Certified Cyber Security Associate (CCSA)

The set of modules in this training Programme gives a strong foundation for the assurance of dependable and security-intensive systems. This certification provides a credential of a learner's mastery of critical security fundamentals.

Module Number	Module Outline	Remarks
1	**Appraising the Security of Systems** • Introduction to Cyber Security • Information security concept • Security triad: Confidential, Integrity, Availability • Focus of control • Security threats and attacks • Cyber terrorism • Cyber deterrence • Good Security management Practice • ICT Governance	
2	**System Security Procedure** • Authentication and access control • Identification • Authentication by passwords • Protecting passwords • Access control structures	
3	**Holistic Information Security Audit** • security labeling • security auditing • security policy • ISO 2700 Guidelines • safeguards and countermeasures • risk mitigation • covert channels	

4	**Ethical Hacking Concepts** • Legal and Ethical Considerations • Potential attacks • Buffer Overflows • Reconnaissance • Footprinting • Session Hijacking • Web Server Attacks • Database Attacks • Password Cracking • Network Devices & Attacks • Trojans and Backdoor Applications • OS Specific Attacks • Denial of Service Attacks • Creating and Implementing a Test Plan • SQL Injection • Phishing	
5	**Network Scanning** • Network security controls • Common mitigation methods • Security Handshake pitfalls, • IP security and Web security considerations • Secure Socket Layer and Transport Layer • Security – Secure electronic transaction • e-mail security • Store and forward Authentication • Source Message Integrity • Proof of submission and delivery • Multipurpose Internet Mail Extension • Firewall design and configurations	
6	**Server Security** • verification of security properties • operating system security • trust management • multi-level security	

7	**Wireless System Security** • Unique vulnerabilities of wireless systems • system security issues in the context of wireless systems, including satellite, terrestrial microwave, military tactical communications, public safety, cellular and wireless LAN networks; • Control of fraudulent usage of networks. • Jamming, interception and means to avoid them.	
8	**Intrusion Detection** • Passive and reactive systems • Network intrusion detection system • Protocol-based intrusion detection system • Evasion techniques • Intrusion prevention system	
9	**Penetration Testing** • Testing Principles • Injection • Cross-site Scripting (XSS) • Bruteforcing • Broken Authentication and Session Management • Security Misconfiguration • Insecure Cryptographic Storage • URL Access Restriction Failure • Transport layer protection loopholes • Unvalidated Redirects and Forwards • Google hacking • Pdf and image files hacking	

10	**Cryptography** • block and stream ciphers • public-key system • key management • Certificates signature • public-key infrastructure (PKI) • digital signatures • non-repudiation and message authentication • security standards and protocols such as DES, AES, PGP, and Kerberos • Cryptographic mechanisms • Encryption • authentication protocols • digital rights management • security protocols for wired, wireless and distributed networks • payment and micropayment protocols • anonymity • broadcast encryption and traitor tracing • quantum cryptography, and visual cryptography	
11	**Social Engineering Designs** • Cellular and wireless LAN networks • Confidentiality, privacy, integrity and availability • Control of fraudulent usage of networks. • Jamming, interception and means to avoid them • Public safety • Case studies examples	
12	**Digital Forensics** • Introduction to Digital Forensics • Forensic Software and Hardware • Analysis and Advanced Tools • Forensic Technology and Practices • Forensic Ballistics and Photography • Face, Iris and Fingerprint Recognition • Audio Video Analysis • Windows System Forensics • Linux System Forensics • Network Forensics	

13	**Cyber Law and Policy** • Substantive legal principles relating to information security Balancing information and civil liberties. Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basic Legal Policies. • Digital laws and legislation, Law Enforcement Roles and Responses • Cyber Crime Issues: Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, • Cyber Crime Investigation: Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidence, Password Cracking • Policy approaches: ITU, Africa Union	
14	**Disaster Recovery Planning** • Testing the ability of network defenders to successfully detect and respond to attacks • Providing evidence to support increased security investments	
15	**Business Continuity Management** • Tabletop test • Documentation errors and missing information Simulation tests • Recovery sites and backup systems • Specialized services	