

Sir / Madam,

[Training Brief For Certified Information Systems Security Professional \(CISSP\)](#)

Course Description

Certified Information Systems Security Professional (CISSP) is the leading certification for today's information systems security professional. It remains the primus inter pares for security professionals because the training providers – The International Information Systems Security Certification Consortium (ISC)2, global leaders in IT and Cyber security, regularly updates its test exams by using subject matter experts to ensure its contents align with today's security industry to evaluate and validate the competencies of personnel saddled with information security functions.

Undertaking a preparatory training course on CISSP expands your know-how by addressing the vital elements of the eight (8) domains that constitutes a Common Body of Knowledge (CBK) for professionals in the information security industry, providing participants with a thorough grasp of information security concepts and industry best practices. That way, participants are able to gain knowledge, new trends and expertise in information security that increases their ability to successfully implement and manage security programs in any organization as well as ready to successfully seat for the very rigorous CISSP exams.

The eight (8) domains for coverage are:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Course Objectives

This is in line with the objectives of the certification organizing body (ISC)2 as clearly enumerated by them as the following:

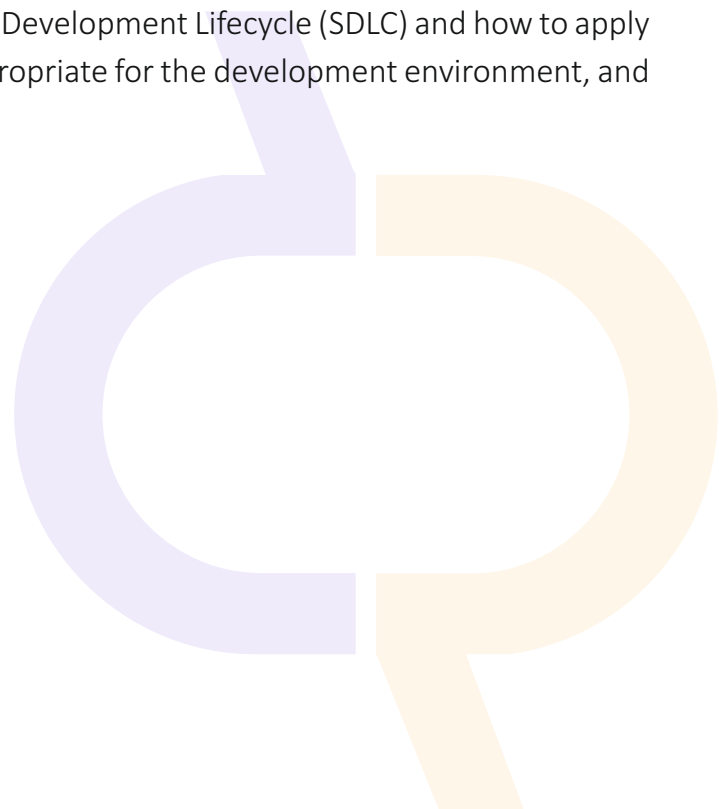
- Understand and apply fundamental concepts and methods related to the fields of information technology and security.
- Align overall organizational operational goals with security functions and implementations.
- Understand how to protect assets of the organization as they go through their lifecycle.

- Understand the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.
- Implement system security through the application of security design principals and the application of appropriate security control mitigations for vulnerabilities present in common information system types and architectures.
- Understand the importance of cryptography and the security services it can provide in today's digital and information age.
- Understand the impact of physical security elements on information system security and apply secure design principals to evaluate or recommend appropriate physical security protections.
- Understand the elements that comprise communication and network security coupled with a thorough description of how the communication and network systems function.
- List the concepts and architecture that define the associated technology and implementation systems and protocols at Open Systems Interconnection (OSI) model layers 1–7.
- Identify standard terms for applying physical and logical access controls to environments related to their security practice.
- Appraise various access control models to meet business security requirements.
- Name primary methods for designing and validating test and audit strategies that support business requirements.
- Enhance and optimize an organization's operational function and capacity by applying and utilizing appropriate security controls and countermeasures.
- Recognize risks to an organization's operational endeavors, and assess specific threats, vulnerabilities, and controls.
- Understand the System Lifecycle (SLC) and the Software Development Lifecycle (SDLC) and how to apply security to it, and identify which security control(s) are appropriate for the development environment, and assess the effectiveness of software security.

