Certified Information Systems Security Professional (CISSP) Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s digital landscape, information security has become a critical priority for organizations worldwide. Certified Information Systems Security Professional (CISSP) Training Course provides comprehensive knowledge and hands-on skills in designing, implementing, and managing robust information security programs. Participants gain expertise in risk management, cybersecurity frameworks, regulatory compliance, threat detection, and incident response, empowering them to protect organizational assets and ensure data confidentiality, integrity, and availability. The course emphasizes emerging technologies, cloud security, IoT, and cyber resilience strategies to address modern threats effectively.

The CISSP course combines theoretical foundations with practical applications, equipping professionals to navigate complex security environments across industries. Through interactive discussions, case studies, and real-world exercises, participants learn to assess vulnerabilities, implement access control mechanisms, perform security audits, and develop enterprise-wide security policies. By the end of the course, learners will be prepared to manage security operations strategically, align information security with business objectives, and achieve certification readiness for CISSP, strengthening both professional capabilities and organizational security posture.

Programme Curriculum

Certified Information Systems Security Professional (CISSP) Training Course

Introduction

In today’s digital landscape, information security has become a critical priority for organizations worldwide. Certified Information Systems Security Professional (CISSP) Training Course provides comprehensive knowledge and hands-on skills in designing, implementing, and managing robust information security programs. Participants gain expertise in risk management, cybersecurity frameworks, regulatory compliance, threat

detection, and incident response, empowering them to protect organizational assets and ensure data confidentiality, integrity, and availability. The course emphasizes emerging technologies, cloud security, IoT, and cyber resilience strategies to address modern threats effectively.

The CISSP course combines theoretical foundations with practical applications, equipping professionals to navigate complex security environments across industries. Through interactive discussions, case studies, and real-world exercises, participants learn to assess vulnerabilities, implement access control mechanisms, perform security audits, and develop enterprise-wide security policies. By the end of the course, learners will be prepared to manage security operations strategically, align information security with business objectives, and achieve certification readiness for CISSP, strengthening both professional capabilities and organizational security posture.

Course Objectives

1. Understand the CISSP domains and information security concepts.
2. Develop expertise in risk management and threat mitigation strategies.
3. Implement access control, identity management, and security architecture.
4. Apply cryptography and encryption techniques to secure data.
5. Design and manage network security systems and protocols.
6. Establish security governance, compliance, and regulatory alignment.
7. Conduct security assessments, audits, and vulnerability management.
8. Develop incident response and disaster recovery strategies.
9. Implement application, cloud, and mobile security best practices.
10. Monitor and respond to emerging threats and advanced persistent threats.
11. Integrate security awareness and training programs across organizations.
12. Enhance business continuity planning and operational resilience.
13. Prepare for CISSP certification with domain-specific knowledge and practice.

Organizational Benefits

- Enhanced enterprise-wide cybersecurity posture
- Reduced risk of data breaches and cyberattacks
- Improved compliance with industry regulations and standards
- Strengthened incident response and disaster recovery capabilities
- Increased efficiency in security operations and resource allocation
- Better protection of intellectual property and sensitive information
- Higher confidence among clients, stakeholders, and regulators
- Development of a skilled, security-aware workforce
- Improved strategic alignment of IT and security initiatives
- Competitive advantage through certified, highly trained staff

Target Audiences

- Information security managers and officers
- IT administrators and network engineers
- Risk management and compliance professionals
- Security auditors and consultants
- System architects and software developers
- Cloud and infrastructure security specialists
- Incident response and cybersecurity analysts

- Senior management responsible for enterprise security

Course Duration: 10 days

Course Modules

Module 1: Security and Risk Management

- Understand security governance frameworks
- Analyze risk management concepts and processes
- Establish organizational security policies
- Apply compliance and regulatory requirements
- Develop security awareness programs
- Case Study: Risk assessment and policy implementation in a multinational company

Module 2: Asset Security

- Classify and manage information assets
- Implement data privacy and protection measures
- Establish retention and disposal policies
- Apply labeling and handling procedures
- Monitor asset usage and compliance
- Case Study: Securing sensitive financial and customer data

