CompTIA - Security+
D5 - Security program manag. and oversight

Policy is the recipe (it would state input/outputs): data, resources…
→ are a statement of intent: desired objectives and principles.
→ are defined by organization itself: reflecting external req.s, goals, legals…

- **AUP**: sets the ground rules for how employees and stakeholders can utilize an org's resources.
- **Information sec**. **policies**: access control, data encryption, password management to ensure CIA
- **BCP**: for data backup, disaster recovery, and continuity of critical functions. These policies go together with COOPs (resilience and recovery)
    - disaster recovery: focus on IT infrastructure and systems → minimizing downtime after a disaster.
- **Incident Response**: are a playbook for addressing cybersecurity incidents effectively: identify, report, and mitigate. The goal here is to prevent a minor issue from escalating into a full-scale crisis.
- **Change Management**: adoption of new technologies and how changes are proposed, evaluated and implemented.
- **SDLC**: creating, testing and deploying sw apps to ensure quality and compliance.
    - SDLC phases:
        - **Develop**: writing
        - **Test**: testing and fix before deployment
        - **Staging**: depoying sw to a staging environment before deploying to production.
        - **Production**: deployment to live production env. for end-users.
    - **final version of the code** is in testing phase, because is where "regression testing"(retesting code to ensure that changes/updates have not introduced bugs/errors and that sw still meets its requirements) is carried out.

Standards define how to achieve those objectives by providing **specific rules** and **guidelines** (ex sector-specific).

- ISO 27001 → ISMS
- ISO 27002 → presents a diverse array of "security **controls"**.
- ISO **27701** → **Privacy**, how to implement a PIMS
- ISO 27017 - Cloud Security: guidelines for both CSP and customers
- ISO **27018** - Cloud **Privacy** (PII): personal data in the Cloud
- NIST 800-53 - Foundation of cybersecurity measures
- PCI-DSS: to safeguard payment card data during transactions.

Privacy is focus on rights of individual (PII)
Confidentiality is ensuring authorized access to data, keeping then protected from unauthorized access.

GDPR -regulated data- “right to be **forgotten**!” **individuals**: orgs are required to process “personal data” in a way that is **transparent** to the **data subject**.

- data owner (legal rights, senior level) control data
- data custodian (“day-to-day) custody, transport…CIA, audit trials: someone in the IT department.

Procedures are the cooking instructions: detail the steps (how to): change management process (IT), of/off boarding, playbook (SOC), runbook (SOAR)…

To assess → due diligence

- before bringing a 3rd party org into your company → due diligence: investigations, questionnaires (straightforward method!).
- before entering in contract with a CSP: review an existing SOC audit (3rd party outcomes)

To mitigate → due care

The most effective Security **Governance structure** depends on organization’s size, complexity, and risk profile:

- *external to org*: **Government entities** (ex healthcare) informing and ensuring compliance with industry regulations and standards.
- *internal to org*:
    - **board**: internal oversight
        - typically integrate/have a Audit committee
    - may create a **committee** (internal task force: specialized group)
        - audit committee, compensation/governance committee
    - **centralized:** consolidate decision-making authority at the top
    - **decentralized**: allows local branches (autonomy)

Risk management:

- Risk Identification

- Risk Security Assessment: prioritizing risks: data exposure, data loss.

- **ad-hoc** assessment: quick, specific events
- **3rd party** ass: costly + time consuming → legal
- **continuous** risk ass: integrated into ongoing processes: real time monitoring.
- **one-time** risk ass: focus on acquisition, new venture, system implementation or organization change. [must know!]
- **recurring** (annual) risk ass: to meet regulatory compliance requirements (no “continuous” because is too frequent!) → scheduled assessment

Overall Vuln. Risk Ass. for the company: list all hw + sw.
Risk Ass: data exposure → downtime.

