ECS Ethiopia

CISSP Certification 'Bootcamp' - Ethiopia

The objective of this course is to prepare experienced security, communications managers and executives for the prestigious international premier cyber security certification – the CISSP (Certified Information Systems Security Professional) of the international organization ISC2.

- Throughout the course we will put an emphasis on analyzing real events and connecting them to the routine work of the organization's information security professional.
- The course is based on the current $(ISC)^2$ program for 2019, in addition to supplemental material and tools that were developed by certified instructors with international experience and credentials.
- Our instructor will share his personal and practical experience and challenges he faced as CISO in different organizations worldwide.
- We have developed an internal testing system with thousands of current and relevant practice questions for the CISSP. All students will be granted access to unlimited exam simulation exercises during the boot camp and for a period of 12 months afterwards.
- The course is planned for 8-15 participants only. This allows for high attention to each participant.
- **94% of our students have passed the CISSP certification exam.**
- Course pre-requisites: 5 years of experience in at least 2 of the 8 CISSP domains (detailed in the course description), and a high level of technical English.

TARGET AUDIENCE

- Information security advisors
- Information security managers
- Information system managers
- IT auditors
- Network communication managers
- Information system analysts
- Information security architects
- Information security analysts

ABOUT THE CISSP EXAM

- Duration: 3 hours
- Questions: 100-150
- Passing score: 700 and above
- Language: English
- Exam method: Computerized Adaptive Testing
- Location: certified exam centers in Addis Ababa

CISSP®

The Instructor: Mr. Chen Heffer - International expert in Cyber Consulting and Training

- Over 20 years of experience that includes working with international organizations including the financial sector in North America, Europe and Africa.
- Specializes in Information & Technology Risk Management, Governance Risk & Compliance, Fraud Management and Strategic Consulting, and in the following regulations & standards: NIST, PCI DSS, HIPAA, ISO 27K, NERC, SOX, COBIT.
- CISO, CISSP, CISM, GISP, CRISC, CISA, PCIP, PCI ISA

REGISTRATION CONTACT **Ms. Frewoini Adane** | Mobile: +251 (0) 910372484 | Mail: fray.adane@ecs-et.com

ECS Ethiopia

DOMAIN 1
SECURITY AND RISK MANAGEMENT (15%)
- Understand and apply concepts of confidentiality, integrity, and availability
- Evaluate and apply security governance principles
- Determine compliance requirements
- Understand legal and regulatory issues that pertain to information security in a global context
- Understand, adhere to, and promote professional ethics
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyze, and prioritize Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modeling concepts and methodologies
- Apply risk-based management concepts to the supply chain
- Establish and maintain a security awareness, education, and training program

DOMAIN 2
ASSET SECURITY (10%)
- Identify and classify information and assets
- Determine and maintain information and asset ownership
- Protect privacy
- Ensure appropriate asset retention
- Determine data security controls
- Establish information and asset handling requirements

DOMAIN 3
SECURITY ARCHITECTURE AND ENGINEERING (13%)
- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models
- Select controls based upon systems security requirements
- Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Assess and mitigate vulnerabilities in web-based systems
- Assess and mitigate vulnerabilities in mobile systems
- Assess and mitigate vulnerabilities in embedded devices
- Apply cryptography
- Apply security principles to site and facility design
- Implement site and facility security controls

DOMAIN 4
COMMUNICATION AND NETWORK SECURITY (14%)
- Implement secure design principles in network architectures
- Apply secure design principle in network architecture
- Network Access Control (NAC) devices
- Implement secure communication channels according to design
- Secure network components
- Implement secure communication channels according to design

DOMAIN 5
IDENTITY AND ACCESS MANAGEMENT (13%)
- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Integrate identity as a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle

DOMAIN 6
SECURITY ASSESSMENT AND TESTING (12%)
- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyze test output and generate report
- Conduct or facilitate security audits

DOMAIN 7
SECURITY OPERATIONS (13%)
- Understand and support investigations
- Understand requirements for investigations types
- Conduct logging and monitoring activities
- Securely provisioning resources
- Understand and apply foundational security operations concepts
- Apply resource protection techniques
- Conduct incident management
- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

DOMAIN 8
SOFTWARE DEVELOPMENT SECURITY (10%)
- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in development environments
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure coding guidelines and standards