Course Content

Module 1: Security and Risk Management

- Security Governance theories
- Concept of Compliance
- Concept of Professional Ethics
- Documentation in Security
- Risk Management Concepts
- Modeling of Possible Threats
- Basics of Business Continuity Plan
- Acquisition Strategy and Practice
- Policies in Personnel Security



- Concepts of Security Awareness and Training

Module 2: Asset Security

- Classification
- Privacy Protection concepts
- Retention of Assets
- Controls in Data Security
- Secure Data Handling

Module 3: Security Architecture and Engineering

- Security in the Engineering Lifecycle
- Security of System Component
- Security Models Concepts
- Controls and Counter steps of Security in an Enterprise
- Information System Security Capabilities
- Design and Architecture Vulnerability Management
- Management of Vulnerability in IT Systems
- Cryptography Detailed Concepts
- Cryptography Techniques
- Site and Facility Design for Physical Security
- Implementation of Physical Security in Sites and Facilities

Module 4: Communication and Network Security

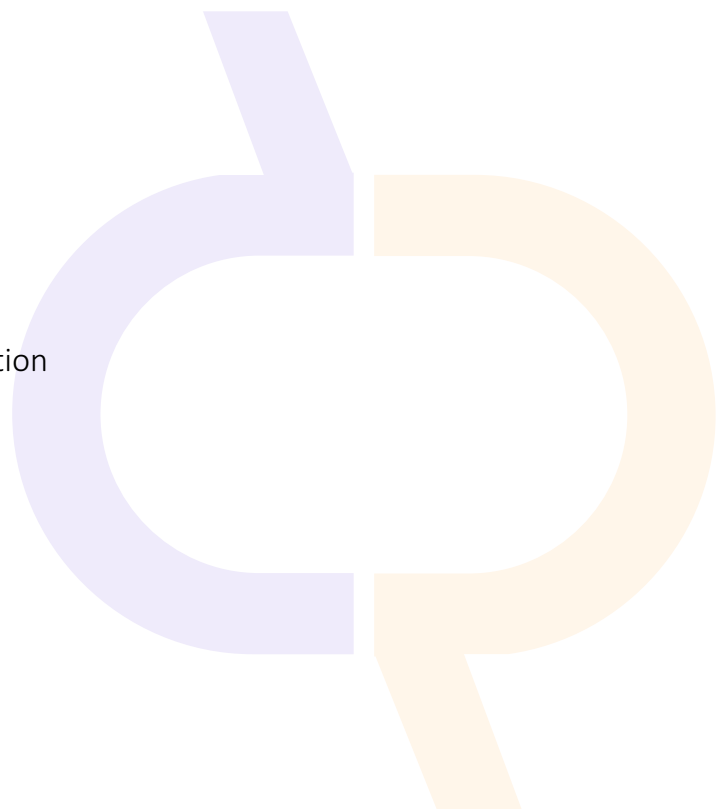
- Network Protocol Security Management
- Network Components Security
- Communication Channel Security
- Network Attack Mitigation

Module 5: Identity and Access Management

- Physical and Logical Access Control
- Concept of Identification, Authentication, and Authorization
- Identity as a Service
- Authorization Procedures
- Access Control Attack Checks

Module 6: Security Assessment and Testing

- Auditing
- System Security Control Testing



- Software Security Control Testing
- Collection of Security Process Data

Module 7: Security Operations

- Security Operations Methods
- Physical Security Concepts
- Personnel Security
- Logging and Monitoring
- Steps in Prevention
- Resource Provisioning and Protection
- Patch and Vulnerability Management
- Change Management
- Incident Response
- Investigations
- Planning of Disaster Recovery
- Strategies in Disaster Recovery
- Implementation of Disaster Recovery

