Domain 2 **Asset Security**

Domain 2 of the CISSP exam covers asset security making up ~10% of the test. Asset security includes the concepts, principles, and standards of monitoring and securing any asset important to the organization.

The Asset Security domain focuses on collecting, handling, and protecting information throughout its lifecycle. The first step is classifying information based on its value to the organization

2.1 Identify and classify information assets

Data Classification

- Managing the data lifecycle refers to protecting it from cradle to grave -- steps need to be taken to protect data when its first created until it's destroyed
- One of the first steps in the lifecycle is identifying and classifying information and assets, often within a security policy
- In this context, assets include sensitive data, the hardware used to process that data, and the media used to store/hold it
- Sensitive data is any information that isn't public or unclassified, and can include anything an organization needs to protect due to its value, or to comply with existing laws and regulations
- **Personally Identifiable Information (PII)** (NIST SP 800-122 provides formal definitions), and **Protected Health Information (PHI)** are two important types to protect
- **Proprietary data**: any data that helps an organization maintain a competitive edge
- Organizations classify data using labels
    - government classification labels include:
        - Top Secret: if disclosed, could cause massive damage to national security, such as the disclosure of spy satellite information
        - Secret: if disclosed, can adversely affect national security
        - Unclassified: not sensitive
    - non-government organizations use labels such as:
        - Confidential/Proprietary: only used within the organization and, in the case of unauthorized disclosure, it could suffer serious consequences
        - Private: may include personal information, such as credit card data and bank accounts. Unauthorized disclosure can be disastrous
        - Sensitive: needs extraordinary precautions to ensure confidentiality and integrity
        - Public: can be viewed by the general public and, therefore, the disclosure of this data would not cause damage
    - labels can be as granular and custom as required by the organization
- It is important to protect data in all states: at rest, in transit, or in use
- The best way to protect data confidentiality is via use of strong encryption

Asset Classification

- It's important to identify and classify assets, such as systems, mobile devices etc.
- Asset classifications should match data classification - i.e. if a computer is processing top secret data, the computer should be classified as a top secret asset
- **Clearance**: relates to access to certain classfication of data or equipment, and who has access to that level or classification
- A **formal access approval process** should be used to change user access; the process should involve approval from the data/asset owner, and the user should be informed about rules and limits
    - before a user is granted access they should be educated on working with that level of classification
- Classification levels can be used by businesses during acquisitions, ensuring only personnel who need to know are involved in the assessment or transition

In general, classification labels help users use data and assets properly, for instance by restricting dissemination or use of assets by their classification

2.2 Establish information and asset handling requirements

- The data and asset handling key goal is to prevent data breaches, by using:
    - **Data Maintenance**: on-going efforts to organize and care for data through it's life cycle
    - **Data Loss Prevention (DLP)**: systems that detect and block data exfiltration attempts; two primary types:
        - Network-Based DLP
        - Endpoint-Based DLP
- **Marking**: (AKA labeling) sensitive information/assets ensures proper handling (both physically and electronically)
- **Handling**: refers to secure transport of media through its lifetime
- **Data Collection Limitation**: prevent loss by not collecting unnecessary sensitive data
- **Data Location**: keep dup copies of backups, on- and off-site
- **Storage**: define storage locations and procedures by storage type; use physical locks for paper-based media, and encrypt electronic data
- **Destruction**: destroy data no longer needed by the organization; policy should define acceptable destruction methods by type and classification (see NIST SP-800-88 for details)
    - **Erasing**: usually refers to a delete operation on media, leaving data remanence
    - **Clearing**: over-writing existing data
    - **Purging**: usually refers to mutliple clearing passes combined with other tools (see below) -- not considered acceptable for top secret data
- **Data Remanence**: data remaining on media after typical erasure; to ensure all remanence is removed, the following tools can help:
    - **Degaussing**: used on magentic media
    - **(Physical) destruction**: used for SSD/electronic components, or in combination with other less-secure methods
    - **Cryptographic Erasure**: AKA cryptoshedding, basically destroying encryption key; may be only secure method for cloud storage

