Hi, I'm Mike Chapple and this is the audio review of the exam essentials for chapter 15 of the official CISSP study guide. Here are the top things you need to know for the exam from this chapter on security assessment and testing.

Understand the importance of security assessment and testing programs. Security assessment and testing programs provide an important mechanism for validating the ongoing effectiveness of security controls. They include a variety of tools such as vulnerability assessments, penetration tests, software testing, audits and security management tasks designed to validate controls. Every organization should have a security assessment and testing program defined and operational.

Conduct vulnerability assessments and penetration tests. Vulnerability assessments use automated tools to search for known vulnerabilities in systems, applications and networks. These flaws may include missing patches, misconfigurations or faulty code that exposes the organization to security risks. Penetration tests also use these same tools, but supplement them with attack techniques where an assessor attempts to exploit vulnerabilities and gain access to the system. Vulnerability management programs take the results of these tests as inputs and then implement a risk management process for identified vulnerabilities.

Perform software testing to validate code moving into production. Software testing techniques verify that code functions as designed and does not contain security flaws. Code review uses a peer review process to formally or informally validate code before deploying it in production. Interface testing assesses the interactions between components and users with API testing, user interface testing and physical interface testing.

Understand the difference between static and dynamic software testing. Static software testing techniques such as code reviews evaluate the security of software without running it by analyzing either the source code or the compiled application. Dynamic testing evaluates the security of software in a runtime environment and is often the only option for organizations deploying applications written by someone else.

Explain the concept of fuzzing. Fuzzing uses modified inputs to test software performance under unexpected circumstances. Mutation fuzzing modifies known inputs to generate synthetic inputs that may trigger unexpected behavior. Generational fuzzing develops inputs based on models of expected inputs to perform the same task, performs security management tests to provide oversight to the information security program.

Security managers must perform a variety of activities to retain proper oversight of the information security program. Log reviews, particularly for administrator activities ensure that systems are not misused.

Account management reviews ensure that only authorized users retain access to information systems. Backup verification ensures that the organization's data protection process is functioning properly. Management should also monitor other security functions such as disaster recovery, business continuity and awareness and training programs.

Key performance and risk indicators provide a high level of view of security program effectiveness. Conductor facilitate internal, external and third-party audits. Security audits occur when a third party performs an assessment of the security controls protecting an organization's information assets. Internal audits are performed by an organization's internal staff and are intended for management use.

External audits are performed by a third-party audit firm and are generally intended for the

organization's governing body. Collect logs and security process data. Many components of the information security program generate data that is crucial to security assessment processes. These components include the account management process, management review and approval, key performance and risk indicators, backup verification data, training and awareness metrics and the data generated by disaster recovery and business continuity programs.

Know how to use cybersecurity exercises to ensure that teams are prepared for security incidents. Exercises are designed to test the skills of security professionals. Blue teams are responsible for managing the organization's defenses. Offensive hacking is used by red teams as they attempt to gain access to systems on the target network. White teams serve as the neutral moderators of the exercise. Purple teaming is conducted after an exercise to bring together the red and blue teams for knowledge sharing. Those are the study essentials that you need to know for chapter 15, security assessment and testing.

From:
https://www.trident365.com/ - **三叉戟**

Permanent link:
https://www.trident365.com/doku.php?id=projects:cissp:chapter15

Last update: **2025/05/18 17:17**