ARO is associated with risk assessment: annual rate of occurrences

Calculating Equipment Loss:

- AV (Asset Value)
- EF (Exposure Factor)

- **SLE (Single Loss Expectancy) = AV * EF**
- ARO (annualized rate of Occurrence)
- **ALE (ann. loss expect) = ARO * SLE**

1. risk **register** (annually) fulfill regulatory compliance:
    a. associated with **KRI** (key risk indicators): critical metrics used to gauge/misurare potential risks
    b. **risk owners**: who is responsible for managing
    c. **risk threshold:** limit at which a risk becomes unacceptable → qualitative (low/med/high) or quantitative (scoring)
2. risk **tolerance**: ability to take on risk: organizations appetite and tolerance are aligned.
3. risk **appetite**: willing to accept without mitigating: *expansionary* (start-up), *neutral*, *conservative* (prefer low risks).
    a. determines risk threshold

4. Risk **Management Strategies**:

- risk **transference**: outsourcing
- risk **acceptance**
- risk **exemption:** unfeasible
- risk **exception:** approved deviation from a set policy.
- risk **mitigation**: minimize impact: ex. segmentation for malware infection.
- risk **avoidance**: applying patches: eliminating a risk from the environment.

risk **expectations** (deviance): when an org accepts a risk, even if it deviates from usual policies.

- last phase of risk assessment -
risk **reporting** (= it's sensitive!) containing detailed risk discovered, it's used to decide which control to implement and which risk to accept.

cybersec analyst audit devices listed in asset register to identify potential vuln. and weakness in the system (no to ensure compliance with…).

BIA

how long? ex. until db and web server are operational.
RTO (time-frame): max tolerable time service can be down = downtime (*after an incident, before there's impact on business).
RPO (point): max age of files that an org must recover from backup storage to resume *

- journaling facilitates db recovery transactions: affect the RPO (amount of data lost during a transaction)

RTO and RPO are *critical components in BIA* for determining acceptable level of data loss and downtime.
MTTR - how long to fix a problem? - important in SLA.
MTBF - included in the equipment info - predict risk of downtime.

fastest **recovery** approach:

- **replication**: sinche the replica is prepared to assume control.
    - **restoration** from alternative storage
- **snapshot**

- **journaling**: depending on time elapsed since the last backup, can introduce delays → it's the best solution for emails (logged and retained for 3 years)!

---

purpose of **Attestation** process: confirm authenticity of various docs, made by employees. it means confirming ownership/validating: "ex driving license" → identity.
-"customer identity verification" is part of the "know-your-customer" process and is separate from the attestation process.

Vendor Assessment

various evaluation dimensions:
pentesting:

- **unknown/known environment or partially known**
- **bug bounty:** on a reward basis to severity of the discovered vuln

For small vendors -supply chain- we must use the **RIGHT-TO-AUDIT CLAUSE** in the contract: contractual obligations:
on-site assessment, docs exchange and review, process/policy review, 3rd party audit (independent).

- in the realm of datacenter co-location and facility rental contracts, right-to-audit clauses are widely used.

You will never audit a public CSP, such as AWS or Microsoft, because you'll be using their standards (really ez to download it!) → no right-to-audit clause.
To evaluate the CSP security of their services, you can "*review an existing SOC audit report* or similar audit artifact", because CSP disallows Vuln. Scans of their production environment to prevent service disruptions.

Evidence of internal audit

Security Audit: external/ compliance. → operational (day-to-day) security controls

- regular audit and VA, monitoring → operational detective
- as part of the attestation process, *attestation is provided by the auditors*. Auditors issue a statement regarding an organization's posture: provide any identified deficiencies.
- GDPR is a regulation → regulatory assessment or audit in this context

Internal Audits:

1. **self-assessment**: confirm organization's compliance status (ex PCI DSS is industry standard, not a regulation/legal mandate)
2. **compliance**: review financial transactions, operational protocols…
3. **audit committee**: primary purpose is to provide oversight, governance and an additional layer of assurance that org's internal audit function is effective.
    a. it reports to the **board** of directors!

External Audits:

1. **regulatory**: confirm that acme is following the rules and regulations applicable to its industry.
2. **examinations**: verify financial records!!

3. **assessment**: verify operational efficiency, risk mitigation and overall security controls.

3rd party audit -independent- : establish credibility and trust providing an impartial evaluation!

