CISSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 6

Security Assessment and Testing

INSIDE CLOUD AND SECURITY

INTRODUCTION: CISSP EXAM DOMAINS

DOMAINS	WEIGHT
1. Security and Risk Management	15%
2. Asset Security	10%
3. Security Architecture and Engineering	13%
4. Communication and Network Security	14%
5. Identity and Access Management	13%
6. Security Assessment and Testing	**12%**
7. Security Operations	13%
8. Software Development Security	10%

Exam Outline

6.1 Design and validate assessment, test, and audit strategies

6.2 Conduct security control testing

6.3 Collect security process data (e.g., technical and administrative)

6.4 Analyze test output and generate report

6.5 Conduct or facilitate security audits

some situations require an expert!

WHAT'S NEW IN DOMAIN 6?

No significant changes

SECURITY ASSESSMENT AND TESTING

Security assessment and testing programs provides a mechanism for validating the ongoing effectiveness of security controls, with a variety of tools to validate controls:

- vulnerability assessments
- penetration tests, software testing
- audits
- security management tasks

Every organization should have a security assessment and testing program defined and operational.

Vulnerability Assessments vs Penetration Tests

Vulnerability assessments

use automated tools to search for known vulnerabilities in systems, applications, and networks.

flaws may include missing patches, misconfigurations, or faulty code that expose the organization to security risks.

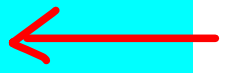
Penetration tests

uses these same tools but supplements them with attack techniques where an assessor attempts to exploit vulnerabilities and gain access to the system.

Penetration Test Strategies

A few strategies that may be employed

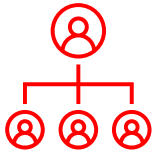
- **War Dialing** – Bank of Modems
- **Sniffing** – Monitor the Network
- **Eavesdropping** – Listening
- **Dumpster Diving** – Just like it sounds
- **Social Engineering** – Human Manipulation



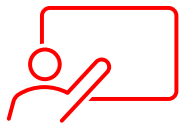
Tests that involve human interaction and analysis will increase cost but are more thorough.

SECURITY PROCESS DATA

Employment Polices and Practices write
Termination process and background checks



Roles and Responsibilities communicate
Management sets the standard and verbalizes the policy



Security Awareness Training train
Prevents Social Engineering, helps with phishing

SOFTWARE TESTING

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.

Static vs Dynamic Software Testing

Static software testing

techniques include code reviews, evaluate the security of software without running it by analyzing either the source code or the compiled application.

Dynamic software testing

evaluates the security of software in a runtime environment and is often the only option for organizations deploying applications written by someone else.

"written by someone else" is not a requirement

FUZZING

Fuzzing

testing technique

Uses modified inputs to test software performance under unexpected circumstances

Modifies known inputs to generate synthetic inputs that may trigger unexpected behavior

Generational fuzzing develops inputs based on models of expected inputs to perform same task

SECURITY MANAGEMENT OVERSIGHT

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 the most important!
ensures that the organization's data protection process is functioning properly.

Key performance and risk indicators
provide a high-level view of security program effectiveness.

INTERNAL AND EXTERNAL AUDITS

Conduct or facilitate internal 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.

Assume audit is 3rd party unless question says otherwise