Take action

A pattern-matching IDS (also known as signature-based detection) has a **low** false-*positive* **rate**. A high false-negative rate isn't a benefit because it is not reporting on an active attack.
A pattern-matching IDS often **misses new attacks** because it doesn't have the signature for the new attacks. An IDS can detect an attack after it enters a network.
An intrusion **prevention** system (**IPS**) can prevent an attack from entering a network because it is placed **in-line.**

This is a false positive. The IPS falsely identified normal web traffic as an attack and blocked it.
A false negative occurs when a system doesn't detect an actual attack.

Domain 4 IDS Types

- **Behaviour** based - creates a baseline of activities to identify normal behaviour and then measures system performance against the baseline to detect abnormal behaviour.
    - Can detect previously unknown attack methods.
- **Knowledge** based signatures are similar to the signature definitions used by anti-malware software.
    - Only effective against known attack methods.

- **HIDS** host based intrusion detection system looking for known events. Log message is generated.
    - A HIDS only monitors a single system. (antimalware/Defender/DLP agent on workstation)
    - A drawback of some HIDSs is that they interfere with a single system's normal operation by consuming too many resources. The other options refer to applications that aren't installed on user systems.
- **HIPS** host based intrusion prevention system packet is rejected
- **NIDS** (network) log message
    - NIDS will monitor all traffic and raise alerts when it detects suspicious traffic.
- **NIPS** (network) packet is rejected.

Both **host** based (HIDS) and **network** based (NIDS) systems can be knowledge based, behaviour based or a **combin**ation of both.

You are installing a Network-based Intrusion Prevention System (NIPS) that management hopes will **reduce** incidents in the network. The setup instructions require you to configure it in line with traffic so that all traffic goes through it **before** reaching the internal network.

Domain 4 Modes of operation

- **Inline** aka **in-band** - on or **near** the firewall as an additional **layer** of security
- **Passive** aka **out-of-band** traffic does not go through the NIPS/NIDS. **Sensors(agents)** and collectors **forward alerts** to the NIDS.

Sensors and collectors

Can be placed on a network to alert NIDS of any changes in traffic patterns on the network. If you place a sensor on the internet side of the network, it can scan all of the traffic from the internet.

Heartbeat

A heartbeat sensor is a mechanism by which the communication pathway is either constantly or periodically checked with a test signal. If the receiving station detects a failed heartbeat signal, such as the loss of the constant signal or missing one or two interval checks, the alarm triggers automatically. This measure is designed to prevent intruders from circumventing the detection and alarm system by cutting power, cutting communication cables, or jamming radio signals.

Domain 4 Secure Network Design

- **Bastion** Host - computer that is exposed on the internet and has been hardened by removing all unnecessary elements, such as services, programs, protocols and ports. Bear necessities.

- **Screened** Host (most secure) - is a firewall-protected system logically positioned just **inside** a private network.
- **Screened** Subnet - similar to the screened host in concept, except a **subnet** is placed between two routers or firewalls and the bastion host is located within the subnet.
- **Proxy** server - functions on behalf of the client requesting service, masking the true origin of the request to the resource.
- **Honeypot** - lure bad people into doing bad things. Lets you watch.
    - Only **entice**, not entrap. You are not allowed to let them download items with enticement.
    - Allow download of a fake payroll HR file would be **entrapment**.
    - Goal is to **distract** from real assets and isolate them in a padded cell until you can track them down.
    - Honeypot - A system set up with intentional vulnerabilities;
- Honeynet -
    - A network set up with intentional vulnerabilities
    - HoneyNet presents the most complex decoy environment for an attacker to explore during an intrusion attempt.
    - A honeynet is a network of multiple honeypots that creates a more sophisticated environment for intruders to explore.
- Pseudo-flaw -
    - An intentionally designed vulnerability used to lure in an attacker
    - use on a honeypot system to consume an attacker's time while alerting administrators
- Darknet -
    - A monitored network without any hosts
    - A darknet is a segment of unused network address space that should have no network activity and, therefore, may be easily used to monitor for illicit activity.

Static NAT required to allow an external client to initiate a communication session with an internal system if the network uses a NAT proxy.

Endpoint Security

Endpoint security is the security concept that encourages administrators to install firewalls, malware scanners, and an IDS on every host.

Endpoint security systems' common challenge is the volume of data created.
Endpoint security solutions face challenges due to the sheer volume of data that they can create. When each workstation is generating data about events, this can be a massive amount of data. Endpoint security solutions should reduce the number of compromises when properly implemented, and they can also help by monitoring traffic after it is decrypted on the local host.

Endpoint detection and response (EDR) is a security mechanism that is an evolution of traditional antimalware products.

EDR seeks to detect, record, evaluate, and respond to suspicious activities and events, which may be caused by problematic software or by valid and invalid users. It is a natural extension of continuous monitoring focusing on both the endpoint device itself and network communications reaching the local interface.
Some EDR solutions employ an on-device analysis engine whereas others report events back to a central analysis server or to a cloud solution.
The goal of EDR is to detect abuses that are potentially more advanced than what can be detected by traditional antivirus or HIDSs, while optimising the response time of incident response, discarding false positives, implementing blocking for advanced threats, and protecting against multiple threats occurring simultaneously and via various threat vectors.

Managed detection and response (MDR) combines antimalware capabilities with a managed service that reduces the burden on the IT team. (ALIF support team in india SOC analyst)

Domain 4 Monitoring and Management

- Network Observability
  - Supports issue ID and troubleshooting
  - Collecting data and gaining visibility into the status and performance of network components and traffic flows
  - Ability to gain insights into the internal workings of a network
- Traffic Flow Shaping
  - Controlling the movement of packets within a network to optimise performance, prioritise critical traffic, and enforce policies
  - Volume and priorities
  - QOS, rate limiting, throttling to API's
- Capacity Management
  - Monitoring and planning network resources to ensure that they meet current and future demands
  - Tracking network utilisation and planning capacity expansion to meet future demands.
  - Utilisation and plan capacity
- Fault Detection and Handling
  - Identifying and diagnosing issues and handling appropriately (automatic remediation, manual intervention, **incident resp**onse, etc.)
  - Discovering, diagnosing and responding to problems like failed devices, connectivity losses, performance slowdowns.
  - Includes alerting and failover me be automated
- Other Monitoring and management
  - Performance monitoring, security monitoring, configuration management, log management, alerting and notification, reporting and analytics, etc.

Observability

- Aggregate and centralize data.
- Enable alerts for critical errors.
- Implement logging using a standardized format.

Observability focuses on the ability to see how an entire system, service, or environment is performing and behaving based on its external outputs.
That means that telemetry data—information about what components are doing—is critical and will be gathered using logs, metrics, and real-time analysis.
This means that centralizing and aggregating data, enabling alerts for critical errors, and implementing logging using standardized formats are all common practices.
Feedback loops are also important, allowing administrators and others to take action when problems or issues are detected.

Software-defined visibility (**SDV**) is a framework to automate the processes of network monitoring and response.

Domain 4 Network Attacks

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

- **Teardrop** attack is a DDOS attack that involves sending **fragmented** packets to a target. Since the machine cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target.
- **Fraggle** attack is a DOS attack that involves sending a large amount of **spoofed UDP** traffic to a routers broadcast address within a network. It is similar to a **Smurf attack** which uses **spoofed ICMP traffic** using a 3rd party network rather than UDP traffic to achieve the same goal.
- **Land** Attack is layer 4 DOS attack in which the attacker sets the source and destination information of a TCP segment to be the same. A vulnerable machine will crash or freeze due to packets being repeatedly processed.
- **SYN flood Attack** is a DOS attack in which an attacker sends a succession of SYN requests to a target in an attempt to consume enough server resources to make the target unresponsive.
    - Enable SYN-ACK spoofing at the firewall to prevent Syn Flood Attack
- **Ping of Death** employs an oversized ping packet, max allowed ping packets is **65536** bytes.
- MAC Flooding -
    - MAC flooding attack, which causes the switch to get stuck in flooding mode. This has taken advantage of the condition that the switch had weak configuration settings. The switch should have MAC limiting enabled in order to prevent MAC flooding attacks from being successful.
    - CAM table flooding

ICMP

Internet Control Message Protocol (ICMP) is primarily used to determine the health of a network or a specific link within a network. PING

TCP ACK Scan

TCP is a connection-oriented protocol, because it uses a handshake.

Know the **TCP 3-way handshake**, a process used in a TCP/IP network to make a connection between the server and client.

1. SYN ⟶
2. SYN-**ACK** ⟵
3. **ACK** ⟶

The **SYN** flagged packet is first sent from the initiating host to the destination host.
The destination host then responds with a **SYN/ACK** flagged packet.
The initiating host sends an **ACK** flagged packet, and the connection is then established.

The TCP ACK scan sends an ACK packet, simulating a packet from the middle of an already established connection.
The TCP ACK scan attempt to simulate an already open network connection.

The **FIN** flagged packet is not used in the TCP three-way handshake to establish a session; it is used in the session teardown process.

Modification Attacks

Captured packets are altered and then replayed against a system.
Packets are designed to bypass the restrictions of improved authentication mechanisms and session sequencing.
Countermeasure: digital signatures, packet checksum verification

ARP Poisoning/Spoofing

Sending ARP packets across the LAN that contain the attackers MAC address and the target's IP address.
ARP resolves IP addresses into MAC addresses.
ARP poisoning can use unsolicited or **gratuitous** replies—specifically, ARP replies for which the local device did not transmit an ARP broadcast request.

Countermeasure: packet filtering, arp spoofing software, TLS/SSH/HTTPS
ARP Poisoning with Cain & Abel tool.

PBX Threats, abuse and fraud

IP Phones can be entry points into your business network and are susceptible to data network attacks.
Use security features on VoIP systems to restrict system access, call types and call hours.
Ensure users delete sensitive voice mails when they are no longer needed.
Countermeasures: use the same precautions and security controls you would employ to protect a typical computer network.
PBX attackers are called "**phreakers**"
The TEMPEST program creates technology that is not susceptible to **Van Eck** phreaking attacks because it reduces or suppresses natural electromagnetic emanations.

Remote dialling is a VoIP PBX concern.
Changing default passwords on PBX systems provides the most effective increase in security.
First step after installing software: Change the default credentials.

PBX systems typically do not support encryption, although some VoIP PBX systems may support encryption in specific conditions.

VOIP

In most cases, VoIP is only able to be encrypted between compatible VoIP solutions, which is usually only those products provided by the same VoIP vendor. In this situation, the only example that could provide a fully encrypted VoIP connection is when using a VoIP app to call a VoIP desk phone.
But the assumption is both these VoIP endpoints are from the same VoIP vendor or provider.

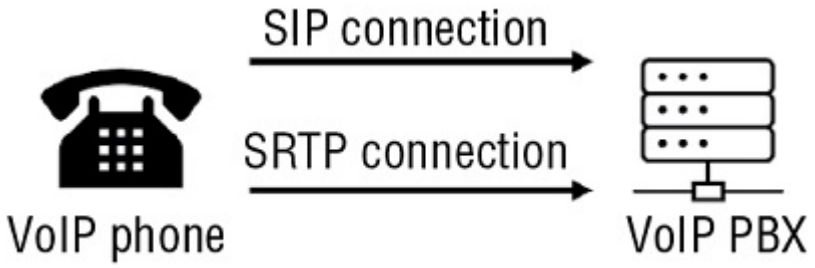
Caller ID falsification and vishing are VoIP security concerns.

VoIP Protocols:
- H.323
- SIP
- RTP
- SRTP

VoIP Attacks:
- Eavesdropping
- Denial of Services (DoS)
- Call ID Spoofing

VoIP Phones potential risks when deployed on same switches as desktop and server systems:
This could allow for 802.1x authentication falsification as well as VLAN and VOIP hopping.
Use VLANs to separate voice and video from other network traffic.

Unencrypted SIP Design Scenario
VoIP environment configuration
diagram shows the use of the Session Initialization Protocol (SIP) instead of SIP Secure (SIPS)



* The session initialization connection is unencrypted and could be viewed.

Diagram shows the use of the Session Initialization Protocol (SIP) instead of SIP Secure (SIPS), meaning that SIP is not encrypted. Fortunately, the voice data via the Secure Real-time Transport Protocol (SRTP) is encrypted. Mikayla should look into using SIPS in addition to SRTP.

SIPS and SRTP are appropriate for a VoIP environment but are not generally a complete solution for a modern multimedia collaboration platform like Microsoft Teams, Zoom, or WebEx.

SIPS ensure that VoIP session initialization is secure.
Use TLS for all traffic for the collaboration platform regarding employees working from home. (WFH)

Types of attacks VoIP call managers and VoIP phones most likely to be susceptible:

- DoS
- host OS attacks

Call managers and VoIP phones can be thought of as servers or appliances and embedded or network devices. That means that the most likely threats that they will face are denial-of-service (DoS) attacks and attacks against the host operating system.

Teams/Zoom Bombing Attacks

Enabling waiting rooms allows hosts to allow only intended attendees for events and meetings. Unfortunately, passcodes are easily shared, resulting in Zoom bombing despite the security they appear to offer. Meeting links are automatically generated and randomized, preventing brute forcing, and HTTPS is enabled by default for meetings.

Remote Access and Telecommuting Techniques

Second, screen scraping is a technology that allows an automated tool to interact with a human interface. For example, some standalone data-gathering tools use search engines in their operation. However, most search engines must be used through their normal web interface. Example: Google.

For Example, Telecommuting clients use many remote access techniques to establish connectivity to the central office LAN:

- Remote node operation aka VPN's
- Remote Control
- Screen scraping
- Service Specific

The Remote Desktop Protocol (RDP) and Secure Shell (SSH) are modern approaches to remote access that include encryption features.

Remote Access Policy Methods

- Using a modem to dial up directly to a remote access server
- Connecting to a network over the internet through a VPN
- Connecting to a WAP
- Connecting to a terminal server system, mainframe, VPC, VDI, or VMI through a thin-client connection
- Connecting to an office-located PC using a remote desktop service
- Using cloud-based desktop solutions

Above list are methods of connection that are considered remote access by the organization.

Domain 4 DNS Attack

Footprinting

Gather DNS domain names and IP addresses.

DNS Shadowing

Create bogus subdomains

DNSSEC

Zone signing validate zone transfers and is done with digital signatures
DNSSEC mitigate Pharming attacks.
Pharming attacks are DNS cache poisoning attacks that attempt to modify a DNS cache by providing invalid information to a DNS server.

DNS Poisoning

Attacker alters the domain-name-to-IP-address mappings in a DNS system.
May redirect traffic to a rogue system OR perform denial-of-service against the system.
man-in-the-middle attacks, which are normally waged through DNS poisoning

Scenario DNS Cache Poison
A user is attempting to access a website, but when they type the FQDN into the address bar of their browser, a different site appears. The user opens a command prompt and performs an nslookup query to obtain the IP address their system is receiving when resolving the FQDN of the website.
The user then checks with a colleague who is working from home (WFH) and they get a different IP address and they have no issue accessing the website. The user checks their IP configuration and sees that the correct DNS server is listed as their query target. The user runs ipconfig /flushdns and then the ipconfig /displaydns commands but does not see the correct website's identity listed in the final result.
Result: Local DNS caching server poisoning

DNS Spoofing

Cache poisoning

Attacker sends false replies to a requesting system, beating the real reply from the valid DNS server.

DNS countermeasures: allow only authorized changes to DNS, restrict zone transfers, verified forwarders and log all privileged DNS activity.

Homograph Attack

Leverages similarities in character sets to register phoney international domain names (IDNs) that appear legitimate to the naked eye.
Counter: update your browser regularly.
Client-side: modern browsers that use punycode
Server-side: policies implemented by ICANN

Hyperlink Spoofing

Similar to DNS spoofing
Can take the form of DNS spoofing or can simply be an alteration of the hyperlink URLs.
The same precautions are used against DNS spoofing, and services that mask and test links in **detonation** chambers. (sandbox)
Microsoft ATP

Domain 5 Identity and Access Management

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!
CISSP 2024 exam changes in DETAIL!
CISSP Exam Cram - 2024 Addendum

- Control physical and logical access to assets
- Manage identification and authentication of people devices and services
- Federate identity with a third party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle
- Implement authentication systems
    - OpenID connect (OIDC) / open Authorization (OAUTH)
    - Security Assertion Markup Language (SAML)
    - Kerberos
    - Remote Authentication Dial-in User Service (RADIUS) / Terminal Access Controller Access Control System Plus (TACACS+)
- Certificate Authentication

identity and access controls to assets

- Information assets - Discretionary access controls (Microsoft File Servers)
- Systems - User accounts with multifactor authentication (MFA)
- Mobile Devices - Biometric authentication (Facial, Finger print)
- Facilities - Badge readers (Physical Building access)
- Partner Applications - Federated identity management (Federation Services)

- Cloud Services (e.g. IaaS, Paas, SaaS, Email, Hosting, Managed IT)

Domain 5 Certificate-based Authentication

Digital certificates may be used as an authentication technique for user, service and device identities.
Certificates used in this process are similar to those that you use to secure websites.
Certificates have both a public and private key.
Certificates usually issued by a certification authority in a public key infrastructure. (**PKI**)

See Domain 3 Security Architecture and Engineering section - Asymmetric cryptography.

Domain 5 AAA Protocols

The required elements of accountability, as defined in AAA services, are as follows:

- identification (which is sometimes considered an element of authentication, a silent first step of AAA services, or represented by IAAA),
- authentication (i.e., identification verification), authorization (i.e., access control), auditing (i.e., logging and monitoring), and accounting.

* Privacy is not necessary to provide accountability.

IAAA

Privacy is not necessary to provide accountability.
The required elements of accountability, as defined in AAA services, are as follows:
identification (which is sometimes considered an element of authentication, a silent first step of AAA services, or represented by IAAA), authentication (i.e., identification verification), authorization (i.e., access control), auditing (i.e., logging and monitoring), and accounting.

Below items provide non-repudiation:

- Identification
  - Unique username/token
- Authentication
  - Type 1 - something you **know**: Passphrase, Password or PIN (SFA Single Factor authentication)
  - Type 2 - something you **have**: Card or **token**
    - Yubikey or Titan Security Key is **token** type of Type 2 authentication factor
  - Type 3 - something you **are**: Biometrics, eye or fingerprint
  - Type 4 - somewhere you **are at:** Location - callback to a landline phone number is an example of a “somewhere you are” factor because of the fixed physical location of a wired phone.
  - MFA - Multi factor authentication combines multiple above types of authentication!

- Authorization
  - Rights and Access to an objects (User Groups)
  - MAC, RBAC, Rule or DAC types
- Auditing
  - Monitoring actions and events tracking subjects
  - Log files
- Accountability
  - Subject is principle that individual is entrusted for their actions
  - Ownership of an event

Several protocols provide centralised **auth**entication, **authoriz**ation and **accounti**ng services.
Network access server is a RADIUS server, and the RADIUS server provides **AAA** services.

- RADIUS (remote access)
  - uses UDP and encrypts the password only
- TACACS+ (admin access to network devices)
  - uses TCP and encrypts the entire session.
  - TACACS+ and RADIUS are primarily used on-site for authentication and authorization for network devices.
  - TACACS+ is the most modern version of TACACS, the Terminal Access Controller Access-Control System. It is a Cisco proprietary protocol with added features beyond what RADIUS provides, meaning it is commonly used on Cisco networks.
- Diameter (4G) is based on RADIUS and improves many of the weaknesses of RADIUS but diameter is not compatible with RADIUS.

The **network access server** is the **client** within a **RADIUS** architecture.

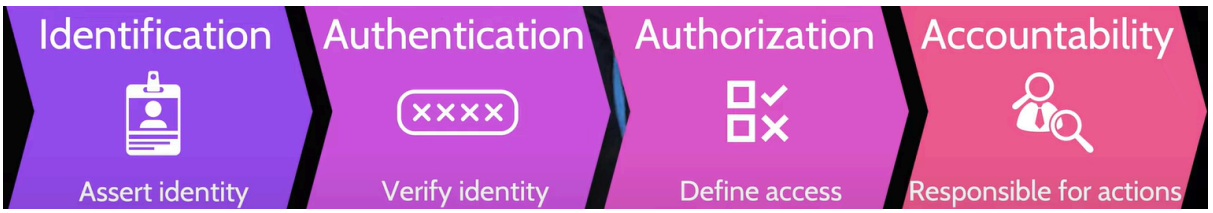
The RADIUS server is the **authen**tication server, and it provides authentication, **authoriz**ation, and **account**ing (**AAA**) services.
The network access server might have a host firewall enabled, but that isn't the primary function.

RADIUS combines authentication and authorization in one process and accounting in a second process.

Implement encryption for RADIUS:
RADIUS supports TLS over TCP. - Implement RADIUS over TCP using TLS for protection.
RADIUS does not have a supported TLS mode over UDP.

Access Control Services

- ➢ Identification - assert identity
- ➢ Authentication - verify identity
- ➢ Authorization - Define access
- ➢ Accountability - Responsible for actions (Accounting)



Factors of Authentication

1. Knowledge
2. Ownership
3. Characteristic

Domain 5 Active Directory

Trusts

A trust that allows one forest to access another's resources without the reverse being possible is an example of a one-way trust.

Scenario Forest Trusts
Jim wants to allow a partner organization's Active Directory forest (B) to access his domain forest's (A)'s resources but doesn't want to allow users in his domain to access B's resources. He also does not want the trust to flow upward through the domain tree as it is formed. What should he do?
Solution:
Set up a one-way nontransitive trust.
Since Jim doesn't want the trust path to flow as the domain tree is formed, this trust has to be nontransitive.

NTLM

Pass-the-hash attack mitigation
Prevent the pass-the-hash attack in windows by Disable NT LAN Manager (NTLM).
Pass-the-hash = NTLM
Pass the hash attack : An attacker used a tool to exploit a weakness in NTLM. They identified an administrator's user account. Although the attacker didn't discover the administrator's password, they did access remote systems by impersonating the administrator.

Kerberos

Primary purpose is **authen**tication as it allows users to prove their identity.
Mutual authentication is an authentication system in which hosts offer proof of identity to each other. Kerberos is an example of a mutual authentication system.

Mutual authentication can prevent a client from divulging information to a rogue server.

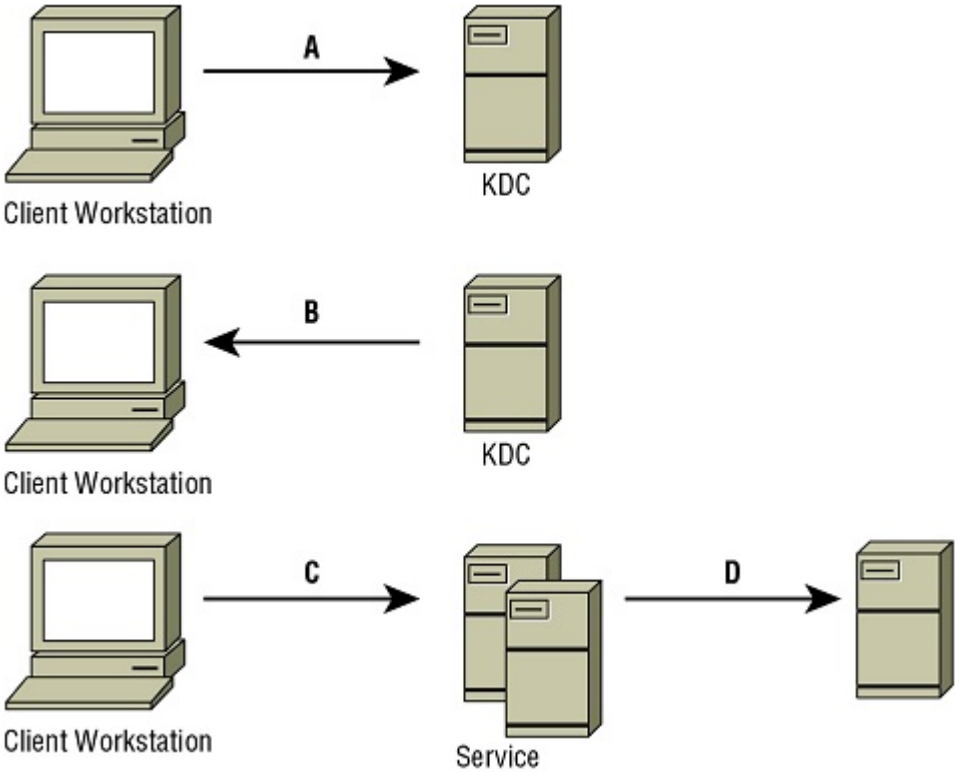
Also provides a measure of confidentiality and **integrity** using **symmetric** key encryption, but these are not its primary purpose.
Kerberos **does not** include logging capabilities so it does not provide accountability.

Common kerberos **attacks** include: ***replay***, pass-the-ticket, golden ticket, and kerberoasting.
Active Directory
Pass-the-hash = **NTLM (Legacy Windows protocol)**
Pass-the-ticket = **Kerberos**
Kerberos uses port 88.

- KRBTGT
  - The KRBTGT account allows the creation of golden tickets.
- Service Ticket (ST)
  - Authorization
  - Service ticket (**ST**) in Kerberos authentication provides proof that a subject is **authorized** to access an object.
- Ticket Granting Ticket (TGT)
  - A TGT (ticket-granting ticket) provides proof that a subject has authenticated with a key distribution center (KDC) and can request network service access.
  - The **TGT** does verify the existence of a user account, but it does much more.
  - It proves the user has authenticated and can request a ticket.
  - TGTs are ***not*** used for accounting.

- **Ticket Granting Service (TGS) - Authorization**
  - **TGS**, or ticket-granting service
  - on the same server as the KDC
  - receives a TGT from the client. It validates the TGT and the user's rights to access the service they are requesting to use. The TGS then issues a ticket and session keys to the client.
- Ticket
  - A ticket (not a ticket-granting ticket) is an encrypted message that proves a user can access an object.

Scenario - Kerberos authentication and authorization



Step C: The client workstation supplies it in the form of a client-to-server ticket and an authenticator.
Step A Client wants to access the resource, client sends its existing valid **TGT** to the KDC and requests access to the resource.

When a client connects to a service server (SS), it sends the following two messages:

1. The client-to-server ticket, encrypted using the service's secret key
2. A new authenticator, including the client ID and timestamp that is encrypted using the client-server session key

The server or service that is being accessed receives all of the data it needs in the service ticket. To do so, the client uses a client-to-server ticket received from the ticket granting service.

The client workstation supplies it in the form of a client-to-server ticket and an authenticator, to validate the ticket of service being accessed.

Configuring a central computer to synchronize its time with an external NTP server and all other systems to synchronize their time with the NTP will likely solve the problem and is the best choice of the available options. Kerberos requires computer times to be within 5 minutes of each other and the scenario, along with the available answers, suggested the user's computer is not synchronised with the Kerberos server. Kerberos uses AES.

Kerberos, *RADIUS*, ADFS, and TACACS+ are all commonly used single sign-on solution used for internal networks

Countermeasure for spoofed logon screens:

The best prevention is to have secure endpoints, where these fake logon screens cannot be implemented.

Service Accounts

Accounts used by applications, services, or systems to interact with other resources, services, or databases without human intervention.
Interactive login for a service account is a critical warning sign, either of compromise or bad administrative practices.

Securing service account
The most important step in securing service accounts is to ensure that they have only the rights that are absolutely needed to accomplish the task they are designed for.
Disabling interactive logins is important as well and would be the next best answer.
Limiting when accounts can log in and using randomized or meaningless account names can both be helpful in some circumstances but are far less important.

Service accounts management
Process of creating, configuring, monitoring, and maintaining service accounts.
Focus on ensuring accounts are secured, reducing the risk of unauthorized access or misuse.

Service Account aka “Service Principal”
When software is installed on a computer or server, it may require privileged access to run and access other resources (system , data).
Essentially a lower-level administrator account without human intervention, and the service account fits the bill.
A service account is a type of administrator account used to run an application. Example: account to run an antivirus application.

In the cloud:
A similar concept exists for cloud resources (like VMs) that provides an identity for that resource to access other resources, like data.
CISSP Exam Cram - 2024 Addendum
Major CSPs all have service accounts, though the name varies:
- Managed identity (Azure)
- Service Role (AWS)
- Service account identity (GCP)

Least privilege and lifecycle management are important for service accounts.

Domain 5 Authorization Mechanisms

- Role-BAC - Used to assign permissions based on job or function
- Rule BAC - Permissions or rights are granted based on parameters like an IP address, time, or other specific details that match requirement
- DAC - model where subjects with the proper rights can assign or pass those rights to other subject

- ABAC - policy-based access control, this model uses information about the subject to assign permission
- MAC - Access control model enforced by the operating system

Need to Know

The principle ensures that subjects are granted access only to what they need to know for their work tasks and **job func**tions.
Subjects with **clearance** to access are only granted if they actually need it to perform a job.
Need to know, security principle involves the knowledge and possession of sensitive material as an aspect of one's occupation.

Clearance and need to know, before granting access to users.

The principle of need-to-know ensures that individuals are granted access to information only if they have a specific requirement or legitimate need to access that information in order to perform their job tasks. This principle is closely related to the concept of least privilege but specifically emphasises that access should be restricted to only the information that is necessary for an individual to fulfil their job responsibilities.

processing an access request
Before granting any user access to information, verify that the user has an appropriate security clearance as well as a business need to know for the information in question.

Least Privilege

Ensures that subjects are granted only the privileges they need to perform their work tasks and **job func**tions. Sometimes lumped together with need to know. The only difference is that least privilege will also include **rights to take action** on a system.

Separation of Duties and Responsibilities

Ensures that sensitive functions are **split into tasks** performed by two or more employees.
Help prevent fraud and errors by creating a system of checks and balances.

The matrix shown in the figure is known as a **segregation of duties matrix.**

Roles/Tasks	Application Programmer	Security Administrator	Database Administrator	Database Server Administrator	Budget Analyst	Accounts Receivable	Accounts Payable	Deploy Patches	Verify Patches
Application Programmer		X	X	X					
Security Administrator	X		X	X	X	X	X	X	
Database Administrator	X	X		X					
Database Server Administrator	X	X	X						
Budget Analyst		X				X	X		
Accounts Receivable		X			X		X		
Accounts Payable		X			X	X			
Deploy Patches		X							X
Verify Patches								X	
	Potential Areas of Conflict								

A scenario describes separation of duties — not allowing the same person to hold two roles that, when combined, are sensitive.

While **two-person control** is a similar concept, it does not apply in this case because the scenario does not say that either action requires the concurrence of two users.
Two qualified administrators must agree to retrieve emergency credentials, is an example of **two-person control**, where two people must concur to perform a sensitive action.

Domain 5 Modern Approach to Least Privilege

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

provisioning lifecycle

If Alex hires a new employee and the employee's account is provisioned after HR manually inputs information into the provisioning system based on data Alex provides via a series of forms, then **workflow-based provisioning** has occurred.

Provisioning that occurs through an established workflow, such as through an HR process, is **workflow-based account provisioning.**
If Alex had set up accounts for his new hire on the systems he manages, he would have been using **discretionary account provisioning.**
If the provisioning system allowed the new hire to sign up for an account on their own, they would have used **self-service account provisioning.**
if there was a central, software-driven process, rather than HR forms, it would have been **automated account provisioning.**

Just-in-time (JIT) (PIM, PAM)

Just-in-time provisioning creates a user account after accessing a third-party website. JIT systems commonly use SAML, but SAML is used for many other purposes.
Allows temporary elevation of privilege (usually time-limited) as it's needed, **revoking** privilege at the end of the allowed window.
Sometimes implemented through ephemeral accounts or a broken and removed access strategy.
lasting for a very short time = ephemeral
Broken strategy
HR Employee Scenario:
An organization has decided to outsource the management of its benefit plans. Management wants to minimize the administrative workload when implementing this.
Just-in-time (JIT) provisioning will create the accounts automatically the first time the employee accesses the benefits site.

Example JIT
The company that Cameron works for uses a system that allows users to request privileged access to systems when necessary. Cameron requests access, and the request is pre-approved due to his role. He is then able to access the system to perform the task. Once he is done, the rights are removed.
Solution
Cameron is using a just-in-time (JIT) system that provides the access needed when it is needed.

Domain 5 Identification and Authentication

Identification
Subjects claim an identity, and identification can be as simple as a **username** for a user.
Authentication
Subjects **prove** their identity by providing authentication credentials such as the matching **password** for a username.

Subject and Object

The subject is active and is always the entity that receives information about, or data from, the object. A subject can be a user, a program, a process, a file, a computer, a database.
The object is always the entity that provides or hosts information or data.
The roles of subject and object can switch.

Domain 5 Authorization and Accountability

Authorization

After authenticating subjects, systems **authorize** access to objects based on their proven identity.