Module 8: Software Development Security

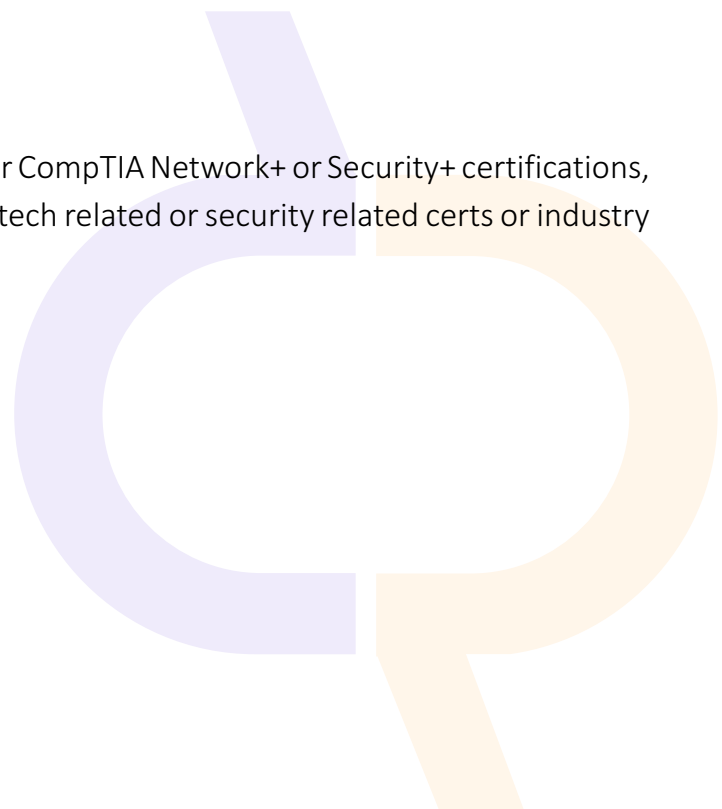
- Security Principles in the System Lifecycle
- Security Principles in the Software Development Lifecycle
- Database Security in Software Development
- Development Setup Security Controls
- Software Security Effectiveness Assessment

Prerequisite

Participants who have certification or training proof in either CompTIA Network+ or Security+ certifications, or any other equivalent cognate industry experience. Also, tech related or security related certs or industry experience will be an added advantage.

Certifications or training proofs in areas like the following:

Red Hat Certified Engineer (RHCE)
Linux Foundation Certified Engineer (LFCE)
Systems Security Certified Practitioner (SSCP)
Cisco Certified Network Professional (CCNP)
CyberSec First Responder (CFR)
Microsoft Certified Solutions Expert (MCSE)
Certified Information Security Manager (CISM)



Certified Information Systems Auditor (CISA) and other relevant certifications / trainings.

Target Audience:

Suited but not limited to IT professionals looking to boost their expertise and gain validation in information system security niche.

Professionals like network or security analysts and engineers, network administrators, information security specialists, and risk management professionals are suitable candidates for the CISSP training and certification. Also, seasoned IT security-related practitioners, auditors, consultants, investigators and so on. Additional requirements include a minimum of five years of direct professional work experience in two or more fields related to the eight CBK security domains, or a university degree and some years of experience.

Course Duration:

95 Training Hours

Deliverables:

Instructional Training Manuals for the Complete Domains
Self Assessment Exam Demo Guides

Certificates Issued:

Upon completion, participants would be issued a certificate of completion in addition to meeting the exam preparation requirements to qualify to sit for the CISSP certification exam.

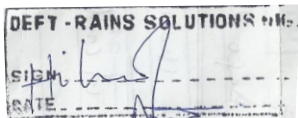
Course Fees:

N350,000.00

CONCLUSION

We hope this meets your satisfaction. If keen, avail us of your proposed start date so we could factor into our training calender and deliberate on a more convenient time for both parties.

Regards and Thanks.



Hilary Okoye
Client Relations/Operations

