CISSP Domain Deep Dive - Security Architecture and Engineering 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 digital landscape is undergoing a rapid transformation, driven by cloud migration, IoT adoption, and the pervasive threat of sophisticated state-sponsored attacks. Traditional perimeter-based security is fundamentally insufficient, making the role of the Security Architect paramount. CISSP Domain Deep Dive - Security Architecture and Engineering Training Course is designed to dive deep into CISSP Domain 3: Security Architecture & Engineering, providing the strategic and technical mastery required to design, implement, and secure modern, resilient enterprise systems. We move beyond theoretical knowledge to focus on practical application of Secure Design Principles and cutting-edge frameworks like Zero Trust Architecture, which are critical for protecting assets in today's complex hybrid cloud and remote work environments. This program is your essential blueprint for building an impregnable security foundation.

Earning the Certified Information Systems Security Professional designation signifies a master level of competency in securing an organization's most critical assets. This specialized training accelerates your journey by drilling into the most complex and career-defining domain: Security Engineering. You will master the deployment of Advanced Cryptography, the application of formal Security Models, and the assessment of vulnerabilities across diverse architectures, from Containerization to SCADA/ICS. Graduates will be equipped to assume senior-level roles, drive security posture management, and influence an organization's long-term cybersecurity strategy, making this an invaluable investment in professional distinction and a significant career salary boost.

Programme Curriculum

CISSP Domain Deep Dive - Security Architecture and Engineering Training Course

Introduction

The digital landscape is undergoing a rapid transformation, driven by cloud migration, IoT adoption, and the pervasive threat of sophisticated state-sponsored attacks. Traditional perimeter-based security is fundamentally insufficient, making the role of the Security Architect paramount. CISSP Domain Deep Dive - Security Architecture and Engineering Training Course is designed to dive deep into CISSP Domain 3: Security Architecture & Engineering, providing the strategic and technical mastery required to design, implement, and secure modern, resilient enterprise systems. We move beyond theoretical knowledge to focus on practical application of Secure Design Principles and cutting-edge frameworks like Zero Trust Architecture, which are critical for protecting assets in today's complex hybrid cloud and remote work environments. This program is your essential blueprint for building an impregnable security foundation.

Earning the Certified Information Systems Security Professional designation signifies a master level of competency in securing an organization's most critical assets. This specialized training accelerates your journey by drilling into the most complex and career-defining domain: Security Engineering. You will master the deployment of Advanced Cryptography, the application of formal Security Models, and the assessment of vulnerabilities across diverse architectures, from Containerization to SCADA/ICS. Graduates will be equipped to assume senior-level roles, drive security posture management, and influence an organization's long-term cybersecurity strategy, making this an invaluable investment in professional distinction and a significant career salary boost.

Course Duration

5 days

Course Objectives

1. Master Zero Trust Architecture (ZTA) principles and deployment across hybrid environments.
2. Apply Secure Design Principles like least privilege, separation of duties, and Privacy by Design (PbD).
3. Analyze and select appropriate Security Models for various business contexts.
4. Assess and mitigate vulnerabilities in Cloud Computing service models and deployment models.
5. Design robust security controls for modern systems, including Container Security and Serverless Computing.
6. Implement and manage the full Cryptographic Lifecycle, covering both symmetric/asymmetric algorithms and Public Key Infrastructure (PKI).
7. Evaluate and integrate security controls for Industrial Control Systems and embedded IoT devices.
8. Understand and secure memory, CPU, and operating system components using Trusted Computing features like TPM.
9. Conduct effective Threat Modeling exercises to identify design flaws and architectural risks early in the System Development Life Cycle (SDLC).
10. Design and implement comprehensive Site and Facility Security controls, utilizing a Defense-in-Depth approach.
11. Secure Distributed Systems, including microservices, high-performance computing (HPC), and edge computing.
12. Compare and contrast different security evaluation criteria, such as Common Criteria and TCSEC, and their practical relevance.
13. Integrate Security Architecture with overall Risk Management Frameworks and Compliance requirements.