2.3 Provision resources securely

- The primary purpose of security operations practices is to safeguard assets such as information, systems, devices, facilities, and apps; these practices help to identify threats, vulnerabilities, and implement controls to reduce the risk to these asssets
- Implementing common security operations concepts, along with performing periodic security audits and reviews demonstrates a level of due care
- **need-to-know** principle imposes the requirement to grant users access only to data or resources they need to perform assigned work tasks
- **least privilege** principle states that subjects are granted only the privileges necessary to perform assigned work tasks and no more

Information and Asset Ownership

- **Data owner**: the person who has ultimate organizational responsibility for data; usually sr. manager (CEO,president, dept. head); data owners typically delegate data protection tasks to others in the org

Asset Inventory

- Software assets are operating systems and applications; software licensing also refers to ensuring that systems do not have unauthorized software installed
- To protect intangible inventories (like intellectual property, patents, trademarks, and company’s reputation, and copyrights), they need to be tracked

2.4 Manage data lifecycle

Data roles

- The **system owner** controls the computer storing the data. Usually includes software and hardware configurations and support services (e.g. cloud implementation). System owner is responsible for system operation and maintenance, and associated updating/patching as well as related procurement activities
- The **data custodian** is responsible for the protection of data through maintenance activities, backing up and archiving, and preventing the loss or corruption and recovering data
- The **security administrator** is responsible for ensuring the overall security of the entire infrastructure; they perform tasks that lead to the discovery of vulnerabilities, monitor network traffic and configure tools to protect the network (like firewalls and antivirus software). They also devise security policies, plans for business continuity and disaster recovery and train staff
- **Supervisors** are responsible for overseeing the activities of all the above entities and all support personnel. They ensure team activities are conducted smoothly and that personnel is properly skilled for the tasks assigned
- **Users** must comply with rules, mandatory policies, standards and procedures. Users have access to data according to their roles and their need to access information

Data Collection

- One of the easiest ways of preventing the loss of data is to simply not collect it
- The guideline: if the data doesn't have a clear purpose for use, don't collect it, and don't store it; this is why many privacy regulations mention limiting data collection

Data Location

- **Data location** in this context, refers to the location of data backups or data copies
- If a company's system is on-prem, keeps data on-site, but regularly backups up data, best practice is to keep a backup copy on site and backup copy off-site
- Consider distance between data/storage locations to mitigate potential mutual (primary and backup) damage risk

Data Maintenance and Retention

- **Data maintenance** refers to managing data as through the data lifecycle (creation, usage, retirement). Data maintenance is the process (often automated) of making sure the data is available (or not available) based on where it is in the lifecycle
- Ensuring appropriate asset protection requires that sensitive data be preserved for a period of not less than what is business-required, but for no longer than necessary
- Encrypt sensitive data
- Safeguard assets via basic security controls to enforce appropriate levels of confidentiality, integrity and availability and act per security policies, standards, procedures and guidelines
- Retention requirements apply to data or records, media holding sensitive data, systems that process sensitive data, and personnel who have access to sensitive data
- Three fundamental retention policy questions:
    - **How to retain**: data should be kept in a manner that makes it accessible whenever required; take taxonomy (or the scheme for data classification) into account
    - **How long to retain data**: general guidelines for business data is 7 years (but can vary by country/region/regulation)
    - **What data** to retain

Data Destruction

- Destroy sensitive data when it is no longer needed
- An organization's security or data policy should define the acceptable methods of destroying data based on the data's classification
- Note again: even when using manufacturers SSD wiping tools, data can remain, and therefore the best SSD wipe method is destruction

2.5 Ensure appropriate asset retention (e.g. EOL, EOS)

- Hardware: even if you maintain data for the appropriate retention period, it won’t do you any good if you don’t have hardware that can read the data

- Personnel: beyond retaining data for required time periods and maintaining hardware to read the data, you need personnel who know how to operate the hardware to execute restoraton processes

- End-Of-Life (EOL): often identified by vendors as the time when they stop offering a product for sale

- End-Of-Support (EOS)/End-Of-Service-Life (EOSL): often used to identify when support ends for a product
- EOL,EOS/EOSL can apply to either software or hardware

2.6 Determine data security controls and compliance requirements

You need security controls that protect data in each possible state: at rest, in transit or in use.

