2025/2026 TRAINING PROGRAM DETAILS

1. INFOSEC CERTIFIED CYBER SECURITY SPECIALIST (CCSS)

Course overview:

A comprehensive foundational program for professionals transitioning into cybersecurity or consolidating their existing knowledge. The curriculum covers network security, incident response, digital forensics, security architecture, and compliance frameworks. Participants gain practical skills and strategic understanding, earning industry-recognized credentials while preparing to operate effectively within modern organizational cybersecurity environments.

DAY	TRAINING DETAILS
1	**Cyber Security and Network Security Fundamentals** • **Introduction to Cybersecurity**: Principles of confidentiality, integrity, availability (CIA triad). • Concepts of network security, including firewalls, VPNs, IDS/IPS, and network segmentation **Cyber Security Architure:** • Models for Business profiling • Securing product and Services • Security in Suplier and Thirdparty environments **Hands-on Lab**: Group discussion on Defense in Depth Security Controls.
2	**Cyber Security Risk Management:** • Identifying, analysing, evaluating, and addressing organisation's Cyber Security threats • Risk Management Frameworks • Cyber Risk Insurance **Compliance and Governance:** • Understanding regulatory requirements (ISO/IEC 27001:2022, NIST CSF, CIS Controls) and how to implement governance frameworks to ensure compliance Hands-on Lab: Develop Risk Register and Guidance on creation of Information Security Policies, standards and guidelines

DAY	TRAINING DETAILS
3	**Cyber Security Prevent** • **Infrastructure Security:** Servers, endpoints, wireless, cloud environments. • System Hardening & Patch Management: Baseline configurations, CIS Benchmarks. • Secure Authentication & Access Control: MFA, IAM, PAM basics. **Hands-on Lab:** Configure enterprise Firewalls and implement secure baseline using CIS Benchmarks **Cyber Security Defense** • Incident Response Lifecycle: Preparation, detection, containment, recovery. • Digital Forensics Basics: Chain of custody, evidence acquisition, log analysis. • SOC & SIEM Operations: Use of SIEM solution for monitoring. • Business Continuity & Disaster Recovery: Crisis management, backup planning. **Hands-on Lab:** Simulated incident response & log collection and analysis investigation (Use Wazuh/Elastic SIEM)
4	**Cyber Security Assurance** • Vulnerability Management: Scanning tools (Nessus, OpenVAS), CVSS scoring. • Penetration Testing Basics: Reconnaissance, scanning, exploitation. • Secure Application Development: OWASP Top 10 threats, SDLC security. • Practical Case Study: Reviewing insecure code snippets. **Hands-on Lab:** Run vulnerability scanning tests and formal Reporting & exploit a test system
5	**Cyber Security Strategy and Governance** • Strategy Development – Defining vision, risk management, aligning with business objectives, and Tanzania's regulatory landscape. • Policy & Oversight – Designing policies, governance structures, KPIs, compliance monitoring, and board-level reporting **Hands-on Lab:** Case studies and simulations to draft strategies and governance frameworks