# Certified Information Systems Security Professional

**Duration: 5 Days** **Course Code: CISSP**

## Overview:

A CISSP is an information assurance professional who defines the architecture, design, management and/or controls that assure the security of business environments. The vast breadth of knowledge and the experience it takes to pass the exam is what sets the CISSP apart.

The CISSP was the first credential in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024. CISSP certification is not only an objective measure of excellence, but a also globally recognized standard of achievement.

## Target Audience:

IT professionals seeking to enhance their careers and gain credibility as information security specialists

## Objectives:

- Best-practice information security management practices, including IS technical skills, risk management and business continuity planning.
- Access control and physical security
- Cryptography
- Security architecture for applications and networks.

## Prerequisites:

The Seminar offers a high-level review of the main topics and identifies areas that students need to study and includes:

- Post-Seminar Self-Assessment
- 100% up-to-date material
- An overview of the scope of the information security field

## Content:

- Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations,Business Continuity)
  - Understand and Apply Concepts of Confidentiality, Integrity, and Availability
  - Apply Security Governance Principles
  - Compliance
  - Understand Legal and Regulatory Issues that Pertain to Information Security in a Global Context
  - Develop and Implement Documented Security Policy, Standards, Procedures, and Guidelines
  - Understand Business Continuity Requirements
  - Contribute to Personnel Security Policies
  - Understand and Apply Risk Management Concepts
  - Understand and Apply Threat Modeling
  - Integrate Security Risk Considerations into Acquisitions Strategy and Practice
  - Establish and Manage Security Education, Training, and Awareness
- Asset Security (Protecting Security of Assets)
  - Classify Information and Supporting Assets
  - Determine and Maintain Ownership
  - Protect Privacy
  - Ensure Appropriate Retention
  - Determine Data Security Controls
  - Establish Handling Requirements
- Security Engineering (Engineering and Management of Security)
  - Implement and Manage an Engineering Life Cycle Using Security Design Principles
  - Understand Fundamental Concepts of Security Models
  - Select Controls and Countermeasures Based Upon Information Systems Security Standards
  - Understand the Security Capabilities of Information Systems
  - 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 and Cyber-PhysicalSystems
  - Apply Cryptography
  - Apply Secure Principles to Site and Facility Design
  - Design and Implement Facility Security
- Communications and Network Security (Designing and Protecting Network Security)
  - Apply Secure Design Principles to Network Architecture
  - Securing Network Components
  - Design and Establish Secure Communication Channels
  - Prevent or Mitigate Network Attacks
- Identity and Access Management (Controlling Access and Managing Identity)
  - Control Physical and Logical Access to Assets
  - Manage Identification and Authentication of People and Devices
  - Integrate Identity as a Service (IDaaS)
  - Integrate Third-Party Identity Services
  - Implement and Manage Authorization Mechanisms
  - Prevent or Mitigate Access Control Attacks
  - Manage the Identity and Access Provisioning Life Cycle
- Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)
  - Design and Validate Assessment and Test Strategies
  - Conduct Security Control Testing
  - Collect Security Process Data
  - Conduct or Facilitate Internal and Third-Party Audits
- Security Operations (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)
  - Understand and Support Investigations
  - Understand Requirements for Investigation Types
  - Conduct Logging and Monitoring Activities
  - Secure the Provisioning of Resources through Configuration Management
  - Understand and Apply Foundational Security Operations Concepts
  - Employ Resource Protection Techniques
  - Conduct Incident Response
  - Operate and Maintain Preventative Measures
  - Implement and Support Patch and Vulnerability Management
  - Participate in and Understand Change Management Processes
  - Implement Recovery Strategies
  - Implement Disaster Recovery Processes
  - Test Disaster Recovery Plan
  - Participate in Business Continuity Planning
  - Implement and Manage Physical Security
  - Participate in Personnel Safety
- Software Development Security (Understanding, Applying, and Enforcing Software Security)
  - Understand and Apply Security in the Software Development Life Cycle
  - Enforce Security Controls in the Development Environment
  - Assess the Effectiveness of Software Security
  - Assess Software Acquisition Security

## Further Information:

For More information, or to book your course, please Email us on:
KENYA - training.kenya@clclearningafrica.com
TANZANIA - training.tanzania@clclearningafrica.com
UGANDA - training.uganda@clclearningafrica.com
RWANDA - training.rwanda@clclearningafrica.com
UAE - training.emea@clclearningafrica.com