Accountability

Auditing logs and audit trails record events including the identity of the subject that performed the action. Historical records
Authentication is necessary to ensure a network supports **account**ability.

Identification + authentication + auditing == Accountability

Scenario:
An administrator has been tasked with reviewing the Human Resources server log files looking for malicious activity.
Accountability is possible by reviewing logs and tracking user activity.
Accountability depends on strong identification and authentication methods, but reviewing logs doesn't provide identification or authentication.
Audit trails are the entire body of data gathered by event logging required to enable accountability.

Domain 5 Primary Authentication Factors

Password-less Authentication

Passwordless method of verifying a users identity without requiring them to enter a password
Relies on alternative forms of verification, such as biometrics, security tokens or a mobile device.

Passwordless Example
Angela uses her smartphone's built-in biometric authentication and an application provided by her employer to log into her account.
Passwordless authentication leverages applications and capabilities such as built-in biometric authentication mechanisms.

Advantages of password-less authentication

- Increased security
- User convenience
- Reduction of phishing

Challenges of password-less authentication
- Dependency on devices
- Biometric Concerns
- Implementation costs

Domain 5 Credential Management System

Credential Management API System

The Credential Management application programming interface (API)
Credential Management Systems
The Credential Management application programming interface (API) will fulfil the company needs to allow customers to be automatically logged on when they visit. API management system was published by the World Wide Web Consortium (W3C) as a working draft in January 2019. Service authentication refers to using service accounts to run services or applications. SSO allows users to log on once and access multiple resources. SSO isn't used for a single site.
Session management is used to close inactive sessions.

Hardware Security Modules

Hardware Security Modules, or HSMs, are the most secure way to store keys associated with a CMS (credential management system).
Hardware Security Modules provide enhanced key management capabilities and are often required to be FIPS certified. In addition to these advantages, an **HSM** can improve cryptographic performance for the organization due to dedicated hardware designed for just that purpose.
Long keys and using AES-256 are good practices, but an HSM provides greater security and will require appropriate cryptographic controls already.

Password Vault

AKA Password Manager

Application designed to store and manage credentials.
Typically, credentials are kept in an encrypted database and protected by a master password.

Stored locally on the device and stores passwords so the user does not need to remember them.
Uses strong encryption (eg. AES-256) for secure storage.
Only as secure as the owner password that is used to protect the vault itself.
Typically uses multi-factor authentication.

Password Vault, securely store and manage passwords for systems including service accounts and other rarely used administrative credentials.

Key Management System (KMS)

Azure key vault, aws kms, gcp cloud kms vault
CSPs offer a cloud service for centralised secure storage and access for application secrets called a vault.
A secret is anything that you want to control access to, such as **API keys, passwords, certificates, tokens, or cryptographic keys.**
Service will typically offer programmatic access via API to support DevOps and continuous integration/continuous deployment (CI/CD)

Access control at vault instance-level and to secrets stored within.

Secrets and keys can generally be protected either by software or by FIPS 140-2 level 2 validated HSMs, or **FIPS 140-3.**

MFA

See Domain 3 Factors of Authentication
Something you **know** (Pin or password)
Something you **have** (Trusted device, Token)
Something you **are** (biometric)

Two-factor authentication requires users to authenticate with two independent proofs of identity.

Example of two-factor authentication
Requiring users to authenticate with something they know (such as a password) and something they have (such as a hardware token) provides two-factor authentication and is the strongest method of those listed.

Multi Factor Authentication

Includes two or more authentication factors
More secure that using a single authentication factor
Passwords are the **weakest** form of authentication
Password policies help increase their security by **enforcing complex**ity and history requirements
Smartcards include microprocessors and cryptographic certificates
Tokens create **one time** passwords.
Biometric methods identify users based on characteristics such as fingerprints.

SMS Messages
SMS messages are not encrypted, meaning that they could be sniffed and captured. While using two factors is more secure than a single factor, SMS is one of the less secure ways to implement two-factor authentication because of this. SMS messages can be spoofed, can be received by more than one phone, and are typically stored on the recipient's phone. The primary threat here, however, is the unencrypted SMS message itself.

MFA Prevents

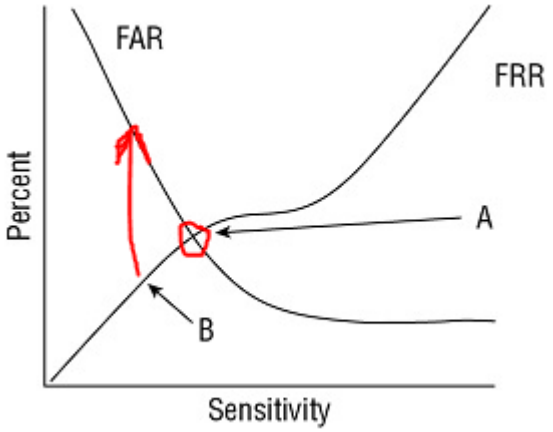
- Phishing
- Spear phishing
- Keyloggers
- Credential Stuffing
- Brute force and reverse brute force attacks
- Man-in-the-middle (MITM) attacks

Biometric Authentication Mechanism

The false acceptance rate (FAR) is the rate at which the system inadvertently admits an unauthorized user, while the false rejection rate (FRR) is the rate at which the system inadvertently rejects an authorized user.
Both the FAR and FRR may be modified by adjusting the sensitivity of the system.
The crossover error rate (**CER**) is the point where both the false acceptance rate and the false rejection rate **cross**.
The CER is less subject to manipulation and is, therefore, the best metric to use for evaluating systems.

Type 1 errors occur when a valid subject is not authenticated.
Type 2 errors occur in biometric systems when an invalid subject is incorrectly authenticated as a valid user. Nobody, except the actual customer should be validated when fingerprints are scanned for banking account authentication.

point A - CER - Crossover error rate in graph & calculations at **point A** in below image:
Point B - false acceptance rate (FAR) will be very high, whereas the false rejection rate (FRR) is relatively low.



FAR = false acceptance rate
FRR = false rejection rate

A higher FRR instead of a higher FAR, When security is more important than usability.

Assess other biometric systems to compare them, if the FAR and FRR shown in this diagram do not provide an acceptable performance level for his organization's needs.

CER is a standard used to assess biometric devices. If the CER for this device does not fit the needs of the organization, Ben should assess other biometric systems to find one with a

lower CER. Sensitivity is already accounted for in CER charts, and moving the CER isn't something Ben can do. FRR is not a setting in software.

Concerned about the FAR associated with her biometric technology, then add a second factor to the biometric access.
Adding a second factor can ensure that users who might be incorrectly accepted are not given access due to a higher than desired false acceptance rate (FAR) from accessing a system.
The CER is the crossover between the false acceptance and false rejection rate (FRR) and is used as a way to measure the accuracy of biometric systems.
Changing the sensitivity to lower the FRR may actually increase the FAR.
Replacing a biometric system can be expensive in terms of time and cost.

hand geometry scanners
A second factor should be added because they are not a good way to reliably distinguish individuals.
Hand geometry scanners assess the physical dimensions of an individual's hand but do not verify other unique factors about the individual, or even verify if they are alive. This means that hand geometry scanners should not be implemented as the sole authentication factor for secure environments. Hand geometry scanners do not have an abnormally high FRR and do not stand out as a particular issue from an accessibility standpoint compared to other biometric systems.

Authenticator App

Authenticator App: Use cases and availability
An authenticator app can be used as a primary form of authentication to sign into popular cloud identities.
Can also be used as an additional verification option during self-service password reset or multifactor auth (MFA) events.

Synchronous soft tokens, such as Google Authenticator mobile app, use a time-based algorithm that generates a constantly changing series of codes.

Example:
To use Microsoft Authenticator, a user must download the phone app and register their account.
The app is available for Android and iOS.
Additional verification = 2nd factor of authentication.

Domain 5 Biometrics

A method of authentication using an individual's physical characteristics, which are unique to the individual.
The registration process is used for internal employees and to collect biometric data.

Biometric systems using a **one-to-many** search provide **identific**ation by searching a database for a match.

Biometric systems using a **one-to-one** search provide **authen**tication.
Biometric systems do **not** provide **authoriz**ation or **accounta**bility.

Fingerprint Scanner

Fingerprint scanners are now very common, and used not only in MFA, but various travel, financial and legal situations.
Following accurately identify fingerprint **minutiae**:

- Ridges
- Bifurcations
- Whorls

Fingerprints can be counterfeited or duplicated.
It is not possible to change fingerprints.
Users will always have a finger available (except for major medical events), so they will always have a fingerprint available.
It usually takes less than a minute for registration of a fingerprint.

Retina Scanner

With appropriate lighting, the retina can be accurately identified as the blood vessels of the retina absorb light more readily than the surrounding tissue.
Though retina scans are more accurate than *iris* scans, they are invasive and can reveal medical conditions such as pregnancy.

Iris Scanner

Confirms the identity of the user by scanning of their iris
Both retina and iris scanners are physical devices.
Iris scanners are the most accurate, noninvasive biometric control from options.

Iris scans have a longer useful life than many other types of biometric factors because they do **not** change throughout a person's life span (unless the eye itself is damaged).
Iris scanners can be fooled in some cases by high-resolution images of an eye.
Iris scanners are **not** significantly cheaper than other scanners.

Voice Recognition

The voice patterns can be stored in a database and used for authentication.
Biometric authentication, "something you are"

Facial Recognition

Look at the shape of the face and characteristics such as mouth, jaw, cheekbone, and nose.
Light and angle/direction can be a factor, especially in software.
Microsoft facial recognition, called **Windows Hello,** was released with Windows 10.
It uses a special **USB infrared camera** and as such is better than other facial recognition programs that can have problems with light.

Vein

Using blood vessels in the palm can be used as a biometric factor of authentication.

Gait Analysis

Gait is the way an individual walks, Identification and authentication using gait is possible even with lower resolution video.

Crossover Error Rate

A false acceptance occurs when an invalid subject is authenticated.
Sometimes called a false positive authentication.
A false rejection occurs when a valid subject is rejected.
CER indicates the point where the false rejection rate equals the false acceptance rate.

A **false rejection**, sometimes called a **false negative auth**entication or a (Type 1) **Type I error**, occurs when an authentication doesn't recognize a valid subject user.
A **false acceptan**ce, sometimes called a **false pos**itive authentication or a (Type 2) **Type II** error, occurs when an authentication system incorrectly recognizes an invalid subject.

Sometimes called a false negative authentication.
False rejection is undesirable but false acceptance is worse!
FAR = false acceptance rate
FRR = false rejection rate

CER

Biometric methods identify users based on characteristics such as fingerprints
The **crossover error rate (**CER) identifies the accuracy of a biometric method.
It Shows where the false rejection rate is equal to the false acceptance rate.
CISSP Exam Cram Full Course (All 8 Domains) - Good for 2024 exam!

Move the **CER** higher or lower, you can increase or decrease the sensitivity of the biometric device.

Domain 5 Single Sign-on

SSO is a mechanism that allows subjects to authenticate **once** and access **multiple objects** without authenticating again.
Common SSO methods and standards include:

- SAML
    - best support federated identity management (FIM)
    - SAML is an XML-based framework used to exchange user information for single sign-on (SSO) between federated organizations within a federated identity management system.
    - TLS provides message confidentiality and integrity, which can prevent eavesdropping. When paired with digital signatures, which provide integrity

and authentication, forged assertions can also be defeated. SAML does not have a security mode and relies on TLS and digital signatures to ensure security if needed.

- SESAME
- KryptoKnight
- OAuth
- OpenID

The three to know for the exam are SAML, Oauth 2.0 and OpenID.

A web developer is implementing single sign-on (SSO) in a web application. The SSO solution is using a JSON token.
OIDC provides SSO and uses a JavaScript Object Notation (JSON) Web Token (JWT).

Shibboleth is a federated identity solution designed to allow web-based SSO.

Session Management

Session management is used to close inactive sessions.
Closing the session after 2 minutes of inactivity is the best choice of the given options. A bank account where users can transfer funds is a high-value application, so the session should be closed at some time. Never closing a session isn't a secure option.
It's common to close sessions of high-value applications sometime between 2 and 5 minutes of inactivity. If it's closed after 5 minutes, it may be closing while a customer is in the middle of a transaction.

Transport Layer Security (TLS) provides the most effective defense against session hijacking because it encrypts all traffic between the client and server, preventing the attacker from stealing session credentials.
TLS token binding is used to make TLS sessions more secure.
Secure Sockets Layer (SSL) also encrypts traffic, **but** it is vulnerable to attacks against its encryption technology.
Complex and expiring cookies are a good idea, but they are not sufficient protection against session hijacking.

Common session management techniques include:

- Cookies
- hidden form fields
- URL rewriting
- built-in frameworks like Java's HTTPS session.

Single sign-on (**SSO**) is the best solution when users are logging on with a single set of credentials. It allows regular users to log on with a single account. Administrators may have two accounts. A password policy can enforce strong passwords, but every system will need a different password policy **without SSO.**

Domain 5 Implement Authentication Systems

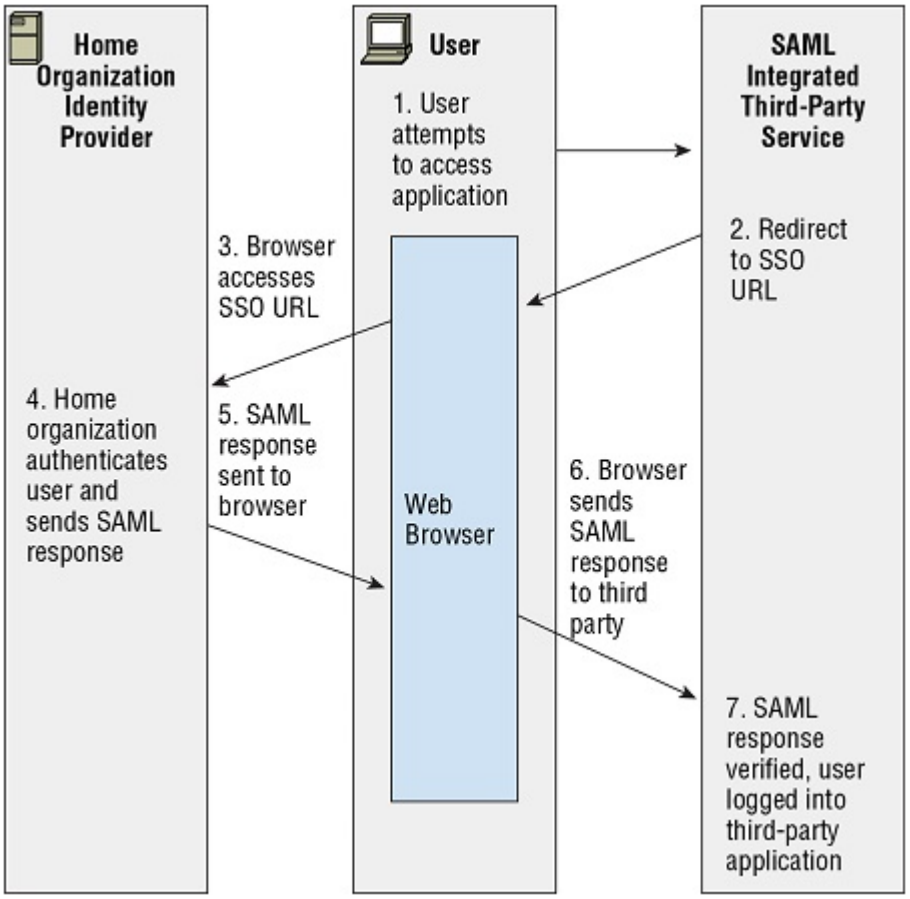
OpenID, Oauth, SAML and RADIUS

Security Assertion Markup Language (**SAML**)

Is an XML-based open standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. Common in federation scenarios.
SAML is an XML-based framework used to exchange user information for single sign-on (SSO) between organizations within a federated identity management system (FIM).
SAML is an XML-based framework used to exchange user information for single sign-on (SSO) between federated organizations within a federated identity management system.

TLS provides message confidentiality and integrity, which can prevent eavesdropping. When paired with digital signatures, which provide integrity and authentication, forged assertions can also be defeated. SAML does not have a security mode and relies on TLS and digital signatures to ensure security if needed.

SAML integration with a major third-party partner drawing



SAML Attacks:

- An awareness campaign about trusted third parties can aid in SSO Redirect concerns

- Eavesdropping: TLS provides message confidentiality and integrity, which can prevent eavesdropping.
- forged assertions: digital signatures, which provide integrity and authentication, forged assertions can also be defeated

Federation Scenario
An organization is considering creating a cloud-based federation using a third-party service to share federated identities.
Their normal account will be used as their login ID.
Users will use their normal account or internal login ID. Users log on within the organization using their normal login ID. When the user accesses cloud-based federation resources, the federated identity management system uses their login ID to retrieve the matching federated identity.

Oauth 2.0

OAuth is the most widely used open standard for authorization and delegation of rights for cloud services.
Is an open standard for authorization, commonly used as a way for Internet users to log into **third party** websites using their Microsoft, Google, Facebook, Twitter X, One Network, etc. **social accounts** without exposing their password.
Developed by IETF, updated thru RFC 6749.

OAUTH allows cloud-based applications to act on internet user behalf to access information from other sites.

You previously configured a web application to use your social media account credentials. Today, you logged onto your social media account and then connected to the web-based application without authenticating again, described OAuth 2.0, an authorization framework described in Request for Comments (RFC) 6749.

Passwords are never stored for web applications in a well-designed environment. Instead, salted hashes are stored and compared to passwords after they are salted and hashed. If the hashes match, the user is authenticated.
The password is never stored; instead, a salted hash is stored in Google's account management system.

Oath Tokens

OATH (Open authentication) is an open standard that specifies how time-bases, one-time password (TOTP) codes are generated.
Software OATH tokens
Example: Microsoft Authenticator App
Typically applications. Entra ID generates the secret key, or seed, that's input into the app and used to generate each OTP.

Hardware OATH tokens
Small hardware devices that look like a key fob that displays a code that refreshes every 30 or 60 seconds, with secret key/seed pre-programmed.

OpenID

OpenID is used for authentication.
As an open standard it provides decentralised authentication, allowing users to log into multiple unrelated websites with one set of credentials maintained by a **third-party service** referred to as an OpenID provider.

OIDC

OpenID Connect authentication technology can be paired with OAuth to perform identity verification and obtain user profile information using a RESTful API.

OpenID Connect (OIDC) uses a JavaScript Object Notation (JSON) Web Token (JWT) that provides both authentication and profile information for internet-based single sign-on (SSO). OIDC is built on the OAuth 2.0 framework. OpenID provides authentication but doesn't include profile information.

OpenID Connect is a widely supported standard that allows a user to use a single account to log into multiple sites, and Google accounts are frequently used with OpenID Connect.

Scenario OIDC:
A web developer implemented an authentication solution on a website allowing users to authenticate with a third party. The website doesn't see or store the user's credentials.
The solution uses technologies described in RFC 6749 but is not maintained by IETF.
OpenID and OIDC (short for OpenID Connect) are open standards maintained by the OpenID foundation.

Authentication Methods

Password **BAD**	Password and.. **GOOD**	Password and .. **BETTER**	Passwordless **BEST**
Password1	SMS	Authenticator App	Windows Hello
123456	Voice	Software OATH Tokens OTP	Authenticator App
qwerty		Hardware OATH Tokens OTP	FIDO2 Security Key

Passwordless is convenient, secure and reduces phishing exposure.

Password-less **does** introduce cost, biometric concerns, and device dependence.

Fido2/Passwordless
Uses public-key (asymmetric) cryptography for user authentication.
User has a physical device (USB or NFC)
Authentication sequence
Provide username → Cryptographic challenge → FIDO2 key to sign challenge → Service verifies response and grants access

Windows Hello for Business
An authentication feature built into Windows 10, replaces passwords with strong two-factor authentication on PCs and mobile devices.
Allows users authenticate to:

- Microsoft Account
- An Entra ID (Azure AD) account
- Identity Provider Services
- Relying party services that support Fast ID Online (FIDO) v2.0 authentication

Windows Hello is for personal devices and uses a pin or biometric gesture
Windows Hello for Business leverages key-based or certificate-based authentication.

Password-less Problems Solved

- Strong passwords can be difficult to remember, and users often reuse passwords on multiple sites.
- Server breaches can expose symmetric network credentials (Passwords).
- Passwords are subject to replay attacks
- Users can inadvertently expose their passwords due to phishing attacks.

Domain 5 Access Control Models

- ➢ Discretionary Access Control (DAC) → Identity Based
  - A model where subjects with the proper rights can assign or pass those rights to other subjects.
- ➢ Role based Access Control (RBAC) → Group Membership

    - Used to assign permissions based on job or function.
- ➢ Rule based access control (ruBAC) → Access Control List (ACL)
    - Permissions or rights are granted based on parameters like an IP address, time, or other specific details that match requirements.
- ➢ Mandatory Access Control → Labels
    - An access control model enforced by the operating system
- ➢ Attribute-based Access Control (ABAC) → SDN software defined network
    - Sometimes called policy-based access control, this model uses information about the subject to assign permissions.
    - Authentication that takes attributes such as location, device, and time of day into account is context-aware authentication. - ABAC (Attribute Based Access Control)

CISSP Practice Questions and Answers | CISSP Exam 2024 | CISSP Questions and A…

The **implicit deny** principle states that any action that is not explicitly allowed is denied. This is an important concept for firewall rules and other access control systems. Implementing **least privilege** ensures that subjects have only the **rights** they need to accomplish their job.

Discretionary Access Control

A Key characteristic of the discretionary access control (**DAC**) model is that every object has an **owner**, and the **owner can grant** or deny access to any other objects.

DAC Examples:

- New technology file system (**NTFS**) Microsoft
- Information Assets

Adam recently configured permissions on an NTFS filesystem to describe the access that different users may have to a file by listing each user individually.
Answer:
Adam created a list of individual users who may access the file. This is an access control list (ACL), which consists of multiple access control entries. It includes the names of users, so it is not role-based, and Adam was able to modify the list, so it is not mandatory access control.

A discretionary access control model allows the owner (or data custodian) of a resource to grant permissions at the owner's discretion.

RBAC Role based access control

A key characteristic is the use of roles or groups. Instead of assigning permissions directly to users, user accounts are placed in roles and administrators assign privileges to the roles. Typically mapped to job roles.
Role-Based Access Control is the model that most closely corresponds with a company's organizational structure.

A key characteristic of the Role-Based Access Control (**RBAC**) model is the use of roles or groups. Instead of assigning permissions directly to users, user accounts are placed in roles and administrators assign privileges to the roles. These roles are typically identified by **job func**tions
RBAC is a technical control used for enforcing access controls in a network.
RBAC primary purpose is assigning access based on job functions

Role-based access control (RBAC) security controls are most effective in preventing a privilege escalation attack. RBAC limits people's permission.

A RBAC model allows users membership in multiple groups.

A role-based access control (RBAC) model can group users into roles based on the organization's hierarchy, and it is a nondiscretionary access control model. A nondiscretionary access control model uses a central authority to determine which objects that subjects can access.

Linux New role for Linux Administrators
The best choice is to define a new role for Linux administrators and assign privileges based on the role definition. Linux systems do not have an Administrators group or a ***sudo*** group. However, you can grant root account access to users by adding them to the **sudoers** file. The ***sudo*** command allows users to run root-level commands by prefixing the command with ***sudo***, and the command will use the user's credentials. In contrast, the ***su*** command requires the password for the root account, and an attacker couldn't run root-level commands with just the user's credentials.
Modify the sudoers file to limit the potential for privilege escalation attacks on Linux hosts.

Rule-based access control

RuBAC - Global rules applied to all users equally.
A key characteristic is that it applies **global rules** that apply to all subjects.
Rules within this model are sometimes referred to as **restrictions or filters.**
Rule based access control, uses **global rules** applied to **all users** equally.

Example: Firewall uses rules that allow or **block traffic** to all users equally.

Risk-Based Access Control

A risk-based access control model can be coded to block malicious traffic from infected IoT devices. It evaluates the environment and the situation and makes decisions to block traffic that is abnormal.
Risk-based access control models determine access based on the environment and the situation.
A risk-based access control model evaluates the environment and the situation and then makes access decisions based on coded policies.
Risk Based Access Control

A risk based access control model grants access after evaluating risk. It evaluates the environment and the situation and makes dynamic risk-based decisions using policies embedded within software code. It uses machine learning to make predictive conclusions about current activity based on past activity.

Scenario:
IT personnel are concerned that attackers may take over some Internet of Things (IoT) devices on the network's border. They want to ensure that any malicious traffic from these devices is blocked.

A risk-based access control model can require users to authenticate with (MFA) multi factor authentication to for example cloud-based resources..

Attribute Based access control

A key characteristic of this model is its use of rules that can include multiple attributes.
This allows it to be much more flexible than a **rule**-based access control model that applies the rules to all subjects equally.
Often used by software defined networks (**SDN**)
Example of ABAC:
An organization's security policy allows users to connect their mobile devices to the internal network. However, it requires that their devices are up-to-date with a current operating system.

Mandatory access control

An access control model assigns access based on a user's need to know combined with organizational policies.
MAC Model is the use of **labels** applied to both subjects and objects.
MAC access control model identifies the upper and lower bounds of access for subjects with labels.
Privilege escalation attacks can be prevented using Mandatory Access Control (MAC).

MAC model environments

- Hierarchical
  - each domain is ordered and related to other domains above and below it
- Compartmentalized
  - there is no relationship between each domain
- Hybrid
  - both hierarchy and compartments are used

Example, if a user has a label of **top secret,** the user can be granted access to a top-secret document. In this example both the subject and the object have matching labels.
Referred to as a **lattice-based** model.

Domain 5 Groups and Roles

Roles

- A set of permissions that correspond to a **job func**tion within an organisation, rather than a group of users.
- When a user is assigned a role, they are granted the permissions associated with that role
- Function-centric, focusing on the **job func**tion and the actions that need to be performed

Groups

- A Collection of users
- Administrators can assign permissions to the group instead of individual users, making it easier to manage large numbers of users
- User-centric, focusing on the collective identity of users

Key Benefits of Groups and roles

Efficiency. Provide centralized management of access control policies, streamlining administration across different scenarios.
Security. Enforce data privacy and the principle of least privilege by tailoring permissions to roles.

On-prem
Historically tied to physical servers and domain controllers (like Active Directory).
Offered granular control but could become complex to manage at scale.

Cloud
Cloud providers like azure or AWS offer their own identity and access management (IAM) systems.
Allows for cloud-native groups and roles, templates, and security integration.

Hybrid
Organizations typically synchronize groups and roles between on-premises systems and cloud environments.
Groups and Roles ensure consistent security policies.

Microsoft Azure Entra ID Demo: Microsoft Azure Entra ID Demo:

Domain 5 Security Controls

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Security controls, countermeasures, and safeguards can be implemented **admin**istratively, **logica**lly, **tech**nically or **phys**ically.
Types of security controls include:

- **Prev**entative

- **Det**ective
- **Corr**ective
- **Deter**rent
- **Comp**ensating - deployed to provide various options to other existing controls to aid in enforcement and support of security policies.
- **Dire**ctive
- **Reco**very

Categories of control include

- Logical / Technical
  - The hardware or software mechanisms used to manage access to resources and systems and provide protection for those resources and systems.
  - Examples: encryption, smart cards, passwords, biometrics, constrained interfaces, access control lists (ACLs), protocols, firewalls , routers, intrusion detection systems (IDS) and **clipping** levels
- Physical
  - Security mechanisms focused on providing protection to the facility and real-world objects
  - Examples: guards, fences, motion detectors, locked doors, sealed windows, lights, cable protections, laptop locks, swipe cards, guard dogs, video cameras, mantraps, and alarms.
- Administrative
  - Policies and procedures defined by an organization's security policy to implement and enforce overall access control. Focus on two areas: personnel and business practices.
  - Examples: policies, procedures, hiring practices, background checks data classification, security training, vacation history, reviews work supervision, personnel controls, and penetration testing

Hiring

The first step in hiring new employees is to create a job description.
Without a job description, there is no consensus on what type of individual needs to be found and hired.
Crafting job descriptions is the first step in defining security needs related to personnel and being able to seek out new hires.

A user account must have an account identifier (also known as a username/samaccount). Other information such as a full name, an email address, and the department where an employee works can also be added, but they are optional. Note that email addresses are sometimes used as the username, but not all systems use the email address as the username.

Promotion opportunities involve an entire organization, **not** a specific job, and thus are not an element of a job description.

When a new employee is hired, they should sign an employment agreement/contract and possibly a nondisclosure agreement (NDA).
These documents define the responsibilities and legal liabilities of the relationship between the employee and the organization.
Signing a noncompete (NCA) or NDA agreement is typically done at hiring.

The employment documents that you will be required to sign if you accept a job position being offered. One of the security policies documents includes the statement "the freedom from being observed, monitored, or examined without consent or knowledge."
This refers to the **Privacy def**inition.

Three primary control types are **prev**entative, **dete**ctive, and **corr**ective.

Court rulings have consistently stated that employees do not have a reasonable expectation of privacy while using business systems. Therefore, though notice and consent may be desirable, they are not required.

Employment contract is a formal, detailed description of the responsibilities between an organization and an employee.

Zero Trust

An approach to security architecture in which no entity is trusted by default:

- Assume breach
- Verify explicitly
- Least Privilege Access

Replaced trust but verify and its network perimeter strategy.
Support by defense in depth, that advises a layered approach to security.

Zero Trust Security

- Addresses the limitations of the legacy
- Network perimeter based security model
- Treats user identity as the control plane
- Assumes compromise / breach in verifying every request.
- No entity is trusted by default.

Access Policy enforcement

- Policy Decision Point (PDP)
    - Responsible for making access control decisions based on predefined access policies and rules
    - Evaluates access requests
    - Where access decisions are made based on various factors such as user identity, device health, and risk assessment.
    - Evaluates the context of an access request and decides whether it should be allowed, denied or subjected to additional controls.

    - It receives authorization requests and sends them to the policy decision point.
    - Considers the 5 W's (Who,What,When,Where, and Why)

- Policy Enforcement Point (PEP)
    - Responsible for enforcing the access control decisions made by the PDP
    - Acts as a gatekeeper
    - Responsible for enabling, monitoring, and terminating connections between a subject (such as a user or device) and an enterprise resource.
    - Acts as the gateway that enforces access control policies.
    - When an access request occurs, the PEP evaluates the request against predefined policies and applies the necessary controls.

CISSP Exam Cram - 2024 Addendum

Domain 5 Zero Trust Network Architecture

Key Elements of Zero Trust Network Architecture NIST 800-207

Control plane

- Adaptive identity
    - Changes the way that the system asks a user to authenticate based on context of the request. Example: location, device, app, risk
- Threat Scope Reduction
    - An end goal of ZTNA, which is to decrease risks to the organization.
- Policy-Driven Access control
    - Controls based upon a users identity rather than simply their systems location. Example: Confidential access in MSFT Entra ID.
- Policy Administrator (PA)
    - Responsible for communicating the decisions made by the policy engine.
- Policy Engine (PE)
    - Example: MSFT Entra ID (Azure Active Directory)
    - Decides whether to grant access to a resource for a given subject.

Drives the policy-based decision logic for zero trust.

Data Plane

- Implicit Trust Zones
    - Part of traditional security approach in which firewalls and other security devices formed a perimeter. Systems belonging to the org were placed inside this boundary.
- Subject/System
    - A **subject** is a user who wishes to access a resource.
    - A system is a non-human entity, often the device used by the user, to access the resource.

- Policy Enforcement Point
    - When a user or system requests access to a resource, the PEP evaluates it against predefined policies and applies the necessary controls.
    - Example: MSFT Entra ID (Azure Active Directory)

Enforces the decisions defined in the control plane.

