AFRICAN ADVANCED LEVEL TELECOMMUNICATIONS INSTITUTE (AFRALTI)

TRAINING WORKSHOP OUTLINE

Title:	Certified Information Systems Security Professional (CISSP)
Duration:	5 days
Location:	AFRALTI

Course Description:

In an increasingly complex cyber world, there is a growing need for information security leaders who possess the breadth and depth of expertise necessary to establish holistic security programs that assure the protection of organizations' information assets. That's where the Certified Information Systems Security Professional (CISSP®) comes in.

The CISSP certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to build and maintain security programs to protecting organizations from growing sophisticated attacks. The CISSP draws from a comprehensive, up-to-date, global common body of knowledge that ensures security leaders have a deep knowledge and understanding of new threats, technologies, regulations, standards, and practices.

Backed by (ISC)2®, the globally recognized, not-for-profit organization dedicated to advancing the information security field, the CISSP was the first credential in the field of information security to meet the stringent requirements of ISO/ IEC Standard 17024. Not only is the CISSP an objective measure of excellence, but also a globally recognized standard of achievement.

Target Audience and Perquisites:

Security Consultant, Security Analyst, Security Manager o Security Systems Engineer, IT Director/Manager o Chief Information Security Officer, Security Auditor, Director of Security, Security Architect, Network Architect

Expected Outcomes:

Upon completion of this course, participants will have a deep understanding of the following CISSP knowledge domains:

- Security and Risk Management (Security, Risk, Compliance, Law, Regulations, and Business Continuity)
- Asset Security (Protecting Security of Assets)
- Security Engineering (Engineering and Management of Security)
- Communication and Network Security (Designing and Protecting Network Security)

- Identity and Access Management (Controlling Access and Managing Identity)
- Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)
- Security Operations (Foundational Concepts, Investigations, Incident Management, and Disaster Recovery)
- Software Development Security (Understanding, Applying, and Enforcing Software Security)

Why CISSP

The CISSP Helps You:

- Validate your proven competence gained through years of experience in information security.
- Demonstrate your technical knowledge, skills, and abilities to effectively develop a holistic security program set against globally accepted standards.
- Differentiate yourself from other candidates for desirable job openings in the fast-growing information security market.
- Affirm your commitment to the field and ongoing relevancy through continuing professional education and understanding of the most current best practices.
- Gain access to valuable career resources, such as networking and ideas exchange with peers.

The CISSP Helps Employers:

- Protect against threats with qualified professionals who have the expertise to competently design, build, and maintain a secure business environment.
- Ensure professionals stay current on emerging threats, technologies, regulations, standards, and practices through the continuing professional education requirements.
- Increase confidence that candidates are qualified and committed to information security.
- Ensure employees use a universal language, circumventing ambiguity with industry-accepted terms and practices.
- Increase organizations' credibility when working with clients and vendors.

CISSP Training at AFRALTI:

CISSP training at AFRALTI is unique, the programme entails instructor-led training covering both theory and practical lessons. The Instructors are not only CISSP certified but are also Certified Ethical Hackers.

Although the CISSP curriculum does not cover the security testing and hacking labs, our training has been enriched with lab exercises. Students will be provided with security related resources and all tools required to perform security testing to enhance their understanding of security principles and their appreciation of the security matters..

Training Contents

Domain 1: Security and Risk Management (Security, Risk, Compliance, Law, Regulations, and Business Continuity)

- Confidentiality, integrity, and availability concepts
- Security governance principles

- Compliance
- Legal and regulatory issues
- Professional ethics
- Security policies, standards, procedures and guidelines
- Business continuity requirements
- Personnel security policies
- Risk management concepts
- Threat modeling
- Risk considerations
- Security education, training, and awareness

Domain 2: Asset Security (Protecting Security of Assets)

- Ownership (e.g. data owners, system owners)
- Protect privacy
- Appropriate retention
- Data security controls
- Handling requirements (e.g. markings, labels, storage)

Domain 3: Security Engineering (Engineering and Management of Security)

- Engineering processes using secure design principles
- Security models fundamental concepts
- Security evaluation models
- Security capabilities of information systems
- Security architectures, designs, and solution elements vulnerabilities
- Web-based systems vulnerabilities
- Mobile systems vulnerabilities
- Embedded devices and cyber-physical systems vulnerabilities
- Cryptography
- Site and facility design secure principles
- Physical security

Domain 4: Communication and Network Security (Designing and Protecting Network Security)

- Secure network architecture design (e.g. IP & non-IP protocols, segmentation)
- Secure network components
- Secure communication channels
- Network attacks

Domain 5: Identity and Access Management (Controlling Access and Managing Identity)

- Physical and logical assets control
- Identification and authentication of people and devices
- Identity as a service (e.g. cloud identity)
- Third-party identity services (e.g. on-premise)
- Access control attacks
- Identity and access provisioning lifecycle (e.g. provisioning review)

Domain 6: Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)

- Assessment and test strategies
- Security process data (e.g. management and operational controls)

- Security control testing
- Test outputs (e.g. automated, manual)
- Security architectures vulnerabilities

Domain 7: Security Operations (Foundational Concepts, Investigations, Incident Management, and Disaster Recovery)

- Investigations support and requirements
- Logging and monitoring activities
- Provisioning of resources
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns

Domain 8: Software Development Security (Understanding, Applying, and Enforcing Software Security)

- Security in the software development lifecycle
- Development environment security controls
- Software security effectiveness
- Acquired software security impact

Lab Activities

This training will be interspersed with the following lab activities to give the learner a practical experience of risk in the cyber space.

1. Footprinting and countermeasures
2. Network scanning techniques
3. Enumeration techniques
4. System hacking methodology and steganalysis attacks
5. Malware attacks
6. Packet sniffing techniques
7. Social Engineering techniques
8. Webserver and web application attacks
9. Wireless hacking
10. Mobile platform attack
11. Cryptography Attacks

For more information, please contact us on
Tel: +254 020 4440633 +254 710 207 061, +254 733 444 421
info@afralti.org
www.afralti.org