ISC2

Domain 3 Key Takeaways

Overall, security professionals reviewing CISSP Domain 3 need to understand the principles of secure system design and the different tools and techniques that can be used to protect information and systems. This includes not only technical controls, such as cryptography and access controls, but also security models and testing methodologies. Additionally, physical security measures are necessary to protect systems and equipment from physical threats.

1. Security architecture and engineering involves designing and implementing security controls to protect information and systems.

2. Secure design principles should be integrated into every aspect of system development, from the initial design to the final implementation.

3. Cryptography is an important tool for protecting information from unauthorized access or modification. Technology professionals should be familiar with different encryption algorithms and how to use them effectively.

4. Access controls are necessary to prevent unauthorized access to information and systems. This includes controls such as authentication, authorization, and accounting.

5. Security models can be used to define and enforce security policies. This includes models such as Bell-LaPadula, Biba, and Clark-Wilson.

6. Security testing is essential to ensure that security controls are working effectively. This includes testing for vulnerabilities, penetration testing, and security audits.

7. Physical security measures, such as access controls and environmental controls, are necessary to protect systems and equipment from theft, damage, or destruction.

Secure Design Principles and Models

- Threat modeling is a form of testing; it is designed to identify critical systems and services and to provide an insight into what vulnerabilities might exist and where they are. Threat modeling does not actually fix a problem, though, it only identifies that a problem is present. The organization still needs to incorporate the results into its processes.

- The explosive growth of cloud services over the past decade, with businesses moving core functions to an external service provider, means maintaining security and compliance must be a shared responsibility of the provider and the customer.

- Least privilege is the practice of granting a user the minimum permissions necessary to perform their explicit job function.

- When designing a system to be secure in default, the default configuration settings of the system should be the most secure settings possible. As security professionals, we should advise and insist on secure defaults both on the vendor side and the customer side.

- When a system is designed to fail securely, it will fail in a secured manner by default. If there is a system crash, potential data exposure and other security risks will be reduced.

- Separation of duties (SoD) means that a sensitive process cannot be completed by a single person, process, or system. As with all security measures, SoD necessarily degrades the efficiency of operations but with the benefit of making the process more secure.

- Security does not have to be complex. Simple designs tend to be easier to test, validate, and demonstrate the correctness of—much more so than a complex, sophisticated design.

Security Capabilities and Vulnerabilities

- Translating theories into the technologies, capabilities, and operational practices that an organization needs for its systems demands a consistent application of security principles to systems development and maintenance activities.

- Security engineering uses generally accepted engineering methods to apply systems security theories to specific situations, problems or needs in practical and effective ways. Both the International Council on Systems Engineering (INCOSE) and NIST recognize systems security engineering as a specialty engineering discipline of systems engineering.

- It is important to emphasize up front that engineering as a discipline embraces change management and configuration control. No matter what kind of engineering activity, its activities revolve around managing the information about the system being engineered. Mission or business needs for safety, security, reliability, and performance will (or should) dictate how detailed and formal those change management processes should be.

- In most cases, systems are developed by starting with statements about business or mission needs and constraints, often expressed as policies. Engineers then use these as starting points to iteratively develop an overall plan (or architecture) for the desired system and its interfaces with the world around it.

- It is important to remember that each system across various architectures, and the architectures themselves, come with vulnerabilities already present in, or related to, their hardware, firmware, software, and patterns of operational use. Hardware can fail; communications links (internal and external) can suffer noise, interference, interruptions, or fail completely; users, systems builders and maintainers can make mistakes or take other incorrect, harmful actions. Attackers are everywhere. General strategies for mitigating the risks posed by these vulnerabilities include robust access control (logical and physical), network segmentation, timely application of software updates and patches, configuration management, and end-user education and training.

Cryptographic Solutions

- Information systems security architectures use encryption as part of resource management and control, identity management, access authentication and, of course, data protection and integrity. Security professionals routinely apply the basic concepts of cryptography to design, deploy, manage, monitor, and assess these types of security capabilities.

- Security professionals need solid working knowledge of the basic concepts of cryptography to use and manage the elements of the cryptographic systems they encounter.

- Systems and security professionals, IT departments, software developers, and end users can and should use off-the-shelf, proven, tested, and validated encryption systems as they design and build more securely. They should not, however, attempt to design their own encryption algorithms or key management systems, or let anyone else on their team do so who is not a cryptographic expert.

- Cryptographic processes must be established in accordance with organizational policies and implemented consistently. Fortunately, well-established bodies of practice exist. NIST Special Publication 800-57 provides several general sets of guidance. ISO 11770 also provides comparable guidance on sound cryptologic business practices, addressing functions such as the generation, storage, distribution, deletion and archiving of keying material. Many regulated industries also have established bodies of practice, including the ANSI X9.24 standard for banks and financial institutions.

Site and Facility Design and Controls

- Physical security is essential to ensuring the information processing activities can be performed, that information is not lost or destroyed through deliberate or accidental physical events, and that the people who do the work are physically safe.

- Crime Prevention through Environmental Design (CPTED) provides direction to solve the challenges of crime with organizational (people), mechanical (technology and hardware), and natural design (architectural and circulation flow) methods.

- There are also building codes and several widely accepted standards that address data center construction and operation.

- The cabling plant, wiring closets, server rooms, media, evidence storage facilities, and many other aspects of the physical space must be considered via risk assessment and risk management processes to determine whether the proper level of confidentiality, integrity, and availability can be met.