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 7

Security Operations

Domain Objectives

1. Describe the characteristics of fundamental information security practices, such as need-to-know, job rotation, separation of duties, and least privilege.
2. Differentiate between methods used to secure privileged accounts and regular user accounts.
3. Describe the facets of each phase of the information lifecycle, in order.
4. Describe the purpose and usage of a service-level agreement (SLA).
5. Describe the purpose and practice of asset inventory/asset management.

Domain Objectives (continued)

6. Detail the reasons for and use of configuration management/change management, to include the composition of a Change Management Board (CMB).
7. List the benefits, challenges, and best ways to implement patch management.
8. Describe techniques for securing media (and the data it contains), including physical, logical, and administrative practices.
9. List typical threats/risks associated with protecting hardware and software assets, and common practices for countering those threats/risks.

Domain Objectives (continued)

10. Discuss comprehensively the common aspects of organizational security that can be tasked to third-party vendors and best practices for securing those relationships.
11. Describe the benefits and challenges of common security practices including the use of sandboxing, honeypots/honeynets, and anti-malware solutions.
12. List phases of a common incident management model, and detail the benefits/challenges associated with each phase.
13. Describe the characteristics commonly associated with various types of investigations (administrative, civil, criminal, and regulatory), and demonstrate familiarity with popular investigatory standards.

Domain Objectives (continued)

14. Describe the challenges and common practices associated with evidence collection and handling, including the chain of custody.
15. List the desired characteristics (for reporting purposes) of evidence.
16. Describe common evidence handling techniques, including digital forensics practices.
17. Name the characteristics and purpose of intrusion detection systems/intrusion prevention systems (IDS/IPS).
18. Describe the purpose and challenges associated with the employment of a security information and event management (SIEM) system.

Domain Objectives (continued)

19. Describe, in detail, the purpose of continuous monitoring practices and the tools currently in common use for achieving that purpose, specifically data leak protection (DLP).
20. Describe the benefits and challenges associated with various common backup strategies and techniques.
21. List the characteristics of common alternate operating site strategies.
22. Describe the technologies and techniques associated with high-availability environments, including differentiating between various redundant array of independent disks (RAID) levels.

Domain Objectives (continued)

23. Describe, in detail, the essential elements of the business continuity and disaster (BCDR) process, including response actions, the personnel involved, communications strategies,
    the practice and risks associated with assessment and recovery, and proper training and awareness for BCDR purposes.
24. Describe the facets and challenges of business continuity and disaster recovery (BCDR) planning and exercises.
25. Describe the characteristics of common types of business continuity and disaster recovery (BCDR) tests.
26. List common security aspects of operational concerns associated with personnel.

Domain Agenda

- Foundational Security Operations Concepts
- Securely Provisioning Resources
- Resource Protection Techniques
- Detective and Preventative Measures
- Incident Management

Domain Agenda (continued)

- Requirements for Investigation Types
- Investigations
- Logging and Monitoring Activities
- Recovery Strategies
- Disaster Recovery (DR) Processes

Domain Agenda (continued)

- Business Continuity (BC) Planning and Exercises
- Test Disaster Recovery Plans (DRPs)
- Personnel Safety and Security Concerns
- Domain Review

Module 1

Foundational Security Operations Concepts

Module Objectives

1. Describe the characteristics of fundamental information security practices, such as need-to-know, job rotation, separation of duties, and least privilege.
2. Differentiate between methods used to secure privileged accounts and regular user accounts.
3. Describe the facets of each phase of the information lifecycle, in order.
4. Describe the purpose and usage of a service-level agreement (SLA).

Foundational Security Operations Concepts

- Need-to-know
- Least privilege
- Separation of duties
- Job rotation

Privileged Account Management

- Increase logging
- Advanced access control
- Temporary access
- Deeper verification
- More extensive audit

Information Lifecycle

Figure 7.1: The Data Lifecycle Phases

Service-Level Agreements (SLAs)

For situations where the organization contracts with an external provider for a particular service (often referred to as a “managed service”), a service-level agreement (SLA) is a preferred mechanism for ensuring both parties are satisfied with the arrangement.