AGREEMENT TYPES

SLA - level of service expected from a service provider: **metrics**, response/resolution time… and define penalties in case of non-compliance.

MOU - less formal than a SLA, no monetary penalties, indicates **intentions**.
MOA - serves as legal contract, more bindingin than a MOU, mutual goal and expectations of a project or partnership.

MSA - contract sets terms and conditions (if you work repeatedly) under which one party will perform services for another: how organizations will collaborate. it should include “breach notification”. (1 MSA - N SOW)
(then) **SOW** - specific tasks, deliverables, timelines of a project → “scope of work”, limited and specific. ex duration of a pentest.
“*A detailed agreement between a client and a vendor that describes the work to be performed on a project*”

An MSA outlines the terms and conditions of a contract and a SOW outlines the vendor’s task, the organization’s expectations, and predefined outcomes.

BPA - outlines the terms and conditions of a business relationship, including their respective contributions and “who makes each type of decision”.

NDA - confidential information

Vendor Monitoring

- **Questionnaires**: structured survey designed to gather info about vendor’s operations such as financial stability, regulatory compliance, performance history and security measures.
- **rules of engagement**: governing interaction between an org and its vendors: it ensures that the security standards expected are laid out!
    - clarity and alignment
    - conflict prevention
    - risk mitigation: rules of eng. can also include clauses related to risk manag.

SLAs can define times for issue resolution, project milestone and uptime.

LOGS
guarantee log **non-repudiation**: *hash the log and then digitally sign them*.
non repudiation is not supported by symmetric encryption due to the use of a shared key.
both symm. and asymm. encryption offer CIA.

FW Logs	system-level events, sec-related activities on a OS
Application Logs	*user interactions*, errors, events within app
Security Logs	crucial for *monitoring*: *auditing* sec activities on a OS like "failed login attempts" and access changes
T	*document* user activities and events: properly recorded for security and compliance"

Ex. To identify the complete SQL queries involved in a SQL injection (SQLi) incident: *[I got this question in the Security+ final exam!!]*
→ The most appropriate log source to identify SQL injection attacks is:
→ **Application Logs**
Application logs, such as those from web servers (e.g., Apache or IIS), are the primary source for detecting SQL injection attempts. These logs capture incoming requests, including URL parameters and payloads, which often contain malicious SQL code. For example, an attacker might attempt to inject SQL code through a login form, and such attempts would be recorded in the application logs

---

Security awareness training: situational awareness training + frequency and duration (up-to-date knowledge) means regular and short training.

Phishing attack: sent randomly to any
- **spear phishing**: targets a group of users
- **whaling**: target is CEO or high-level executive
- **smishing**: text messages untargeted

A **phishing campaign** wants to assess *how vulnerable employees are to phishing attempts*.

Anomalous Behavior Recognition (ABR)
- **risky**: carry a heightened level of risk or potential arm, while not necessarily malicious.
- **unexpected**: actions that deviates from historical/normal pattern:
  - top3 = sharing login credentials, shadow it or installing web apps (also in SaaS), uploading of files to personal storage like Dropbox
- **unintentional**: due to human error or accidents such as misconfigurations, accidental data leaks or actions taken by users who have been tricked by social engineering attacks! → unintentional behavior can be caused by a lack of awareness or insufficient training.

Some useful definitions you MUST KNOW:

PEM: a cryptographic standard (and a file format) used for the storage and transmission of private keys in email communications.

Email security gateway: the best choice for real-time protection against spam and phishing attacks. SEGs are essential security tools that act as a first line of defense against unwanted or fraudulent emails, *preventing them from reaching inboxes*.

Network Access Control (**NAC**) defines a set of rules enforced in a network that the clients attempting to access the network must comply with. With NAC, policies can be enforced before (pre-admission NAC) and/or after end-stations gain access to the network (post-admission NAC). NAC can be implemented with the use of agent software which can be installed on the client machine permanently (this type of software is referred to as permanent agent) or used only temporarily during checks (this type of software is known as dissolvable agent). Another implementation option is agentless NAC, where checks are performed remotely by an external security device without the need for any client software agents.