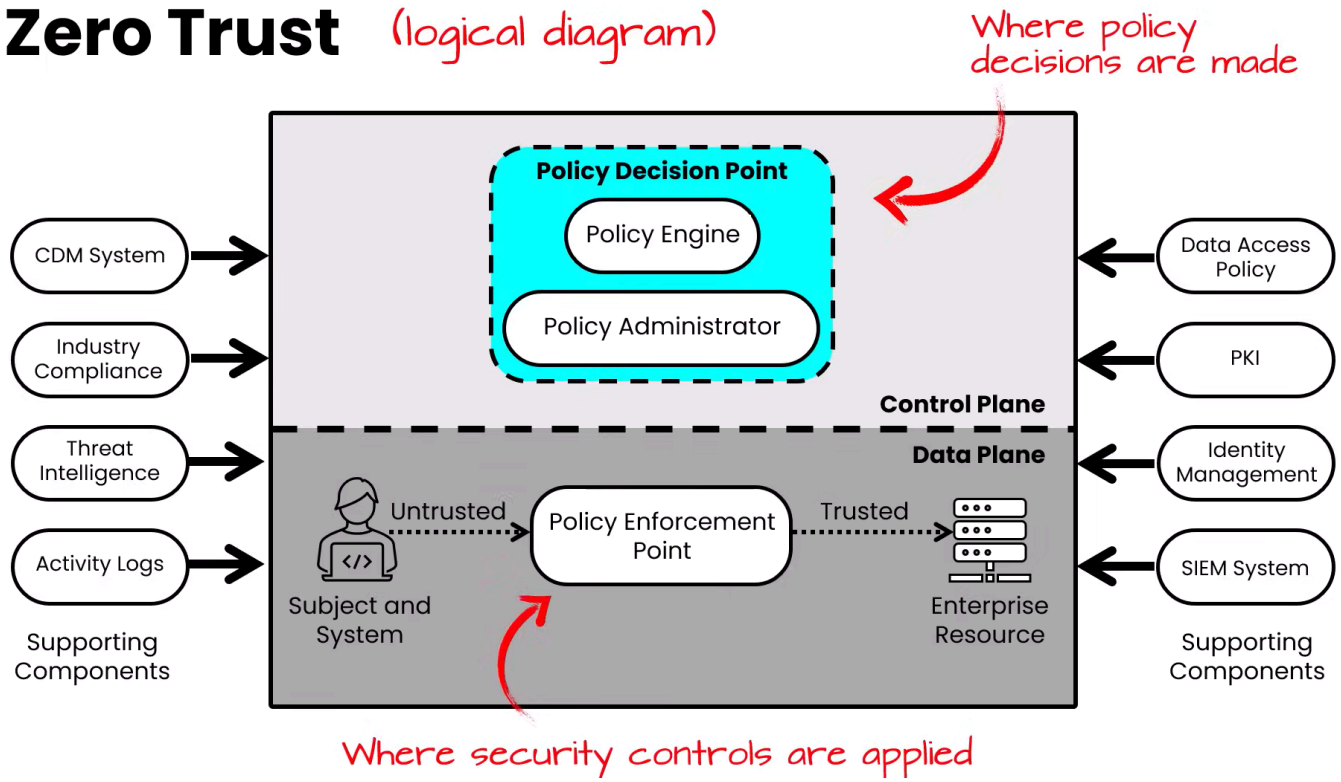
Reference in NIST SP 800-207
SP 800-207, Zero Trust Architecture | CSRC

Domain 5 Zero Trust Logical Diagram

In a zero trust network architecture, the **policy engine** is responsible for making policy decisions based upon rules and external data sources.
Policy Engine uses a trust algorithm to decide whether to grant, deny, or revoke access, considering factors like identity management, threat intelligence, and security information and event management (SIEM) data.
Policy Decision Points encapsulate the Policy Engine and Policy Administrator.
The **policy administrator**, on the other hand, acts based on the decisions made by the policy engine, establishing or removing communication paths and managing session-specific credentials.
The **policy enforcement point** enforces these decisions by controlling access to resources based on instructions from the policy administrator.
Lastly, the **subject** refers to users, services, or systems that request access or attempt to use rights and are not involved in decision-making.

In a zero trust reference model-based design, subjects connect through a **policy enforcement point.**
The **policy engine** makes policy decisions based on rules that are then acted on by the policy administrator, granting or denying access to enterprise resources.
Constrained interfaces limit user actions but are not the component connected through to conduct transactions.

Zero Trust logical diagram



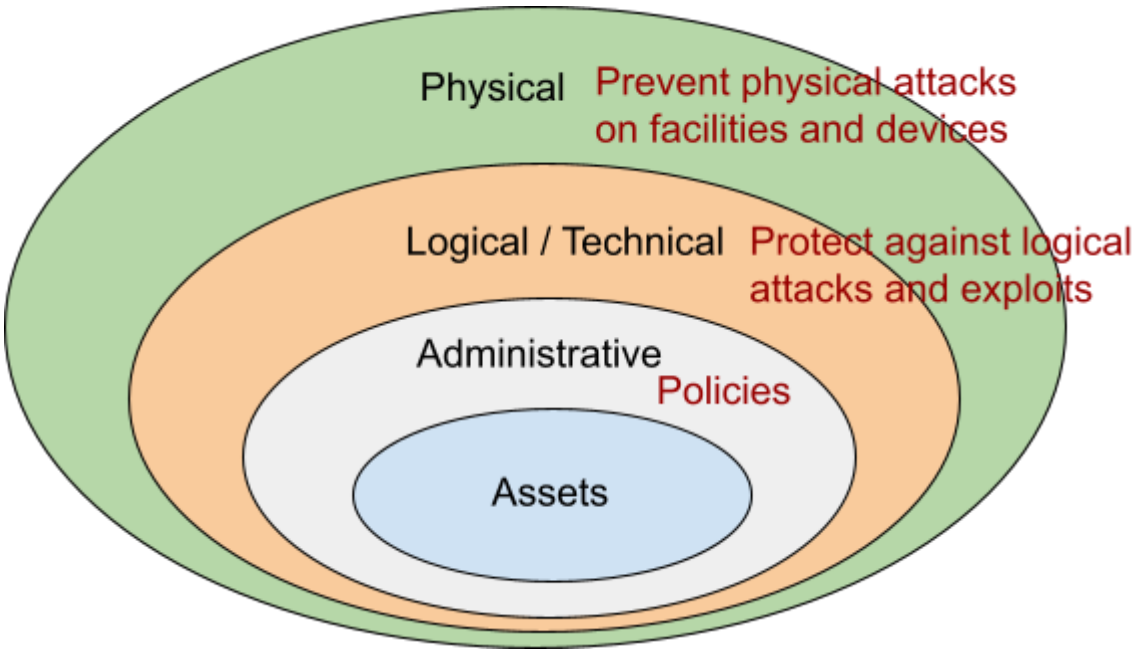
CISSP Exam Cram - 2024 Addendum

Domain 5 Categories of Security Controls

- **Logical** / Technical the hardware or software mechanisms used to manage access to resources and systems and provide protection for those resources and systems.
  - Encryption
  - smart cards
  - Passwords
  - Biometrics
  - Constrained interfaces
    - A constrained or restricted interface is implemented within an application to restrict what users can do or see based on their privileges. The purpose of a constrained interface is to limit or restrict the actions of both authorized and unauthorized users.
    - Protect following security functions: Confidentiality and Integrity
  - Access control lists (ACLs)
  - Protocols
  - Firewalls
  - Routers
  - Intrusion detection systems
  - **Clipping** levels
- **Physical** security mechanisms focused on providing protection to the facility and real world objects
  - Guards

    - Fences
    - Motion detectors
    - Locked doors
    - Sealed windows
    - Lights
    - Cable protections
    - Laptop locks
    - Swipe cards
    - Guard dogs
    - Video cameras
    - Mantraps
        - An access control vestibule (also known as a mantrap)
    - Alarms
- Administrative, Policies and procedures defined by an organisation's security policy to implement and enforce overall access control. Focus on two areas, personnel and business practices.
    - Policies
    - Procedures
    - Hiring practices
    - Background checks
    - Data classification
    - Security training
    - Vacation history
    - Reviews
    - Work supervision
    - Personnel controls
    - Testing

Domain 5 Security Controls Layers



Domain 5 Types Security Controls

Preventative

Preventive access controls are designed to prevent the activity from occurring..

Deployed to stop unwanted or unauthorized activity from occurring.

- Fences
- Locks
- Biometrics
- **Mantraps**
    - Preventing unauthorized physical access to a data center
    - An access control vestibule (or mantrap) uses two sets of doors, only one of which can open at a time.
    - An access control vestibule is a type of preventive access control, although its implementation is a physical control.
- Alarm systems
- Job rotation
- Data classification
- Penetration testing - PenTest
- Access control methods

Detective

Deploy to discover unwanted or unauthorised activity. Often are **after-the-fact** controls rather than real time controls.

- Security guards
- Guard dogs

- Motion detectors
    - Example: A capacitance motion detector senses changes in the electrical or magnetic field surrounding a monitored object.
    - A photoelectric motion detector senses changes in visible light levels for the monitored area.
    - Photoelectric motion detectors are usually deployed in internal rooms that have no windows and are kept dark.
    - An infrared PIR (passive infrared) or heat-based motion detector monitors for significant or meaningful changes in the heat levels and patterns in a monitored area
- Job rotation
- **Mandatory vacations**
    - discover evidence of fraud and theft.
    - Most security professionals recommend at least one, and preferably two, weeks of vacation to deter fraud.
    - One week mandatory vacation shortest effective length
- Audit trails
- Intrusion detection systems
- Violation reports
- Honey pots
- Incident investigations

Detective controls identify incidents, while corrective controls correct the underlying issues.
Detective access controls operate after the fact and are intended to detect or discover unwanted access or activity.

Corrective

Deployed to **rest**ore systems **to norm**al after an unwanted or unauthorized activity has occurred such as a security incident.
Corrective controls return an environment to its original status after an issue occurs.

- Intrusion detection system
- Antivirus solutions
- Alarms
- Mantraps
- Business continuity planning
- Security policies

Once a system is compromised, **Corrective access control** is deployed to restore it to its previous known-good state.

Compensating

Deployed to provide options to other existing controls to **aid in the enforce**ment and support of a security policy.

- **Disaster recovery plan** with an alternative office location in the event of fire suppression fails and building is damaged

Directive

Directive access controls limit or direct the actions of subjects to ensure compliance with policies.

A form of security control is used to guide the implementation of an organizational security mechanism and/or encourage compliance with security policies.
Deployed to direct, confine, or control the actions of **subj**ects to **for**ce or **enco**urage **comp**liance with **sec**urity **pol**icies.

- Security guards
- Guard dogs
- Security policy
- Posted notifications
- Escape route
- Exit signs
- Monitoring
- Supervising
- Work task procedures
- Awareness training

Recovery

Deploy to repair or restore resources, functions and capabilities after a violation of security policies.
More **adv**anced or complex capability to respond to access violations than a **corrective access control.**

- Backups and restores
- Fault tolerant drive systems
- Server clustering
    - adds a degree of fault tolerance, protecting against the impact of a single server failure.
- Antivirus software
- Database shadowing
    - Database shadowing requires two or more databases that are running simultaneously. Updates made to the primary database are replicated to one or more shadow databases at remote sites.

Prevent future compromise, downtime, and disaster events or at least reduce it significantly:

- RAID
    - RAID 0 is also known as disk striping.
    - RAID 1 is called disk mirroring.
    - RAID 5 is called disk striping with parity.
        - RAID 5 level is commonly used for distributed parity, allowing for resilience while being space efficient
    - RAID 10 is known as a stripe of mirrors.
- UPS
- Dual power supplies
- Offsite backups of system images and snapshots

- Replication
- Clustering

Deterrent

Deployed to discourage the violation of security policies.
A deterrent control picks up where prevention leaves off.

- Locks
- Fences
- Security badges
- Security guards
- Mantraps
- Security cameras
- Trespass
- Intrusion alarms
- Separation of duties
- Awareness training encryption
- Auditing
- Firewalls

Security Cameras

- Cameras should be **positioned** to **watch** exit and entry points allowing any change in authorization or access level.
- Cameras should be positioned to have **clear sight lines** of all exterior **walls**, entrance and **exit points**, and interior hallways.
- Some camera systems include a **system on a chip** (SoC) or embedded components and may be able to perform various specialty functions, such as **time-lapse** recording, tracking, facial recognition, object detection, or infrared or color-filtered recording.
- Cameras should also be used to monitor activities around valuable assets and resources as well as to provide additional protection in public areas such as parking structures and walkways;
- Security cameras can be overt and obvious in order to provide a deterrent benefit, or hidden and concealed in order to primarily provide a detective benefit;
- Some cameras are fixed, whereas others support remote control of automated pan, tilt, and zoom (PTZ);
- Simple motion recognition or motion-triggered cameras may be fooled by animals, birds, insects, weather, or foliage.

Motion Detector

Installing a motion detector to protect a sensitive work area that uses high-frequency microwave signal transmissions to identify potential intruders.

- Wave Pattern

Motion Detection Types

- **Wave pattern** motion detectors transmit ultrasonic or microwave signals into the monitored area, watching for changes in the returned signals bouncing off objects.
- **Infrared heat**-based detectors watch for unusual heat patterns.
- **Capacitance** detectors work based upon electromagnetic fields.

Domain 5 Risk Elements

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Basic elements of risk

Risk
Is the possibility of **likelihood** that a threat can exploit a vulnerability and cause damage to assets.
Asset valuation
Identifies value of assets, threat modelling identifies threats against these assets.
Vulnerability analysis
Identifies weaknesses in an organisation's valuable assets.

Domain 5 Access Control Attacks

CISSP Exam Cram - Cyber Attacks and Countermeasures (+ Quantum for CISSP 2021)

Dictionary Attacks

These are programs with built in dictionaries. They would all use dictionary words to attempt and find the correct password in the hope that a user would have used a standard dictionary word.

Brute force

This type of attack is attempting to break the password by trying all possible words.
Password complexity and attacker tools/compute determine efficacy.

Spoofed logon screens

The last access control attack is to implement a fake logon screen, and when a user attempts to login, the login screen will send the username and password to the hacker.
CISSP Exam Cram - Cyber Attacks and Countermeasures (+ Quantum for CISSP 2021)

Sniffer Attacks

In a sniffer attack (or snooping attack) an attacker uses a **packet capturing tool** (such as a sniffer or protocol analyzer) to capture, analyse and read data sent over a network.
Attackers can easily read data sent over a network in cleartext.
Encrypting **data in transit** stops this type of attack.

Scenario:

Administrators routinely connect to servers in the data center from remote locations using their administrator accounts.
Protecting **data in trans**it is a prime concern when doing remote desktop connections.

Spoofing Attacks

Spoofing is pretending to be something or someone else, and it is used in many types of attacks, including access control attacks. Attackers often try to obtain the credentials of users so that they can spoof the users identity.
Spoofing attacks include email spoofing, phone number spoofing, and IP spoofing.
Prevent IP Spoofing Attacks:

- Block packets with internal source addresses from entering the network.
- Block packets with external source addresses from leaving the network.
- Block packets with private IP addresses from exiting the network.

Many phishing attacks use spoofing methods.

Social Engineering

An attempt by an attacker to **convince someone** to provide info (like password) by being persuaded.
Perform an action they would not normally perform such as **click**ing on a malicious **link**)

Social engineers often try to gain access to the IT infrastructure or the Physical facility.
Best defense is security awareness training and user education.
To reduce the likelihood of **insider threats** and data breaches is to do security **awareness training** and this is the primary goal of the program.

Indicators message is a hoax:

- Lack of a digital signature verifying the origin
- Claimed sender confirms they did not send the message
- Threat of damage to your computer system
- Encouragement to take specific steps to resolve a concern which are not based on standard company procedures

A **hoax** is a social engineering attack that is attempting to trick a user into taking actions that will harm them through the use of fear that not taking action would actually cause harm.
If you contact the claimed sender and they confirm they did not send the message, then it could be a hoax or at least a spoofed message.
Hoaxes often use the threat of damage or harm to encourage the victim to take action, and those actions are often provided steps that will actually cause the victim harm.

Poor grammar, bad spelling, and hyperlinks in the message are all characteristics of both valid and invalid email messages.

Claiming to be from a trusted authority is the attempt to use the social engineering principle of authority and/or intimidation, which is **not** uniquely a feature of a **hoax**, but many spam, business email compromise (BEC), and phishing attacks do as well.

But the claim of being a trusted authority could be valid as well.

Phishing

Commonly used to try to trick users into giving up personal information (such as user accounts and passwords), click a malicious link, or open a malicious attachment.
Business email compromise (BEC) is often performed by taking advantage of the social engineering principle of **authority**.
In an example, a false invoice that was apparently received from the CEO makes it seem as if it originated from a proper **authority**.

Spear Phishing

Targets specific groups of users.

Whaling

Targets the high value executives.

Vishing

uses voice VOIP technologies.
Countermeasure: User Training / Awareness training

Example of Vishing:
A secretary receives a phone call from a person claiming to be a client who is running late to meet the CEO. The caller asks for the CEO's private cell phone number so that they can call them.

Typosquatting

Taking advantage of users who mistype the domain name or IP address of an intended resource.
Infringement of trademarks:

- Typosquatting - tailspintoy.com instead of tailspintoys.com
- Dilution - 10 grams of salt are dissolved in 1 liter of water as a solvent
- Cybersquatting - e.g. Walrmart44.com or xofnews.com

Access Aggregation

Is a type of attack that combines, summarize or aggregates non-sensitive information to learn sensitive information and is used in reconnaissance attacks.
Aggregation attacks involve the use of specialized database functions to combine information from a large number of database records to reveal information that may be more sensitive than the information in individual records would reveal.
Aggregate functions summarize large amounts of data and provide only summary information as a result. When carefully crafted, aggregate functions may unintentionally reveal sensitive information.

Domain 5 Prevent Access Control Attacks

Password Policy

- Passwords should be long, complex and changed periodically.
- There should be a strong password policy in place to enforce
- Also **enforcing** other measures such as account **lockout** after X logon attempts etc.
- Spoofed logon screens, have secure endpoints, where these fake logon screens cannot be implemented.

Modern recommendations from the National Institute of Standards and Technology (NIST) are that users should not be forced to change their passwords through the use of password expiration policies. More information on these recommendations can be found in NIST Special Publication (SP) 800-63B, "Digital Identity Guidelines."

Example:

User	Last Login Length	Last Password Change
Bob	4 hours	87 days
Sue	3 hours	38 days
John	1 hour	935 days
Kesha	3 hours	49 days

If user John Last Password Change is at **935** days, then the password maximum age security control should be correct to enforce.

Domain 5 Other Attacks

Tempest

Allows the electronic emanations that every monitor produces to be read from a distance, effective on CRT monitors. Legacy.
Shoulder surfing for monitor displays.
If an employee with a lower level of clearance can be present in an area of higher clearance, then that employee may be able to see sensitive information on displays (i.e., shoulder surfing).

White Noise

Broadcasting **false traffic** at all times to mask and hide the presence of real emanations.
While all of the controls mentioned protect against unwanted electromagnetic emanations, only White noise is an active control.
White noise generates false emanations that effectively "jam" the true emanations from electronic equipment.

A Faraday cage is an enclosure that blocks or absorbs electromagnetic fields or signals such as wireless networks.
Faraday cage containers, computer cases, rack-mount systems, rooms, or even building materials are used to create a blockage against the transmission of data, information, metadata, or other emanations from computers and other electronics.

Domain 5 Asset Management

An effective asset management program helps prevent losses by tracking and protecting assets throughout their lifetime.

Sensitive data scanning tools are designed to scan for and flag sensitive data types using known formatting and structure. Social Security numbers, credit card numbers, and other regularly structured data that follows known rules can be identified and then addressed as needed.
Example tools: panhunt
Scanner tools Penetration Testing Tools

RFID, Barcoding and Inventory
Represent the ability to **prevent theft**, which reduces risk.
RFID (radio-frequency identification) is effectively a field-powered proximity device. A passive proximity device is often a magnet; an RFID does not use a magnet, but an antenna to generate current from a magnet field provided by an external source.
A self-powered proximity device has its own battery, which RFID does not, but NFC may.

proximity card

RFID inventory control process in a cost-effective manner.

Microsoft Configuration Manager (ConfigMgr) provides this capability and is designed to allow administrators to evaluate the configuration status of Microsoft Windows 11 workstations and servers, as well as providing **asset management data.**

Domain 6 Security Assessment & Testing

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

- Design and validate assessment, test, and audit strategies
    - Location (on-premise, cloud, hybrid)
- Conduct security control testing
- Collect security process data eg. technical and administrative
- Analyse test output and generate report
- Conduct or facilitate security audits
    - Location (on-premise, cloud, hybrid)

Note: Answer may be to call an expert for penetration testing.
Call an expert, you are the manager.

Security assessments include many types of tests designed to identify vulnerabilities, and the assessment report normally includes **recommend**ations for **mitig**ation. The assessment does **not**, however, include **actual mitiga**tion of those vulnerabilities.

Red Book

The Red Book, formally known as the Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria, extends the security evaluation criteria found in the Orange Book (TCSEC) to networked systems. It provides guidelines on how to apply the Orange Book's criteria to systems that involve network communications.
The Red Book (Trusted Network Interpretation) is the U.S. Department of Defense standard that describes security evaluation criteria specifically for networked systems. It builds on the Orange Book to address the unique challenges and security requirements of networked systems.

Domain 6 Security Assessment and Testing programs

Provides a mechanism for **valida**ting the **ong**oing **effecti**veness of **sec**urity controls, with a variety of tools to **valid**ate **cont**rols.

- Vulnerability assessments
- Penetration tests, software testing
- Audits
- Security management tasks

Penetration testing is a reactive approach (aka adversarial approach) form of threat modeling, which takes place after a product has been created and deployed.

Every organization should have a security assessment and testing program defined and operational.

Misuse Case Testing

Misuse case testing identifies known ways that an attacker might exploit a system and tests explicitly to see if those attacks are possible in the proposed code.
In misuse case testing the testers first enumerate known misuse/abuse cases. They then attempt to exploit those use cases with manual and/or automated attack techniques.

Example misuse:
focused on functions that a system should not allow

Every organisation should have a security assessment and **testing program** defined and operational.
Primary goal of security assessment or audit is to identify vulnerabilities and weaknesses.

Security assessment reports should be addressed to the organization's management. For this reason, they should be written in plain English and avoid technical jargon.

Security testing in the context of system development life cycle (SDLC) is to identify security vulnerabilities and weaknesses.

Naming & Scoring

- Common Configuration Enumeration (**CCE**) provides a naming system for system configuration issues.
- Common Vulnerabilities and Exposures (**CVE**) provides a naming system for describing security vulnerabilities.
    - list of information security vulnerabilities in applications, devices, and operating systems
- Common Platform Enumeration (**CPE**) provides a naming system for operating systems, applications, and devices.
- The Common Vulnerability Scoring System (**CVSS**) provides a standardized scoring system for describing the severity of security vulnerabilities.

Above SCAP components suited to common naming schemes.

Vulnerability Assessments vs Penetration Tests

Vulnerability Assessments

Use automated tools to search for known vulnerabilities in systems, applications and networks.
Flaws may include missing patches, **misconfig**urations, or faulty **code** that expose the organisation to security risks.
<u>Vulnerability Assessment Process Steps</u>

1. Reconnaissance
2. Enumeration - testing if ports open

3. Vulnerability Analysis
4. ~~Execution - Done in penetration test NOT vulnerability assessment~~
5. Document Findings

Penetration tests

You should never conduct a formal or informal penetration test against any company without the advanced knowledge and express consent of management.
PenTest aims to identify and document security **weaknesses**.
Uses these same tools but supplements them with **attack techniques** where an assessor attempts to **exploit** vulnerabilities and **gain** access to the system.

Consideration planning security assessment testing schedule:

- Sensitivity of the information stored on the system (Crown Jewels)
- Difficulty of performing the test (Mainframe, Thick App, Mobile, etc.)
- Desirability of the system to attackers (Hack Value)

The desire to experiment with new testing tools should ***not*** influence the production testing schedule.

Reactive threat modelling, is performing threat hunting, ethical hacking, penetration testing, source code review, and fuzz testing.

Threat hunting is the process of actively searching for infections or attacks within a network. Security administrators are regularly monitoring threat feeds and using that information to check systems within the network. Their goal is to discover any infections or attacks that haven't been detected by existing tools.

Penetration Test Strategies

- War dialling - bank of modems (legacy)
- Sniffing - monitor the network
- *Eavesdropping* - listening
- Dumpster Diving - Just like it sounds
    - Gleaning valuable information from printed documents, glue shredded docs from trash collection
- Social Engineering - Human Manipulation

Tests that involve human interaction and analysis will increase cost but are more thorough. Ethical Hacking/Penetration testing is most effective for identifying unknown vulnerabilities that are not disclosed publicly.

Penetration test Risks

- Application crashes
- Denial of Service
- Data Corruption

Location

Location is of concern, as audit strategy and execution change in the public cloud.

- On-premises
  - Physical access - auditors typically need physical access to hardware, network devices, and data centres for inspection, configuration reviews and testing.
  - Control and visibility - the organization retains greater control over its infrastructure thus auditors have more direct visibility into security configurations.
  - Scope - audits may be focused on traditional IT infrastructure, including network security, operating systems, physical safeguards, etc.
  - Focuses on evaluating the security measures and infrastructure within an organisation's physical data centres and facilities.
- Cloud
  - Shared responsibility - security is a shared responsibility between the organization and the cloud provider. Audit focus shifts towards how the organization uses the cloud services.
  - **Documentation and APIs** auditors rely heavily on cloud provider documentation, service configurations, and access to relevant APIs for gathering evidence.
  - **Compliance Focus** - emphasis often on meeting cloud-specific security standards (eg. SOC 2, ISO **27001**, **FedRAMP**) and the organizations configuration of cloud services.
  - Focuses on assessing the security of data and applications hosted in cloud service providers
  - The distributed nature and scale of the cloud make conducting an audit of 100% of infrastructure challenging
  - Cannot audit the underlying infrastructure managed by the cloud service provider (CSP)
- Hybrid
  - Increased Complexity - hybrid environments present the greatest complexity due to the mix of on-premises and cloud components that need auditing.
  - **Data Flows** - understanding how data moves between on-premises and cloud environments is crucial for risk assessment.
  - **Integrated controls** - auditors must evaluate the effectiveness of security controls across the entire hybrid landscape.
  - Assess the connectivity and security measures in place between on-premises and cloud resources.
  - Access management integration, data flow security controls, etc.)

Assurance Challenges with Virtualization & Cloud

The cloud is made possible by **virtualization** technologies that enable dynamic environments needed for a global provider platform.

Depending on the cloud architecture employed, a cloud security professional must perform multiple layers of auditing.
To be effective, the auditor must understand the virtualization architecture of the cloud provider.
Cloud Service Provider (**CSP**) - audits of controls over the hypervisor will usually be the purview of the CSP (Microsoft, Amazon Google)
Customer - VMs deployed on top of that hardware are usually owned by the customer. (Cloud Consumers)

Right to audit in the cloud

Use of vulnerable;lty scanners and pen testers may be limited by your CSPs terms of service.
Customers should understand the type and frequency of testing the CSP allows.
CSPs typically have penetration testing and scanning rules of engagement.

Cloud Contract Management

Right to audit
The customer can request the right to audit the service provider to ensure compliance with the security requirements agreed in the contract.
Contracts often written to allow the CSP standard audits (eg. SOC 2, ISO 27001 certification) to be used in place of a customer-performed audit.
Metrics
If there are specific indicators that the service provider must provide to the customer, they can be documented in a contract.
Tell you how compliance with the agreement will be measured.
Major cloud service providers make **SOC 2 Type II** (or other report) available on demand as submitting to every customer's audit request is not possible.

Daomin 6 Penetration Testing

Exercise Types / Security Teams
Red Team

- Be the threat
- Offensive security
    - Are internal or external entities dedicated to testing the effectiveness of a security program by emulating the tools and techniques of likely attackers in the most realistic way possible
- Ethical Hacking
- Penetration Testing
- Social Engineering
- Threat Intelligence

When assessing the security of an industrial control system (ICS), simulating realistic cyberattacks to test ICS defense is the primary focus of a Red Team engagement.

Blue Team

- Stop the threat
- Defensive security
    - The internal security team that defends against bot real attackers and red teams
- Security Monitoring
- Incident Response
- Digital Forensics
- Security Operations

Purple - Combined Collaborate
- Red and blue teams work together
- Information sharing
- Lessons learnt
    - Process improvement
    - Exist to ensure and maximise the effectiveness of the red and Blue teams

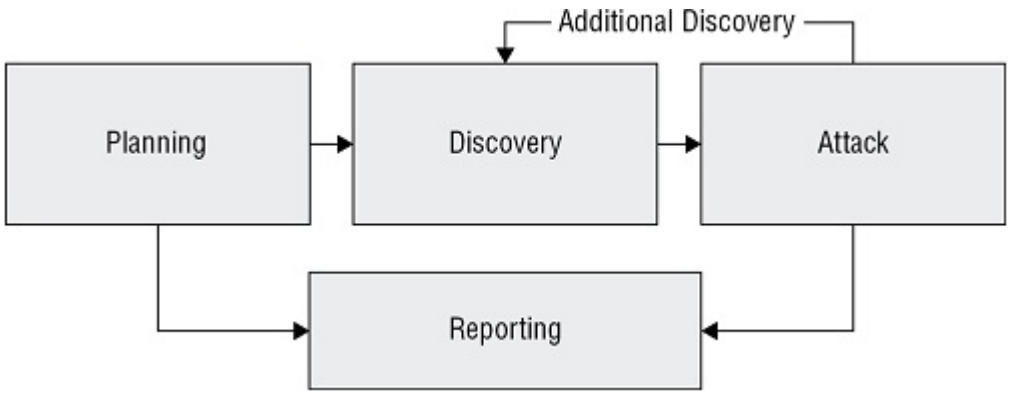
White Team - judge / referee / manager
- Responsible for overseeing an engagement or competition between a red team of mock attackers and a blue team of actual defenders.

Attack Phases

Please refer to the following scenario. NIST Special Publication 800-115, the Technical Guide to Information Security Testing and Assessment, provides NIST's process for penetration testing.

1. Planning
2. Discovery
3. Attack
4. Additional Discovery
    a. Repeat/Return to Discovery
5. Reporting

Use this image as well as your knowledge of penetration testing



NIST specifies four attack phase steps:
- gaining access
- escalating privileges

- system browsing
- installing additional tools
    - Once attackers install additional tools, return to first phase - Gaining Additional Access
- Repeat / report

Once additional tools have been installed, penetration testers will typically use them to gain additional access. From their new foothold they can further escalate privileges, search for new targets or data, and, once again, install more tools to allow them to pivot further into infrastructure or systems.

NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
See Section - 5.2.1 Penetration Testing Phases

Scan Privileges

When a tester does not have raw packet creation privileges (Root/Administrator), such as when they have not escalated privileges on a compromised host, a TCP connect scan can be used.
TCP SYN scans require elevated privileges (SUDO) on most Linux systems due to the need to write raw packets.
A UDP scan will miss most services that are provided via TCP.
an ICMP is merely a ping sweep of systems that respond to pings and won't identify services at all.

Domain 6 Security Process Data

- **Employmen**t Policies and practices - **termin**ation process and background checks (***Write***)
- **Roles and Resp**onsibilities - management sets the standard and verbalises the policy (***Communicate***)
- Security **awareness train**ing - prevents social engineering, helps with phishing (***Train***)

Domain 6 Software Testing

Application programming interfaces (APIs), user interfaces (UIs), and physical interfaces are all tested during the software testing process.
Programmatic interfaces are another term for APIs.

Performs software testing to **valid**ate **code** moving into production

- **Soft**ware **test**ing
    - techniques verify that code functions as designed and does not contain **security flaw**s.
    - A test coverage analysis is often used to provide insight into how well testing covered the set of use cases that an application is being tested for.

    - APIs, UIs, and physical interfaces
- **Code Review**
    - uses a **peer review** process to formally or informally validate code before deploying it in production
    - Source code reviews look at the code of a program for bugs, not necessarily at a use case analysis
    - Code review may be automated
    - Code reviewers may expect to review several hundred lines of code per hour.
- **User interface testing**
    - **User interface testing** includes assessments of both graphical user interfaces (GUIs) and command-line interfaces (CLIs) for a software program.
- **Interface Testi**ng -
    - assesses the interactions between components and users with **API** testing user interface testing, and **physical interf**ace testing.
    - APIs typically transfer data for web applications via HTTPS, meaning that the API itself is not responsible for encryption. If Frank's team discovers that TLS is not enabled, they will need to work with the infrastructure or systems administration team to ensure that TLS is enabled and in use rather than making API changes.
    - Test exchange data process

OWASP Top 10 API Security Risks – 2023

Code Review and user **acceptance** testing are valuable in preventing security vulnerabilities but are typically conducted later in the SDLC and more critical step in prevention of security vulnerabilities is doing requirements gathering.

Regression testing

Regression testing is software testing that runs a set of known inputs against an application and then compares the results to those produced by an earlier version of the software. It is designed to capture unanticipated consequences of deploying new code versions prior to introducing them into a production environment.

Verify that the most recent patch for his organization's critical application did not introduce issues elsewhere, through regression testing.

key performance measure to measure the effectiveness of regression testing:
- measuring the rate of defect recurrence is appropriate
- defect recurrence rates

Most important reason for including security controls in the system development life cycle (SDLC) is to ensure secure coding practices are followed.

