Welcome to the (ISC)2 Certified Information Systems Security Professional (CISSP) Training Course

Course Agenda

- Domain 1: Security and Risk Management
- Domain 2: Asset Security
- Domain 3: Security Architecture and Engineering
- Domain 4: Communication and Network Security
- Domain 5: Identity and Access Management (IAM)
- **Domain 6: Security Assessment and Testing**

Course Agenda (continued)

Domain 7: Security Operations

Domain 8: Software Development Security

Domain 6

Security Assessment and Testing

Domain Objectives

1. Name primary methods for designing and validating test and audit strategies.
2. Choose appropriate strategy to design and validate test and audit functions that support business requirements.
3. Describe how to maintain logs related to security control testing and prepare logging systems for relevant review and protection.
4. Classify the various security control testing techniques related to application development and delivery.

Domain Objectives (continued)

5. Select the relevant security processing data administration that supports testing and assessment related to account management and process approval.
6. Apply the appropriate security control testing techniques for use internally and externally for an organizational system.
7. List essential elements of and differentiate between training and awareness that are aligned with organizational governance, compliance, policy, and capabilities.
8. Recognize relevant procedures to protect sensitive information when utilizing test data.

Domain Objectives (continued)

9. Define the process of a service provider audit.
10. Associate the appropriate use of an audit type based upon the business support requirements.

Domain Agenda

- Design and Validate Assessment, Test, and Audit Strategies
- Security Control Testing
- Security Process Data
- Test Output and Generate Report
- Conduct or Facilitate Security Audits
- Domain Review

Module 1

Design and Validate Assessment, Test, and Audit Strategies

Module Objectives

1. Name primary methods for designing and validating test and audit strategies.
2. Choose appropriate strategy to design and validate test and audit functions that support business requirements.

Internal

- Testing accomplished from inside a network system
- Designed to simulate insider threat
- Carnegie Mellon University-Software Engineering (CMU-SEI) list insider threat as a primary concern

External

- Testing accomplished from outside of a network
- Designed to simulate external adversary
- External test performed first when doing both internal and external testing

Third-Party

Following are frequent reasons for justification of third-party assessments:

- Meeting regulatory requirements
- Increase assurance of service capabilities to clients
- Support or augment internal teams

Module 2

Security Control Testing

Module Objectives

1. Describe how to maintain logs related to security control testing and prepare logging systems for relevant review and protection.
2. Classify the various security control testing techniques related to application development and delivery.
3. Apply the appropriate security control testing techniques for use internally and externally for an organizational system.

Vulnerability Testing

- Targets known threats
- Determines path(Risk) levels
- Determines services that should not be enabled
- Determines improperly configured systems

Penetration Testing

Penetration testing identifies vulnerabilities often exploited by adversaries.

PHASES:

- Planning (can be overt/covert)
- Discovery
- Attack
- Reporting

Log Reviews

- Identified as a primary component of log management.
- Logs are made consequential with reviews.
- Log reviews support audit function, forensic analysis, and internal and external investigations.

Key Logging Practices

- Organizational process standard for log management.
- Logs management should follow policies within organization related to generation, transmission, storage, analysis, and disposal.
- Provide adequate support for all staff with log management responsibilities.

Log Security

- Secure log infrastructure should be created and maintained.
- Logging facilities should be protected from tampering and unauthorized access.
- Logs need to be protected from breaches of confidentiality and integrity.

Synthetic Transactions

- Real user monitoring (RUM)
  - Web monitoring captures analyzes every transaction of every user of website or application
  - Supports user experience monitoring
- Synthetic performance monitoring
  - Agents or scripts emulate actions of a user
  - Can be used to verify performance as in SLAs

Code Review and Testing

- Planning and design
- Application development
- Testing techniques
- Testing method considerations
- Misuse/use case
- Negative/positive testing
- Interface testing

Case: Team Consultation for Critical Incident

INSTRUCTIONS

1. Working in small teams, select one team member to share a critical incident that caused a degradation or disruption in service.