- SLA performance metric example
- SLA enforcement mechanism

Module 2

Securely Provisioning Resources

Module Objectives

1. Describe the purpose and practice of asset inventory/asset management.
2. Describe the reasons for and use of configuration management/change management, to include the composition of a Change Management Board (CMB).
3. List the benefits, challenges, and best ways to implement patch management.

Asset Inventory/Asset Management

- Determining what assets the organization possesses
- Determining the value of each asset (to assign appropriate protection)
- What the inventory includes
- What it reflects

Configuration Management and Change Management

The Change/Configuration Management Board (CMB) typically handles both kinds of CM activity.

Typical CMB process:

- Request
- Review
- Recommend
- Implement
- Monitor/administration
- Disposal

Configuration Management and Change Management (continued)

Typical CMB composition:

- IT department
- Senior management
- Security office
- User community
- General counsel
- Accounting/finance
- Human resources (in some cases)

Configuration Management and Change Management (continued)

- Role of the security practitioner in the CMB
- Best CMB practices for security practitioners

Patch and Vulnerability Management

- Routine/reactive
- Patching challenges:
  - Interoperability
  - Poorly crafted patches
  - Required downtime
  - Added expense
  - Virtualization-specific concerns
  - Timing

Patch and Vulnerability Management (continued)

Typical formal patch process:

1. Receive notice
2. Determine applicability
3. Determine potential impact
4. Test
5. Perform full backup
6. Apply patch
7. Confirm installation
8. Solicit/receive user feedback
9. Prepare for rollback
10. Document

Patch and Vulnerability Management (continued)

Vulnerability management

- Manual/automated
- Definition-based challenges

Module 3

Resource Protection Techniques

Module Objectives

1. Describe techniques for securing media (and the data it contains), including physical, logical, and administrative practices.
2. List typical threats/risks associated with protecting hardware and software assets, and common practices for countering those threats/risks.

Media Management

- Technical/logical
- Physical
- Administrative – backup policy,

Hardware and Software Asset Management

- Hardware protection similar to media management
- Software management
  - Inventory and tracking
  - Licensing
  - Vulnerability scans
  - Patching and updating

Module 4

Detective and Preventative Measures

Module Objectives

1. Discuss comprehensively the common aspects of organizational security that can be tasked to third-party vendors and best practices for securing those relationships.
2. Describe the benefits and challenges of common security practices including the use of sandboxing, honeypots/honeynets, and anti-malware solutions.

Third-Party Provided Security Services

Common third-party services:

- Threat intelligence
- Network monitoring
- Physical security
- Network management
- Audit

Third-Party Provided Security Services (continued)

Best practices for third-party arrangements:

- Review of governance
- Service-level agreements (SLAs)
- Nondisclosure agreements (NDAs)
- Insurance/bonding
- Audit/testing
- Strong contract language
- Regulator approval

Sandboxing

- Hardware sandboxing
- Software sandboxing

Honeypots/Honeynets

- Purpose
- Placement
- What to avoid
  - Policy language
  - Hackback

Anti-Malware

- Installation location
- Common characteristics

Module 5

Incident Management

Module Objective

1. List phases of a common incident management model, and detail the benefits/challenges associated with each phase.

Incident Management

A standard approach to incident management involves these phases:

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

Detection

- Mechanisms:
  - IDS/IPS systems
  - Anti-malware solutions
  - Log analysis
  - Firewalls
  - Vulnerability scan results
  - DAMs
  - Data leak protection/DLP tools
  - DRM solutions
  - Users
- Overreporting versus underreporting

Response

Determining whether the reported activity is an actual incident, including use of:

- Other security team members
- Personnel from other departments
- Devices
- Data

Mitigation

These are the main variables affecting how an incident is initially addressed:

- Time
- Risk
- Impact

Can involve a team with members from:

- Security practitioners
- IT administrators/architects
- General counsel
- Human resources (HR)
- Public relations
- Management