EDR: a security solution that provides the capability for detection, analysis, response, and real-time monitoring of cyber threats at the device level.

User behavior analytics: a cybersecurity approach aimed at identifying insider threats, compromised accounts, or malicious activity.

IAM: a framework for managing access control to digital resources.

- **De-provisioning**: the technical process of removing a user's access to an organization's systems and resources such as removing individual accounts on file servers, single machines and authentication servers, such as Microsoft Active Directory.
- **Offboarding**, on the other hand, is the broader process of managing an employee's departure, including deprovisioning, but also encompassing activities like returning company property, receiving feedback, and completing necessary administrative tasks.

LDAP: a protocol designed for accessing and managing information related to user accounts, groups, devices, and other resources within an organization.

A common implementation of identity and access controls used in federated SSO systems includes OpenID Connect(Authentication) and OAuth 2.0(Authorization) used in conjunction.

What are the characteristic features of **SAML**?
Handles both authentication and authorization for SSO
Uses XML for data exchange
Commonly used in enterprise environments and legacy systems

Attestation: the process of confirming the integrity and compliance status of various components such as devices, software, configurations, and user privileges.

Mandatory Access Control (**MAC**) model:
Users are not allowed to change access policies at their own discretion
Labels and clearance levels can only be applied and changed by an administrator
Every resource has a sensitivity label matching a clearance level assigned to a user

Discretionary Access Control (**DAC**) is an access control model based on user identity. In DAC, every object has an owner who at his/her own discretion determines what kind of permissions other users can have for that object.

RuBAC (Rule-Based): allows for defining granular rules that consider user roles, time constraints, and network access restrictions.
→ when the question involves “natural language” or shifts or timetable such as “access only on monday from 6-10 am” → the answer is always **RuBAC!**

ABAC: defines access control rules with the use of statements that closely resemble natural language.

FRR (False Reject Rate): A measure of the likelihood that a biometric security system will incorrectly reject an access attempt by an authorized user.

Authentication process can be based on various categories of authentication factors. These include **knowledge-based factors** such as usernames, passwords, PINs, or security question answers ("something you know"), **possession-based factors** (i.e., physical tokens) such as smart cards, key fobs, or security keys ("something you have"), **inherence-based factors** that include unique physical traits of each individual, such as fingerprints, iris scans, facial recognition, or voice patterns ("something you are"), or **location-based factors** such as geolocation data or IP addresses ("somewhere you are"). A multifactor authentication system requires the implementation of authentication factors from two or more distinct categories.

PAM: A security solution that provides control over elevated (i.e., administrative type) accounts.

Which of the answers listed below refers to a solution designed to minimize the risk of unauthorized access to privileged accounts?

- Just-in-time-permissions (Missed) Principle of least privilege Passwordless authentication Multifactor authentication (Your answer)

Agent-based web filtering

- Requires installing software on each device that needs to be monitored
- Provides flexibility and granular control over web activity at the device level
- Involves increased management overhead and system resource consumption

Web filtering via centralized proxy:

- Does not require software to be installed on each individual device
- Simplifies administration and ensures consistent enforcement of web filtering policies across the network.
- Requires a functioning central server for web filtering to operate

Which of the answers listed below refer to filtering techniques that can allow or block access to a site based on its web address? (Select 2 answers)
SSL/TLS inspection **URL scanning** (Your answer) Content categorization **DNS filtering** (Missed) Reputation-based filtering (Your answer)

What is **SELinux**? A security **feature** in Linux OSs (Missed)
Which of the following answers refers to a security mechanism imposed by SELinux over system access? **MAC**

Which of the following answers refers to a *deprecated protocol* designed as a secure way to **send emails from a client to a mail server and between mail servers**? **SMTPS**

Which of the protocols listed below enable secure **retrieval of emails from a mail server** to an email client? (Select 2 answers) **IMAPS**, **POP3S**

Which of the following protocols enables secure **access and management of emails on a mail server** from an email client? **IMAPS (Internet Message Access Protocol)**

- Which of the answers listed below refers to a protocol used to set up secure connections and exchange of cryptographic keys in IPsec VPNs? **IKE**
- Which part of the IPsec protocol suite provides data integrity and authentication but not encryption? **AH**
- Which part of IPsec provides confidentiality, data integrity, and authentication? **ESP**

Which of the IPsec modes provides entire packet encryption? **Tunnel**
An IPsec mode providing encryption only for the payload (the data part of the packet) is referred to as: **Transport mode**.