2. Do a post mortem of the incident by all other team members holding an interview. The interview should take no more than six minutes.

3. Following the interview, each team member takes three minutes to reflect on what type of testing may have been prescribed to expose the vulnerability that led to the critical incident. Select a methodology from this module and write it down on a sheet of paper.

4. Fold your answer and hand to the member who shared the incident, then have that member read aloud the answers.

Module 3

Security Process Data

Module Objectives

1. Select the relevant security processing data administration that supports testing and assessment related to account management and process approval.
2. List essential elements of and differentiate between training and awareness that are aligned with organizational governance, compliance, policy, and capabilities.

Account Management

- Assigning account managers for information systems accounts
- Establishing conditions for group or role membership
- Specifying authorized users of information systems
- Requiring approval for authorizations, creating, enabling, modifying, disabling, and removing access

Management Review and Approval

ISO 27001:2013 outlines concerns for management reviews of an information system by stating:

> *"Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness."*

Key Performance and Risk Indicators

Committee of Sponsoring Organizations of the Treadway Commission (COSO) December 2010 report on *How Key Risk Indicators can Sharpen Focus on Emerging Risks* states that:

- Key performance indicators (KPIs) typically "shed insights about risk events that have already affected the organization."
- Key risk indicators (KRIs), "typically help to better monitor potential future shifts in risk conditions or new emerging risks so that management and boards are able to more proactively identify potential impacts on the organization's portfolio of risks."

Training and Awareness

Roles to be involved and addressed:

- Executive management
- Security personnel
- System owners
- System administrators and IT support personnel
- Operational managers and system users

Module 4

Test Output and Generate Report

Module Objectives

1. Recognize relevant procedures to protect sensitive information when utilizing test data.

Protection of Test Data

- Use of personally identifiable information (PII) should be avoided.
- Verify access controls and procedures are in place.
- When testing is completed, sensitive information should be completely erased.
- Logs should trace all copying of production data.

Module 5

Conduct or Facilitate Security Audits

Module Objectives

1. Define the process of a service provider audit.
2. Associate the appropriate use of an audit type based upon the business support requirements.

Service Organization Control (SOC) 2

SOC 3

The Trust Services Principles and Criteria are specifically defined for

- **Security**
- **Availability**
- **Confidentiality**
- **Processing integrity**
- **Privacy**

SOC 1

SOC 1 reports require that a service organization describes its system and defines its control objectives and controls that are relevant to users' internal control over financial reporting.

SOC 1 and 2

Type 1
Report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.

Type 2
Report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

Module 6

Domain Review

Domain Summary

- Security and assessment testing are integral to an organization managing a portfolio of risks.
- Key to security assessment and testing are the ability and competency to determine, select, tailor, optimize, and execute on strategies that are related to exposing vulnerabilities before they are exploited by adversaries or dysfunctional implementations.
- All relevant security frameworks support developing a robust security assessment and testing organizational plan and practice that is continually improved.

Domain Review Questions

1. If an organization's security assessment and testing plans include both internal and external testing in what order should the test be performed?

A. Always choose the order based upon cost/benefit analysis.
B. Internal testing should be performed first.
C. External testing should be performed first.
D. Internal and external testing should be performed simultaneously.

Answer

The correct answer is C.

External testing is performed first so as not to provide leakage from insider information to outsider environments. Internal and external testing would not be done simultaneously otherwise the identification of vulnerabilities sources could be misconstrued. Cost/benefit analysis would not be a primary justification for choosing which testing should be accomplished first.

Domain Review Questions

2. This type of testing would inform an organization of the vulnerabilities that could be exposed by a bad actor with little or no information about the organization's systems.

A. Internal testing
B. Nocturnal testing
C. External testing
D. White-box testing

Answer

The correct answer is C.

External testing is done to emulate an attacker that is outside of the organization’s perimeter. Nocturnal testing doesn’t exist. External testing by its definition doesn’t have insider information that would be identified with white-box testing.