Secure coding techniques
- Using stored procedures
- Using code signing

- Using server-side validation

System development security controls
- Systems should be designed to operate in a secure manner if the user performs no other configuration.
- Systems should be designed to fall back to a secure state if they experience an error.
- Systems should be designed to incorporate security as a design feature.
- Systems should be designed in a manner that keeps their functionality as simple as possible.

Nonregression testing checks to see whether a change has had the effect it was supposed to.

Domain 6 Static Vs Dynamic Testing

Program understanding, program comprehension, pair programming, software inspections, and software walk-throughs are all human-centric methods for reviewing code.

Static program analysis, reviews are typically performed by an automated tool.
Static program reviews are typically performed by an automated tool.

Human-centric Code Review Methods

- Program understanding
- program comprehension
- pair programming
- software inspections
- software walk-throughs

Static program code review is not typically performed by a human, an example of a tool, SonarQube or Infer Static Analyzer.

Static Code Testing

Static software testing
Techniques include code reviews, evaluating the security of software **without running code** by analysing either the source code or the compiled application.
Static analysis is most suitable for evaluating the security posture of an application source code.

Code coverage testing:
- **Branch cover**age
  - evaluates whether every **if statement** has been executed under all **if and else** conditions.
  - all branches have been fully explored
- **Statement coverage** tests verify that every line of code was executed during the test.

    - verifies that every line of code was executed
    - each statement has been executed
- **Condition** coverage tests whether every logical test in the code has been executed under all sets of **input**.
    - Each condition has been evaluated for all possibilities.
- **Function** coverage verifies that every function in the code has been **called** and returned results.
    - requires that every function has been called
- **Loop** coverage verifies that every loop in the code has been executed under conditions that cause code execution **multiple times, only once, and not at all**.

Defect Density is a secure development metric that attempts to determine the average number of defects per lines of code (LoC).

Code coverage testing most frequently requires that every function has been called, that each statement has been executed, that all branches have been fully explored, and that each condition has been evaluated for all possibilities.

Dynamic software testing

Evaluates the security of software in **a runtime env**ironment and is often the only option for organisations deploying applications written by someone else.
Written by someone else, is not a requirement.

Domain 6 Fuzzing & Testing

fuzzing tests invalid inputs.

Fuzzing test technique

Uses modified inputs to test software performance under unexpected circumstances
Modifies known inputs to generate synthetic **inputs** that may **trigger** unexpected behaviour
Synthetic inputs

generational fuzzing

Generational fuzzing develops inputs based on models of **expected inputs** to perform the same task.

Mutation fuzzing

Mutation fuzzing uses bit flipping and other techniques to **slightly modify previous inputs** to a program in an attempt to detect software flaws.
Mutation testing or generational fuzzing will help determine how the program responds to expected inputs but does not test the business logic.

Mutation testing is a method used to automatically design new software tests and to ensure the quality of tests.
Mutation testing modifies a program in small ways and then tests that mutant to determine if it behaves as it should or if it fails.

Manual testing

Able in identifying business logic flaws.
Manual testing uses human understanding of business logic to assess program flow and responses.
Interface testing ensures that data exchange between modules works properly but does not focus on the logic of the program or application.

Automated Functional Test

Business logic errors are most likely to be missed by automated functional testing.
If a complete coverage code test was conducted, runtime, input validation, and error handling issues are likely to have been discovered by automated testing. Any automated system is more likely to miss business logic errors, because humans are typically necessary to understand business logic issues.

Synthetic transactions

Synthetic transactions application security testing technique uses scripts containing routine activity with known results and then compares the actual results of executing the script with expected outcomes
Synthetic transactions are **scripted** transactions with known expected results. This is a type of dynamic, not static, application security testing.
Mutation testing and other fuzzing techniques are also a dynamic testing option but they do not use predefined scripts of known transactions. Ffuf

Ethical Disclosure

However, the ethical disclosure principle also suggests that those reporting a vulnerability should provide the vendor with a reasonable amount of time to correct the vulnerability and, if it is not corrected, then publicly disclose the vulnerability so that other security professionals may make informed decisions about their future use of the product
Ethical (or responsible) disclosure practices will provide companies and organizations with a reasonable period of time to fix a flaw and to get that fix into the hands of their customers.
Ethical disclosure involves informing organizations of flaws and issues. Unlike **bug bounties**, this does not rely on organizations providing financial or other rewards.
Ethical disclosure may involve timeframes to ensure that companies do not ignore issues, but a focus on collaboration and public safety is common.
CVEs are created when flaws are reported to the CVE program.
There is no **blackmail** behavior involved in this description.

Domain 6 Security Management Oversight

Security managers must perform a variety of activities to retain proper oversight of the information security program.

Log reviews
Particularly for administrator activities, ensure that systems are not misused.
Log review traffic information between parts of the network, use **flow logging** of network logging type to perform this analysis.
Network flow (NetFlow) logs are particularly useful when investigating security incidents. These logs provide records of the connections between systems and the amount of data transferred.

Account management reviews
Ensure that only authorised users retain access to information systems

Backup Verification - the most important
Ensures that the organisation's data protection process is functioning properly.
The backup verification process ensures that backups are running properly and thus meeting the organization's data protection objectives.

Key performance and risk indicators (KPI)

KPIs are used to determine how effective practices, procedures, and staff are.
Provide a high-level view of security program effectiveness. Evolution of processes and handle changes and improvements.
key performance and risk indicators for organization's information security program.
KPI Measure Matrix:

- Mean time to detect a compromise
- time to resolve vulnerabilities
- the number of account compromises
- the number of attempts by users to visit malicious sites
- the number of repeat audit findings.

Training and Awareness

Training and awareness programs play a crucial role in preparing an organisation's workforce to support information security programs.
Security **awareness prog**ram purpose is to To educate employees about security risks and best practices.
To gather information about security awareness in an organization, to assess the broad range elements that make up security awareness, run surveys.
Most organizations use surveys to assess security awareness.

Social engineering awareness campaigns are tested by performing a phishing simulation.

Training is teaching employees to perform their work tasks and to comply with the security policy. Training is typically hosted by an organization and is targeted to groups of employees with similar job functions.

Awareness establishes a common baseline or foundation of security understanding across the entire organization and focuses on key or basic topics and issues related to security that all employees must understand. Although it is provided by the organization, it is not targeted to groups of workers since it applies to all employees.

Check for **content relevancy** is the primary purpose of a periodic content review for the security training material.

Domain 6 Internal and External Audits

Conduct or facilitate internal and third party audits

Security audits

Occur when a third party performs an assessment of the security controls protecting an organisation's information assets.

Internal Audits

Are performed by an **organisation's internal staff** and are intended for executive and management use.
External audits are performed by a third-party audit firm and are generally intended for the organisation governing body.
*Assume the audit is **3rd party** unless the question in the exam says otherwise!

The chief audit executive (CAE) should report to the most senior possible leader to avoid conflicts of interest. Of the choices provided, the chief executive officer (CEO) is the most senior position and the best option. It is also possible to provide an added degree of independence by having the CAE report to the board of directors, either as a primary reporting line or as a dotted line relationship.

Information security office would be least likely to report to the internal audit department. Internal auditors are generally tasked with evaluating how the company's employees are handling business processes, including IT security. Therefore an information security officer reporting to the internal audit department could be seen as a conflict of interest.

Network events logs are most likely to be audited to determine whether users are sharing illegal copies of software. Network events logs can record unauthorized or inappropriate activity that is occurring on the network. Logs show evidence of traffic to unauthorized services, such as a peer-to-peer file sharing network, could be evidence of illegal file sharing. Bittorrent utorrent torrents

Impact of Distributed IT Model

Cloud computing enables distributed IT service delivery, with systems that can **automatically replicate data globally.**
One impact of this distributed model is the additional geographic locations auditors must consider when performing an audit.

Geofencing - identify location of users accessing systems, limiting location conditional access policies.
It may also be worth considering that for devices that exit and enter the premises a geofencing type system be used, where wireless connection devices are deactivated as the equipment enters the facility.

Geofencing is the designation of a specific geographical area that is then used to implement features or trigger settings automatically on mobile devices.
A geofence can be defined by GPS coordinates, WiPS, or the presence of or lack of a specific wireless signal.
A device can be configured to enable or deactivate features based on a geofenced area, such as an onboard camera or the Wi-Fi capability.
If geofencing is available, it may be possible to use MDM/UEM to implement a location-specific hardware-deactivate profile to turn off the camera (or other components) while the device is on company premises but return the feature to operational status once the device leaves the geofenced area.

A common technique in cloud audits is sampling, which is the act of picking a subset of the systems physical infrastructure to inspect.
Example: Sampling 20 servers of 100 servers across many regional data centres can save time & expense and maintain accuracy.

CSPs have found ways to collect evidence that provides auditors with sufficient assurance that they have collected a representative sample.

Domain 7 Security Operations

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!
CISSP Exam Cram - 2024 Addendum

- Understand and comply with investigations
- Conduct logging and monitoring activities
- Perform configuration management
- Apply foundational security operations concepts
- Apply resource protection
- Conduct incident management
- Operate and maintain detective and preventive measures
- Implement and support patch and vulnerability management (VM)

- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery DR processes
- Test Disaster recovery plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

- Threat feeds
- User and entity behaviour analytics (UEBA) - monitor end user activity for signs of compromise
- Next generation firewalls
- Web application firewalls
- Use of machine learning and artificial intelligence

Domain 7 Conduct incident management

Basic security controls that can prevent many attacks:

- Keep systems and applications up to date.
- Remove or disable unneeded services or protocols.
- Use up-to-date antimalware software

Also appropriate to place a network WAF firewall at the border (between the Internet and the internal network), but web application firewall (WAF) only filters traffic going to a web server.

CISSP 7 Incident Management Steps - Objectives:

- Detection
- Response
- Mitigation
- Reporting - Incidents should be reported before recovery.
- Recovery
- Remediation
- Lessons Learned

Domain 7 Modern Firewalls

Covered with other FW types in ***Domain 4***

- **WAF**, web application firewall, filtering and monitoring HTTP traffic between a web application and the internet. Protects web apps from **common attack**s, XSS, CSRF, SQL injection, etc.
- **NGFW (Next Generation FireWall)**, deep packet inspection firewall that moves beyond port protocol inspection and blocking. Adds application level inspection, intrusion prevention and brings **intelligence from outside** the firewall.

Domain 7 SIEM and SOAR

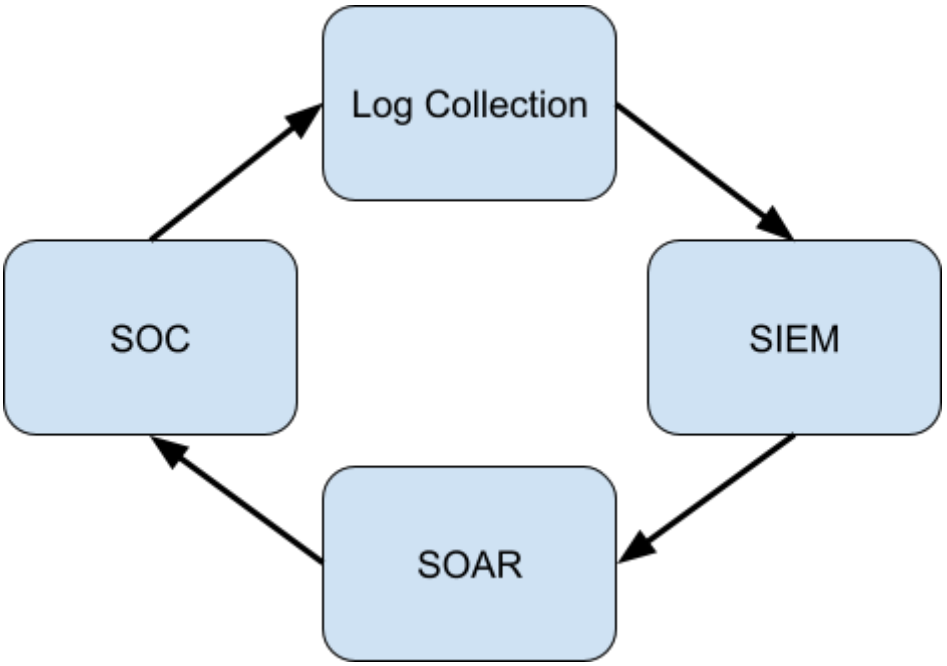
SIEM - Security Information Event Management
System that collects data from many other sources within the network.
Provides real-time monitoring, traffic analysis & notification of potential attacks.

SOAR - Security Orchestration Automation Response
Centralised alert and response automation with threat-specific playbooks and runbooks.
Response may be fully automated or single click

These capabilities are commonly delivered together in a single solution.
Often use AI, ML and threat intelligence, ChatGPT, copilot, LLM, etc.

Security Orchestration Automation & Response (SOAR)

Tooling that allows an organization to define incident analysis and response procedures in a digital workflow format.



Integrates your security processes and tooling in a central location.
Response automation, using machine learning and artificial intelligence.
These make it faster than humans in identifying and responding to true incidents.
Reduces MTTD and accelerates response.
Mean time to detect (MTTD) is a measure of how long a problem exists in an IT deployment before the appropriate parties become aware of it. MTTD is also known as mean time to discover or mean time to identify. MTTD is a common key performance indicator (KPI) for IT incident management.
Uses playbooks that define an incident and the action taken.
Capabilities vary by situation and vendor.
Over time should produce faster alerting and response for the SOC team.

Syslog

Syslog is a widely used protocol for event and message logging.
Syslog, message logging standard is commonly used by network devices, Linux and Unix systems, and many other enterprise devices.

SYSLOG System support:

- Enterprise wireless access points
- Linux web servers
- Enterprise firewall devices

To send syslog events, Windows systems require a helper application or tool.

Logging, Storage & Analysis of Data Events

Logs are worthless if you do nothing with the log data. They are made valuable only by **review**.

Log management systems factors:

- The volume of log data
- Data storage security requirements
- Network bandwidth
- effort required to analyze

Log management system designs must take into account the volume of log data and the network bandwidth it consumes, the security of the data, and the amount of effort required to analyze the data.

That is they are valuable only if the organization makes use of them to identify activity that is unauthorized or compromising.
SIEM (security Information Event Monitoring) tools can help to solve some of these problems by offering these key features:

- Log centralization and aggregation
- Data **integrity**
- Normalisation
- Automated or continuous monitoring
- Alerting
- Investigative monitoring

SIEM and SOAR are often integrated, with SOAR runbooks invokable from the SIEM

Playbook - Paperwork
A Document or checklist that defines how to verify an incident.

Runbook - Technology
Implements the playbook data into an automated tool.

Key SIEM features necessary to optimise event detection and visibility and scale security operations:

Log centralization and aggregation

Rather than leaving log data scattered around the environment on various hosts, the SIEM platform can gather logs from a variety of sources, including:

- Operating systems
- Applications
- Network appliances
- Cloud infrastructure
- Cloud services
- User devices

Investigative Monitoring

When manual investigation is required, the SIEM should provide support capabilities such as querying log files, generating reports.

< Data <> Apps <> Identities <> Endpoints <> Infrastructure >
Broad SIEM visibility across the environment means better context in log searches, and security investigations.

Passive monitoring

Passive monitoring works only after problems have occurred.
Passive monitoring works only after issues have occurred because it requires actual traffic.

Passive Monitoring Example:
performing passive monitoring, which uses a network tap or SPAN port to capture traffic to analyze it without impacting the network or devices that it is used to monitor.
Passive monitoring uses a network span, tap, or other device to capture traffic to be analyzed.
Passive monitoring uses a span port or other method to copy traffic and monitor it in real time.

Synthetic transaction monitoring

monitoring uses simulated traffic to a website to monitor performance

Synthetic monitoring uses simulated or recorded traffic and thus can be used to proactively identify problems.

Proactive monitoring, aka synthetic monitoring, uses recorded or generated traffic to test systems and software.
Both synthetic and passive monitoring can be used to detect functionality issues.

Synthetic transaction monitoring uses emulated or recorded transactions to monitor for performance changes in response time, functionality, or other performance monitors.

Scenario: Synthetic, use case testing
Emily builds a script that sends data to a web application that she is testing.
Each time the script runs, it sends a series of transactions with data that fits the expected requirements of the web application to verify that it responds to typical customer behavior.

Synthetic, or active, monitoring uses recorded or generated traffic to test for performance and other issues.

Real User Monitoring RUM

Real user monitoring (RUM) is a **passive monitoring** technique that records user interaction with an application or system to ensure performance and proper application behavior.
RUM is often used as part of a pre-deployment process using the actual user interface.
RUM passive monitoring technique records all user interaction with an application or website to ensure quality and performance

Domain 7 Intelligence in Threat Modelling

UEBA

Entity **behav**iour is collected and input into a threat model
Model establishes a **baseline** of "**normal**" based on historical data.
Enables analysis to uncover more details around **anoma**lous events
Automated investigation also exists in some platforms.
The UEBA system identify abnormal actions taken by an end user.

Threat Intelligence

Threat Feeds
Activities an organisation undertakes to **educate** itself about changes in the **threat** landscape.
To provide real-time information about emerging threats.
Often a **feed** containing malicious **entities** ingested by cybersecurity tools
A single feed may be composed of many sources, including open source intelligence
Entity **=** IP, Website, threat actor, file hash, and more.

CAPEC, or Common Attack Pattern Enumeration and Classification, is a dictionary of known attack patterns. STIX is the Structured Threat Information eXpression language used to describe threats in a standardized way, and TAXII, the Trusted Automated eXchange of Indicator Information, defines how threat information can be shared and exchanged. All of these are examples of threat intelligence feed standards.

Domain 7 Role of AI & ML

Analysing and improving cybersecurity posture is no longer a human-scale problem. Artificial Intelligence (**AI**) based tools for cybersecurity have emerged to help information security teams reduce breach risk and improve their security posture efficiently and effectively.

Machine learning uses mathematical approaches to analyse data, searching for patterns that predict future activity.

Along with AI, **machine learning (ML)** has become critical technologies in information security, in quickly analysing millions of events and identifying many different types of threats.
Histories of behaviour build profiles on users, assets, and networks, allowing AI to **detect** and respond to **deviations** from established norms.
Know that AI and ML factor in anti-malware, SIEM, IPS/IDS and IDAAS and more.

- The use of **labelled data**sets is found in supervised learning approaches.
- The other major category of machine learning techniques, unsupervised learning, uses **unlabeled data**sets.

See Domain 1.

Domain 7 Limiting Access & Damage

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Need-to-know and the principle of **least privilege** are two standards IT security principles implemented in secure networks.

They **limit access** to data and systems so that users and other subjects have **access only** to what they **require**.
They help **prevent** security **incidents**
They help **limit** the **scope** of incidents when they **occur**.

When these principles are not followed, security incidents result in far greater damage to an organisation.

Domain 7 Prevent Fraud and Collusion

Collusion is an agreement among multiple persons to perform some unauthorized or **illegal** actions.
Separation of duties
A basic security principle that ensures that no single person can control all the elements of a critical function or system.
Separation of duties is an access control principle that is designed to create a system of checks and balances on employees who have privileged access.

Job rotation
Employees are rotated into different **jobs**, or tasks are assigned to different employees.
A financial organization commonly has employees switch duty responsibilities every 6 months.

Implementing these policies helps **prevent fraud** by limiting actions individuals can do without **colluding** with others.

Group user accounts allow for multiple people to log in under a **single user** account. This allows **collusion** because it prevents individual accountability. Separation of duties, restricted job responsibilities, and job rotation help establish individual accountability and control access (especially to privileged capabilities), which in turn limits or restricts **collusion**.
Example of bad practice: Retail stores using same login account

Domain 7 Monitoring privileged operations

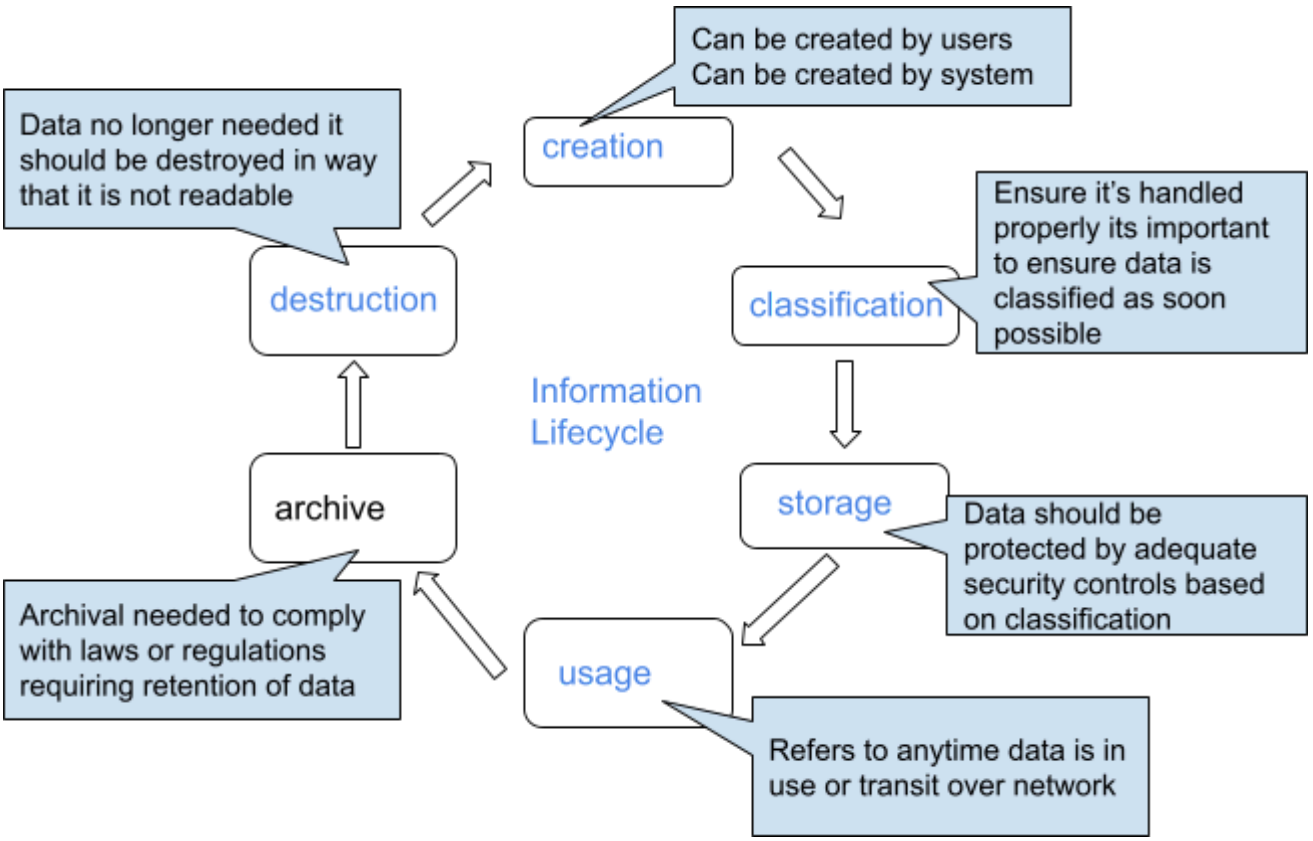
Privileged entities are trusted but they can abuse their privileges.
It is important to monitor all assignment of privileges and the use of privileged operations.

Goal
To ensure that trusted employees do not abuse the **special priv**ileges they are granted.

Monitoring these **oper**ations can also **detect** many attacks because attackers commonly use special privileges.

Domain 7 Information Lifecycle

See Domain 2 The Data Lifecycle.



CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Service Level Agreements

A service level agreement (**SLA**) is an agreement between an organization and an outside entity, such as a vendor. The SLA stipulates performance expectations and often includes penalties if the vendor doesn't meet these expectations.
A service-level agreement (**SLA**) can provide monetary penalties if a third-party provider doesn't meet its **contractual** requirements.

To define the expectations and responsibilities of both parties.

Stipulate **perfo**rmance **exp**ectations such as **max**imum downtimes and often include penalties if the vendor does not meet expectations. OLA between org departments.

Multiparty risk exists when several entities or organizations are involved in a project. The risk or threats are often due to the variations of objectives, expectations, timelines, budgets, and security priorities of those involved.

Service Level Requirement

A service-level requirement (SLR) is a statement of the expectations of service and performance from the product or service of a vendor. Often, an SLR is provided by the customer/client prior to the establishment of the service-level agreement (SLA) (which

should incorporate the elements of the SLR if the vendor expects the customer to sign the agreement).

Resource capacity agreement

A resource capacity agreement (RCA) is the most appropriate for concerns that the cloud provider his organization relies upon for disaster recovery may not be able to meet their needs in the event that a disaster strikes multiple customers simultaneously, as it specifically addresses the availability of resources in a disaster scenario.

Resource Capacity Agreements
Pre-arranged agreements with vendors to secure the necessary resources needed after a disruptive event
Ensure an organisation has access to resources at a recovery site.

A business partners agreement (BPA) and interconnection security agreement (ISA) could also be viable in defining and establishing minimum security requirements for the third party.

An interconnection security agreement (ISA) is a formal declaration of the security stance, risks, and technical requirements of a link between two organizations' IT infrastructures. The goal of an ISA is to define the expectations and responsibilities of maintaining security over a communications path between two networks. Connecting networks can be mutually beneficial, but it also raises additional risks that are related to third-party connectivity.

Secure Provisioning

Resources includes ensuring that resources are deployed in a **sec**ure **man**ner and maintained in a secure manner throughout their life cycles.
Docker container golden images do not contain malicious code content.
Scenario:
Security administrators are considering different configuration management methods.
Using images, is the MOST effective method of configuration management provisioning

Domain 7 Virtual Assets

Virtual assets include:

- Virtual machines (**VM**)
- Virtual Desktop infrastructure (**VDI**)
    - A nonpersistent system or static system is a computer system that does not allow, support, or retain changes.
- Software defined networks (**SDN**)
- Virtual storage area networks (**SAN**)

Hypervisors are the primary component that manages **virtual ass**ets, but also provide attackers with an additional target.
Hypervisors and VMs need to be **patch**ed.

Scenario - Secure BYOD remnant data

Valerie needs to control access to applications that are deployed to mobile devices in a BYOD environment.
What type of solution will best allow her to exercise control over the applications while ensuring that they do not leave remnant data on the devices used by her end users?
Answer
Use a virtual hosted application/virtual desktop infrastructure (**VDI)** environment that requires authentication using enterprise credentials.
When very high levels of control are needed or when endpoint devices cannot be trusted, using a centralized environment with remote connectivity and enterprise authentication can provide appropriate security.

VM escape protection

Virtual Machine (VM) escaping occurs when software within a guest OS is able to breach the isolation protection provided by the hypervisor in order to violate the container of other guest OSs or to infiltrate a host OS. This is a serious concern that must be addressed before full deployment into production of this new infrastructure solution.
This is **not** a data sovereignty issue. Data sovereignty is the concept that, once information has been converted into a binary form and stored as digital files, it is subject to the laws of the country within which the storage device resides.

Security issues with cloud-based assets
Storing data in the cloud increases the risk, so steps may be necessary to **protect** the **data**, depending on its **value**.

CASB to aid in finding **shadow IT** assets.

When leasing cloud based services, you should know who is **resp**onsible for maintenance and security.
Shared responsibility model for cloud based services.

The cloud service provider (**CSP**) provides the least amount of maintenance and good security in the **IaaS** model.

Domain 7 Shared Responsibility model

Responsible
CSP
Customer

Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime

Middleware	Middleware	Middleware	Middlewaref
OS	OS	OS	OS
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
On-Premises	**IAAS**	**PAAS**	**SAAS**

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Organizations have the most responsibility for maintenance and security when leasing Infrastructure as a Service (IaaS) cloud resources.

Software-defined security

Software-defined security (SDS) is an increasingly common approach to security that involves using software solutions and policies to secure environments, rather than traditional hardware-based approaches.
Software-defined security strategy allows for flexible and dynamic security configurations, particularly suited to the cloud's scalable nature.
SDS risk is blue screening windows operating systems through software defined security updates.

CrowdStrike - 2024 human error risk materialised globally

Software-defined security is an example of infrastructure as code (IaC)
SDS is commonly used within an Agile development framework.
DevOps approach links together development and operations but is generally called DevSecOps when it also includes SDS.

Example of SDS
Nathan recently completed a software development project where he integrated the organization's network operations stack with their development processes. As a result, developers can modify firewall rules from their code on an as-needed basis.
This is an example of software-defined security (SDS), where security infrastructure may be easily manipulated by code.

Scalability and Elasticity

Scalability refers to the ability of a system to handle additional workloads by adding additional resources.
Example: server has 16 GB of random access memory (RAM), but it can support 64 GB of RAM. It's possible to shut down the server and add additional RAM to scale it up.

Elasticity refers to a system's ability to add and remove resources dynamically, based on increasing or decreasing load.
Example, an e-commerce web server with 16 GB of RAM and a four-core processor. Marketing launches an excellent advertising campaign (black friday) along with a sale. Suddenly, the server is overwhelmed with traffic.
A cloud provider that supports elasticity can dynamically add more RAM and processors to meet the increased workload. When the sale ends and the workload decreases, the cloud provider can dynamically remove the additional resources.

Scenario:
Your company is evaluating several cloud providers to determine which is the best fit to host your **custom services as a custom app**lication solution.
There are many aspects of security controls you need to evaluate, but the primary issues include being able to **process signi**ficant amounts of **data** in short periods of time, controlling which applications can access which assets, and being able to prohibit **VM sprawl** or repetition of operations.
The following is relevant to this selection process:

- **Collections of entities**, typically users, but can also be applications and devices, which can be **granted or denied access** to perform specific tasks or access certain resources or assets - requirement of controlling which applications can access which assets
- Elasticity - The ability of a cloud process to use or consume more resources (such as compute, memory, storage, or networking) **when needed**
- prohibiting VM sprawl - A management or security mechanism able to **monitor** and differentiate between numerous **instances** of the same VM, service, app, or **resource**

VM Sprawl
Sprawl occurs when organizations fail to plan their IT/IS needs and just deploy new systems, software, and VMs whenever their production needs demand it. This often results in obtaining underpowered equipment that is then overtaxed by inefficient implementations of software and VMs.

Domain 7 Configuration & Change Management

Can prevent incidents and outages.
Ensuring that changes do not reduce security.

Steps included in a change management process:

- requesting a change

- creating a rollback plan for the change
    - Backout plans are required in some change management processes to ensure that the thought process and procedures for what to do if something does not go as planned are needed. Validating backout plan quality can be just as important as the change, and you may find, in many organizations, if nobody is watching, that backout plans may read, “Undo the change we made.”
- Documenting the change

IT service management, or ITSM, tools include change management and thus the type of approvals and review processes.

Scenario - Change management processes:
While troubleshooting a network problem, a technician realized the problem could be resolved by opening a port on a firewall. The technician opened the port and verified the system was now working. However, an attacker accessed this port and launched a successful attack. Change management process could have prevented incidents and outage problems.

Configuration Management

Scoping, is the review of a list of baseline security controls and identifies the security controls that apply to this database server.
Ensures that systems are configured similarly, configurations are known and documented.
Baselining ensures that systems are deployed with a **common** baseline or starting point, and imaging is a common baselining method.
Security baseline provides a starting point for secure system configuration.
Using **policy** for applying security means settings are **consistent**.
Shift and **Drift** resulting in gabs.
An organization has recently added a configuration management system (CMS) to automate configuration management, and it also provides hardware asset management.

Change Management

Helps **reduce outages** or **weak**ened **sec**urity from **unauth**orized changes.
Versioning uses a labelling or numbering system to track changes in updated versions of software.
Change management program aims to ensure that any change does not result in unintended outages or reduce security.
Requires changes to be **req**uested, **appr**oved, **test**ed, and **doc**umented.

Domain 7 Patch Management

Update Management
Ensures that systems are kept **up-to-date** with current security **patches**.
Will **evalu**ate, **test**, **appr**ove, and **depl**oy patches.
System **audits** verify the deployment of approved patches to the system.

Intertwined with change and configuration management to ensure that documentation **reflects** changes.

Patch management Policy:
- Evaluate patches.
- Test patches.
- Audit patches.

Orgs without patch management will experience outages from **known issues t**hat could have been **prev**ented.
Implement a patch management program that tests patches before deploying them.

Patch management program

- ☐ **Evalu**ate patches
- ☐ **Test** patches
- ☐ **Appr**ove the patches
- ☐ **Deploy** the patches
- ☐ **Verify** the patches are deployed
- ☐ **Vulne**rability scans can identify missing patches - **external source of truth**

The availability of vendor support and updates, is key risks associated with a new **software app**lication consideration.

Domain 7 Vulnerability Management

Vulnerability **Man**agement (VM) includes routing vulnerability **scans** and periodic vulnerability assessments.
Vulnerability scanners is a tool that scans a system for available services and then connects to them to collect banner information to determine what version of the service is running. It then provides a report detailing what it gathers, basing results on service fingerprinting, banner information, and similar details it gathers combined with CVE information.