Each state requires a different approach to security. There aren't as many security options for data in use as there are for data at rest or data in transit. Keeping the systems patched, maintaining a standard computer build process, and running anti-virus/malware are typically the real-world primary protections for data in use

The three data states are at rest, in transit, and in use

- **Data at rest**: any data stored on media such as hard drives or external media
- **Data in transit**: any data transmitted over a network
- Encryption methods protect data at rest and in transit
- **Data in use** refers to data in memory and used by an application
- Applications should flush memory buffers to remove data after it is no longer needed

Scoping and Tailoring

After selecting a control baseline, orgs fine-tune with tailoring and scoping processes. A big part of the tailoring process is aligning controls with an organization's specific security requirements

- **Tailoring:** refers to modifying the list of security controls within a baseline to align with the organization's mission
    - includes the following activities:
        - Identifying and designating common controls
        - Applying scoping considerations
        - Selecting compensating controls
        - Assigning control values
- **Scoping**: part of the tailoring process and refers to reviewing a list of baseline security controls and selecting only those controls that apply to the systems you're trying to protect
    - Scoping processes eliminate controls that are recommended in a baseline

Standards Selection

- Organizations need to identify the standards (e.g. PCI DSS, GDPR etc) that apply and ensure that the security controls they select fully comply with these standards
- Even if the organization doesn't have to comply with a specific standard, using a well-designed community standard can be helpful (e.g. NIST SP 800 documents)
- **Standards selection** is the process by which organizations plan, choose and document technologies or architectures for implementation. (For example, you might evaluate three vendors for a security control; you could use a standards selection process to help determine which solution best fits the organization)

- Vendor selection is closely related to standards selection but focuses on the vendors, not the technologies or solutions

The overall goal is to have an objective and measurable selection process. If you repeat the process with a totally different team, the alternate team should come up with the same selection

Data Protection Methods

Data protection methods include:

- **digital rights management (DRM)**: methods used in attempt to protect copyrighted materials
- **Cloud Access Security Brokers (CASBs)** - software placed logically between users and cloud based resources, that can ensure that cloud resources have the same protections as resources within a network.

Note that Entities must comply with the EU GDPR, use additional data protection methods such as pseudonymization, tokenization, and anonymization

Options for protecting your data vary depending on its state:

- Data at rest:consider encryption for operating system volumes and data volumes, and backups as well. Be sure to consider all locations for data at rest, such as tapes, USB drives, external drives, RAID arrays, SAN, NAS, and optical media.
    - DRM is useful for data at rest because DRM "travels with the data" regardless of the data state. DRM is especially useful when you can’t encrypt data volumes
    - A CASB solution often combines DLP, a web application firewall with some type of authentication and authorization, and a network firewall in a single solution. A CASB solution is helpful for protecting data in use (and data in transit)
- Data in transit: think of data in transit wholistically -- moving data from anywhere to anywhere. You can use encryption for data in transit.
    - Example: a web server uses a certificate to encrypt data being viewed by a user, or IPsec encrypting a communication session. There are many options. The most important point is to use encryption whenever possible, including for internal-only web apps
    - DLP solutions are useful for data in transit, scanning data on the wire, and stopping the transmission/transfer,based on the DLP rules set (e.g. outbound data that contains numbers matching a social security number pattern, a DLP rule can be used to block that traffic)