Domain Review Questions

Scenario Questions 3–6:

Your organization develops security-as-a-service software that is consumed via your private cloud. You employ 50 developers that practice agile discipline in releasing tools to market. A potential client approaches your organization with the intent to acquire your services. Before the potential client commits to a contractual agreement, they have informed your organization that they need to be provided with the highest degree of assurance possible that risks to your operational effectiveness are well contained or mitigated, and they will receive your services delivered in the same operable form they were created in without being changed.

Domain Review Questions

3. What report would be most appropriate to answer the needs of the potential client?

A. SOC 2 Type II
B. SOC 2 Type I
C. SOC 1 Type II
D. SOC 1 Type I

Answer

The correct answer is A.

SOC 2 Type II is a report on technology security controls within an organization. Type II proves design effectiveness. SOC 2 Type I would only confirm the design. SOC 1 is for reviewing financial controls.

Domain Review Questions

4. What report would be good for attracting additional clients yet unknown to your business?

A. SOC 5 Type II
B. SOC 3
C. SOC 5 Type II New Client
D. SOC 5 Type I Existing Client

Answer

The correct answer is B.

SOC 3 is an executive summary that can be used as a web seal to advertise a summary opinion of technical controls. The summary can be posted to a website to advertise for potential customers. There are no SOC 5 reports.

Domain Review Questions

5. What is the difference between a Type I and a Type II SOC report?

A. Type I is developed over a time period; Type II is a snapshot.
B. There are no Type I or II reports.
C. Type I is longer than Type II.
D. Type I is concerned with control design; Type II is concerned with control effectiveness.

Answer

The correct answer is D.

Type I is concerned with control design; Type II is concerned with control effectiveness.

Domain Review Questions

6. For the potential client to understand the probability that your department of 50 developers remain properly compensated and incentivized to continue to support the security-as-a-service that they wish to consume, what report might they consider?

A. SOC 2 Type II
B. SOC 2 Type I
C. SOC 1 Type II
D. SOC 1 Type I

Answer

The correct answer is C.

A SOC 1 Type II report would be appropriate since it would reflect what the effectiveness of the internal controls over financial reporting is. Special attention could be associated with benefits management. SOC 1 is for reviewing financial controls. Type II proves design effectiveness design of the financial control. SOC 1 Type I is proof of the design of the financial control alone. SOC 2 Type II & I are reports on technology security controls within an organization.

Domain Review Questions

7. To simulate a malicious agent trying to gain access to a system via vulnerability, which test best fits the description?

A. Misuse case
B. Penetration test
C. Use case
D. Vulnerability assessment

Answer

The correct answer is B.

Penetration test is intended to test the security state of a system as if an adversary is trying to gain unauthorized access. Misuse case is designed to emulate a misuse of a software application. Use case is proper or expected use of a software application. Vulnerability assessments are designed to verify compliance.

Domain Review Questions

8. According to ISO 27002 a backup policy should define____

A. How many times a tape has been used
B. Retention and protection requirements
C. All the information that can be used in business requirements
D. Technical training for all backup administrators

Answer

The correct answer is B.

ISO 27002 states that a backup policy should define retention and protection requirements. None of the other statements are true concerning what is stated in ISO 27002.

Domain Review Questions

9. What statement is true of key risk indicators (KRIs)?

A. Aid in monitoring emerging risks
B. Aid in understanding if goals have been met
C. Aid in shedding light on performance metrics
D. Aid in alerting when team metrics haven't been met

Answer

The correct answer is A.

KRIs are designed to monitor risk to take proactive action. B, C, and D are all key performance indicator (KPI) markers.

Domain Review Questions

10. What is the key difference between training and awareness?

A. Training is serious whereas awareness is lighthearted.
B. Training is concerned with skills, and awareness is concerned with issue focus.
C. Training and awareness are not different at all.
D. Training is issue focus, and awareness is concerned with skills.

Answer

The correct answer is B.

Training is concerned with skills, and awareness is concerned with issue focus. A, C, and D are all wrong.