Vulnerability **scan**ners can detect **known security vuln**erabilities and weaknesses, absence of patches or **weak pass**words.
Once a vulnerability scanner identifies a potential problem, validation is necessary to verify that the issue exists.
Reporting, patching, or other remediation actions can be conducted once the vulnerability has been confirmed.

Vulnerability **Ass**essments extend beyond just technical **scans** and can include reviews and **aud**its to detect vulnerabilities.
Example products: Qualys / Tenable

Authenticated scan

Authenticated scans use a read-only account to access configuration files, allowing more accurate testing of vulnerabilities.
Authenticated scan accesses configuration information from the systems it is run against as well as information that can be accessed via services available via the network

Security Content Automation Protocol (SCAP)
The Security Content Automation Protocol (SCAP) is a suite of specifications used to handle vulnerability and security configuration information. The National Vulnerability Database provided by NIST uses SCAP to standardize its vulnerability management program.

The CVE component of SCAP can be used to reconcile the identity of vulnerabilities generated by different security assessment tools.

The Common Vulnerabilities and Exposures (CVE) database provides a consistent reference for identifying security vulnerabilities. The Open Vulnerability and Assessment Language (OVAL) is used to describe the security condition of a system. The Extensible Configuration Checklist Description Format (XCCDF) is used to create security checklists in a standardized fashion. The Script Check Engine (SCE) is designed to make scripts interoperable with security policy definitions.

See Domain 7 Threat Intel Feeds!

Domain 7 Managing Incident Response

Primary objective of a **security inci**dent **resp**onse plan is to identify and respond to security incidents promptly.
Communication and coordination with relevant stakeholders is critical consideration when developing an **inci**dent **resp**onse **plan**.

cybersecurity **incident response team** (CSIRT)
CSIRT representation normally includes at least representatives of senior management, information security professionals, legal representatives, public relations staff, human resources, and engineering/technical staff.
Law enforcement personnel would **not** be included on such a team and would only be consulted as necessary.

Incident response plan

The incident response (IR) process steps

1	Detection	***D -*** monitoring tools, IPS, firewalls, users, notification to management and help desk	
2	Response	***R*** - Triage is it really an incident, decision to declare	Limit Damage
3	Mitigation	***M*** - First containment effort or	Activate the **incident response**

		step create team	**team.** Contain an incident
4	Reporting	***R*** - Relevant stakeholders, customers, vendors, law	**Management decisions**
5	Recovery	***R*** - Return to normal operations	**Management decisions**
6	Remediation	***R*** - Root cause is addressed	Include root cause analysis Security personnel perform a root cause analysis during the remediation stage. A root cause analysis attempts to discover the source of the problem. Implement new security controls to prevent recurrence
7	Lessons Learned	***L*** - Helps prevent recurrence, improve IR process. post-incident review	postmortem review of a security incident, create lessons learned document. areas for improvement.

Detection is the first step.

After **detection** of a security incident, the next step in the process is **response**, which should follow the organization's formal incident response procedure. The first step of this procedure is activating the appropriate teams (Mitigation), including the organization's computer security **incident response team** (CSIRT).

The most crucial step immediately after detecting and responding in a security incident is to identify the scope and impact of the incident.

implement containment and mitigation measures.
Containment and mitigation are crucial steps, but they should be based on an understanding of the incident's scope and impact. Premature action without proper assessment could lead to incomplete or ineffective responses.

During a remediation operational investigation, root cause analysis is undertaken to prevent similar incidents in the future.

In the context of security incident response, the most important consideration when determining the **severity** of an incident is the financial impact on the organisation.

The primary purpose of a post-incident review is to assess the effectiveness of the response and identify areas for improvement.

Given the CVE-2023-12345 with a CVSS v3 base score of 9.8, the vulnerability is of critical severity and poses significant potential harm. CVSS v3 base score ranges from 0.0 to 10.0 with higher values indicating higher severity.

A score of 9.8 is considered **critical**, suggesting the vulnerability poses a significant threat if exploited.

Scenario
A security analyst observes multiple unauthorized data extraction attempts from a database server. Upon investigation, all extraction attempts have been traced back to a single user account.
Which of the following should be the analyst immediate action:

- Isolate or disable the account and initiate an incident response.

Context: It's appropriate to disable an account when an employee takes a leave of absence for 30 days or more.

Security incident

Any attempt to undermine the security of an organization or violation of a security policy is a security incident.

Events constitute a security incident:

- An attempted network intrusion
- A successful database intrusion
- A malware infection
- A violation of a confidentiality policy
- An unsuccessful attempt to remove information from a secured area

Above list of events described meet security incident definition and should be treated as an incident.

The exception is a successful attempt to access a file is certainly a security event, but it is not a security incident unless it is established that the individual accessing the file was not authorized to do so.

Domain 7 Denial-of-Service Attacks

Common characteristic of a denial-of-service (DoS) attack is **overload**ing a system to **disrupt** services.
DOS attacks prevent a system from responding to legitimate requests for service.

In a DDoS attack the most important mitigation strategy during detection and response phase is the mitigating of the attack and restoring of services.

Denial-of-service (DoS)

Is a resource consumption attack intended to prevent legitimate activity on a victimised system.

Distributed Denial-of-service (DDoS)

A DDoS attack utilising multiple compromised computer systems as sources of attack traffic.

Countermeasures: firewalls, routers, intrusion detection (IDS), disable broadcast packets entering / leaving, disable echo replies, patching.
Verifying DDoS attack using:

- A network-based intrusion detection systems (NIDS)
- Logs on a border firewall
- A security information and event management (SIEM) system

Common DoS Attacks

- **SYN flood** attack, which disrupts the TCP three-way handshake
    - The attacker starts a TCP handshake but does not complete it.
- **Smurf Attack** employs an **amp**lification **net**work to send numerous response packets to a victim
- **Ping-of-death** attacks send numerous **oversized** ping packets to the victim, causing the victim to freeze, crash or reboot.

DDoS Scenario:
John is configuring a router that will stand between the network 10.8.6.0/24 and the Internet. He would like to configure egress filtering rules to minimize the potential of malicious actors originating a distributed denial-of-service (DDoS) attack from his network. What type of traffic should be filtered out to help achieve this goal?

- Outbound traffic with a source address outside the range 10.8.6.0/24

Domain 7 Botnets, controllers, & BOT Herders

Represent significant threats due to the massive number of computers that can launch attacks.
Botnet
A collection of compromised computing devices, often called bots or **zombies**.
Bot Herder
Criminal who uses a command-and-control (**C2**) server to remotely control the zombies.
Often use the botnet to **launch attacks** on other systems, or to send spam or phishing emails.
attackers leverage botnets to perform:

- Mining cryptocurrency - blockchain
- Conducting brute-force attacks
- Scanning for vulnerable systems
- sending out spam messages

Domain 7 Honeypot, Padded cell, Pseudo Flaws

Honeypot
A system that often has **pseudo** flaws and **fake** data to **lure** intruders.

Lures and **distracts** attackers.
Detect and analyse malicious activity using honeypot.
As long as attackers are in the honeypot, they are not in the live network.
Some IDSs have the ability to transfer attackers into a **padded cell** after detection.
Padded cell is a hardened honeypot.

Domain 7 Block Malicious Code

Multiple approaches, generally used together, best layered defense depth layers.
Anti-malware software
With up-to-date definitions installed on each system, at the boundary of the network, and on email servers.
Policies
Enforce basic security principles, like principle of **least privi**lege, prevent regular users from installing potentially malicious software.
Education
Educating users about the **risks** and the methods attackers commonly use to spread viruses helps users understand and avoid dangerous behaviours.
Most effective in preventing malware infection from malicious email attachments is email content **filtering**.

Domain 7 Penetration Tests

Start by discovering vulnerabilities and then mimicking an attack to **identify** what **vuln**erabilities can be **exploit**ed.

Senior management needs to approve penetration tests because of the risk to the organization and the potential impact of the test.
Should not be done without express **consent** and knowledge from management.
Can result in damage, so should be done on **isolated systems** whenever possible.

- **Black** box testing
  - User perspective with no access to nothing
  - (**Zero** knowledge - no access to source code)
  - In a black box test, the tester must not have access to the application's source code.
- **White** box testing
  - **Developer** with source code perspective
  - (**Full** knowledge)
  - White-box tests also have access to the source code but perform testing from a developer's perspective. .
  - software testers are required to test **every code path**, including those that will be used only when an error condition occurs.
- **Grey** box test
  - Gray box **user** perspective with source code
  - (**Partial** Knowledge)

- gray-box test, the tester evaluates the software from a user perspective but has access to the source code as the test is conducted.
- testing provides detail on the scope of a penetration test—including items like what systems would be targeted—but does not provide full visibility into the configuration or other details of the systems or networks the penetration tester must test

Domain 7 IDS vs IPS Response

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

IDS - reactive

Can respond passively by **logging** and sending notifications or actively by changing the environment.
IDS not capable of generating an active response to a security event.

IPS - proactive

Is place in line with the traffic and includes the ability to **block** malicious traffic before it reaches the target. More **proactive** to incidents.

HIDS (Host-based IDS)

Can monitor activity on a single system only. A drawback is that attackers can discover and disable them

NIDS (Network based IDS)

Can monitor activity on a network and a NIDS is not as visible to attacks.
NIDS is most likely to detect DoS attacks.

Anomaly-based IDS

Anomaly-based IDS requires a baseline, and it then monitors traffic for any anomalies or changes when compared to the baseline.
Anomaly-based Intrusion detection system is also called behavior based and heuristics based.
An anomaly-based IDS (also known as a behavior-based IDS) can detect new security threats.
Heuristic-based antimalware software has a higher likelihood of detecting a zero-day exploit than signature-based methods. Heuristic-based software does not require frequent signature updates because it does not rely upon monitoring systems for the presence of known malware.
The trade-off with this approach is that it has a higher false positive rate than signature detection methods.

Domain 7 Espionage & Sabotage

Espionage - external

When a competitor tries to steal information, they may **use an internal empl**oyee.

Scenario Espionage
Colin was recently hired by your organization as a product tester. Colin has been issued a company notebook with **cellular data service**. After a few weeks, you notice that there are blog postings that include details about a product in development that has not been publicly announced.
You suspect that Colin is an espionage agent from a competitor.
You carefully review the network edge DLP and firewall logs and see no indication that Colin transferred the confidential files out of the company network. You also confirm that the company computer never left the building.
Leak method: Using his company-issued device **with cellular data service** to create a bypass.

Sabotage - insider

Malicious **insiders** can perform sabotage against an org if they become **disgruntled** for some reason.
A company's security policy states that user accounts should be disabled during the exit interview for any employee leaving the company, to prevent sabotage.

An employee has left the organization and will start a new job tomorrow, the account can be deleted.

Domain 7 Zero-day Exploits

An attack that uses a vulnerability that is either **unknown to anyone** but the attacker or known only to **a limited group** of people.
Zero-day exploit Definition:
An attack that exploits a vulnerability that doesn't have a patch or fix

Basic security practices can often be **preventive** against zero day exploits.
Countermeasure: User behaviour analytics (UBA) driven AI antivirus and EDS/XDS solutions.

Method to quickly identify vulnerable systems:
- Identify affected versions and check systems for that version number using an automated scanner.
- In many cases when an exploit is initially reported, there are no prebuilt signatures or detections for vulnerability scanners, and the CVE database may not immediately have information about the attack. Jacob's best option is to quickly gather information and review potentially vulnerable servers based on their current configuration.

Domain 7 Log Files

Data is recorded in databases and different types of **log files.**

Common log files include **sec**urity logs, **sys**tem logs, **app**lication logs, **firewall** logs, **proxy** logs.

System logs record system events such as when services start or stop.
Should be **protected** by centrally storing them and using **perm**issions to restrict access.
Archived logs should be set to **read-only** to prevent modifications.
Immutable and integrity of logs.

Accountable Logs

Accurate **identific**ation and **authen**tication are required to support accountability.
Logs record events, including who took an action, but without accurate **identification** and **authentication**, the logs can't be relied on.
Authorization grants **access** to resources after proper **authen**tication.
Auditing occurs **after** logs are **created**, but identification and authentication must occur first.

Domain 7 Monitoring

A form of **audit**ing that focuses on active review of the log file data.
Monitoring is used to hold subjects accountable for their actions.
Also used to **mon**itor **sys**tem **perf**ormance.

Tools such as IDS or SIEM **auto**mate **monitor**ing and provide **real-time** analysis of **event**s.
SIEM's primary function is to monitor and analyze security events.

Scenario
This morning, the intrusion detection system alerted because the network began to receive an unusually high volume of inbound traffic. Ann received this alert and began looking into the origin of the traffic.
At this point in the incident response process, Security Event.

Tuning

Tuning of the SIEM to Reduce **false pos**itives but not getting **false neg**atives.
A **false neg**ative occurs when there is an attack but the IDS doesn't detect it and raises an alarm.

Audit Trails

Records created by recording **info**rmation about **event**s and occurrences into one or more databases or log files.
Used to reconstruct an event, to extrac**t info**rmation about an **incid**ent.
Used to **prove** or disprove **culpability**.
A passive form of **detecti**ve security control

Audit trails are **essential** evidence in the **prosecu**tion of **crim**inals.
Example of microsoft logging set to **common** is the least level of auditing trail needed to aid in investigating events. Minimum required in logging.

Domain 7 Sampling

Sampling
The process of **extracting elements** from a large body of data to construct a meaningful representation or summary of the whole.

Statistical sampling
Uses precise mathematical functions to extract meaningful information from a **large vol**ume of data.

Clipping
Is a form of non-statistical sampling that records only events that **exceed a thres**hold.
Clipping is a form of nonstatistical sampling that reduces the amount of logged data based on a clipping-level threshold.

Log analysis reviews log information looking for trends, patterns, and abnormal or unauthorized events.
An alarm trigger is a notification sent to administrators when specific events or thresholds occur.

Domain 7 Maintaining Accountability

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Accountability
Is maintained for individual **subjects** using auditIng.
Logs record user activities and users can be held accountable for their logged actions.
Directly promotes good user behaviour and compliance with the organisation's security policy.

Domain 7 Security Audits and Reviews

Security audits and reviews help ensure that management programs are effective and being followed.
Commonly associated with **account man**agement practices to prevent **violations** with **least** privilege or **need-to-know** principles.
Can also be performed to ***oversee*** many programs and processes

- Patch management
- Vulnerability management
- Change management
- Configuration management

Frequency of IT Security Audits

Auditing a **methodica**l **examin**ation of an environment to **ensure compliance** with regulations and to detect **abnorm**alities, unauthorized occurrences, or outright **crimes**.
Audit Serves as a primary type of detective control.

Frequency is based on **risk**.
Degree of **risk** also affects how often an **audit** is performed

PCI DSS

PCI DSS allows organizations to choose between performing annual web vulnerability assessment tests or installing a web application firewall (WAF).

Secure IT environments rely heavily on auditing and many **regulations** require it.
Example is the **PCI DSS** environment audits.

Large organizations hire QSAs, or qualified security assessors, to conduct compliance checks. Third-party certification is required for large organizations by PCI-DSS, although smaller organizations can self-certify.

Domain 7 Concept of Due Care

Do Correct = Due Care
The due care principle states that an individual should react in a situation using the same level of care that would be expected from any reasonable person.
Due care is a legal liability concept that defines the minimum level of information protection that an organisation must achieve.

Due Care : reasonable care to protect the interests of your organization, legal liability
Due Diligence : planning ongoing execution and monitoring of **Due Care !**

Auditing and **due care**
Best represents the concept of "due care" in security governance is exercising reasonable security measures to protect assets.
Security audits and effectiveness reviews are key elements in displaying due care, without them, senior management will likely be held accountable and **liable** for any asset losses that occur.

The absence of **Periodic security audits,** can result in the perception that **due care** is not being maintained

Act with **common sense**, **prudent** management, responsible **action**.
Prudent actions refer to actions or decisions that are marked by a high degree of caution, care, and foresight. They are characterized by careful consideration of potential risks, a focus on preventing harm, and a commitment to acting in a manner that is consistent with established best practices or industry standards.

Example of Prudent Action:
A CISO has spent considerable time investigating the issues regarding a newly identified threat. After considering as many aspects of the concern as possible, a risk response decision has been made to implement specific security technology changes as well as adjustments to certain work procedures.
Prudent Action performed by the CISO.

Due Diligence

Do Detect = Due Diligence
The due diligence principle is a more specific component of due care that states that an individual assigned a responsibility should exercise due care to complete it accurately and in a timely manner.
Due diligence is a key principle of security governance, emphasizing the importance of thorough research and investigation when making security decisions.
Due diligence, describes the preparation and research undertaken before decisions and actions are made.

Due diligence is establishing a plan, policy, and process to protect the interests of an organization.
Example: Annual review by board of directors of the BCP process to ensure that adequate measures are in place to minimise the effect of disaster on company continued viability.

Due care is practising the individual activities that maintain the security effort.

Security Governance

Security governance should include acquisitions, **divestitures**, and governance committees. Disaster recovery planning focuses on preventing interruptions and recovering from disasters. Standards and baselines focus on establishing mandatory configuration requirements for systems. Trusted recovery planning focuses on restoring the assurance of a system after a failure.

- Security governance is the collection of practices related to supporting, defining, and directing the security efforts of an organization.
- Security governance is the implementation of a security solution and a management method that are tightly interconnected.
- Security governance directly oversees and gets involved in all levels of security.

Divestiture

A **divestiture** occurs when something is being removed from the organization, whether a device, service, employee, or partnership.
Security processes should be implemented at these times to reduce the risk of data loss and leakage, such as sanitising assets, removing and destroying storage media, and debriefing ex-employees.

The protection of intellectual property is a greater concern during a divestiture, where a subsidiary is being spun off into a separate organization, than an acquisition, where one firm has purchased another.

Acquisition concerns include
- consolidating security functions

- Document of security policies
- integrating security tools.

Domain 7 Controlling access to audit reports

CISSP Exam Cram Full Course (All 8 Domains) - Good for 2024 exam!
Audit reports often contain **sensitive info**rmation
Often include purpose and **scope** of the audit, and **results** discovered or **reveal**ed.
Can include **sensit**ive **info**rmation such as **prob**lems, standards, causes and **recommend**ations.
Only people with sufficient privilege should have access
Senior security administrators = **full detail** access
Senior management = **high level sum**mary access

Domain 7 User entitlements & Access reviews

Access Reviews
Ensure that **obj**ect **access and account man**agement practices support the **sec**urity **pol**icy.

User Entitlements
Ensure that the principle of **least priv**ilege is followed and often focus on **priv**ileged accounts.

Account Access Reviews

IAM/IDM - Recertification Identity Access Management Reviews
Privileged access reviews are one of the most critical components of an organization's security program because they ensure that only authorized users have access to perform the most sensitive operations.

- take place whenever a user with privileged access leaves the organization
- changes roles
- on a regular, recurring basis/periodic basis

Service Provisioning Markup Language (SPML) is used to provision users, resources, and services

Account reviews (IAM) can detect instances of creeping (model on accounts) privileges or excessive privileges.
Periodically or when change occurs perform account reviews.

Privilege creep is a constant concern when staff change roles over time. Privileges from previous roles may be easy to forget or to retain during transition because staff may continue to help cover the tasks or processes the individual previously performed. Over time, these forgotten rights and privileges can stack, leaving the staff member with rights that their current role should not have.

Account access reviews can detect security issues for service accounts such as the sa account (short for system administrator) account in Microsoft SQL Server systems. Reviews can ensure that service account passwords are strong and changed often.

Example:
A recently acquired piece of equipment is not working properly. Your organization does not have a trained repair technician on staff, so you have to bring in an outside expert. **Privileged account** should be issued to a trusted third-party repair technician that requires above normal access level.

The ***management review and approval*** process ensures that each account was appropriately authorized and remains necessary to meet business needs.

Privileged account management (**PAM**)

Privileged account management ensures that personnel do not have more privileges than they need and do not misuse their privileges.
Microsoft domains include a **privileged account management (PAM)** solution that grants administrators elevated privileges when they need them but restrict the access using a time-limited ticket.

Audit Access Controls

Effectiveness of access controls should be reviewed / **audited regular**ly
Can track **logon success** and **fail**ure of any account
Can include resource (object) access and **action performed on reso**urces
Intrusion **detecti**on **syst**ems can **mon**itor these logs and easily identify attacks and notify administrators

Often **auto**mated, auto-**reporti**ng, and supported by ***AI.***

Microsoft Co-pilot and Windows 11 Recall.
Google Gemini, ChatGPT, Meta, etc.

Domain 7 Computer Crime

A **crime** or **violation** of a **law** or regulation that is directed against, or directly **involve**s a **computer**.

6 Categories of computer crime

- **Military and intelligence atta**cks - To obtain secret and restricted information from military or law enforcement sources
- **Busi**ness attacks
- **Fin**ancial attacks
- **Terro**rist attacks - Damaging the ability to communicate and respond to a physical attack.
- **Grud**ge attacks - purpose of such an attack is to "**get back**" at someone.

- **Thrill** Attacks
    - Bragging rights
    - Pride of conquering a secure system

Six categories of computer ***crimes***. (Bacon)

Enticement

Enticement occurs when an individual who was already planning to commit a crime is eventually lured into doing so at the urging of law enforcement.
A companion concept to enticement is **entrapment**, which occurs when an individual who otherwise had no intention of committing a crime is lured into doing so at the urging of law enforcement.

Financial attacks

- Accessing services that you have not purchased
- Transferring funds from an unapproved source into your account
- Selling a botnet for use in a DDoS attack

Grudge Attacks

- Disclosing embarrassing personal information
- Launching a virus on an organization's system
- Sending inappropriate email with a spoofed origination address of the victim organization

Domain 7 Electronic Discovery

Organisations expecting lawsuits have a duty to preserve **digital evid**ence in a process called **eDiscovery.**
Electronic Discovery Reference Model process includes:

- **Infor**mation **identi**fication and governance
    - Identification locates the information that may be responsive to a discovery request when the organization believes that litigation is likely.
- **Preserv**ation and collection
    - Collection gathers the relevant information centrally for use in the eDiscovery process.
    - Preservation ensures that potentially discoverable information is protected against alteration or deletion.
- **Processi**ng
    - Processing screens the collected information to perform a "rough cut" of irrelevant information, reducing the amount of information requiring detailed screening.
    - Processing screens the collected information to perform a "rough cut" of irrelevant information, reducing the amount of information requiring detailed screening.

- **revie**w, analysis
    - **Review** examines the information resulting from the Processing phase to determine what information is responsive to the request and **remove any info**rmation protected by **attorney-client priv**ilege.
- **Prod**uction
    - Production places the information into a format that may be shared with others and delivers it to other parties, such as opposing counsel.
- Presentation
    - Presentation displays the information to witnesses, the court, and other parties.

Often uses **tag**ging, **classi**fication, target specific **custod**ian.

Domain 7 Gather info in Investigations

To gather sufficient information from the equipment, software, and data from equipment requires.

Possession

You must have possession of equipment, software or data to analyse it and use it as evidence.

Modification

You must acquire the **evidence without mod**ifying it or allowing anyone else to modify it.

Law enforcement establishes a **chain of evid**ence, aka **chain of custody**, to document all **who handle** it.

Competence of Evidence

To be admissible, evidence must be relevant, material, and competent.

If the court ruled that the search of the apartment that resulted in police finding the hacker laptop was unconstitutional, then this indicates a problem of evidence competence.

Forensic Methods provide the most reliable means of collecting and preserving the contents of network traffic:

- SPAN ports
- network taps

The most reliable mechanisms for gathering network traffic.

Network analysis is the type of analysis to review web server logs and is the process of examining Network traffic.

NetFlow

NetFlow data contains information on the source, destination, and size of all network communications, including botnet traffic that infected the network and is routinely saved as a matter of normal activity.

NetFlow records contain an entry for every network communication session that took place on a network and can be compared to a list of known malicious command-and-control servers.

Netflow and syslog are more commonly used for diagnostic and analysis tasks.
Real-time fault monitoring for network devices and connections often relies on SNMP and ICMP-based monitoring capabilities.

Aid forensic investigation.
NetFlow data is a reliable source of evidence, but it only captures information about the parties involved in a communication and the amount of data exchanged.
Netflow does not include the contents of network traffic.

Locard's Forensic principle

Locard's principle is most relevant to forensic investigation for **trace digital evidence,** as it suggests that any contact between two objects results in an exchange of materials. In the context of digital forensics, this principle implies that there is always some form of digital trace or residue left behind when devices interact or when data is transferred.
Locard principle is looking for elements of trace digital evidence.

Kerckhoffs

Kerckhoff's principle states that a system's security should not depend on the secrecy of its algorithm but rather on the secrecy of its keys.
Kerckhoffs' principle says that a cryptographic system should be secure even if everything about the system, except the key, is public knowledge.

Heisenberg's Uncertainty Principle states that there is inherent uncertainty in the act of measuring a variable of a particle. Commonly applied to the position and momentum of a particle, the principle states that the more precisely the position is known the more uncertain the momentum is and vice versa.

In the context of forensic investigations, demonstrating the **integrity** and authenticity of the evidence, best describes the primary purpose of **maintaining a chain of custody**.

Responsible Individuals for maintaining Chain of Custody:
- Policy investigators
- Evidence Technicians
- Attorneys

Alternatives to confiscating evidence

Voluntary surrender
The person who owns the evidence could **voluntarily** surrender it for investigation.

Subpoena
Could be used to **compel** the subject to surrender the evidence.

Search Warrant
Most useful when you need to **confiscate evid**ence without giving the subject an opportunity to alter or destroy evidence.

To obtain a search warrant, investigators must have probable cause that demonstrates that they will likely collect evidence related to a crime.

Domain 7 Retaining Investigatory Data

Because you will discover some incidents after they have occurred.
You will **lose valuable evidence** unless you ensure that critical log files are **retain**ed for a reasonable **period** of time.
You can retain log files and system status information either **in-place or in archives**.

Data retention should be defined in security **policies**.

Domain 7 Evidence

- Best - **Original**
- Secondary evidence - **Copy**
- Direct - proves or disproves an **act based on the five senses**.
- Conclusive - **incontrovertible** from other info - example on CCTV camera footage
- Circumstantial - **inference** from other info
- **Corroborative** - supporting evidence but cannot stand on its own
- Opinions - **expert** and non-expert
- Hearsay - **not** based on **first-hand** knowledge

Evidence must be **relevant**, **complete**, **sufficient** and **reliable**.

Domain 7 Evidence Admissibility

Types of evidence that may be used in a criminal or civil trial.

- **Real evidence**
  - consists of actual objects that can be brought into the courtroom.
  - Real evidence must be either uniquely identified by a witness or authenticated through a documented chain of custody.
  - Real evidence consists of **tangible** items brought into court as evidence.
  - Real evidence consists of things that may actually be brought into a courtroom as evidence.
- **Doc**umentary **evid**ence
  - consists of written documents that provide insight into the facts.
  - refers to written documents that are brought into court to prove a fact
  - Example: Server Logs.
  - Documentary evidence consists of written records used as evidence in court.
- **Testimonial evid**ence
  - consists of verbal or written statements made by **witnesses**.
  - Witness testimony is an example of **intangible** evidence that may be offered in court.
- Expert opinion
  - Expert opinion evidence allows individuals to offer their opinion based upon the facts in evidence and their personal knowledge. Expert opinion evidence

may be offered only if the court accepts the witness as an expert in a particular field.

- Direct Evidence
  - Direct evidence is when witnesses testify about their direct observations.
- **Civil** investigations typically follow the "**preponderance** of the evidence" standard.
  - preponderance: the quality or fact of being greater in number, quantity, or importance.
- **Demonstrative** evidence
  - The diagram that person will use to support this testimony is best classified as demonstrative evidence. It is not real or documentary evidence because it is not being used as proof itself, but rather to illustrate a concept.
- **Parol Evi**dence
  - The **parol** evidence rule states that when an agreement between parties is put into written form, the written document is assumed to contain all the terms of the agreement, and no verbal agreements may modify the written agreement.
  - The **parol evidence rule** states that when an agreement between two parties is put into written form, it is assumed to be the entire agreement unless amended in writing. The best evidence rule says that a copy of a document is not admissible if the original document is available.

Requirements for evidence to be admissible in a court of law:
Evidence To be admissible:

- Evidence must be **relevant** to a fact at issue in the case
- The fact must be **material** to the case
- The evidence must be competent or **legally collect**ed

Evidence rules

<u>Scenario - Hearsay - Court</u>
George is assisting a prosecutor with a case against a hacker who attempted to break into the computer systems at George's company. He provides system logs to the prosecutor for use as evidence, but the prosecutor insists that George testify in court about how he gathered the logs.
What rule of evidence requires George's testimony?
<u>Answer</u>:
hearsay rule
The hearsay rule says that a witness cannot testify about what someone else told them, except under very specific exceptions.
The courts have applied the hearsay rule to include the concept that attorneys may not introduce logs into evidence unless they are authenticated by the system administrator.
In this scenario, George might also be able to provide a sworn affidavit, but the question doesn't include that option.
The best evidence rule states that copies of documents may **not** be submitted into evidence if the originals are available.
The parol evidence rule states that if two parties enter into a written agreement, that written document is assumed to contain all of the terms of the agreement.

Testimonial evidence is a type of evidence, not a rule of evidence.

Criminal investigations

Criminal investigations typically follow the "***beyond a reasonable doubt"*** standard of evidence.
Criminal investigations may result in the imprisonment of individuals and, therefore, have the highest standard of evidence to protect the rights of the accused.

Evidence is **considered competent** if it complies with certain **traditional notion**s of reliability.

- Administrative investigations are for internal purposes and are not applicable when a third party is being investigated.
- Operational investigations are performed by internal teams to troubleshoot performance or other technical issues.
- Criminal and regulatory investigations may only be initiated by those with regulatory authority, typically government agencies.

Scenario Civil Investigation:
Evelyn believes that one of her organization's vendors has breached a contractual obligation to protect sensitive data and would like to conduct an investigation into the circumstances. Based upon the results of the investigation, it is likely that Evelyn's organization will sue the vendor for breach of contract.
This is an example of a civil investigation because it relates to a contract dispute and will likely wind up being litigated in **civil court.**

Domain 7 Collecting Evidence

Importance of collecting evidence
As soon as you discover an incident.
You must begin to collect evidence and as much information about the incident as possible.

Evidence can be used in a subsequent legal action or in finding the attacker's identity.
Evidence can also assist you in determining the **extent of damage.**

Context, preparing to create a forensic image of a hard drive from a system involved in a security incident.
Write blockers are hardware devices used to prevent the accidental writing of data to media that was collected as evidence.

Domain 7 Natural Disasters

Know the common types of **natural disaster**s that may threaten an organisation.

- Earth**quake**s
- **Floods**
    - Most general business insurance and homeowner's insurance policies do **not** provide any protection against the risk of **flooding** or flash **floods**. If floods

pose a risk to your organization, you should consider purchasing supplemental **flood** insurance under FEMA's National **Flood** Insurance Program.

- Tornado
- **Storm**s / Hurricane
- Tsunamis
- **Volc**anic eruptions
- Wildfires

Acts of nature.

Man-Made Disasters

Types of Man-Made Disasters that threaten an organisation:

- **Explo**sions
- Electrical **Fire**s
- **Terror**ist acts
- Power outages
- Hacking Incidents
- Other utility failures

Domain 7 Recovery Sites Types

Cold Site

A recovery cold site is essentially just data centre space power and network connectivity that is ready and waiting for whenever you might need it.
Cold sites take the longest time to activate but have the lowest cost to implement.
A cold site is any facility that provides only the physical space for recovery operations while the organization using the space provides its own hardware and software systems.

To Recover
If disaster strikes, your engineering and logistical support teams can readily help you move your hardware into the data centre and get you back up and running.
Cost = Low
Effort = **High**

Warm

A preventative warm site allows you to pre-install your hardware and pre-configure your bandwidth needs
To Recover
If disaster strikes, all you have to do is load your software and data to restore your business systems.
Cost = Medium
Effort = **Medium**

Hot Site

A proactive hot site allows you to keep servers and a live backup site up and running in the event of a disaster. You replicate your production environment in that data centre.
The alternate processing facility contains a full complement of computing equipment in working order with copies of data ready to go.
To Recover
This allows for an immediate cutover in case of disaster at your primary site. A hot site is a must for mission critical sites.
Cost = High
Effort = **Low**

Service Bureau

A company that **leases** computer time. Service bureaus own large server farms and often fields of workstations. May be **onsite or remote**.

Mobile Site

Non Mainstream alternatives to traditional recovery sites. They typically consist of **self-contain**ed **trailer**s or other easily relocated units.
nontraditional alternative recovery site is made up of transportable relocation units

Multiple sites

Just what it says, may **mix-and-match** some combination of the aforementioned options.

