CISSP Domain Deep Dive - Security Assessment and Testing Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The modern digital landscape demands more than just security implementation; it requires continuous, rigorous validation to ensure organizational resilience. This intensive, deep-dive training focuses exclusively on CISSP Domain 6: Security Assessment and Testing, which constitutes a critical 12% of the Certified Information Systems Security Professional Common Body of Knowledge. Successful security leaders must master the methodologies to objectively measure the effectiveness of security controls, moving beyond a passive compliance mindset to a proactive, risk-driven assurance posture. CISSP Domain Deep Dive - Security Assessment and Testing Training Course is engineered to equip cybersecurity professionals with advanced, hands-on expertise in designing, executing, and analyzing sophisticated assessment strategies, including penetration testing, vulnerability management, and comprehensive security audits.

This specialized program transcends typical certification prep by offering a practical, executive-level understanding of assurance processes. We emphasize the strategic alignment of assessment activities from black-box testing to detailed log analysis with organizational business objectives and governance, risk, and compliance requirements. Key learning outcomes revolve around interpreting test outputs, differentiating between false positives and false negatives, and generating actionable security metrics that drive informed decision-making. By mastering the intricate balance between technical testing and management reporting, participants will be prepared to validate security posture and ensure a robust, continuously monitored defense against the latest cyber threats and zero-day exploits.

Programme Curriculum

CISSP Domain Deep Dive - Security Assessment and Testing Training Course

Introduction

The modern digital landscape demands more than just security implementation; it requires continuous, rigorous validation to ensure organizational resilience. This intensive, deep-dive training focuses exclusively on CISSP Domain 6: Security Assessment and Testing, which constitutes a critical 12% of the Certified Information Systems Security Professional Common Body of Knowledge. Successful security leaders must master the methodologies to objectively measure the effectiveness of security controls, moving beyond a passive compliance mindset to a proactive, risk-driven assurance posture. CISSP Domain Deep Dive - Security Assessment and Testing Training Course is engineered to equip cybersecurity professionals with advanced, hands-on expertise in designing, executing, and analyzing sophisticated assessment strategies, including penetration testing, vulnerability management, and comprehensive security audits.

This specialized program transcends typical certification prep by offering a practical, executive-level understanding of assurance processes. We emphasize the strategic alignment of assessment activities from black-box testing to detailed log analysis with organizational business objectives and governance, risk, and compliance requirements. Key learning outcomes revolve around interpreting test outputs, differentiating between false positives and false negatives, and generating actionable security metrics that drive informed decision-making. By mastering the intricate balance between technical testing and management reporting, participants will be prepared to validate security posture and ensure a robust, continuously monitored defense against the latest cyber threats and zero-day exploits.

Course Duration

5 days

Course Objectives

1. Master the design and validation of risk-based assessment and audit strategies.
2. Execute advanced vulnerability assessments and differentiate between types
3. Perform comprehensive, multi-staged penetration testing on modern infrastructures.
4. Apply Breach and Attack Simulation techniques for continuous validation of security controls.
5. Analyze log data and security events to collect security process data effectively.
6. Understand and validate controls related to Cloud Security Assessment
7. Conduct static, dynamic, and interactive Application Security Testing for secure code assurance.
8. Facilitate and manage internal and third-party security audits and attestations
9. Develop actionable reports and present risk-based findings to executive leadership.
10. Implement and utilize security metrics using the SMART framework.
11. Differentiate between and manage false positives and false negatives in security testing outputs.
12. Deeply analyze threat modeling outputs to prioritize testing efforts.
13. Integrate security testing into the DevSecOps pipeline using automated tools.

Target Audience

1. Cybersecurity Analysts and Engineers.
2. Experienced IT Auditors.
3. Security Managers and aspiring CISOs.
4. Security Consultants.
5. Current CISSP candidates focusing on Domain 6 mastery.
6. Penetration Testers.
7. Risk Management Professionals.
8. Compliance Officers.

Course Modules

Module 1: Foundational Assessment & Audit Strategy

- Design and validate a formal, risk-aligned assessment program.
- Develop a Security Control Testing approach
- Understand and utilize common assessment and testing methodologies
- Establish scope, boundaries, and clear rules of engagement for all testing.
- Case Study: Designing a continuous security assessment strategy for a financial services firm following PCI DSS guidelines.

Module 2: Security Control Testing & Validation

- Techniques for technical and operational control validation.
- Performing manual and automated configuration reviews and baseline compliance checks.
- Validation of cryptographic controls and key management systems.
- Testing the effectiveness of security awareness and training programs.
- Case Study: Validating the Zero Trust Architecture enforcement points across a corporate network using simulated user access scenarios.

Module 3: Vulnerability Assessment Deep Dive

- In-depth planning and execution of vulnerability scanning across networks and applications.
- Advanced techniques for vulnerability analysis and severity rating
- Managing and prioritizing vulnerabilities using a risk-based approach and ticketing systems.
- The difference between authenticated and unauthenticated scanning and their respective use cases.
- Case Study: Implementing a vulnerability management program for an Industrial Control System environment and managing high-risk operational technology findings.

Module 4: Advanced Penetration Testing Techniques

- Executing all phases of a penetration test
- Understanding and exploiting common web application vulnerabilities
- Conducting social engineering testing and physical security assessments.
- Techniques for evading security defenses and maintaining persistence.
- Case Study: Conducting a Red Team and Blue Team exercise to test a mature Security Operations Center (SOC)'s detection and response capabilities.

Module 5: Application Security Testing (AST)

- Integrating SAST into the secure Software Development Life Cycle
- Performing DAST and IAST for in-production and development environments.
- Reviewing security within code repositories and supply chain security controls.
- Fuzz testing, misuse case testing, and software composition analysis
- Case Study: Identifying and remediating a critical vulnerability in a new customer-facing web application through combined SAST/DAST efforts.

Module 6: Collecting and Analyzing Security Data

- Configuring and reviewing logging and monitoring systems for critical data collection.
- Techniques for log analysis, aggregation, and normalization.
- Implementing and tuning Intrusion Detection/Prevention Systems.
- Deploying and utilizing honeypots and honeynets for advanced threat intelligence gathering.

- Case Study: Developing a custom SIEM correlation rule to detect a sophisticated, multi-stage attack based on a known threat actor Tactics, Techniques, and Procedures

Module 7: Reporting, Remediation, and Metrics

- Analyzing test outputs and distinguishing between true positives, false positives, and false negatives.
- Creating Executive-level risk reports and technical remediation plans.
- Defining, calculating, and reporting security metrics
- Communicating assessment findings to management, application owners, and technical teams.
- Case Study: Presenting a comprehensive security assessment report to the Board, focusing on Residual Risk and budget allocation for the next quarter's remediation strategy.

Module 8: Auditing & Regulatory Compliance

- Planning and executing both internal and external security audits.
- Understanding the roles of auditors and assessors
- Techniques for auditing Cloud Service Providers and managing shared responsibility.
- Analyzing audit results and managing corrective actions.
- Case Study: Facilitating an external FedRAMP audit, specifically preparing and presenting evidence for the security assessment controls.

Training Methodology

The course employs a high-engagement, Blended Learning approach combining advanced theoretical knowledge with extensive practical application:

- Instructor-Led Deep Dives.
- Virtual Cyber Range Labs.
- Case Study Analysis.
- Simulation Exams & Quizzes.
- Executive Presentation Workshop.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com