Module 3: Security Architecture and Engineering

- Design secure systems and network architectures
- Implement security models and frameworks
- Apply cryptographic solutions to data protection
- Protect hardware and software infrastructures
- Evaluate emerging security technologies
- Case Study: Designing secure cloud-based infrastructure

Module 4: Communication and Network Security

- Secure network protocols and communication channels
- Implement firewall, VPN, and intrusion detection systems
- Apply segmentation and network monitoring strategies
- Manage wireless and remote access security
- Monitor traffic for anomalies and threats
- Case Study: Network security design for a global enterprise

Module 5: Identity and Access Management (IAM)

- Implement authentication and authorization mechanisms
- Manage user identities and roles effectively
- Apply Single Sign-On (SSO) and federation techniques
- Secure privileged accounts and credentials
- Monitor and review access controls
- Case Study: IAM deployment in a financial institution

Module 6: Security Assessment and Testing

- Conduct vulnerability assessments and penetration tests
- Evaluate security controls and compliance
- Perform risk analysis for systems and applications
- Monitor and report security metrics
- Implement continuous testing and improvement
- Case Study: Penetration testing results and remediation planning

Module 7: Security Operations

- Monitor security events and incidents
- Implement logging and audit mechanisms
- Manage incident response and escalation
- Develop operational security procedures
- Coordinate with internal and external stakeholders
- Case Study: Security operations center (SOC) incident response

Module 8: Software Development Security

- Integrate security into SDLC processes
- Apply secure coding standards and practices
- Test applications for vulnerabilities
- Implement software patching and version control
- Monitor for application-level threats
- Case Study: Secure software development for a banking application

Module 9: Cloud Security

- Assess cloud service models and deployment types
- Implement cloud access control and monitoring
- Secure cloud data and applications
- Apply cloud governance and compliance frameworks
- Evaluate shared responsibility models
- Case Study: Cloud migration with full security compliance

Module 10: Mobile and Endpoint Security

- Secure mobile devices and endpoints
- Implement device management and encryption
- Monitor endpoint activities and threats
- Develop policies for BYOD and remote access
- Evaluate vulnerabilities in mobile applications
- Case Study: Endpoint security implementation for remote workforce

Module 11: Cryptography

- Apply symmetric and asymmetric encryption
- Implement digital signatures and certificates
- Manage key lifecycle and cryptographic policies
- Use encryption in network and data storage security
- Evaluate emerging cryptographic technologies
- Case Study: Cryptography deployment in secure communication channels

Module 12: Physical Security

- Secure facilities and critical infrastructure
- Control access to sensitive areas
- Implement surveillance and monitoring systems
- Integrate physical and logical security measures
- Develop disaster recovery and contingency plans
- Case Study: Physical security upgrade in a data center

Module 13: Business Continuity and Disaster Recovery

- Develop continuity and recovery plans
- Conduct business impact analysis (BIA)
- Implement redundancy and failover strategies
- Test and update continuity plans regularly
- Coordinate with stakeholders for crisis management
- Case Study: Disaster recovery exercise in a multinational organization

Module 14: Incident Management and Response

- Establish incident response policies and procedures
- Detect and analyze security incidents
- Coordinate response and communication
- Implement containment, eradication, and recovery
- Conduct post-incident review and lessons learned
- Case Study: Handling ransomware attack in a financial institution

Module 15: Legal, Regulations, Compliance, and Ethics

- Understand applicable laws and regulatory frameworks
- Apply compliance in operational security management
- Implement ethical practices in information security
- Monitor compliance metrics and reporting
- Conduct audits and ensure governance adherence
- Case Study: Regulatory compliance audit in a multinational IT company

Training Methodology

- Instructor-led presentations and discussions on CISSP domains
- Hands-on labs and practical exercises for security tools and frameworks
- Case study analysis and group problem-solving activities
- Real-world scenario simulations for incident response and risk mitigation
- Peer learning, assessments, and group presentations
- Action plan creation and feedback sessions

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	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 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