Domain 7 RPO and RTO

Disaster recovery plan key consideration: Defining recovery time objectives (**RTOs**) and recovery point objectives (**RPOs**)

Recovery Point Objective (RPO)

Is the **age of files** that must be recovered from backup storage for normal operations to **resume** if a system or network goes down.
The recovery point objective (RPO) specifies the maximum amount of data that may be lost during a disaster and should be used to guide backup strategies.

Recovery Time Objective (RTO)

Is the **duration** of **time** and a service level within which a business process must be restored after a disaster in order to **avoid unacceptable** consequences associated with a break in **continuity**.
The criticality of business functions is a crucial aspect to consider when creating a recovery time objective(**RTO**).
The recovery time objective (RTO) is the amount of time that it may take to restore a service after a disaster without unacceptable impact on the business. The RTO for each service is identified during a business impact assessment (BIA).

Example protect against RTO risk:
Deploy multiple servers behind a load balancer.

Maximum Allowable Downtime (MAD)

Maximum Allowable Downtime or MAD is the absolute maximum time that the system can be unavailable without direct or indirect ramifications to the organization.
The Maximum Allowable Downtime (MAD) is the length of time an organization can suffer the loss of its critical path before ceasing to be a viable enterprise.

Maximum Tolerable Downtime (MTD)

The maximum tolerable downtime (MTD) and recovery time objective (RTO) are related to the duration of an outage.
MTD is the business continuity metric that identifies the longest period of time that a business function may be unavailable without causing irreparable harm to the business.

MTD is the sum of the **RTO** and **WRT**.
WRT = Work recovery time
RTO = Recovery Time Objective

Domain 7 Mutual Assistance Agreements (MAA)

Benefits of an MAA
Mutual assistance agreements (**MAA**) provide an inexpensive alternative to disaster recovery sites.

Risk of an MAA
Organisations participating in an MAA may also be shut down by the same disaster, and MAA's raise confidentiality concerns.

Why are **MAAs uncommon**?
They are not commonly used because they are difficult to enforce.

Domain 7 Business Continuity Planning (BCP)

Goal of BCP
Calm and Efficient response to enhance a company's ability to recover from a disruptive event promptly.

Everyone in the organization must get initial business continuity plan training.

RTO < MTD
The goal of the business continuity planning **BCP** is to ensure that the recovery time objective **RTO** is **less < than** your maximum tolerable downtime **MTD**.

Business continuity planning (BCP) Steps:

1. Project **scope** and planning
    a. a structured analysis of the organization,
    b. creation of a BCP team
    c. assessment of available resources
    d. analysis of the legal and regulatory landscape.
2. Business **impact** assessment (BIA)
    a. Identify **critical** business processes and their dependencies
    b. BIA does **NOT** consider industry standards!
3. Continuity **plan**ning
4. Approval and **implement**ation

Above Steps of Business continuity planning.

During the **planning** phase, the most significant resource utilisation will be the time dedicated by members of the **BCP** team to the planning process. This represents a significant use of business resources and is another reason that buy-in from senior management is essential.

Chief information officer CIO is the most effective organizational owner for an information security program.
A CEO is the ideal person to approve an organization's business continuity plan (BCP).

The owner of information security programs may be different from the individuals responsible for implementing the controls. This person should be as senior an individual as possible who is able to focus on the management of the security program. The president and CEO would not be an appropriate choice because an executive at this level is unlikely to have the time necessary to focus on security. Of the remaining choices, the CIO is the most senior position who would be the strongest advocate at the executive level.

Consider updating Business Continuity Plan (BCP) when:

- When it is a year since the last review/update
- When the senior management changes
- When there is a major component change
- When the company splits into several companies or merges

Everyone in the organization should receive basic training on the nature and scope of the business continuity program. Those with specific roles, such as first responders and senior executives, should also receive detailed, role-specific training.

RAID technology provides fault tolerance for hard drive failures and is an example of a business continuity (BCP) action.
Restoring from backup tapes, relocating to a cold site, and restarting business operations are all disaster recovery (DRP) actions.

Domain 7 Business Impact Analysis

We approach the BIA in several stages:

BIA Process

Four stages of preparing to create a BCP

1. Identification of priorities
    a. Identify business priorities.
    b. first create a list of assets
    c. Develop a value for each asset
2. Risk identification
    a. Identify vulnerability in each asset
    b. Identify threats facing each asset
    c. Determine the risks facing the asset
3. Likelihood assessment
    a. The likelihood assessment is a component of a risk assessment that determines the likelihood that a risk will materialise, not the impact of **intang**ible issues such as the loss of customer **goodwill**.
4. **Impact analysis**
5. **Resource prioritisation**
    a. Monetary value assigned quantitative values to assets as part of the priority identification exercise.

Quantitative Analysis

Quan**tita**tive Impact Assessment Involves the use of numbers and formulas to reach a decision. This type of data often expresses options in terms of the dollar value to the business.

- Quantitative analysis uses numeric ratings to address tangible risks, not intangible ones.
- A purely quantitative analysis is not possible
- Quantitative risk analysis assigns real dollar figures to the loss of an asset.

Qualitative Assessment

Qua**lita**tive Impact Assessment Takes non-numerical factors, such as reputation, investor/customer confidence, workforce stability, and other concerns, into account. This type of data often results in categories of prioritization (such as high, medium, and low).

- The qualitative analysis portion of the business impact analysis (BIA) allows you to introduce intangible concerns, such as loss of customer goodwill, into the BIA planning process.
- Qualitative risk analysis assigns subjective and intangible values to the loss of an asset.

In the BIA management meeting, The annualized loss expectancy (ALE) represents the amount of money a business expects to lose to a given risk each year. This figure is quite

useful when performing a quantitative prioritisation of business continuity resource allocation.
Alternative Systems is a type of mitigation, where redundant systems are provisioned in response to a finding during the organization's BIA.

BCP Definitions

BCP (Business Continuity Plan)
The overall organisational plan for **how to continue** business.

COOP (Continuity of Operations Plan)
The plan for continuing to do business until the IT infrastructure can be restored.

DRP (Disaster Recovery Plan)
The plan for recovering from an IT disaster and having the IT infrastructure back in operation.
Example of triggers that will invoke DRP:

- Power Outage
- Terrorist Attack
- Hurricane

During the business impact analysis (BIA) phase, you must identify the business priorities of your organization to assist with the allocation of BCP resources. You can use business priorities information to drive disaster recovery planning (DRP) business unit prioritization.

BRP (Business Resumption Plan)
The plan to move from the disaster recovery site back to your business environment or **back to normal** operations.

MTTF Mean time to Failure
Mean time to failure (MTTF) is the expected typical functional lifetime of the device given a specific operating environment.
identify the expected lifetime of a piece of hardware.

MTBF (Mean time between Failures)
A time determination for how long a piece of IT infrastructure will continue to work before it fails.
Mean time between failures (MTBF) is an estimation of the time between the first and any subsequent failures.
Indicates the average time between hardware collapses.

MTTR (Mean time to repair)
A time determination for how long it will take to get a piece of hardware or software repaired and back on-line.
Mean time to repair (MTTR) is the average length of time required to perform a repair on the device or service after a failure.

MTD (Max tolerable downtime)

The amount of time we can be without the asset that is unavailable BEFORE we must declare a disaster and initiate our disaster recovery plan.
Recovery time objective (**RTO**), needs to ensure that the organization can recover from an outage in less than the maximum tolerable downtime (**MTD**) time.

SLA service level agreement
A service level agreement (SLA) clearly defines the response time a vendor will provide in the event of an equipment failure emergency.
A service-level agreement may require you to meet the business continuity objectives of your customers.

Domain 7 Goals of DR and BCP

Disaster recovery planning picks up where business continuity planning leaves off.
Minimising the effects of a disaster by:

- **Improving** responsiveness by the employees in different situations.
- Easing **confusion** by providing **written proce**dures and participation in drills.
- **Help**ing make logical decisions during a **crisis**.

The **lessons learned session** captures discoveries made during the disaster recovery process and facilitates continuous improvement.
For the Lessons learned, call an external consultant to be an independent moderator.
DRP Lessons learned sessions may identify deficiencies in training and awareness or in the business impact analysis.

The executive summary provides a high-level view of the entire organization's **disaster recovery efforts.** This document is useful for the managers and leaders of the firm as well as public relations personnel who need a **nontechnical perspec**tive on this complex effort.

5 Types of Disaster Recovery Plan Tests

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

1. **Read**-through
2. Structured **walk-through**
3. **Sim**ulation test
4. **Parallel** test
5. **Full interrupt**ion test

Read-through-test

You distribute copies of disaster recovery plans to the members of the disaster recovery team for review.
Simplest, is the read-through test, you distribute copies of the disaster recovery plan to key personnel for review but do not actually meet or perform live testing.

Structure walk-through - table-top exercise

Members of the disaster recovery team gather in a large conference room and role-play a disaster scenario.
Usually, the exact scenario is known only to the test moderator, who presents the details to the team at the meeting.
The team members refer to the document and discuss the appropriate responses to that particular type of disaster.
Above DR tests only talk about disaster plan actions around the table top.

Simulation Test

Similar to structure walk-through, except some of the **response measure**s are then tested on non-critical functions.

Parallel test

Involves **relocating personne**l to the alternate recovery site and implementing site activation procedures. The employees relocated to the site perform/mimicking their disaster recovery responsibilities just as they would for an actual disaster.
Parallel tests involve moving personnel to the recovery site and gearing up operations, but responsibility for conducting day-to-day operations of the business remains at the primary operations center.
Disaster recovery plan, test fully and evaluates operations at the backup facility but does not shift primary operations responsibility from the main site

Full interruption Test

Like parallel tests but involves actually **shut**ting **down** operations at the primary site and shifting them to the recovery site.
Full-interruption tests activate the alternate processing facility and take the primary site offline.

Above 3 involve some form of **action taking tests**.

Recovery Team
Is used to get critical business functions running at alternate sites.

Salvage Team
Is used to return(restore) the primary site to normal processing conditions.

BCP & DRP Statements

True statements about business continuity planning and disaster recovery planning:

- Disaster recovery planning (DRP) picks up where business continuity planning (BCP) leaves off.
- Business continuity planning (BCP) is focused on keeping business functions uninterrupted when a disaster strikes.

- Organizations can choose whether to develop business continuity planning (BCP) or disaster recovery planning plans (DRP).
- Disaster recovery planning (DRP) guides an organization through recovery of normal operations at the primary facility.

Domain 7 Backup Strategies

CISSP Exam Cram Full Course (All 8 Domains) - Good for 2024 exam!

Electronic Vaulting
Is used to transfer database backups to a remote site as part of a bulk transfer.
Electronic vaulting copies full data to a backup site but does not do so in real time.
In an electronic vaulting approach, automated technology moves database backups from the primary database server to a remote site on a scheduled basis, typically daily.

Remote Journaling
Transmitting only the journal or transaction logs to the off-site facility and not the actual files.
Remote journaling copies only transaction log entries to the remote site.
Transaction logging is not a recovery technique alone; it is a process for generating the logs used in remote journaling. Remote journaling transfers transaction logs to a remote site on a more frequent basis than electronic vaulting, typically hourly.

Remote Mirroring
A live database server is maintained at the backup site.
Remote mirroring technology maintains mirrored images of servers at both the primary and alternate sites.
The most advanced database backup solution and also tends to be the most **expensive** of these strategies for backups.
Remote mirroring is the only backup option in which a live backup server at a remote site maintains a bit-for-bit copy of the contents of the primary server, synchronized as closely as the latency in the link between primary and remote systems will allow.
Remote mirroring maintains a live database server at the backup site and mirrors all transactions at the primary site on the server at the backup site.

Deduplication
The most likely cause of the inability to recover files from the SAN in a scenario is deduplication. Deduplication replaces multiple copies of a file with a pointer to one copy. If the one remaining file is damaged, then all of the linked copies are damaged or inaccessible as well.

Backup storage strategies

Determine how and where data is stored for recovery in case of data loss, corruption, or disaster.
3 - 2 - 1 Rule

- 3 Copies of critical files
- 2 backups on different media
- 1 backup stored offsite

Backup Tape Rotation Schemes
- The Grandfather-Father-Son
- Tower of Hanoi
- Six Cartridge Weekly schemes

Different approaches to rotating backup media that balance reuse of media with data retention concerns.

Onsite
Storing backup data within the same location as the source data (aka local backup)
Offsite
Storing backup data at a different location from where the original data is stored
(ideally geographically remote)
Cloud
Storing backup data in the cloud
(Scalability, high-availability, pay-as-you-go)

Geographic location of the backup data centre is the most critical consideration when designing a disaster recovery plan for a data centre.
Geographical diversity ensures that critical systems are located in different geographic locations, reducing the risk of a single disaster affecting all of them.

Differential backups

A Differential backup stores only those files that have been set with the archive bit and have been modified since the last complete backup.

Fastest backup restoration time option: Any backup strategy must include **full backups** at some point in the process. If a combination of full and **differential backups** is used, a maximum of **two** backup sets must be restored.

Scenario:
Barbara configures a system to perform full backups on Sundays and differential backups on Mondays through Saturdays. The system fails on Thursday.
- **Sunday** and **Wednesday** only applied to recover.

Differential backups involve always storing copies of all files modified since the most recent full backup, regardless of any incremental or differential backups created during the intervening time period.

Incremental Backups

Fastest backup creation time is using Full backups and incremental backups.
With incremental backups, you must first restore the most recent full backup and then apply all incremental backups that occurred since that full backup. Therefore, the administrator must restore the backups from Sunday (full), Monday (Incremental), Tuesday (Incremental), and Wednesday (Incremental).

Incremental backups provide the option that includes the smallest amount of data.

Categories of disruption

- **Non-disaster** disruption in **service** from device malfunction or user error
- **Disaster** entire facility **unusable** for a day or longer
- **Catastrophe** major disruption that **destroys** the facility altogether. Requires a short term and long term solution.

Software Escrow Arrangements

A software escrow arrangement is a unique tool used to protect a company against the failure of a software developer to provide adequate support for its products or against the possibility that the developer will go out of business and no technical support will be available for the product.
Software escrow agreements place the application source code in the hands of an independent third party, thus providing firms with a "safety net" in the event a developer goes out of business or fails to honour the terms of a service agreement.

Domain 7 Communications

Test disaster recovery plan (DRP)

DR testing communications encompass various internal and external stakeholders with different needs and communication methods.

Internal Stakeholders

Disaster recovery Team.
Reliable real-time channels for real-time coordination, problem-solving, and division-making. Slack, Discord, Microsoft Teams, WhatsApp and Zoom.
Management
Periodic updates on progress and potential impacts on normal operations.
Wider Company
General awareness and ahead of schedule tests minimises confusion, with pre- and post-test announcements.

External stakeholders

Customers/Clients
In large-scale tests or real-life scenarios, proactive, controlled communications about potential service disruptions.
And when impacts occur, ETAs for resolution are important for preserving trust and managing expectations.
Partners

If testing may impact joint systems or operations, inform partners with relevant timelines and agree on coordination channels.
Regulators
Certain industries have reporting requirements.
For tests triggering significant downtime of a regulated system, advance notification or post-test reports might be mandated.
Include compliance experts in DR plan creation and testing.

Domain 8 Software Development Security

CISSP Exam Cram - 2024 Addendum

- Identify and apply **security controls in software** development ecosystems
  - Programming languages
  - Libraries
  - Tool sets
  - Integrated Development Environment (IDE)
  - Runtime
  - Code repositories - example Git
  - Continuous Integration and Continuous Delivery (CI / CD)
  - Software Configuration Management (SCM)

Continuous integration with security testing is the best assurance of an application's security posture over time.
Assurance, when it comes to software, is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. It is a term typically used in military and defense environments.

Programming Languages

VBScript and JavaScript are examples of interpreted languages.
C++, Java, and Fortran are compiled languages.

Object Oriented Programming (OOP)
High coupling and low cohesion is the OOP phrase that best describes an object that greatly depends on other objects.
OOP languages use objects instead of procedures and functions.
In object-oriented programming, the **Class** term describes a collection of the common methods from a set of objects that defines the behavior of those objects.

The easiest way (and the best way) to implement session management is with a web development framework, such as one recommended by the Open Web Application Security Project (OWASP).

Domain 8 Devops and DEVSECOPS

The three elements of the DevOps model are **software dev**elopment, **quality ass**urance, and **IT op**erations.
The DevOps approach to technology management seeks to integrate software development, operations, and quality assurance in a cohesive effort. It specifically attempts to eliminate the issue of taking problems and "throwing them over the fence" by building collaborative relationships between members of the IT team.

The DevOps approach to technology management seeks to integrate software development, operations, and quality assurance in a seamless approach that builds collaboration between the **three** disciplines.

Information security is only introduced in the Dev**Sec**Ops model.
DefectDojo - DEVSECOPS

Code Repositories
This is where source code and related artefacts such as libraries are stored

- Do not **commit sensitive infor**mation
- **Protect** access to your code repositories
- Sign your work - **code signing**
- Keep your development tools (IDE) up-to-date
    - visual studio code or Notepad++

Most code repositories today use ***GIT***, the world's most widely used modern version control system. Github
Linux and GIT creator is **Linus Benedict Torvalds.**

In a DevSecOps environment the responsibility for security primarily lies in the context of CI.CD vs Agile is equally distributed across all teams in both CI/CD and **agile**.

SAFECode is community driven program to aid in the use and development of safe and secure coding programming practices. SAFECode is a global nonprofit organization that brings business leaders and technical experts together to exchange insights.

Domain 8 Code Libraries

Code reuse is the inclusion of preexisting code in a new program. Code reuse can be a way to quicken the development process by adopting and reusing existing code. If there are software libraries that have code elements that perform the functions needed by the project, this can be a way to meet the project requirements and the deadline.
However, third-party code could introduce vulnerabilities so this technique should be used with caution.

Code Libraries for some important core functions can improve application security and reduce risk.

Certain languages are prone to certain types of attacks.
In lower-level languages (like C#) use of safe memory allocation and string manipulation libraries can reduce risk of buffer overflow attacks.

Libraries help with Encryption, handling secrets, bulk data transfer to improve security.

Open Source Libraries

- Open source libraries should be tested for security vulnerabilities.
- Open source library use within the organization should be tracked.

Open-source libraries are commonly used by software developers and do not necessarily pose a higher risk than commercially available libraries.

The OpenSSL package is a widely used implementation of TLS encryption that is available as an open-source package.

The ability to inspect open-source software (OSS) means that organizations can inspect it but more importantly that others can and often have also inspected it. This results in software that has had far more review than some closed-source or commercial packages (although large organizations may perform more review).
open-source software package give the ability to inspect the code - more secure

OWASP recommends four critical best practices for libraries and frameworks:

- using libraries and frameworks from trusted sources that are broadly used and well maintained,
- maintaining an inventory of third-party libraries,
- updating libraries and components proactively,
- reducing attack surface by limiting what functions can be used.

Runtime

Describe the period of time during which a software program is running
This is when **dynamic** application security testing (**DAST**) evaluates security of an application
Assessing software security at runtime is generally the only option for purchased software.

Example: The JVM is the runtime virtual machine that allows the execution of Java code on a device. The JVM implements the Java sandbox but that is only one of its many functions.

Both source code and runtime scan is a best practice
Containers, scan images at build time and runtime.

Domain 8 CI/CD

Continuous **Int**egration **Conti**nuous **Deli**very **(CI / CD)**
Continuous integration/continuous delivery approaches are designed to facilitate the release of code on an extremely frequent basis.
Implement identity and access management include **MFA**
Store secrets securely and scan code to ensure no **hard coded secret**s

Implement **role-based access** control (RBAC) and **least priv**ilege access to the environment.
Automate vulnerability **scan**ning in your **CI/CD pipe**line.
Release **version**ing will improve recoverability and issues tracking.

When organizations adopt a continuous integration/continuous delivery (CI/CD) approach to software development, they may deploy code extremely rapidly. In fact, some organizations deploy new code to production hundreds or even thousands of times per day using this approach.

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Domain 8 Configuration Management

Tracks the way that systems are set up:
Hardware and software (OS and applications)

Common reasons to support the logging of changes in a software development environment:

- Support audits
- Support investigations
- Support troubleshooting
- Support analysis efforts

SCM

Software configuration management
Baselining is an important component of configuration management.
A baseline is a snapshot of a system or application at a given point in time.
Should also create **artifacts** that may be used to help understand system configuration such as diagrams.
System and component-level **version**ing.

Applications depend on compute **resources** and software **component**s (Java/JVM frameworks, etc.)

Static

Application security testing
Analysis of computer software performed **without** actually **executing** programs
Tester has access to the underlying framework, design, and implementation
Require source code
Tests “inside out”

Dynamic

A program which communicates with a web application **executes** the **app**lication.
Tester has **no knowledge** of the technologies or frameworks that the application is built on
No source code required
Test “**outside in**”

Domain 8 NoSQL

A key-value store is an example of a NoSQL database that does not follow a relational or hierarchical model like traditional databases.
A graph database is another example of a NoSQL database, but it uses nodes and edges to store data rather than keys and values.
NoSQL database is not structured like a relational database but allows users to store data using a key-value store.

Domain 8 Relational Database MGMT Systems

Other DB Security Mechanisms

The mechanisms related to semantic integrity, for instance, are common security features of a DBMS.
Semantic integrity ensures that user actions don’t violate any structural rules. It also checks that all stored data types are within valid domain ranges, ensures that only logical values exist, and confirms that the system complies with any and all uniqueness constraints.

Concurrency is the database security feature used to perform a locking mechanism to prevent simultaneous edits of cells.

Basic architecture of **RDBMS**

Distributed data model
The distributed data model has data stored in more than one database, but the data is still logically connected. The user perceives the database as a single entity, even though it comprises numerous parts interconnected over a network.

Tables (relations)
Contains a number of attributes, or fields. Each attribute corresponds to a column in the table.

The **cardinality** of a table refers to the number of rows in the table.
The **degree** of a table is the number of columns.

In a scenario, a table has three columns (name, telephone number, and customer ID), so it has a degree of **three**.

Rows (records/tuples)
A data record within a table. Each row which represents a complete record of specific item data, holds different data within the same structure.

Columns (fields/attributes)
A set of data values of a particular type, one value for each row of the database.

table

Company ID	Company Name	Address	City	State	ZIP Code	Telephone	Sales Rep
1	Acme Widgets	234 Main Street	Columbia	MD	21040	(301) 555-1212	14
2	Abrams Consulting	1024 Sample Street	Miami	FL	33131	(305) 555-1995	14
3	Dome Widgets	913 Sorin Street	South Bend	IN	46556	(574) 555-5863	26

row

Company ID	Company Name	Address	City	State	ZIP Code	Telephone	Sales Rep
1	Acme Widgets	234 Main Street	Columbia	MD	21040	(301) 555-1212	14
2	Abrams Consulting	1024 Sample Street	Miami	FL	33131	(305) 555-1995	14
3	Dome Widgets	913 Sorin Street	South Bend	IN	46556	(574) 555-5863	26

column

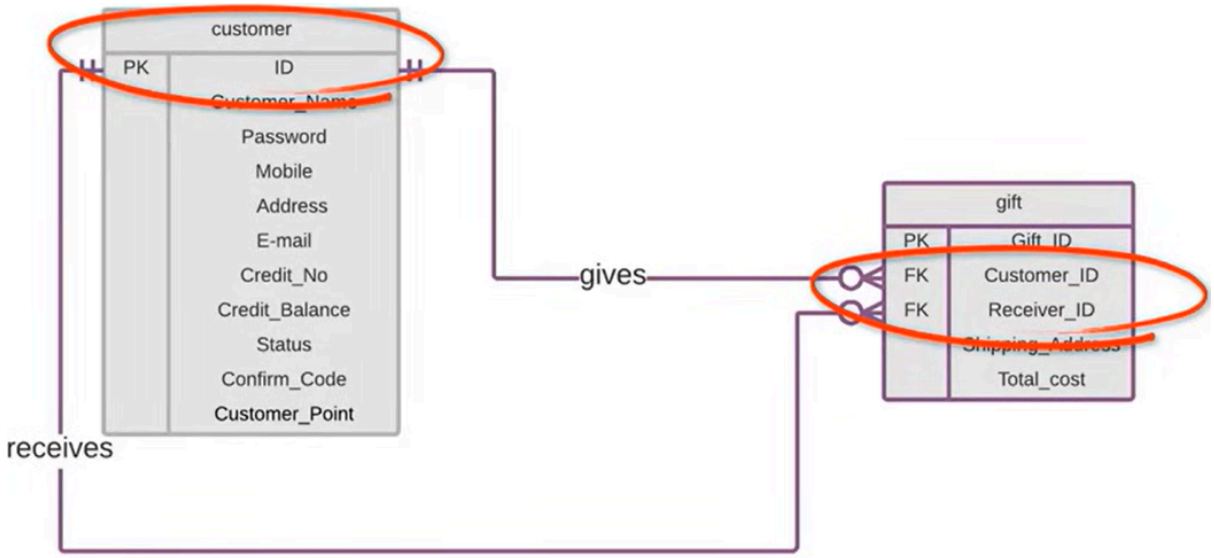
Company ID	Company Name	Address	City	State	ZIP Code	Telephone	Sales Rep
1	Acme Widgets	234 Main Street	Columbia	MD	21040	(301) 555-1212	14
2	Abrams Consulting	1024 Sample Street	Miami	FL	33131	(305) 555-1995	14
3	Dome Widgets	913 Sorin Street	South Bend	IN	46556	(574) 555-5863	26

Candidate keys
A subset of attributes that can be used to **uniquely identify** any record in a table. No two records in the same table will ever contain the same for all attributes composing a candidate key.

Primary keys
One per table set by designer
Selected from the set of candidate keys for a table to be used to uniquely identify the records in a table, each table has only one primary key, selected by the database designer from the set of candidate keys.

Foreign Keys
Used to enforce relationships between two tables, also known as **referential integrity**.
Referential **integrity** ensures that if one table contains a foreign key, it corresponds to a still-existing **primary** key in the other table in the relationship.

Foreign Key Example Relationship between Customer ID tables in ecommerce retail application:
Gift Registry Example RDBMS



Perturbation is the use of false or misleading data in a database management system in order to redirect or thwart information confidentiality attacks.

Scenario

Kim's database uniquely identifies aircrafts by using their tail number.
terms would **not** necessarily accurately describe the tail number:
There is no information provided that the tail number is a foreign key used to reference a different database table.
True valid options:

- Database field
- Primary key
- Candidate key

Database Transactions

Together, these four principles are known as the **ACID** model.

- **Atomicity** of database transactions requires transaction execution in an all-or-nothing fashion.
- **Isolation** principle states that two transactions operating on the same data must be temporarily separated from each other such that one does not interfere with the other.
- **Consistency** principle says that the database must always be in a state that complies with the database model's rules.
    - Consistency ensures that all transactions are consistent with the logical rules of the database, such as having a primary key.
- The **Durability** principle says that transactions committed to the database must be preserved.
    - Durability requires that once a transaction is committed to the database it must be preserved. *Together, these properties make up the ACID model.*

Atomicity

Atomicity ensures that if any part of a database transaction fails, the entire transaction must be rolled back as if it never occurred.
A database failure in the middle of a transaction causes the rollback of the entire transaction. In following example statements, the database would not execute either command because doing so would violate the atomicity property of the transaction.

```
BEGIN TRANSACTION

UPDATE accounts
SET balance = balance + 250
WHERE account_number = 1001;

UPDATE accounts
SET balance = balance - 250
WHERE account_number = 2002;

COMMIT TRANSACTION
```

The database would roll back the transaction, ignoring the results of both commands.

Open Database Connectivity

Open Database Connectivity (**ODBC**) is a database feature that allows applications to communicate with different types of databases without having to be directly programmed for interaction with each type.
ODBC acts as a **proxy** between applications and back-end Database drivers, giving application programmers greater freedom in creating solutions without having to worry about the back-end database system.
Open Database Connectivity (ODBC) is a database feature that allows applications to communicate with different types of databases without having to be directly programmed for interaction with each type. ODBC acts as a proxy between applications and backend database drivers, giving application programmers greater freedom in creating solutions without having to worry about the backend database system.

Domain 8 RDBMS Threats and Vulnerabilities

Common RDBMS **threats** include aggregation and inference attacks.

Aggregation

Multiple pieces
Aggregation is the act of collecting multiple pieces of nonsensitive or low-value information and combining it or aggregating it to learn sensitive or high-value information.

Aggregation is a security issue that arises when a collection of facts has a higher classification than the classification of any of those facts standing alone.

Aggregation attacks involve the use of specialized database functions to combine information from a large number of database records to reveal information that may be more sensitive than the information in individual records would reveal.
The ability to create sensitive information by combining non-sensitive data from **separate** sources.
CounterMeasures: Need-to-know and least privilege can prevent this attack.

Inference

A piece
Inference attacks use deductive reasoning to reach conclusions from existing data.
The ability to **deduce** or assume sensitive information from observing non-sensitive pieces of information.
CounterMeasures: **Blurring** data and database partitioning may prevent this attack.

Other attacks on RDBMS in previous domains:

- SQL injection
- TOC/TOU - Time of check / Time of Use
- Backdoor
- DoS

Inference refers to the process by which a user deduces or infers sensitive information from available non-sensitive data. Inference can occur when a user can piece together bits of information to uncover something they should not have access to. While inference is a security concern, it does ***not*** specifically describe a function that summarizes data.

Domain 8 Database Security

Polyinstantiation

Polyinstantiation allows the storage of multiple different pieces of information in a database at different classification levels to prevent attackers from conducting aggregation or inference attacks.
Polyinstantiation allows the insertion of multiple records that appear to have the same primary key values into a database at different classification levels.
Polyinstantiation includes multiple records in a table with the same primary key.
Each record is designed for users of a specific security clearance level.
In a multilevel database system, polyinstantiation is the presence in the system of multiple instances of the same real world fact or entity, where the instances differ for the access class associated with them
Polyinstantiation database technique can be used to prevent unauthorized users from determining classified information by noticing the absence of information normally available to them.

Determining classified information by noticing the absence of information prevented by Polyinstantiation.

Aggregation

Aggregation attacks involve the use of specialised database functions to combine information from a large number of database records to reveal information that may be more sensitive than the information in individual records would reveal.
Aggregation is the use of multiple queries that summarize information to obtain sensitive information.

Inference attacks use deductive reasoning to reach conclusions from existing data.
Manipulation is the authorized or unauthorized alteration of data in a database.
Contamination is the mixing of data from a higher classification level and/or need-to-know requirement with data from a lower classification level and/or need-to-know requirement.

Polyinstantiation allows the storage of multiple different pieces of information in a database at different classification levels to prevent attackers from inferring anything about the absence of information.
Input validation, server-side validation, and parameterization are all techniques used to prevent web application attacks and are not effective against inference attacks.

A redundant commit statement is an element in database replication.

Domain 8 Type Storage

Primary (real) memory
Consist of the main memory resources directly available to a system CPU. Normally consists of **volatile RAM** and is usually the most **high-perfo**rmance storage available.

Secondary Storage
Consists of more inexpensive, **nonvolatile** storage resources available to a system for **long-term** use. Include magnetic and optical media, such as tapes, disks, hard drives, flash drives, and compact disc/ digital versatile disc (CD/DVD) storage.

Virtual memory
Allow a system to simulate additional primary memory resources through the use of secondary storage.
Example: a system low on **RAM** makes a **hard disk available** for direct SPU addressing.

Virtual Storage
Allows a system to simulate **secondary storage** resources through the use of **primary storage**. Most common example is **RAM disk** that presents itself to the operation system as a secondary storage device but is actually implemented in **volatile RAM.**
Provides a very fast file system for apps but no recovery capability.

Random access storage
Allows the operating system to request contents from any point within the media.
RAM and **hard drive**s

Sequential access storage
Requires scanning through the entire media from the beginning to reach a specific address. A common example is magnetic tape.

Volatile storage
Loses its contents when power is removed from the resource
RAM is the most common example

Nonvolatile storage
Does not depend upon the presence of power to maintain its contents.
Magnetic / optical media and nonvolatile RAM (NVRAM)

Domain 8 Machine Learning and Neural networks

Expert Systems
Consist of two main components: a knowledge base that contains a series of **"if/then"** rules and an inference engine that uses that information to draw conclusions about other data. Expert systems contain business logic and do not build models.

Machine Learning
Techniques that attempt to algorithmically **discover knowledge** from data sets.
Machine Learning is a subset of AI that involves training algorithms to recognize patterns in data and make decisions or predictions based on it. There are various types of ML, including supervised, unsupervised, and reinforcement learning.

