Domain 6 Key Takeaways

Overall, security professionals reviewing CISSP Domain 6 must understand the principles of security assessment and testing and the different tools and techniques used to identify vulnerabilities and evaluate the effectiveness of security controls.

1. Security assessment and testing involves evaluating the effectiveness of security controls and identifying vulnerabilities in information systems.

2. Security assessment and testing includes a range of techniques, such as vulnerability scanning, penetration testing, and social engineering.

3. Vulnerability scanning involves using automated tools to identify known vulnerabilities in information systems.

4. Penetration testing involves attempting to exploit vulnerabilities in a controlled environment to determine the effectiveness of security controls.

5. Social engineering involves using psychological techniques to trick users into divulging confidential information or performing actions that compromise security.

6. Security assessment and testing should be conducted on a regular basis to identify new vulnerabilities and ensure that security controls are effective.

7. The results of security assessment and testing should be used to prioritize remediation efforts and improve security controls.

Assessments, Tests, and Audits

- Systems security assessment as a discipline and practice has been driven by standards and frameworks, across the whole gamut of data protection needs.

- There are a number of potential standards applicable to different industries or organizations, and many organizations will find themselves subject to multiple compliance frameworks. Security professionals may work with organizations that already have compliance requirements to adhere to; if not, they may be driven to informally achieve partial or complete compliance as their international business base grows, or they develop strategic relationships with organizations that do have formal compliance requirements to meet.

- Self-assessment requires organizational rigor and a willingness to seek answers to hard questions. Many organizations that have been breached find their internal culture did not encourage rigorous introspection of organizational activities and processes. The process for internal assessment will vary between organizations, but successful organizations have a consistent methodology for performing internal assessments.

- External audits are regularly chartered by organizations to report on risk, governance, and financial status. These audits typically employ an independent organization with no conflict of interests related to the organization they evaluate. In other cases, the compliance body performs the audit as part of their interactions with the covered organizations. Regardless, the audited organization is responsible to demonstrate their compliance with the applicable standard.

Security Control Testing

- Controls assessment can be done by any combination of testing, examination, and interview. These provide the means to measure a system for its compliance with requirements and design specifications or standards. Controls can also be assessed via modeling, simulation, and analysis, which may combine testing and inspection with evaluation of data (artifacts) from the operational environment. Each method is an important part of the overall assessment process.

- Proper selection and use of each assessment method are needed to correctly assess the performance of a control. Controls assessment must be performed in a consistent, structured, and repeatable manner. This requires effective organizational assessment policies, proper construction of the assessment tools, and effective reporting of the results so that risk judgments can be applied to the findings.

- Vulnerability assessments are an essential task when evaluating a systems' security. A vulnerability is a weakness which, if exploited, could potentially compromise the confidentiality, integrity, or availability of an asset. However, the existence of a weakness does not mean it can be effectively exploited by a threat.

- Penetration testing simulates the actions of a threat actor using information the threat actor is likely to have. This form of testing is a controlled process, with clearly defined rules of engagement (RoE) that detail the circumstances under which the penetration is attempted. This approach to testing is useful in determining if an organization's controls are effective, but improperly conducted, presents a significant risk to the organization's operations, systems, and reputation.

- Ethical penetration testing activities are performed in a predictable, defined fashion which is controlled and specified by a lawful and legally binding contract between the penetration tester and the owners or responsible executive officers of the system under test. The methodology must be followed rigorously, as it directly affects the evaluation of the risks associated with the testing activities.

- The evolution of the threat has resulted in a number of continuous testing approaches. These approaches complement the frameworks, which expect continuous monitoring of risk and organizations to respond to risk in a timely manner. Breach attack simulation tools automate the testing activities so they can be performed continuously against the organization's infrastructure.

- Another approach to vulnerability assessment and ethical penetration testing attempts is to force production systems to fail, so that the organization's incident detection, response, and recovery capabilities can be evaluated. This is sometimes referred to as the chaos engineering approach because its no-notice test strategies place high stresses on the people and systems of the organization. This is not an approach to be considered lightly.

Many systems are not engineered with the resilience necessary to sustain production shutdown without significant cost to the organization.

- No single approach will provide an absolute guarantee of the effectiveness of an organization's control environment. Selecting the right approaches to the security controls' assessment requires consideration of the organization's business goals, technical capabilities, compliance obligations, and maturity.

Collect Security Process Data

- The security professional must be able to identify the systems that provide the information, correlate it, and act on the results in a timely manner. It is in this area where the tools used by operations and the information systems assessors overlap.

- Reviewing the activities associated with IAM requires access to a broad range of documentation and information, much of which is kept in different data structures. This includes the organization's identity policies and procedures, information from the system owners defining the access privileges to be granted, details related to the organization's access control architecture and configuration, and the organization's identity provisioning records.

- Audit or detailed examination of the various information sources provides a rich set of data upon which systems security assessments can be made.

- A practical example of the use of synthetic transactions for monitoring can be found in Microsoft's System Center Operations Manager software. With this, you can create a variety of synthetic transactions that can be used to monitor across databases, website, and TCP port usage. Before the monitoring settings for an operations manager are created to use in a synthetic transaction, you should plan the actions that the synthetic transaction should perform. For example, if you want to create a synthetic transaction that measures the performance of a website, actions can be planned that are typical for a customer, such as logging on, browsing web pages, and completing a transaction like placing an item in a shopping cart and making a purchase.

- The objective of the activities related to management review and approval should be to support continual process improvement. While many organizations continue to rely on subjective judgments of performance to prioritize changes to the control environment, best practice in the major frameworks requires the use of statistical methods, metrics, and benchmarks to determine whether changes to the controls' environment are warranted. The reliance on these metrics demands that the logging and monitoring tools actually provide information that supports data-driven decision making.

- The rapid change in the information security profession has challenged traditional educational models because the body of knowledge changes so rapidly. Consequently, education for security professionals cannot stop once their formal training in the body of knowledge is complete.

- Successful security education, training, and awareness (SETA) programs have meaningful evaluation measures that demonstrate SETA program effectiveness. The results of the evaluation programs are used for a variety of purposes, including retraining and program reevaluation. As with all controls, continuous process improvement methods should be used to maintain training and awareness relevance, cultural change, compliance, and impact.

- Availability services provide another source for security process data, which allows the organization to determine the effectiveness of its controls. Availability data is routinely subject to assessment and audit, and careful planning is necessary to ensure the organization can demonstrate its compliance to controls assessors.

Analyze Test Output and Generate Report

- Key performance indicators (KPIs) are different from Key Risk Indicators (KRIs). KPIs can be viewed as looking to the past while KRIs involve peering into the future. KPIs, by definition, mean the activity has already happened. KRIs use modeling, analysis or educated guesswork to set anticipated levels for risk indicators as a prediction of events yet to occur.

- Building an organizational culture that embraces change is difficult. Recognizing that change is necessary and will happen in a predictable manner makes it easier for organizations to improve their security posture.

- During an assessment or audit, circumstances may suggest that illegal, unethical, or dangerous actions have been committed by a person or persons within the organization’s span of responsibilities or control. In the absence of a legal obligation, there may still be an ethical obligation for disclosure of some or all these indicators or findings.