Which of the following answers refers to a cybersecurity framework that combines network and security functions into a single cloud-based service? **SASE**

Which of the answers listed below refers to a situation where sensitive data is stored in a separate location and can be retrieved with a non-sensitive replacement that can also be processed just like the original data without the risk of revealing the contents of original data? **Tokenization**

Which of the answers listed below refers to a technology that provides control over the usage of a mobile device within a designated area? **Geofencing**

Explanation:
External audits such as **a SOC 2**, **Type 2 audit** must be performed by an independent third party to be deemed valid. Internal audits or self-assessments, regardless of the approving entity, are not employed for this purpose.
Additionally, penetration tests do not yield SOC 2 audit reports.

Chuck has implemented a service that combines SD-WAN, zero trust, cloud access security broker (CASB), and firewall services within a cloud-based security environment, as a replacement for conventional VPNs. What type of service has Chuck deployed? **SASE**.

Nora recently sought information regarding a scientific discovery by posing a query to an AI large-language model, requesting a summary and references. The AI model provided Nora with a summary of the discovery along with several citations. However, upon conducting a search for the cited articles, Nora discovered that they were non-existent. How would this situation be classified as? **Misinformation**.

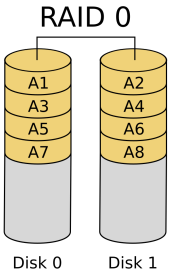
What security control type involves implementing a business continuity plan?
Managerial corrective

During which phase of asset management is inventory typically conducted?
Assignment/accounting: Inventory is usually conducted during the assignment/accounting phase to ensure that all assets are recorded and tracked accurately.

Having discovered a vulnerable server within his organization's critical infrastructure, Wayne realizes that the vendor no longer supports it, and there are no available patches. However, each time Wayne scans the server using his vulnerability scanner, the services on the device crash. What course of action should Wayne take?
→ *Document an exemption, remove the server from automated scans, and implement compensating controls.*

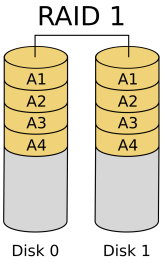
RAID

Which of the following RAID levels does not offer **fault tolerance**?
RAID 0



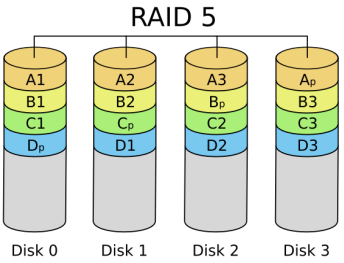
Hardware **RAID Level 0**: (Select all that apply)

- Requires a minimum of 2 drives to implement
- Is also known as disk striping
- Decreases reliability (failure of any disk in the array results in the loss of all data in the array)
- Is suitable for systems where performance has higher priority than fault tolerance



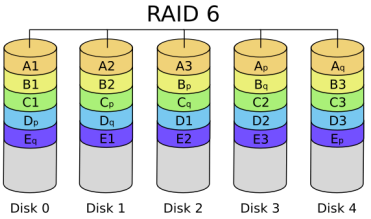
Hardware RAID Level **1**:

- Requires at least 2 drives to implement
- Offers improved reliability by creating identical data sets on each drive (failure of one drive does not destroy the array as each drive contains identical copy of the data)
- Is also referred to as disk mirroring



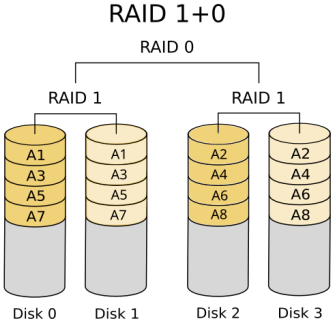
Hardware RAID Level **5**:

- Requires at least 3 drives to implement
- Offers increased performance and fault tolerance (single drive failure does not destroy the array and lost data can be re-created by the remaining drives).
- Is also known as disk striping with parity



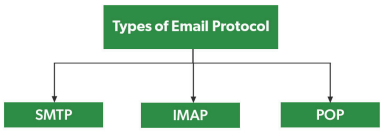
Hardware RAID Level **6**:

- Requires at least 4 drives to implement
- Offers increased performance and fault tolerance (failure of up to 2 drives does not destroy the array and lost data can be re-created by the remaining drives).
- Is also known as disk striping with double parity.