Neural Networks
Simulate function of the **human mind** by arranging a series of layered calculations to **solve problem**s. Require extensive training on a particular problem before they can offer solutions. Neural Networks are a class of ML models inspired by the human brain's structure and function. They consist of layers of interconnected nodes (neurons) that process data in complex ways. Deep learning is a subset of ML that uses neural networks with many layers (deep neural networks).

Artificial intelligence (AI)

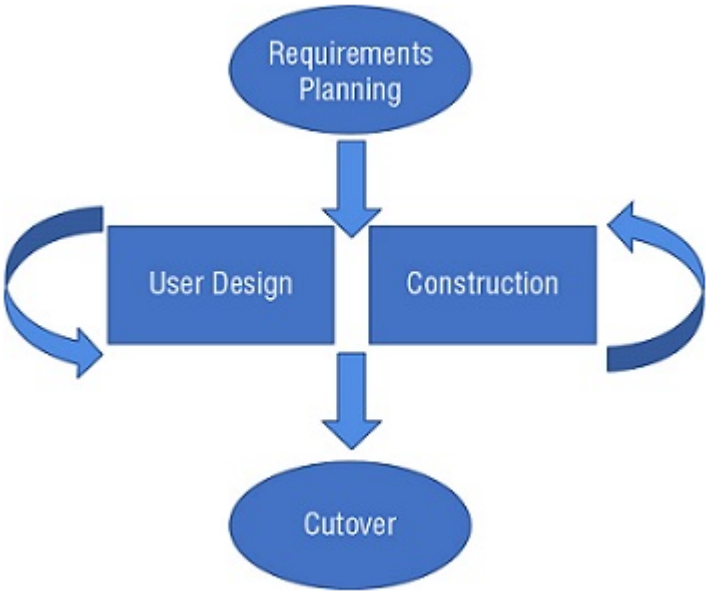
ChatGPT and other large language models (LLMs) fit into the broader context of artificial intelligence (AI), specifically under the subfields of machine learning (ML) and neural networks.
In essence, ChatGPT and similar LLMs represent an advanced intersection of machine learning and neural networks.

Domain 8 System Development Modules

Integrated Product Teams (IPTs) were introduced in 1995 by DoD to bring together stakeholders and foster parallel decision-making. The Agile and DevOps approaches also foster a parallel decision-making approach, but they came into practice many years later and were first embraced in the private sector.

Rapid Application Development

Rapid Application Development, or RAD, focuses on fast development and the ability to quickly adjust to changing requirements.
RAD uses four phases: requirements planning, user design, construction, and cutover.

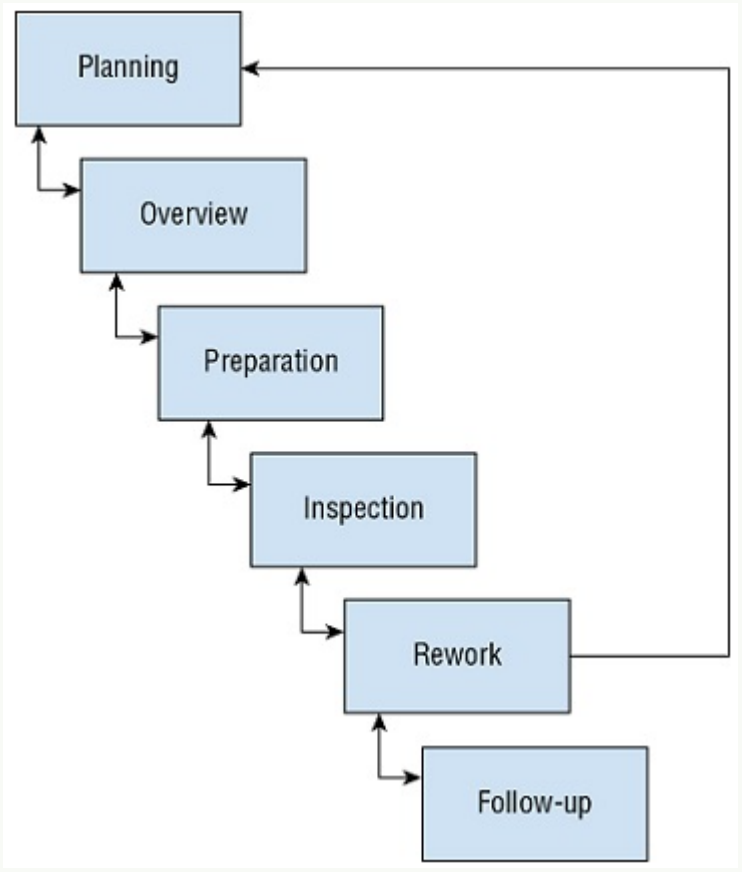


Fagan

Fagan Inspection Model six formal steps for rigorous code reviews:

1. Planning
2. Overview
3. Preparation
4. Inspection
5. Rework
6. follow-up to conduct a formal code review process.

The Fagan inspection process concludes with the follow-up phase.



Fagan inspection is a highly formalized review and testing process that uses planning, overview, preparation, inspection, rework, and follow-up steps.

Iterative waterfall

Time and cost are less important than correctly functioning software.

The iterative waterfall model uses a seven-stage approach to software development and includes a feedback loop that allows development to return to the previous phase to correct defects discovered during the subsequent phase.

Despite many organizations moving to Agile, DevOps, or other more responsive development methodologies, waterfall remains a strong contender when clear objectives and stable requirements are combined with a need to prevent flaws and to have a high level of control over the development process and output.

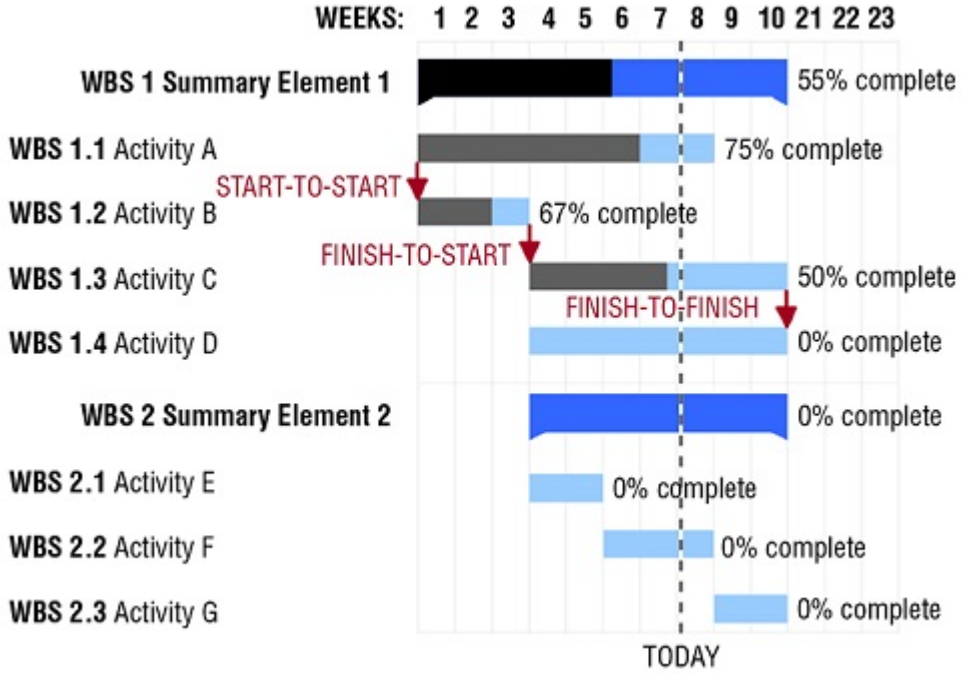
Spiral

Uses several **iterations** of the **waterfall** model to produce a number of fully specified and tested prototypes.
The spiral model allows developers to repeat iterations of another life cycle model (such as the waterfall model) to produce a number of fully tested prototypes.
The spiral model of project management does not directly relate to configuration management.

Charts

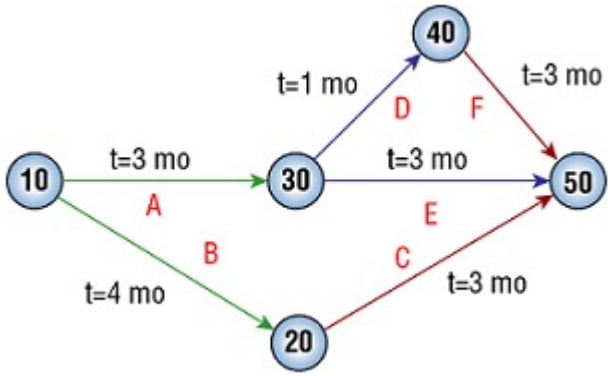
Gantt

A **Gantt** chart is a type of bar chart that shows the interrelationships over time between projects and schedules. It provides a graphical illustration of a schedule that helps to plan, coordinate, and track specific tasks in a project.



PERT

A **PERT** chart focuses on the interrelationships between tasks rather than the specific details of the schedule.



BAR

Bar charts are used to present data

VENN

Venn diagrams are used to show the relationships between sets.

Development Methodologies

- Waterfall
  - Linear approach - each phase must be completed fully before the next begins. Can be inflexible.
- Agile
  - Focuses on interactive development and frequent feedback loops - collaboration between small self-organising, cross-functional teams
- Scaled Agile Framework
  - Allows for large organisations with multiple teams to coordinate, collaborate, and deliver products effectively.
- DevOps
  - Combines software development (Dev) and IT operations (Ops) aiming to shorten the systems development life cycle and provide continuous delivery
- DevSecOps
  - Extends the DevOps approach by integrating security practices

Domain 8 Agile

Agile places an emphasis on the needs of the customer and quickly develops new functionality that meets those needs in an iterative fashion.

Model for software development based on the following four principles:

- **Individuals** and interactions over processes and tools
- **Working software** over comprehensive documentation
- **Customer collaboration** over contract negotiation
- **Responding to change** over following a plan

Manifesto for Agile Software Development - 2001

Agile Model

Model for software development based on the following four principles:

1. Individuals and interactions over processes and tools
2. Working software over comprehensive documentation
3. Customer collaboration over contract negotiation
4. Responding to change over following a plan

* It also states that the most efficient method of conveying information is face to face

Agile first described in the Manifesto for Agile Software development (Manifesto for Agile Software Development) in 2001.

Agile is the opposite of the Waterfall Model.

Place an emphasis on the needs of the customer and **quickly** develop **new** functionality that meets those **needs** in an interactive fashion.
Agile software development may assist with the goal of releasing software many times per day, but Agile does not directly facilitate code release as much as CI/CD does.

- The highest priority is to satisfy the customer through early and continuous delivery of valuable software.
- Business people and developers working together
- paying continuous attention to technical excellence

Agile software development technique includes as a basic principle that Agile values responding to change over following a plan.

The Agile development process requires that business **users** interact with developers on a **daily** basis.

Agile 12 Principles

Core Principle of Agile Manifesto

- Simplicity is essential.
- Working software is the primary measure of progress.
- The best designs emerge from self-organising teams.
- Build projects around motivated individuals and give them the support they need
- Welcome changing requirements, even late in the development process.
- The Agile approach emphasizes delivering software frequently
- maximizing the amount of work **not** done is essential
- ?

Sprint is when developers actively write code for an application.
in an Agile sprint phase and is likely developing code based on user stories. Planning includes stakeholder stories, as well as design and test case preparation. Testing involves ensuring that the code works properly and meets requirements. Deployment includes the actual deployment of the application, as well as additional verification and testing.

Scrum Methodology

An Agile methodology that helps agile teams to work together and deliver complex products. Primarily used by software development teams but has now grown to be accepted within other industries.
Scrum provides a specific set of rules, practices, and roles to put those Agile principles into action.

The daily stand-up meeting is a hallmark of the Scrum methodology. The meetings are called scrums and are essential to the process.
Scrum is a methodology that embraces the Agile philosophy, but not all Agile approaches use the daily scrum.
The waterfall and spiral models do not normally use these daily meetings.

SAFe - Scaled Agile Framework

Scaled Agile framework (SAFE) is a set of organization and workflow patterns for implementing agile practices at an enterprise scale.
Includes structure guidance on roles and responsibilities, how to plan and manage the work, and values to uphold.
Promotes alignment, collaboration, and delivery across large numbers of agile teams.

Developed by leveraging three primary bodies of knowledge:

- Agile software development
- Lean product development
- Systems thinking

Builds on Agile in several respects

- **Coordination** across teams
- **Strategic alignment** with the org\s business objectives
- Emphasises **quality** sas a non-negotiable aspect of delivery
- **Architectural guidance** for future evolution and scaling
- **Cadence** and **synchronisation** through program increment (**PI**) planning and demos
- Lean-Agile **leadership**

SAFe Configurations

- Full SAFe is designed to support enterprises in building and maintaining large integrated solutions with the collaboration of hundreds of practitioners. It provides the most extensive level of guidance, with roles, responsibilities, and activities needed to sustainably deliver complex solutions.
- Essential SAFe focuses on the basic elements of the framework needed to be agile,
- Large Solution SAFe is for developing large and complex solutions that do not require the constructs of the portfolio level.
- Portfolio SAFe is for aligning enterprise strategy with execution but does not address the complexity of building large solutions that Full SAFe is designed for.

Remember:
SAFe does not replace Agile. Rather, it adds necessary layers to make Agile work in a large enterprise-level context.

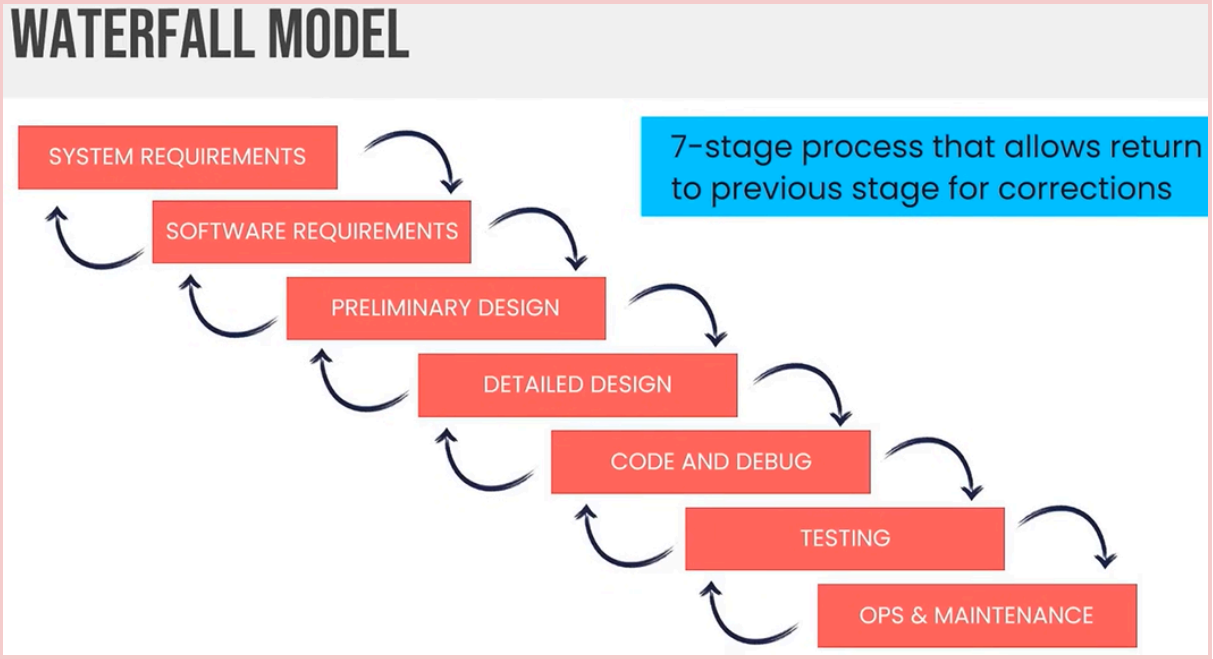
Domain 8 Waterfall Model

Waterfall Model

Time and cost are less important than correctly functioning software.
Describes a **sequential** development process that results in the development of a finished product.

7 stage process that allows return to previous stage for corrections in Waterfall mode

1. System **require**ments
2. Software **require**ments
3. **Preli**minary design
4. **Detail**ed design
5. **Code** and debug
6. **Test**ing
7. **Operations** and **Maint**enance



Only one stage back allowed

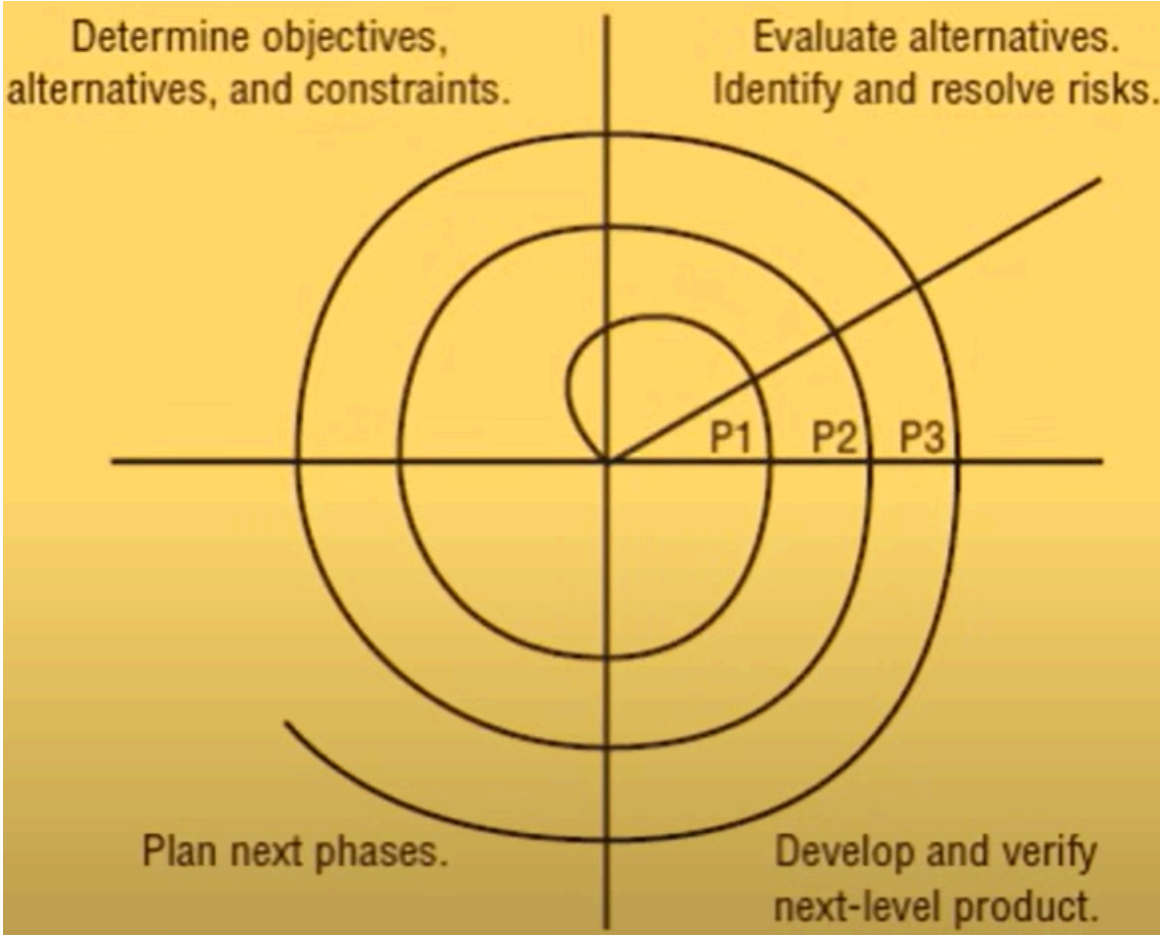
Domain 8 Spiral Model

Lifecycle mode that allows for multiple iterations of a waterfall-style process
Known as a **metamodel**, or a **model of model**s.
The spiral model seeks to iteratively produce new prototypes of a system during the development process.

Each ***loop*** of the spiral results in the development of a **new** system **prototype**

Provides a solution to the major criticism of the waterfall model:
It allows developers to return to the planning stages as demands change.

In a word - "**Iterative**"



Domain 8 Software Development Maturity Models

Help software organisations **improve maturity** and quality of their software process by implementing an **evolutionary** path from ad hoc, **chaotic** processes to **mature**, disciplined software processes.
SW CMM and **IDEAL** models

Domain 8 Capability Maturity Model (SW-CMM)

5 step model measuring software development orgs:

1. Level 1 **Initial** -
    a. no plan
    b. "*whatever it takes*" to get software out the door
2. Level 2 **Repeatable** -
    a. **Basic Lifecycle Ma**nagement
    b. Requirements Management,
    c. Software Project Planning,
    d. Software Project Tracking
    e. Oversight,
    f. Software Subcontract Management,

   g. Software **Quality Assurance**,
   h. Software Configuration Management.
3. Level 3 **Defined** -
   a. **formal doc**umented software development processes
   b. documented software development processes
   c. But at this stage **no quantitative** management of these process are not in place
4. Level 4 **Managed** -
   a. ***YES quantitative*** measures to gain detailed understanding
   b. Managed phase, level 4 of the SW-CMM, the organization uses quantitative measures to gain a detailed understanding of the development process.
   c. Software Quality Management
5. Level 5 **Optimised** (CI/CD) -
   a. continuous development process with feedback loops

The **Repeatable** phase (level 2) is where basic lifecycle processes are introduced.
The **Defined** phase (level 3) is where developers operate according to a set of formal, documented development processes.
The **Managed** phase (level 4) of the SW-CMM involves the use of quantitative development metrics. The Software Engineering Institute (SEI) defines the key process areas for this level as Quantitative Process Management and Software Quality Management.
The **Optimizing** phase (level 5) is where a process of continuous improvement is achieved.

Domain 8 Software Assurance Maturity Model (SAMM)

The Software Assurance Maturity Model (SAMM) is an open source project maintained by the Open Web Application Security Project (OWASP). It seeks to provide a framework for integrating security activities into the software development and maintenance process and to offer organisations the ability to assess their maturity.
OWASP SAMM

SAMM divides the software development process into **five** business functions:

- **Governance**
  - The activities an organization undertakes to manage its software development process.
  - This function includes practices for strategy, metrics, policy, compliance, education, and guidance.
  - Education and guidance programs, including training & awareness and organization & culture are components of the Governance function under the Software Assurance Maturity Model (SAMM).
- **Design**
  - The process used by the organization to define software requirements and create software.
  - Design function includes practices for **threat modell**ing, **threat assess**ment, security requirements, and **security arch**itecture.

- **Implementation** The process of building and deploying software components and managing flaws in those components. This function includes the secure build, secure deployment, and defect management practices.
- **Verification** The set of activities undertaken by the organization to confirm that code meets business and security requirements. This function includes architecture assessment, requirements-driven testing, and security testing.
- **Operations** The actions taken by an organization to maintain security throughout the software lifecycle after code is released.
    - **Incident** management, **detection**, and **response** are all security practices under the Operations business function.

Domain 8 IDEAL Model

Many of the SW-CMM attributes

- **Init**iating - Business reasons outlined, support & infrastructure for initiative put in place.
- **Diag**nosing - Engineers analyse current state of org and make recommendations for change
- **Establish**ing - Org takes recommendations & develops plan to achieve those changes
- **Act**ing
    - Plan put into action.
    - Org develops solutions, tests, refines & implements.
    - develop, test, refine, and implement solutions
    - In the acting phase, it's time to stop "talking the talk" and "walk the walk." The organization develops solutions and then tests, refines, and implements them.
- **Learn**ing - Org continuously analyses efforts and results, proposes new actions to drive better results.

Domain 8 Change and Configuration Management

Role of change configuration management in software development

Request Control

Change Request, The request process begins with a user-initiated request for a feature. Change request processes are initiated by users rather than developers.

Provides an organised framework within which users can request modifications, managers can conduct cost/benefit analysis and developers can prioritise tasks.
Request control provides users with a framework to request changes and developers with the opportunity to prioritize those requests.

Change control

Used by **developers** to re-create the situation encountered by the user and analyse the appropriate changes to remedy the situation.

Change Control helps multiple developers work on code at the same time.
Change control provides an organized framework within which multiple developers can create and test solutions prior to rolling them out into a production environment.

Configuration control

Configuration control of the software configuration management (SCM) process ensures that changes to software versions are made in accordance with the change control and configuration management policies.
The c**onfiguration control process** ensures that changes to software versions are made in accordance with the change control and configuration management policies. Updates can be made only from authorized distributions in accordance with those policies.

Release Control

Change Control and release control are initiated by **developers** seeking to implement changes.
Once the changes are finalised, they must be approved for release through the release control procedure.
Release control includes user acceptance testing (UAT) to ensure that any alterations to end-user work tasks are understood and functional.
One of the responsibilities of the release control process is ensuring that acceptance testing is performed.

UAT - User acceptance testing (UAT) is typically the last phase of the testing process, and usually occurs last and is executed against test scenarios.

Changes = code changes
Should also include acceptance testing to ensure that any alterations are understood and functional.
Before releasing any code into production, the DevOps manager should verify the hashes of the files to be released. This is to ensure that only the actual final, tested, and approved version of files is released and that those files were **not corrupted or infected** with malware prior to distribution.

Configuration audit is part of the configuration management process not part of the change control process.

Domain 8 Application Security Testing

Software Testing
Thoroughly test any software **before** distributing it internally or releasing it to market.

The programming team should develop special data sets that exercise all paths of the software to the fullest extent possible.
Some tests may be automated, and others manual.

Application Security Testing

- **Static** Application Security Testing (SAST)
  - Testing method that analyses source code
  - Static analysis of computer software performed without actually executing programs
  - Tester has access to the underlying framework, design and implementation
  - Requires source code
- **Dynamic** Application Security Testing (DAST)
  - Examines an application while it **is running**
  - A program which communicates with a web application (executes the application)
  - Tester has no knowledge of the technologies or frameworks that the application is built on
  - No source code required!
- **Interactive** Application Security Testing (IAST)
  - Combines elements of both SAST and DAST
  - Testing performed as the application is **running** (DAST) with access to source **code** (SAST)
  - Analyses code for vulnerabilities while it is being used
  - Focuses on real time reporting to optimise testing and analysis process
  - Often built into CI/CD automated release testing
  - Unlike static and dynamic testing, IAST analyses the internal functions of the application while it is running.
- Software Composition Analysis (SCA)
  - Is used to track the components of a software package or application
  - Is of special concern for apps built with open-source software components
  - Because open-source components often involve reusable code libraries
  - SCA tools identify flaws/vulnerabilities in these included components, ensure latest versions are in use, etc.
  - ***Automated, combines application security and patch management***

Domain 8 Virus Propagation Techniques

- **File infection** - infect different types of executable files and trigger when the operating system attempts to execute them. (.exe and .com on windows)
- **Service injection -** escape detection by injecting themselves into trusted runtime processes of the operating system, such as svchost.exe, winlogin.exe and explorer.exe
- **Boot sector infection** - infect the legitimate boot sector and are loaded into memory during the operation system load process.
- **Macro infection** - infect and spread through code in macros often using visual basics for apps in MS office documents.

Domain 8 Types of Viruses

- **Multipartite** Viruses use more than one propagation technique in an attempt to penetrate systems that defend against only one method or the other.
- **Stealth** Viruses
  - **hide themselves** by actually tampering with the operating system to fool antivirus into thinking that everything is functioning normally.
  - intercepting read requests from the antivirus software and returning a correct-looking version of the infected file.
- **Polymorphic**
  - Viruses actually **modify** their **own code** as they travel from system to system.
  - Polymorphic viruses mutate each time they infect a system by making adjustments to their code that assists them in evading signature detection mechanisms.
  - Polymorphic is a term often used in programming and object-oriented design, where it describes a function or method that can operate on different data types or objects.
- **Encrypted Viruses** use ***cryptographic*** techniques to avoid detection.
- **Hoaxes** are a nuisance that result in wasted resources. Used to spread through "email from a friend" but have changed with social media.
- **Logic Bombs** are **malicious code** objects that **infect** a **system** and lie dormant until they are **triggered** by the occurrence of one or more **conditions**, such as date/time, program launch, website logon, etc.
  - A developer added a subroutine to a web application that checks to see whether the date is April 1 and, if it is, randomly changes user account balances.
- **Trojan Horse** a software program that appears good and harmless but carries a malicious, hidden payload that has the potential to wreak havoc on a system or network. Defense only allows software from trusted sources. Do not let users install software.
  - Adversaries will use any and all means to harm their targets. This includes mixing attack concepts together to make a more effective campaign. A Trojan Horse Attack is a type of malware that uses social engineering to trick a victim into installing it.
  - Whitelist trusted list application
- **Worm**
  - uses built-in propagation mechanisms that exploit system vulnerabilities to spread
  - Worms have built-in propagation mechanisms that do not require user interaction, such as scanning for systems containing known vulnerabilities and then exploiting those vulnerabilities to gain access.
- **Ransomware** infects a target machine and then uses encryption technology to encrypt documents, spreadsheets, and other files stored on the system with a key known only to the malware creator. User/victim is then unable to access their files and receives an ominous pop-up message warning that the files will be permanently deleted unless a ransom is paid within a short period of time.
  - Backup up your computer
  - Store backups separately

- User awareness training
- Cloud hosted email and files storage
- Update and patch computers
- Use caution with web links
- Use caution with email attachments - user awareness training
- Verify email senders
- Preventative software programs

Ransomware attack consideration paying the ransom

- There is no guarantee that he will receive the decryption key.
  - no guarantee that the attackers will deliver the decryption key after he makes payment.
- Paying ransoms may be illegal
  - payment of the ransom may be illegal depending upon the circumstances.
- Cannot be sure that the attackers **do not** have access to his information, as the ransomware may have copied data for the attackers' use.
- Restoring from backup is a good method to regain access to information encrypted by ransomware.

Cryptolocker ransomware attack screen

Your personal files are encrypted!

CISSP Exam Cram - Cyber Attacks and Countermeasures (+ Quantum for CISSP 2021)

Hoax Message Indicators

- Lack of a digital signature verifying the origin
- Threat of damage to your computer system
- Encouragement to take specific steps to resolve a concern which are not based on standard company procedures

A hoax is a social engineering attack that is attempting to trick a user into taking actions that will harm them through the use of fear that not taking action would actually cause harm. A hoax will not have a digital signature from a verifiable origin, so its source is questionable. Hoaxes often use the threat of damage or harm to encourage the victim to take action, and those actions are often provided steps that will actually cause the victim harm.

Example of phishing, hoax, watering hole attack:
A website claims to offer free temporary access to their products and services but requires that you alter the configuration of your web browser and/or firewall in order to download the access software

Domain 8 Antivirus Software

Antivirus Software uses **signature** based detection algorithms to look for telltale patterns of known viruses. Critical signatures are **updated frequently.**
Today many use **behaviour** based detection monitoring target systems for unusual **activity** and either **blocking** it or flagging it, even if the software does not match a known malware signature.

Awareness training/Educating users is an important part of preventing virus infections and works with technical controls such as antimalware software. Awareness establishes a common baseline or foundation of security understanding across the entire organization and focuses on key or basic topics and issues related to security that all employees must understand.

Domain 8 Techniques to Compromise Password Security

CISSP Exam Cram Full Course (All 8 Domains) - Covers latest exam!

Password crackers

Designed to take credential data stolen in a data breach or other hack and extract passwords from it.

Dictionary Attacks

Uses a large dictionary file with thousands of words and then runs an encryption function against all words to obtain their encrypted equivalents. Type of brute force attack.

Social Engineering Attacks

Consists of simply calling the user and asking for their password or posing as a technical support representative or other authority figure who needs the information immediately.

Familiarity social engineering pretext attack where the victim, Mary, is asked about a coworker Sue (who doesn't actually exist, but Mary does not know that initially). Familiarity or liking as a social engineering principle attempts to exploit a person's native trust in that which is familiar. This could include claiming to know a coworker even when that person doesn't exist. This is designed to put Mary in a mindset that might be more willing to help the caller by providing answers to questions, since the person they asked to talk to is either not there or unknown. This is not an example of a social networking or social media attack.

Examples:

- You receive an email warning about a dangerous new virus spreading across the internet. The message tells you to look for a specific file on your hard drive and delete it, since it indicates the presence of the virus.
- A website claims to offer free temporary access to their products and services but requires that you alter the configuration of your web browser and/or firewall in order to download the access software.
- A secretary receives a phone call from a person claiming to be a client who is running late to meet the CEO. The caller asks for the CEO's private cell phone number so that they can call them.

Note: above examples are socially engineered because there is interaction with the victim.

Privilege Escalation

Multifactor authentication (MFA) is most likely to limit horizontal privilege escalation by making it difficult to access user accounts and to authenticate to a compromised account. Limiting permissions for groups and accounts can also help, but disabling unused ports and services and sanitizing user inputs both address threats that are most frequently associated with vertical privilege escalation attacks.

