

CompTIA Security+

Course outline · issued 14 September 2026

Technology areas	Cybersecurity
Level	Intermediate
Short course	5 days
One-month track	4 weeks · 16 training days · 96 contact hours
Two-month track	8 weeks · 32 training days · 192 contact hours
Delivery	In person, Virtual, Hybrid
Class size	8 to 20 participants
Certification	CompTIA Security+ exam preparation
Entry requirements	Basic networking knowledge, or CompTIA Network+.

Who it is for

ICT security, infrastructure and audit staff who protect taxpayer systems.

REVENUE USE CASE

Hardening the systems that hold taxpayer identity, assessment and payment records.

By the end, participants can

- Assess threats, vulnerabilities and attack surfaces across agency systems
- Apply identity, cryptography and access controls proportionate to the risk
- Run incident response, and support governance, risk and compliance work

Short course modules (5 days)

1. Threats, attacks and vulnerabilities
2. Architecture and design
3. Identity and access management
4. Cryptography and PKI
5. Operations, incident response and exam preparation

One-month track — weeks 1 to 4

4 weeks · 16 training days · 96 contact hours

Week 1 — Threats, attacks and vulnerabilities

- Threat actors and their motivation
- Attack types across the estate
- Vulnerability scanning and interpreting results
- Threat intelligence and its practical use

Practical: Run and interpret a vulnerability scan on a lab environment.

Week 2 — Architecture and design

- Secure network and system architecture
- Segmentation, zero trust and defence in depth
- Cloud and virtualisation security
- Resilience, backup and recovery design

Practical: Redesign a flat lab network into secured zones.

Week 3 — Identity and access management

- Authentication, authorisation and accounting
- Multi-factor authentication and federation
- Privileged access and least privilege
- Account lifecycle and access review

Practical: Implement and test a least-privilege access model.

Week 4 — Cryptography and PKI

- Symmetric, asymmetric and hashing in practice
- Certificates, PKI and trust chains
- Transport and storage encryption
- Key management and what goes wrong

Practical: Issue, deploy and validate certificates in the lab.

Checkpoint: the one-month track is assessed [here](#).

Two-month track — continues through weeks 5 to 8

8 weeks · 32 training days · 192 contact hours

Week 5 — Operations and monitoring

- Logging, SIEM and detection engineering
- Hardening baselines and configuration management
- Endpoint, email and web controls
- Penetration testing and red teaming in outline

Practical: Build a detection rule and prove it fires on a simulated attack.

Week 6 — Incident response and forensics

- The incident response lifecycle
- Evidence handling and preservation
- Containment, eradication and recovery decisions
- Post-incident review and reporting

Practical: Run a full incident response exercise on a compromised host.

Week 7 — Governance, risk and compliance

- Risk assessment and treatment
- Policies, standards and frameworks
- The Nigeria Data Protection Act and taxpayer data
- Audit, evidence and third-party risk

Practical: Produce the security assessment and remediation plan.

Week 8 — Examination preparation and capstone

- Full syllabus review and gap analysis
- Performance-based question technique
- Full mock examination under timed conditions
- Presenting the remediation plan and booking the exam

Practical: Sit a full mock Security+ paper and present the remediation plan.

Capstone assessment and post-course evaluation.

Capstone

A security assessment and remediation plan for one agency system, plus a full mock Security+ paper sat under examination conditions.

About this outline

Indicative extended tracks. The one-month track runs weeks 1 to 4; the two-month track continues through week 8 with deeper labs, certification preparation and a capstone. Weeks, contact hours and cohort sizes are finalised with each client.

Prepared by	Dividend Consulting Nigeria Limited
RC number	463831
Contact	0806 022 0612 · imudiagra@gmail.com
