

# Certified Information Systems Security Professional (CISSP) 'Bootcamp' in Addis Ababa

The objective of this course is to equip cybersecurity professionals with the skills to design, implement, and manage enterprise security programs. Aligned with the (ISC)<sup>2</sup> CISSP CBK, it strengthens capabilities in governance, risk management, security architecture, cryptography, network/cloud security, and incident response - enabling participants to lead security initiatives and prepare for the CISSP exam.

**10 FULL DAYS | <DATE - TBD> | TRAINING FACILITIES AT <LOCATION>**

- Fully aligned with (ISC)<sup>2</sup> CISSP CBK learning objectives.
- Deep coverage of enterprise security architecture, governance, IAM, risk & asset management.
- Scenario-based learning with real-world case discussions and policy design exercises.
- Hands-on security labs hosted on the CyCube SaaS Platform - no installation required.
- Learn to design security programs, implement controls, evaluate risk, and support business resilience.
- Ideal for professionals preparing for CISSP Examination or targeting security leadership roles.
- **Course Prerequisites:** Strong InfoSec fundamentals; 2–3 years' experience in IT/cybersecurity; familiarity with governance, networking, and access control; recommended Security+ or equivalent background.

## TARGET AUDIENCE

- Information Security Managers
- Cybersecurity Analysts & Engineers
- SOC & Blue Team Professionals
- System/Network Administrators
- Security Consultants & Auditors
- Security Architects
- Professionals preparing for CISSP certification

## THE INSTRUCTOR

Delivered by senior instructors with 10+ years of experience in cybersecurity and ICT systems, with strong hands-on and professional training expertise. Practical, scenario-based learning and hands-on labs are emphasized.

## ABOUT ECS ETHIOPIA

ECS Ethiopia is a technology-driven company working with government bodies, municipalities, and large corporations to bring advanced global solutions to Ethiopia. As part of the ECS Group (UK), we help finance and execute major projects while fostering strong partnerships and innovation across the country.

## GLOBAL TRAINING PARTNERSHIPS

Our training programs and learning platform were developed in close collaboration with leading international training organisations. Thousands of professionals worldwide have successfully completed these programs using this training content and learning system.



## MODULE 01

### SECURITY AND RISK MANAGEMENT

Understand the fundamental principles of security governance, risk management, and compliance. Learn about security policies, business continuity, professional ethics, and frameworks such as ISO 27001 and NIST. Study risk assessment, mitigation, and information classification.

## MODULE 02

### ASSET SECURITY

Study the lifecycle of information assets, including classification, ownership, and retention. Learn secure data handling, privacy protection, and media management techniques to maintain data confidentiality, integrity, and availability.

## MODULE 03

### SECURITY ARCHITECTURE AND ENGINEERING

Explore secure design principles for systems, networks, and hardware. Understand cryptography, security models (Bell-LaPadula, Clark-Wilson), and hardware security mechanisms. Learn physical security, secure architecture frameworks, and trusted computing principles.

## MODULE 04

### COMMUNICATION AND NETWORK SECURITY

Examine secure network architecture, protocols, and transmission methods. Learn about firewalls, VPNs, IDS/IPS, and secure communication channels. Study network segmentation, zero-trust models, and emerging network technologies.

## MODULE 05

### IDENTITY AND ACCESS MANAGEMENT (IAM)

Understand identity lifecycle management, access control models, and authentication systems. Study SSO, MFA, federation, and privilege management. Learn how to design and implement IAM policies across diverse environments.

## MODULE 06

### SECURITY ASSESSMENT AND TESTING

Learn how to plan, conduct, and analyze security tests and assessments. Study vulnerability assessments, penetration testing concepts, and audit management. Understand continuous monitoring and metrics for control effectiveness.

## MODULE 07

### SECURITY OPERATIONS

Examine operational processes such as change control, incident response, and forensic investigations. Learn about SOC operations, digital forensics, threat monitoring, and maintaining operational resilience.

## MODULE 08

### SOFTWARE DEVELOPMENT SECURITY

Understand secure coding practices and software assurance principles. Learn SDLC integration, threat modeling, supply chain security, and common software vulnerabilities like injection attacks and buffer overflows.

## MODULE 09

### GOVERNANCE, COMPLIANCE, AND LEGAL ISSUES

Study global regulatory and legal requirements in information security. Understand privacy laws (GDPR, HIPAA, CCPA), intellectual property, cybercrime laws, and legal considerations in digital evidence handling.

## MODULE 10

### SECURITY ARCHITECTURE DESIGN AND IMPLEMENTATION

Learn to develop enterprise-wide security architectures. Study reference models, layered defense strategies, and integration of technical and administrative controls. Understand alignment with business goals and risk appetite.

## MODULE 11

### CRYPTOGRAPHY AND KEY MANAGEMENT

Understand encryption algorithms, PKI, key lifecycle management, hashing, and cryptanalysis. Learn how cryptography ensures confidentiality, authentication, integrity, and non-repudiation.

## MODULE 12

### BUSINESS CONTINUITY AND DISASTER RECOVERY

Learn strategies for resilience and continuity. Study backup, failover, crisis management, and DR planning aligned with business impact analysis and risk frameworks.

## MODULE 13

### SECURITY OPERATIONS MANAGEMENT

Study daily operational activities including logging, patching, auditing, and configuration baselines. Learn incident coordination across distributed environments.

## MODULE 14

### RISK-BASED SECURITY MANAGEMENT

Learn approaches to advanced risk assessment and mitigation. Study quantitative/qualitative models, cost-benefit evaluation, residual risk, and threat modeling.

## MODULE 15

### EMERGING TECHNOLOGIES AND SECURITY TRENDS

Explore security implications of cloud, IoT, AI, and quantum computing. Study evolving threat landscapes, modern defenses, and future-driven security strategies.

## MODULE 16

### PHYSICAL AND ENVIRONMENTAL SECURITY

Understand physical protection mechanisms: access controls, power redundancy, fire suppression, and facility security design.

## MODULE 17

### SECURITY METRICS AND PROGRAM MANAGEMENT

Learn how to measure and strengthen security maturity using KPIs, metrics, reporting, and continuous improvement processes.

## MODULE 18

### SECURITY AWARENESS AND TRAINING

Understand human factors in security. Learn how to create awareness programs, reduce social engineering risks, and build security-minded culture.

## MODULE 19

### THIRD-PARTY AND SUPPLY CHAIN RISK MANAGEMENT

Study vendor assessment, outsourcing risks, and contractual security controls. Learn methods for monitoring third-party compliance.

## MODULE 20

### INTEGRATING SECURITY INTO ENTERPRISE STRATEGY

Combine all domains to build organization-wide security strategy. Learn communication with executives, alignment with business goals, and leading security initiatives effectively.