Reporting

Stakeholders:

- Customers
- Vendors
- The public
- Regulators
- Users/employees
- Law enforcement

Recovery

- Often entails appreciable expense
- All efforts made by personnel in this phase, and any interruption to personnel productivity, need to be documented and assessed financially

Remediation

- Root cause analysis
- Senior management decides ultimate solution

Lessons Learned

- Allows the organization to better deal with the same type of incident if it ever happens again
- Allows the organization to improve the overall incident management process for use in all future incident management activity

Module 6

Requirements for Investigation Types

Module Objective

1. Describe the characteristics commonly associated with various types of investigations (administrative, civil, criminal, and regulatory), and demonstrate familiarity with popular investigatory standards.

Requirements for Investigation Types

- Administrative
- Criminal
- Civil
- Regulatory
- Industry standards

Module 7

Investigations

Module Objectives

1. Describe the challenges and common practices associated with evidence collection and handling, including the chain of custody.
2. List the desired characteristics (for reporting purposes) of evidence.
3. Describe common evidence handling techniques, including digital forensics practices.

Evidence Collection and Handling

All material associated with an incident could be pertinent to an investigation and used as evidence:

- Data that may have been compromised.
- Systems (hardware, software, and media) that may have been compromised.
- Data about the incident (all monitoring data from assets reviewing the data/systems that may have been compromised).
- Information from people with knowledge of the incident.
- Information about the incident scene.

Evidence Collection and Handling (continued)

Some common practices for handling evidence that the security professional should be aware of:

- Chain of custody
- Copies of all data/system states
- Analyze copies instead of originals where possible
- Appointment of evidence custodian

Reporting and Documentation

Evidence will be presented to the following:

- Court
- Regulators
- Insurance adjusters
- Investors/shareholders
- Other stakeholders

Reporting and Documentation (continued)

Evidence should adhere to these tenets:

- Admissibility
- Accuracy
- Comprehensibility
- Objectivity

Investigative Techniques

- Automated capture
- Interviews
- Manual capture
- External requests

Digital Forensics Tools, Tactics, and Procedures

- Document everything
- Avoid unrecorded/unintended modification
- Collection is a sensitive process
- No amateur involvement

CASE


SHERIFF'S OFFICE
JEFFERSON
LOUISIANA
STATE OF
LOUISIANA
1825
PARISH

Module 8

Logging and Monitoring Activities

Module Objectives

1. Name the characteristics and purpose of intrusion detection systems/intrusion prevention systems (IDS/IPS).
2. Describe the purpose and challenges associated with the employment of a security information and event management (SIEM) system.
3. Describe, in detail, the purpose of continuous monitoring practices and the tools currently in common use for achieving that purpose, specifically data leak protection (DLP).

Intrusion Detection and Prevention

Intrusion detection system/intrusion prevention system (IDS/IPS)

- Placement
- Detection
- Tradeoffs

Security Information and Event Management (SIEM)

Benefits:

- Aggregation
- Normalization
- Correlation
- Secure storage
- Analysis
- Reporting

Continuous Monitoring

- Ingress monitoring
- Egress monitoring
  - DLP
    - Detection
    - Deployment
    - Protection effort
      - Discovery
      - Monitoring
      - Enforcement

Module 9

Recovery Strategies

Module Objectives

1. Describe the benefits and challenges associated with various common backup strategies and techniques.
2. List the characteristics of common alternate operating site strategies.
3. Describe the technologies and techniques associated with high-availability environments, including differentiating between various redundant array of independent disks (RAID) levels.

Backup Storage Strategies

- Onsite
- Offsite
- Full
- Differential
- Incremental
- Versioning
- Validation

Activity: How Many Versions?

Alice is in charge of orchestrating backups for Ostrich, Inc., her midsize retail company. Employees at Ostrich work between the hours of 7:00 a.m. and 8:00 p.m. (individual employees each work eight-hour days, but they are spread across several time zones), Monday through Friday. Backups are made on Saturday night to allow for integrity checks and repetition on Sunday if the process was faulty or interrupted. Alice has decided to augment the weekly full backups with partial backups Monday through Friday, at the end of each workday, to capture data that has changed between full backups.