Rootkit (escalation of privilege)

Freely available on the internet, used as a **2nd step** by attackers to exploit known vulnerabilities in various operating systems enabling attackers to **elevate privi**lege.

Domain 8 Application Attacks

Attackers use it to exploit poorly written software.

Buffer overflow

Exists when a developer does not validate user input to ensure that it is of an appropriate size, allowing input that is too large can "overflow" memory buffer.

```
int myarray[10];
myarray[10] = 8;
```

Above is an example of an overflow type of buffer overflow known as an off-by-one error. The first line of the code defines an array of 10 elements, which would be numbered 0 through 9. The second line of code tries to place a value in the **11th** element of the array (remember, array counting begins at 0!), which would cause an overflow.

Parameter checking, or input validation, is used to ensure that input provided by users to an application matches the expected parameters for the application.

ASLR Memory address randomization
implemented address space layout randomization, a memory protection methodology that randomizes memory locations, which prevents attackers from using known address spaces and contiguous memory regions to execute code via overflow or stack smashing attacks.

Back Door

Often used during development and debugging
Undocumented command sequences that allow individuals with knowledge of the back door to bypass normal access restrictions

Time of Check to Time of Use

Time-of-check-to-time-of-use is a **timing vuln**erability that occurs when a program checks access permissions too far in advance of a resource request.
Race Condition, is not likely to be found by a web vulnerability scanner.

Rootkit(escalation of privilege)

Freely available on the internet and exploit known vulnerabilities in various operating systems enabling attackers to **elevate priv**ilege.
Countermeasures: Keep security patches up-to-date and anti malware software to prevent rootkit exploits.

Fileless malware

Malware that leaves no trace of its presence nor saves itself to a storage device, but is still able to stay resident and active on a computer is fileless malware. This is similar to a rootkit, which can be described as an invisibility shield. But its core features are that it interferes with low-level communications of the operating environment to hide itself and then hide other things, such as files and/or processes.

Domain 8 Web Application Vulnerabilities

Used to compromise web **front-end** and **backend** databases
Most important for preventing common vulnerabilities like SQL injection (**SQLi**) and cross-site scripting (XSS) is by implementing:

- input validation
- output encoding
- Defensive Coding
- Escaping Metacharacters

Validating and sanitising user input is a key consideration when implementing secure coding practices for web applications.

By validating and sanitising user input, developers can prevent common security vulnerabilities such as SQL injection, cross-site scripting (XSS), and command injection attacks. This practice helps ensure that only expected and safe input is processed by the application, thereby reducing the risk of exploitation by malicious actors.

JavaScript remains the one mobile code technology that may affect the security of modern browsers and their host OSs.

Cross site Tracing (XST)

Nikto lists OSVDB-877, noting that the system may be vulnerable to XST.
Cross-site tracing (XST) leverages the HTTP TRACE or TRACK methods and could be used to steal a user's cookies via cross-site scripting (XSS).

Cross-site scripting (XSS)

Occur when web apps contain **reflected** input
A type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.
Occur when an attacker uses a web application to send malicious code to a different end user.
Countermeasures: Input validation is the best defense. Validate data length AND data type. This filters out malicious input (like a <SCRIPT> tag)

Cross-site scripting uses reflected input to trick a user's browser into executing untrusted code from a trusted site.

Persistent XSS - storing payload on a web site and executing when a user visits the site.
Stored xss

Example:

```
<SCRIPT>alert('Enter your password')</SCRIPT>
```

Controls to prevent or protect against XSS:

- validating input
- coding defensively
- escaping metacharacters
- rejecting all script-like input

Content Security Policy (CSP) is a computer security standard introduced to prevent cross-site scripting, clickjacking and other code injection attacks resulting from execution of malicious content in the trusted web page context

Cross-site request forgery (XSRF or CSRF)

Similar to cross-site scripting attacks but exploit a different trust relationship.
Exploits trust that a user has in a website to execute code on the user's computer.
Countermeasure: Create web apps that use secure tokens, and sites that check the referring URL in request to ensure it came from a local site.
Cross-site request forgery (XSRF or CSRF) attacks exploit the trust that sites have in a user's browser by attempting to force the submission of authenticated requests to third-party sites.
XSRF/CSRF attack - forced the submission of an authenticated request to a third-party site is exploiting trust relationship
The creation and exchange of state tokens is intended to prevent CSRF.

SQL injection attacks

Use unexpected input to a web application to **gain unauthorized** access to an underlying database.
Countermeasures: Input validation, user prepared statements and limit account privileges.
The single quote character ***(')*** is used in SQL queries and must be handled carefully on web forms to protect against SQL injection attacks.

Control at the database level: parameterized queries, the SQL statement is defined within the application and variables are bound to that statement in a safe manner.

A SQL injection directly attacks a database through a web application.

Preventing SQL Injection attacks

- Escaping / Input validation
- Parameterization
- Prepared statements
- Limiting database permissions

SQLi Example

```
CARROT'&1=1;--
```

Client-side input validation

Client-side input validation is not an effective control against any type of attack because the attacker can easily bypass the validation by altering the code on the client. Escaping restricted characters prevents them from being passed to the database, as does parameterization. Limiting database permissions prevents dangerous code from executing.

Session hijacking

Session hijacking attacks attempt to steal previously authenticated sessions but do not force the browser to submit requests.

Web Cache Attacks

The temporary internet files cache if accessed by an adversary could result in a split-response attack, cache poisoning, and/or DOM XSS.

- **Split-response attacks** can cause the client to download content and store it in the cache that was not an intended element of a requested web page. Once files have been poisoned in the cache, then even when a legitimate web document calls on a cached item, the malicious item will be activated.
- **DOM XSS** may be able to access and use locally cached files to execute malicious code or exfiltrate data.
- **Cache access** might allow for some forms of spoofing, masquerading, or impersonation of websites, but it is unlikely to contain enough information about the person using the system to be able to perform actual identity theft.

Directory Traversal Attacks

In this case, the .. operators are the telltale giveaway that the attacker was attempting to conduct a directory traversal attack. This particular attack sought to break out of the web server's root directory and access the /etc/passwd file on the server.

```
http://www.mycompany.com/../../../etc/passwd
```

File upload attacks

File upload attacks seek to upload a file to the server.

Domain 8 Network Reconnaissance Techniques

Techniques used by attackers **preparing** to attack a network

IP Probes
Automated tools simply attempt to ping each address in a range.
Systems that respond to the ping request are logged for further analysis.

Ping sweep
reconnaissance on a remote target and discovers that pings are allowed through his target's border firewall. Using Ping probes can identify Which systems respond to pings, a rough network topology, and potentially the location of additional firewalls.

Port Scans
Scan a system for open or listening ports. Often web servers, file servers, and other servers supporting critical operations are prime targets.

Vulnerability Scans
Used to discover specific vulnerabilities in a system. Popular tools for this purpose include nessus, OpenVAS, Greenbone, Qualys, Core Impact.

Security Tools

NMAP
- network discovery scans
- detect live systems and the status of ports
- port scanning tool
- Default Nmap scans only 1000 TCP and UDP ports by default, including ports outside the 0–1024 range of "well-known" ports. By using the defaults for nmap, user missed 64,535 ports.
- OS fingerprinting won't cover more ports but would have provided a best guess of the OS running on the scanned system.

OpenVAS
- OpenVAS is an open-source vulnerability scanning tool that will provide CISSP with a report of the vulnerabilities that it can identify from a remote, network-based scan.
- perform network vulnerability scans
- network vulnerability scanner

Nessus
- Nessus are closed-source tools, although Nessus was originally open source.

DD
- create a forensic copy of a hard drive that will be used in an investigation

Metasploit Framework
- exploitation framework that can cause damage to assessed systems (MSFCONSOLE)
- Metasploit Framework is an automated exploit tool that allows attackers to easily execute common attack techniques.
- Metasploit provides an extensible framework, allowing penetration testers to create their own exploits in addition to those that are built into the tool. Unfortunately, penetration testing can only cover the point in time when it is conducted. When conducting a penetration test, the potential to cause a denial of service due to a fragile service always exists, but it can test processes and policies through social engineering and operational testing that validates how those processes and policies work.

Mimikatz
- Mimikatz tool is indicative of an attempt to capture user password hashes for use in a pass-the-hash attack against Microsoft Active Directory accounts

Nikto
- web application scanner

SQLMAP
- sqlmap is custom-designed to identify database vulnerabilities in web applications.

Burp Suite
- Burp Suite is an application proxy.

Wapiti
- Web application vulnerability scanner

ZZUF
- zzuf is a transparent application input fuzzer.
- It works by intercepting file operations and changing random bits in the program's input.
- Test a web browser's handling of unexpected data using an automated tool.
- perform mutation fuzzing as part of her testing of new code moving into production.
- Zzuf is a tool that automates the process of mutation fuzzing.
- Fuzzers may not fully cover the code.

FFUF
- FFUF (Fuzz Faster U Fool) is a tool that automates the process of fuzzing.
- Ffuf finds vulnerabilities in web applications. Ffuf does this by sending a large number of requests to a target with various payloads.

Netcat
- Netcat is a tool used to read and write to network connections.

Tripwire
- Tripwire is a file integrity management package.

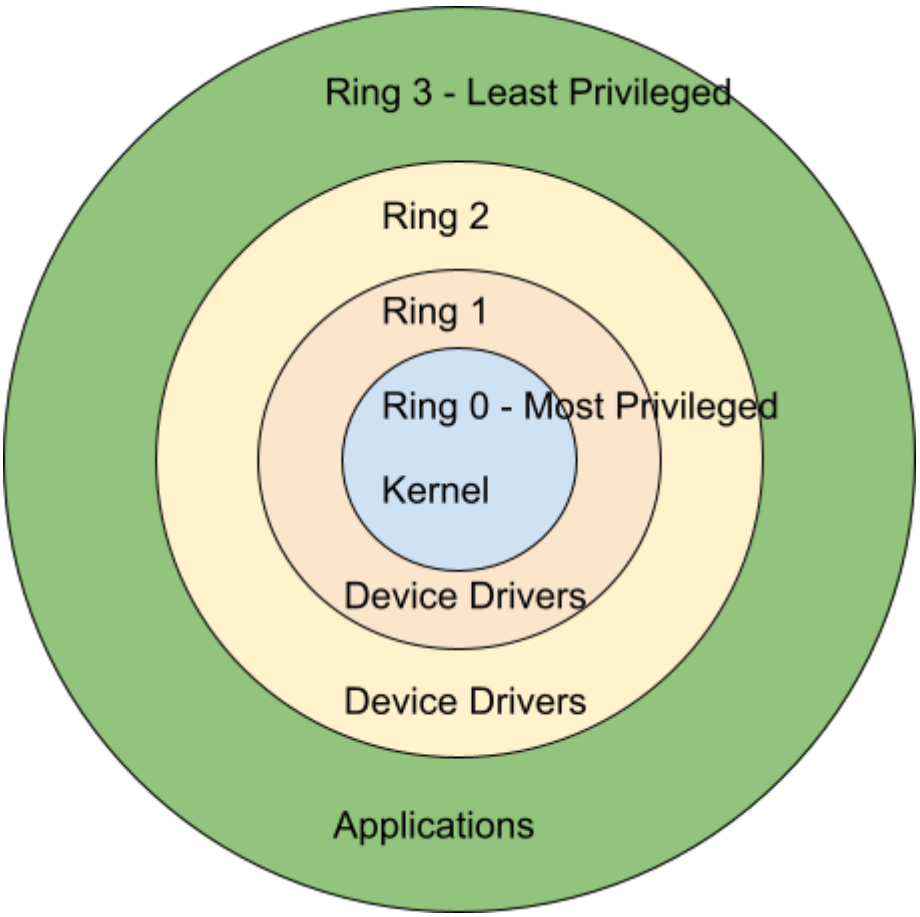
Git
- Git is a code repository management tool that would help manage the organization's code repository.
- commonly used by software developers to interact with and manage code that is stored in code repositories

aircrack-ng
- Wireless network penetration test, use aircrack-ng against the network intending to capture a password as part of the four-way handshake and then crack the password offline. Password cracking may fail due to WPA3 uses SAE and does not transfer the password over the air.

lsof
- Linux command lsof is used to "list open files."

Domain 8 Protection Rings

Aka "Hierarchical protection domains"
In the **Ring Protection** scheme design concept, layer 1 is not normally implemented.
Layers(rings) 1 and 2 contain device drivers but are not normally implemented in practice, since they are often collapsed into layer 0.
Layer 0 always contains the **security kernel.** (ring 0)
Layer 3 contains user applications. (ring 3)
Layer 4 does not exist in the design concept, but it may exist in customized implementations.



Domain 8 Software Development Lifecycle

SDLC

1. **Requir**ements analysis
2. **Design (**identify potential threats and vulnerabilities)
3. **Implem**entation
4. **Test**ing
5. **Evolu**tion

REAL **D**EVELOPERS **I**DEAS **T**AKE **E**FFORT

SDLC approaches include steps to provide operational training for support staff as well as end-user training.
The SDLC may use one of many development models, including the waterfall and spiral models.
The SDLC allows for either iterative or sequential approaches.

Microsoft SDL

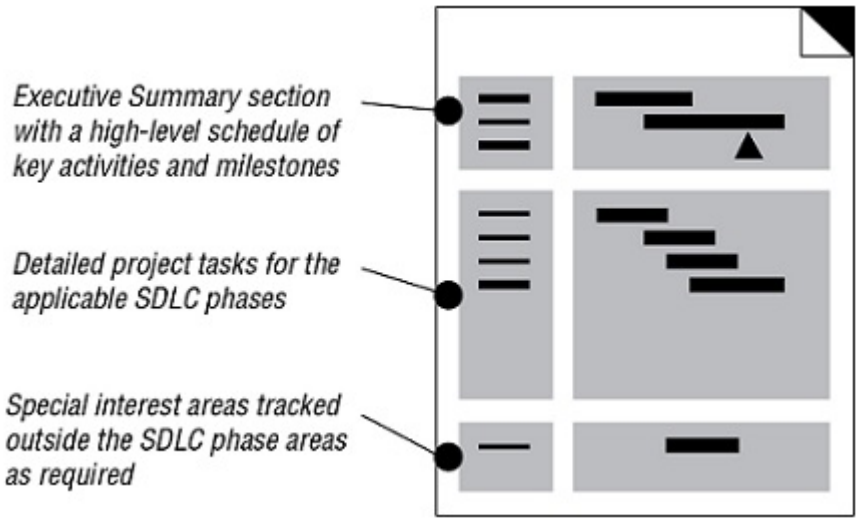
Microsoft Security Development Lifecycle
Fuzz testing is performed during the verification phase of Microsoft's SDL.

Discover how an application will respond to garbage data.

Work Breakdown Structure (WBS)

In the context of a security project, the Work Breakdown Structure (WBS) might include tasks like threat modeling, security requirements analysis, and system hardening, each of which could be further broken down into more specific tasks. The WBS aids in tracking project progress, managing dependencies, and assigning resources.

- Executive Summary with high level schedule of key activities and milestones
- Detailed project tasks for the applicable SDLC phases
- Special interest areas tracked outside the SDLC phase areas as required.
- The primary objective of a secure software development life cycle (SDLC) is to integrate security measures from the beginning of the development process.



Project plans describe timing or resources.
Test analyses are used during later phases of the development effort to report test results.
Functional requirements may be included in a work breakdown structure, but they are not the full WBS.

Domain 8 Concentric Circle Security

Several **mutually independent** security applications, processes, or services that operate toward a single common goal.
Avoids a monolithic security stance
Every individual security mechanism has a flaw or a workaround
Intelligent combination of **countermeasures**,**layered defense**, will **resist** significant and persistent attempts of compromise.
Concentric circle security represents a layered defense aka ***defense in-depth.***

Domain 8 Acquired Software Security Impact

Operating System Attacks
Attackers always try to search for operating system vulnerabilities, like buffer overflow, OS bugs, unpatched operating systems.

Application-level attacks
Overflow, active content, cross-site script, denial of service, SQL injection, session hijacking, phishing.

Shrink Wrap Code Attacks
An act of exploiting holes in **unpatched** or poorly configured software you buy and install. Often also often contain sample scripts or code.

Misconfiguration Attacks
Target poorly configured service or device, or one left in default configuration like wireless router left in **default** WIFI **settings**.
Example: A compromise of a newly installed Wi-Fi connected baby monitor enabled a hacker to virtually invade a home and play scary sounds to a startled toddler.

Domain 8 Cloud Services

IaaS, PaaS, SaaS
Known the considerations around cloud services when assessing the impact of acquired software.

1. Data security and privacy
2. Shared responsibility
3. CSP Security Practices
4. Multi-Tenancy & Isolation
5. Identity & Access Management
6. Monitoring, Logging, Auditing
7. Incident Response & Notification
8. Compliance and Regulatory
9. Data Portability and Exit Strategy
10. Supply Chain Security

Clear understanding of **contractual** responsibilities of your CSP is important for security, availability, and compliance.
CISSP Exam Cram - 2024 Addendum

Data security and Privacy

Evaluating the CSP's data security measures, encryption practices, access controls is crucial to confidentiality and **integrity** of the organizations data.
Data residency and privacy (GDPR, PCI, etc) may vary by the cloud services you choose.

Shared Responsibility Model

Knowing the model and having a clear definition of the responsibilities for each party is essential to avoid security gaps or overlaps.
Know your responsibilities with any cloud service hosting your apps or data

Cloud Service Provider Security Practices

Assessing the providers security policies, incident response procedures, and their track record in addressing security incidents is essential.

Multi-Tenancy and Isolation

Evaluating the CSPs tenant isolation mechanisms is crucial to prevent unauthorized access or data leakage between tenants.
Logical and physical isolation options are fairly consistent across the big 3 CSPs.

Identity and Access Management (IAM)

Assessing the CSPs IAM capabilities, including auth mechanisms (eg. MFA) and role-based access controls to ensure granular and just-in-time control.
Verify support for your apps preferred identity providers

Monitoring Logging and Auditing

Evaluating the CSPs monitoring and logging capabilities, log retention policies, and the organization ability to access and analyse relevant logs is important.
Cloud services hosting your app should have a consumable audit trail.
Think of the 5 pillars.

Ensure that users cannot bypass logging by switching to the root user using sudo su -.
Instead, users who need the ability to perform privileged actions should be added to the sudoers list and then logged as themselves performing the actions.
Sudo su -

Incident Response and Notification

In the event of a security incident or data breach, it is essential to have a clear understanding of the CSPs incident response procedures, notification protocols.
Contractual details matter, because you cannot transfer accountability.
If your CSP is breached and your customer data is compromised, your organizations responsibility to your customers is the same.

Compliance and Regulatory Requirements

Depending on the orgs industry and the type of data involved, there may be specific compliance and or regulatory requirements that the CSP must adhere to
Assessing the CSPs compliance with these requirements and their ability to provide relevant certifications or **attestations** is essential.
The 3 CSPs each have a portal where you can download **SOC 2 Type II** reports with attestation of regulatory compliance.
Attestation means: evidence or proof of something.

Data Portability and Exit Strategy

Organization should have a clear understanding of their ability to migrate or exit the cloud service if necessary.
Evaluate the CSPs data portability capabilities, export formats and the organization ability to retrieve its data in the event of service termination.
This is crucial for maintaining business continuity and avoiding vendor lock-in.

Supply Chain Security

Cloud services often involve complex supply chains, with multiple third-party components and services integrated into the overall solution.
Evaluating the CSPs supply chain risk management processes is important to mitigate potential vulnerabilities or threats introduced through the supply chain.

Glossary

Acronym/ Abbreviation	Description / Definition
2FA	Two-factor authentication
AAA	authentication, authorization, and accounting
AIC	Availability, Integrity, and Confidentiality
ALE	annualized loss expectancy
AI	Artificial intelligence
AICPA	American Institute of Certified Public Accountants
ABAC	Attribute-Based Access Control
ACS	annual cost of the countermeasure/safeguard
ACID	Atomicity Consistency Isolation Durability Model (all-or-nothing)
AES	Advanced Encryption Standard
AH	Authentication Header
API	application programming interface
APT	advanced persistent threats
AMP	asymmetric multiprocessing
AO	Authorizing Official
ARO	Annualised rate of Occurrence
ATO	authorization to operate
AV	Asset Value
BAA	business associate agreement
BAS	Breach and attack simulation
BCP	business continuity plan
BEC	Business email compromise
BGP	Border Gateway Protocol
BIA	Business impact assessment
BIS	Bureau of Industry and Security

BPA	business partners agreement
BYOD	Bring your own device
CALEA	Communications Assistance for Law Enforcement Act
CASB	cloud access security broker
CBC	Cipher Block Chaining
CC	Common Criteria
CCE	Common Configuration Enumeration
CCM	Counter with Cipher Block Chaining Message Authentication Code mode
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol
CCPA	California Consumer Privacy Act 2018
CDN	content distribution network content delivery network
CEH	Certified Ethical Hacker (EC Council)
CEO	chief executive officer
CFAA	Computer Fraud and Abuse Act
CFCE	Certificatied Forensic Computer Examiner by IACIS
CFTT	Computer Forensic Tool Testing by NIST
CIA	confidentiality, integrity, and authentication
CI/CD	continuous integration/continuous deployment
CIS	Center for Internet Security
CISA	U.S. Cybersecurity and Infrastructure Security Agency
CMM	capability maturity model
COBIT	Control Objectives for Information and Related Technologies
COBO	corporate-owned, business-only
COMS	corporate-owned mobile strategy
COPPA	Children's Online Privacy Protection Act
CORBA	Common Object Request Broker Architecture
COPE	corporate-owned, personally enabled
COSO	Committee of Sponsoring Organizations (risk management framework)

COTS	commercial-off-the-shelf
CPA	Certified Public Accountant
CPE	Common Platform Enumeration
CPTED	Crime Prevention Through Environmental Design
CRL	certificate revocation list
CRM	customer relationship management
CSIRT	cybersecurity incident response team
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance IEEE 802.11
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection IEEE 802.3
CSP	cloud service provider
CSP	cloud security policy
CSRF	Cross-site request forgery
CTR	Counter (CTR) modes
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CYOD	choose your own device
CXL	Compute Express Link
DAC	discretionary access control
DAST	dynamic application security testing
DCE	distributed computing environment
DCOM	Distributed Component Object Model
DevSecOps	development, security, and operations
DISA	Direct inward system access
DKIM	DomainKeys Identified Mail
DLP	Data loss prevention
DMARC	Domain Message Authentication Reporting and Conformance
DMCA	Digital millennium copyright act
DREAD	**D**amage potential, **R**eproducibility, **E**xploitability, **A**ffected users, and **Di**scoverability

DRM	digital rights management
EAL	Evaluation Assurance Levels
EAP	Extensible Authentication Protocol
EAP-FAST	EAP Flexible Authentication via Secure Tunnelling
ECB	Electronic Code Book
ECC	elliptic curve cryptosystem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECPA	Electronic Communications Privacy Act
EDR	Endpoint detection and response
EOL	End-of-life
EOS	End-of-Support
EF	Exposure Factor
ENT	Enterprise Wi-Fi authentication, aka IEEE 802.1X
ERP	enterprise resource planning
ESP	Encapsulating Security Payload (IPsec)
FAIR	Factor Analysis of Information Risk (risk management framework)
FCoE	Fibre Channel storage communications over Ethernet
FDE	Full-disk encryption
FDDI	Fiber Distributed Data Interface
FedRAMP	Federal Risk and Authorization Management Program
FERPA	Family Educational Rights and Privacy Act (Students)
FIM	federated identity management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FQDN	fully qualified domain name
GCM	Galois/Counter Mode
GDPR	European Union’s General Data Protection Regulation
GEO	Geostationary orbit
GLBA	Gramm–Leach–Bliley Act

GRC	Governance, risk, and compliance
HIPAA	Health Insurance Portability and Accountability Act
HOTP	HMAC-based one-time password
HPC	High-performance computing
HRU	Harrison–Ruzzo–Ullman
HVAC	heating, ventilation, and air-conditioning
IAAA	identification, authentication, authorization, auditing, Accountability
IaC	Infrastructure as code
IBoE	InfiniBand over Ethernet
ICS	Industrial control systems
IDE	Integrated development environments
IDEAL	Initiate,Diagnose, Establish, Acting, Learn
IDL	interface definition language
IDS	intrusion detection system
IDaaS	Identity as a service
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
IKE	Internet Key Exchange
IPT	Integrated Product Teams (1995)
IPSEC	Internet Protocol Security (VPN)
ISA	interconnection security agreement
ISACA	Information Systems Audit and Control Association (risk management framework)
ISAKMP	Internet Security Association and Key Management Protocol
ISFW	internal segmentation firewalls
ISMS	information security management system
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library (CCTA UK)

ITSEC	Information Technology Security Evaluation Criteria (ITSEC)
IV	initialization vector
JIT	Just-in-time
JSON	JavaScript Object Notation
JWT	JavaScript Object Notation (JSON) Web Token
KBA	Knowledge-based authentication
KDC	key distribution center
KPI	key performance indicators
L2F	Layer 2 Forwarding (VPN)
L2TP	Layer Two Tunneling Protocol (VPN)
LEAP	Lightweight Extensible Authentication Protocol
LEO	Low Earth orbit
LiFi	light fidelity
MAA	Mutual Assistance Agreements
MAC	Mandatory Access Control
MDF	main distribution frame
MDR	managed detection and response
MFA	Multifactor authentication
MFP	multifunction printer
ML	machine learning
MOA	memorandum of agreement
MOU	memorandum of understanding
MMORPG	massively multiplayer online role-playing game
MPLS	Multiprotocol Label Switching
MPP	massive parallel processing
MSSP	managed security service provider
MTBF	Mean time between failures
MTD	maximum tolerable downtime
MTTD	Mean time to detect

MTTF	Mean time to failure
MTTR	Mean time to repair
MUX	multiplexer
NAC	Network access control
NAR	nuisance alarm rate
NAT-PT	Network Address Translation-Protocol Translation
NCA	non-compete agreement
NDA	nondisclosure agreement
NGEP	next-generation endpoint protection
NIST	National Institute of Standards and Technology
NIST CSF	NIST Cybersecurity Framework
NSA	National Security Agency
NVD	NIST's National Vulnerability Database
OCSP	Online Certificate Status Protocol
OCTAVE	Operationally Critical Threat, Asset, And Vulnerability Evaluation (risk management framework)
ODBC	Open Database Connectivity
OFB	Output Feedback
OFDM	Orthogonal Frequency-Division Multiplexing
OIDC	OpenID Connect maintain by OpenID Foundation
OSPF	Open Shortest Path First
OWASP	Open Web Application Security Project
PASTA	Process for Attack Simulation and Threat Analysis
PAT	Port address translation
PCI DSS	Payment Card Industry Data Security Standard
PbD	Privacy by Design
PHI	protected health information
PIA	Privacy Impact Assessment
PIDAS	perimeter intrusion detection and assessment system

PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
PIPL	Personal Information Protection Law (China)
POPIA	Protection of Personal Information Act (South Africa)
PP	protection profiles
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol (VPN)
PUF	physically unclonable functions
PVC	permanent virtual circuit
QKD	quantum key distribution
QoS	Quality of Service
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant array of inexpensive disks
RBAC	Role-Based Access Control
RCA	Resource Capacity Agreement
RDMA	remote direct memory access
RFC	request for change
RFID	radio-frequency identification
RIP	Routing Information Protocol
RMF	Risk Management Framework (RMF) defined by NIST
RMM	Risk Maturity Model
RoE	Rules-of-engagement
RPC	remote procedure calls
ROI	return on investment
ROSI	Return on Sustainability Investment
ROT	silicon root of trust (RoT), hardware root of trust
RTO	recovery time objective
RTOS	real-time operating system
SaaS	Software as a Service

SABSA	Sherwoord Applied Business Security Architecture
SAE	Simultaneous authentication of equals
SAML	Security Assertion Markup Language
SAMM	Software Assurance Maturity Model
SAFe	Scaled Agile Framework
SAN	Storage area network
SASE	Secure Access Service Edge
SAST	Static Application Security Testing
SBOM	software bill of materials
SCA	security control assessment
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCIF	Sensitive compartmented information facility
SCRM	supply chain risk management
SD3+C	Secure by Design, Secure by Default, Secure in Deployment and Communication
SDK	Software development kits
SDL	Security Development Lifecycle
SDLC	Software Development Life Cycle
SDLC	synchronous data link control network protocol
SDN	software-defined networks
SDV	Software-defined visibility
SDWAN SD-WAN	Software-defined wide-area networks
SEA	software escrow agreement
SEI	Software Engineering Institute
SIEM	Security information and event management
SKEME	Secure Key Exchange Mechanism
SLA	service-level agreement
SLE	single loss expectancy

SLR	service-level requirement
SNR	Signal-to-noise ratio
SOA	Service-oriented architecture
SOAR	Security orchestration, automation, and response
SoC	system on a chip
SOC	Service Organization Control reports
SoD	Segregation of duties
SPF	Sender Policy Framework
SRTP	Secure Real-time Transport Protocol
SSID	service set identifier
SSO	single sign-on
SSAE	Statements on Standards for Attestation Engagements
ST	security targets
STRIDE	Spoof, Tamper, Repudiation, Info disclose, Denial of service, Elevation of privilege
SQL	Structured Query Language
SW-CMM	Software Capability Maturity Model
SVC	Switched virtual circuit
TACACS+	Terminal Access Controller Access-Control System Plus
TARA	Threat Agent Risk Assessment (risk management framework)
TCB	trusted computing base
TCO	total cost of ownership
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria (TCSEC) Orange Book
TFTP	Trivial File Transfer Protocol
TGT	ticket-granting ticket
TOE	target of evaluation
TOTP	Time-based one-time password
TSB	trusted computing base

UDP	User Datagram Protocol
UEBA	User and entity behavior analysis
UEM	Unified endpoint management
UPS	Uninterruptible power supply
USPTO	U.S. Patent and Trademark Office
VAST	Visual, Agile, and Simple Threat (AGILE)
VLANs	virtual LAN is a hardware-imposed network segmentation digital virtual network segments
VMS	vendor management system
VXLAN	Virtual eXtensible LAN
W3C	World Wide Web Consortium
WAF	web application firewall
WAP	Wireless Access Point
WPA2	Wi-Fi Protected Access2
XCCDF	Extensible Configuration Checklist Description Format (SCAP)
XSRF	Cross-site request forgery
XML	Extensible Markup Language
ZTNA	zero trust network access
⊕	XOR
~	NOR
∨	OR
∧	AND
®	trademarks for official registration ®
™	Unofficial trademark before receiving USPTO
©	copyright

EXAM DAY

READ Strategy - Know your role? Manager / CISO priorities

Review - what is being asked? Frameworks or regulatory requirements
Eliminate - See any wrong options? Unimportant details
Analyze - What are the solution requirements? Human safety, CISO priorities!
Decide - What answer options remain, one that include multiple requirements?

CISSP Exam Cram - 2024 Addendum

The CISO Priorities:

1. Human safety
2. Risk Management
3. Keep Business running
4. Legal and Regulatory
5. Standards, Frameworks and best practices

Resources

Practice Question Sites

CISSP Practice Exam | Boson

OSG 10th = 800 Questions
OPT 4th = 1300 Questions

Wiley Test Bank Questions 10th Edition

ExSim-Max for CISSP = 700 Questions

CISSP Exam Cram - 2024 Addendum shows the wiley learning site registration

Videos & Playlists Channels

Inside Cloud and Security - Pete Zerger Long full course videos

Prabh Nair

Technical Institute of America / questions

591Cert channel questions

Destination Certification

Tactical Security Inc. Gwen

CyberPlatter

Nicolas Moy

Gerard O'Brien

Security Certification Roadmap - Paul Jerimy Media

LLM AI ChatGPT Study

knowing that in some cases more than one of the answers could be acceptable.

AI Prompt Question to aid as CISSP study partner

Assume the role of CISSP study partner that asks me questions, based on the updated document attached provided. Ask me questions in the form of multiple choice, with the options all answer options very similar, almost all correct. Make the questions in the form that a manager in the security department will select the one from the multiple answers that are more correct then the other choices. Ask me one question and give the multiple choices answers, but do not move to the next question until I provide an answer. If I answer incorrectly then, give me an explanation of the valid answer when I answer incorrectly. Then only pose a new question after my answer provided from the same CISSP domain until I get 3 correct from one of the 8 domains based on the CISSP domain sections. Goal Primary goal endpoint Most Mostly Most important Most appropriate Most critical Most effective Unlikely Incorrect Not typically not commonly not normally Not one not true not an essential process not an effective not a consideration not a common step Least

LEAST likely
is least likely
avoid
advantage
shouldn't