(Nested RAID levels, also known as hybrid RAID)
Hardware RAID Level **10** (a.k.a. **RAID 1+0**):

- Requires a minimum of 4 drives to implement
- Is referred to as stripe of mirrors, i.e., a combination of RAID 1 (disk mirroring) and RAID 0 (disk striping).
- Offers increased performance and fault tolerance (failure of one drive in each mirrored pair of disk drives does not destroy the array)



SMTP (Simple Mail Transfer Protocol) uses TCP as the transport layer protocol. It handles the sending and receiving of messages between email servers over a TCP/IP network.

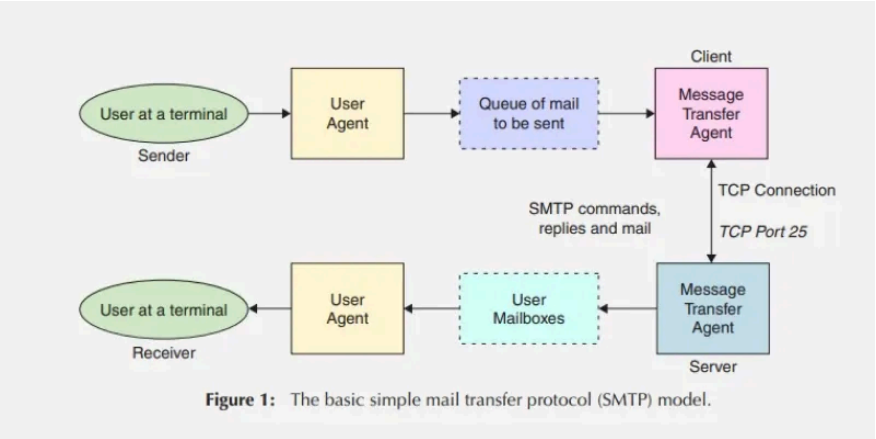
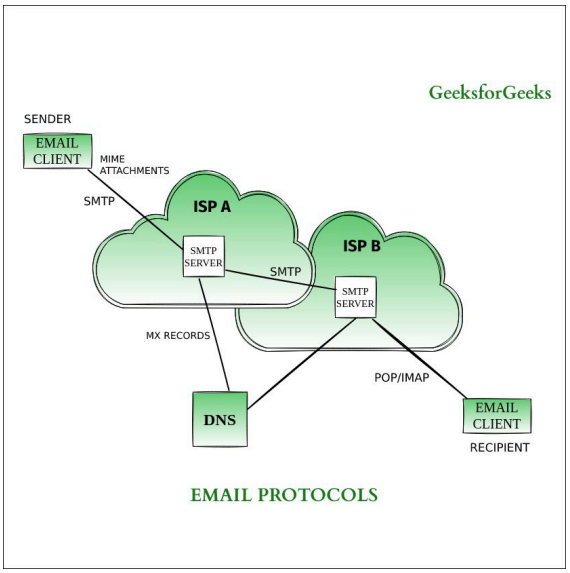


Figure 1: The basic simple mail transfer protocol (SMTP) model.

TCP p25
p 587 using TLS

POP(Post Office Protocol) is an application layer protocol. → To access the message it has to be **downloaded**. POP allows only a single mailbox to be created on the mail server. POP does not allow search facilities.

TCP p 110
p 995 using TLS



IMAP is an application layer protocol. IMAP **allows to access email without downloading** them and also supports email download. The emails are maintained by the remote server. It enables all email operations such as creating, manipulating, delete the email without reading it.

TCP p143
p 993 using TLS