Activity: How Many Versions? (continued)

INSTRUCTIONS

As a group, work through the following thought problems. You have 10 minutes.

1. If Alice opts to do differential backups during the week, which data would be captured on Wednesday night?
2. If Alice opts to do incremental backups during the week, which data would be captured on Thursday night?
3. If Alice opts to do differential backups during the week, and the backup copy made Tuesday night is corrupt, which data would be lost?

Activity: How Many Versions? (continued)

ANSWERS

1. All data created/modified during the workdays of Monday, Tuesday, and Wednesday.
2. All data created/modified during the workday Thursday.
3. All data created/modified during the workdays Monday and Tuesday.

Recovery Site Strategies

- Redundant
- Hot
- Warm
- Cold
- Mobile
- Cloud
- Joint operating agreement (JOA)/memorandum of understanding (MOU)

Multiple Processing Sites

- Some organizations that seek to minimize downtime and enhance BCDR capabilities utilize multiple processing sites to obviate the effects of an impact to any single site.
- This can be perceived as a JOA/MOU between internal bodies within the organization.
- Geographically separated branches can serve as alternate production sites for each other in the event of a contingency.

System Resilience, High Availability, Quality of Service (QoS), and Fault Tolerance

- Sufficient spare components
- Clustering
- Power
- RAID
- Centralized data storage:
  - Storage area network (SAN)
  - Network-attached storage (NAS)

Module 10

Disaster Recovery Processes

Module Objectives

1. Describe in detail, the essential elements of the business continuity and disaster recovery (BCDR) process, including response actions, the personnel involved, communications strategies, the practice and risks associated with assessment and recovery, and proper training and awareness for BCDR purposes.

Response

The organization must determine:

- Criteria for initiating the response action
- Personnel authorized to initiate the BCDR action
- Information stream/chain to provide sufficient data

Personnel

Specifically task participants

- Critical path personnel
- Responders
  - IT
  - Security
  - Legal
  - Human resources (HR)
  - Finance/accounting
  - PR/communications
- Management

Communications

- Internal
- External
  - Law enforcement/first responders
  - Regulators
  - Public/news
  - Business partners
- Principles:
  - Single voice
  - Trained professionals
  - Immediacy versus accuracy

Assessment

Enumeration can be used in:

- Criminal prosecution
- Civil litigation
- Investor reporting
- Informing regulators

Restoration

Ultimate goal: resuming full normal operations:

- Returning to original primary site
- Restoring data to the production environment

Training and Awareness

- Personnel specifically tasked (participating in response)
- All personnel in the organization

Module 11

Business Continuity Planning and Exercises

Module Objectives

1. Describe the facets and challenges of business continuity and disaster recovery (BCDR) planning and exercises.

Business Continuity Planning and Exercises

Continuity methods and resources must be tested.

When testing both a failover process and a backup procedure, some fundamental concepts should be considered:

- Test can result in actual contingency
- Test can be scaled down
- Tests involve costs
- Tests may be mandatory

Module 12

Test Disaster Recovery Plans

Module Objectives

1. Describe the characteristics of common types of business continuity and disaster recovery (BCDR) tests.

Test Disaster Recovery Plans

- Read-through/Tabletop
- Walk-through
- Simulation
- Parallel
- Full interruption

Module 13

Personnel Safety and Security Concerns

Module Objectives

1. List common security aspects of operational concerns associated with personnel.

Travel

- Encryption
- Secure remote access
- Additional jurisdictional concerns
- Personnel protection
- Condition monitoring

Security Training and Awareness

- Location-specific orientation for travelers
- Emergency procedures
- Incident reporting procedures
- Users’ role(s) in incident detection and response
- How to recognize attack attempts directly targeting individuals

Emergency Management

Elements of the security program specific to personnel safety should include:

- Fire detection/suppression systems
- Evacuation practice
- Coordination with external entities
- Localized threats (climate, civil unrest, etc.)
- Asset protection secondary
- Relocation strategies

Duress

- Personnel should have a means to report to the organization if they are ever put under duress (threatened or hindered in movement).
- This is especially true for travelers, senior management, and critical personnel, all who may be subject to crimes that target those roles (kidnapping, terror attacks, etc.).
- Subtle/covert
- Training and practice
- Regular schedule change

Module 14

Domain Review

Domain Summary

The organization’s operations incur considerable security risks; it is important for the security practitioner to remember that the security effort supports operations and production and that every security decision comes with an associated tradeoff in productivity.

Domain Review Question

1. All of the following are types of alternate operating sites *except*:

A. Joint operating agreement

B. Mobile site

C. Cloud

D. Full interruption

Answers

The correct answer is D.

Full interruption is a type of BCDR exercise; all the other answers are types of alternate operating sites.

Domain Review Question

2. Which of the following is paramount in all emergency actions/responses?

A. Asset protection

B. Health and human safety

C. Regulatory compliance

D. Confidentiality

Answers

The correct answer is B.

Health and human safety is always the most important aspect of security.

Domain Review Question

3. A duress code should be _____.

A. reusable

B. immediately recognizable

C. covert

D. complex

Answers

The correct answer is C.

The duress code should be something subtle and unrecognizable to anyone outside the organization, simple enough to remember in times of stress, and of limited duration.

Domain Review Question

4. The organization should provide specific BCDR plan training to _____.

A. all members of the security team

B. critical personnel and response team members

C. all stakeholders

D. members of external first response teams (fire, police, medical, etc.)

Answers

The correct answer is B.

Organizational personnel who will be involved in an actual BCDR response should receive specific training from the organization. External responders will be trained by their agencies. Not all members of the security team will be involved in BCDR actions.

Domain Review Question

5. Honeypots/honeynets are intended to _____ attackers.

A. deter

B. attract

C. distract

D. prevent

Answers

The correct answer is C.

A honeypot/honeynet is meant to occupy the attacker’s time, attention, and efforts while the organization collects information about the attack. Honeypots/honeynets will not deter or prevent attacks and should not be construed as attractive.

Domain Review Question

6. Which of the following backup methods requires the most number of data versions to conduct restoration?

A. Full

B. Incremental

C. Differential

D. Composite

Answers

The correct answer is B.

Incremental backups copy all data changed since the last full or incremental backup; this would, on average, require more versions for restoration than full backup (requires one version) and differential (requires two). There is no such thing as composite backup.

Domain Review Question

7. Which of the following is *not* true about emergency response testing?

A. Tests involve cost

B. Tests might result in actual emergencies

C. Tests may be mandatory

D. Tests are performed by the security department

Answers

The correct answer is D.

Emergency response testing should include all affected parties (which can include all personnel in the organization) and is not limited to the security department.

Domain Review Question

8. Which of the following is true about evidence?

A. Evidence is useless if the original version has been changed in any way

B. Evidence can expire

C. Electronic evidence is inadmissible

D. Evidence should be believable

Answers

The correct answer is D.

Evidence is material supporting an argument; it must be believable to be effective.

Domain Review Question

9. Which of the following is true about incident detection?

A. It is better to have overreporting than underreporting

B. It is better to have underreporting than overreporting

C. Incidents must be ended within 24 hours of detection

D. Detection of incidents should be limited to the IT and security departments

Answers

The correct answer is A.

In general, responding to possible incidents that turn out to be harmless is preferable to not knowing when an actual incident occurs (even though false responses still do incur some cost).

Domain Review Question

10. Which of the following is true about vulnerability scans?

A. They prevent attacks

B. They deter attacks

C. They are all automated

D. They typically don’t detect zero-day exploits

Answers

The correct answer is D.

Vulnerability scans typically can only detect known vulnerabilities (which is how they work) but cannot detect zero-day exploits, which are based on attacks unknown to the industry to that point in time.