Target Audience Profiles

1. Aspiring CISSP Candidates

2. Security Architects and Engineers.
3. Senior Information Security Analysts.
4. Cloud Security Specialists.
5. IT/Security Consultants.
6. Technology Risk Managers.
7. System and Network Engineers.
8. Security Managers.

Course Modules

Module 1: Foundational Secure Design Principles

- Least Privilege, Separation of Duties, Defense in Depth, Fail-Securely.
- Integrating Privacy by Design and Security by Design into the SDLC.
- Formal Security Models and their application to system design.
- Trusted Computing Base and security mechanisms in operating systems
- Case Study: Analyzing a Fortune 500's successful shift from perimeter defense to a Secure-by-Design methodology after a major breach.

Module 2: Zero Trust Architecture (ZTA) Implementation

- Detailed breakdown of the ZTA model
- Micro-segmentation, Identity-Centric Security, and Context-Aware Access Control.
- Integrating Identity and Access Management with ZTA policies
- Transitioning from traditional VPN/firewalls to modern secure access service edge architectures.
- Case Study: Designing a ZTA rollout plan for a global, remote-first organization to secure cloud-based SaaS applications.

Module 3: Cloud and Virtualization Security Architecture

- In-depth analysis of security responsibilities in IaaS, PaaS, and SaaS models.
- Securing virtualized environments.
- Advanced Cloud Security Posture Management and Cloud Access Security Broker deployment.
- Vulnerability assessment for cloud-native technologies: Container Security and Serverless Functions.
- Case Study: Mitigating a common cloud misconfiguration incident through automated CSPM tools and policy enforcement.

Module 4: Applied Cryptography and PKI Management

- Selection and management of symmetric and asymmetric algorithms.
- Deep dive into Hashing, Digital Signatures, and Message Authentication Codes
- Designing and operating a robust Public Key Infrastructure, including certificate and key management.
- Understanding the risks and migration path toward Post-Quantum Cryptography.
- Case Study: Developing a full-disk encryption and secure communication protocol for a sensitive R&D team using a tiered PKI structure.

Module 5: Vulnerability Assessment of Systems

- Assessing security in client-based, server-based, and Database Systems
- Securing High-Performance Computing, Distributed Systems, and Edge Computing environments.
- Identifying and mitigating risks in Web Application Architecture based on current OWASP Top 10.
- Securing mobile and embedded systems, including Enterprise Mobility Management and BYOD policies.

- Case Study: Performing a risk assessment on a new IoT product line, identifying and securing embedded firmware and network vulnerabilities.

Module 6: ICS/SCADA and IoT Security Engineering

- Unique challenges and architectural requirements for securing industrial environments
- Implementing security controls for Supervisory Control and Data Acquisition and Industrial Control Systems.
- Risk assessment and mitigation strategies for embedded systems and System-on-a-Chip devices.
- Understanding common protocols and segmentation techniques for critical infrastructure protection.
- Case Study: Developing a network segmentation strategy to isolate a critical manufacturing SCADA network from the corporate IT network.

Module 7: Physical Security and Site Design

- Applying the Defense-in-Depth strategy to physical security controls.
- Designing secure sites.
- Implementing Environmental and Life Safety controls
- Perimeter security, access control mechanisms, and intrusion detection systems.
- Case Study: Designing the physical security plan for a new data center, balancing cost, compliance, and operational resilience.

Module 8: System Acquisition and Risk Management

- Integrating security throughout the entire System Development Life Cycle and acquisition phases.
- Evaluating system security using criteria like Common Criteria and formal models.
- Vendor management, supply chain risks, and securing third-party dependencies.
- Conducting Threat Modeling as an ongoing practice to maintain security posture.
- Case Study: Analyzing the procurement process of a new third-party SaaS vendor, developing a risk-based acceptance report based on security architecture review.

Training Methodology

The training employs an Accelerated Blended Learning approach, designed for maximum knowledge retention and practical skill development:

1. Lecture & Concept Review.
2. Scenario-Based Learning.
3. Hands-on Labs.
4. Deep-Dive Case Studies.
5. Review and Practice Quizzes.

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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