ISC2

Domain 2 Key Takeaways

Security professionals reviewing CISSP Domain 2 need to understand the importance of asset security and the different measures that can be used to protect assets throughout their life cycle. This includes not only technical controls but physical security measures, disaster recovery planning, and privacy considerations. Additionally, third-party relationships must be carefully managed to ensure assets are properly protected.

1. Information and assets need to be protected throughout their life cycle. This includes the creation, use, storage, and destruction of information.

2. Identification and classification of assets is crucial for effective asset security management. This involves understanding the value, sensitivity, and criticality of different types of information and assets.

3. Physical security measures are essential to protect assets from theft, destruction, or damage. This includes controls such as access controls, locks, and environmental controls.

4. Logical security measures are necessary to protect assets from unauthorized access, disclosure, or modification. This includes controls such as authentication, authorization, and encryption.

5. Data backups and disaster recovery planning are critical to ensure that assets can be recovered in the event of a disaster or system failure.

6. Third-party relationships, such as outsourcing or cloud services, require special attention to ensure that assets are properly protected. This includes the use of contracts and agreements to define roles and responsibilities.

7. Privacy considerations are important for protecting personal and sensitive information. This includes complying with relevant laws and regulations, as well as implementing appropriate security controls.

Identify and Classify Information and Assets–Provision Resources Securely

- There are two life cycle models that shape the context for information security: the IT asset management life cycle and the data security life cycle. Both affect data classification and categorization decisions as part of overall information risk management.

- Most of the information security conversation about classification and categorization has focused almost exclusively on the three attributes of the CIA triad. Creating, updating, and deleting data items or datasets have direct bearing on the integrity, availability, authenticity, and even the non-reputability of that data.

- Other than the obvious benefit of protecting assets based on value, there are other potential benefits that can be realized by using asset classification and categorization systems:

    - Awareness among employees and customers of the organization's commitment to protect information.
    - Identification of critical and sensitive information.
    - Identification of vulnerability to modification.
    - Focus on integrity controls.
    - Sensitivity to the need to protect valuable information.
    - Understanding the value of information.
    - Meeting legal requirements.

- Asset classification and categorization may have some other issues that the organization needs to address. These can be sources of errors leading to information security compromises, and may include but are not limited to:

- Human error
- Data owners' limited breadth and depth of knowledge
- Inconsistent classification and categorization methods
- Inconsistent, arbitrary, or capricious classification or categorization determinations
- Confusing, unclear or incomplete labeling of all classified and categorized items
- Inadequate or incomplete processes for downgrading or destroying sensitive information, including recording media

Handling, Management, Controls and Compliance Requirements

- Many laws and regulations dictate certain accountabilities and responsibilities that organizations need to assign. Protection of data requires the clear distinction of roles, accountabilities, and responsibilities to be clearly identified and defined.

- Understanding the three basic states of how information and data can be represented (at rest, in motion, and in use) allows an organization to apply appropriate security measures in each state.

- Organizations use different types of controls to help reduce risks. Controls can be divided into three main types: administrative controls, technical/logical controls and physical controls. Controls are also divided into categories based on how they take effect, but this form of categorization is not absolute or distinct. Many controls can fall into several categories, depending on their implementation and operation.

    - Relying on a single control type or category can be considered as a single point of failure and increases the chances of an aggressor's success.

    - Using multiple types and categories of controls forces an aggressor to prepare multiple means of attack instead of just one. This can deter the attacker, send them to find an easier target, and help prevent and detect a successful attack.

- Security professionals need to be familiar with a wide range of standards and frameworks and the organizations and entities that are responsible for each of them. These range from

U.S.-based entities, such as NIST, to transnational entities, such as the European Union Agency for Cybersecurity (ENISA), the International Telecommunication Union (ITU), and the ISO.

- When choosing to implement security frameworks, baselines, or standards, organizations may decide to only implement specific parts, through the process of scoping and tailoring. Be aware of the value that scoping, tailoring, and supplementation can bring to the security architectures being planned and assessed for the enterprise. The use of scoping and tailoring to properly narrow the focus of the architecture will ensure that the appropriate risks are identified and addressed based on requirements.