Course Name	**CompTIA Security+**
Course Code	**SY0-601**
Course Duration	5 Days
Course Structure	Instructor-Led
Course Overview	This course maps to the CompTIA Security+ certification exam (SY0-601) and establishes the core knowledge required of any cybersecurity role, as well as providing a springboard to intermediate-level cybersecurity jobs. This course emphasizes both the practical and hands-on ability to identify and address security threats, attacks and vulnerabilities. CompTIA Security+ is a globally trusted, vendor-neutral certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career. CompTIA Security+ is also a DoD Approved 8570 Baseline Certification and this course meets DoD 8140/8570 Training requirements
Audience Profile	This course is designed for information technology (IT) professionals who have networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks; familiarity with other operating systems, such as macOS®, Unix®, or Linux®; and who want to further a career in IT by acquiring foundational knowledge of security Lessons or using CompTIA Security+ as the foundation for advanced security certifications or career roles. This course is also designed for students who are seeking the CompTIA Security+ certification and who want to prepare for the CompTIA Security+ SY0-601 Certification Exam.
Course Prerequisites	Before attending this course, students must have: • CompTIA A+ and CompTIA Network+
Course Outcome	After completing this course, students will be able to: • Prepare for the CompTIA Security+ exam • Confidently explain and define an array of security vulnerabilities • Navigate the complexities of secure system and network design • Explore the defensive measures like PKI, firewalls and IDS • Implement robust identity management and access control

Assessment/Evaluation	This course will prepare delegates to take the exam: SY0-601 CompTIA Security+ Successfully passing this exam will result in the attainment of the CompTIA Security+ Certification and Certificate of Attendance issued by IT-IQ Botswana

Course Details	
Lesson	**TOPIC 1: COMPARING SECURITY ROLES AND CONTROLS** Lesson 1A: Compare and Contrast Information Security Roles Lesson 1B: Compare and Contrast Security Control and Framework Types **TOPIC 2: EXPLAINING THREAT ACTORS AND THREAT INTELLIGENCE** Lesson 2A: Explain Threat Actor Types and Attack Vectors **TOPIC 3: PERFORMING SECURITY ASSESSMENTS** Lesson 3A: Assess Organizational Security with Network Reconnaissance Tools Lesson 3B: Explain Security Concerns with General Vulnerability Types Lesson 3C: Summarize Vulnerability Scanning Techniques Lesson 3D: Explain Penetration Testing Concepts **TOPIC 4: IDENTIFYING SOCIAL ENGINEERING AND MALWARE** Lesson 4A: Compare and Contrast Social Engineering Techniques Lesson 4B: Analyze Indicators of Malware-Based Attacks **TOPIC 5: SUMMARIZING BASIC CRYPTOGRAPHIC CONCEPTS** Lesson 5A: Compare and Contrast Cryptographic Ciphers Lesson 5B: Summarize Cryptographic Modes of Operation Lesson 5C: Summarize Cryptographic Use Cases and Weaknesses Lesson 5D: Summarize Other Cryptographic Technologies

	TOPIC 6: IMPLEMENTING PUBLIC KEY INFRASTRUCTURE Lesson 6A: Implement Certificates and Certificate Authorities Lesson 6B: Implement PKI Management **TOPIC 7: IMPLEMENTING AUTHENTICATION CONTROLS** Lesson 7A: Summarize Authentication Design Concepts Lesson 7B: Implement Knowledge-Based Authentication Lesson 7C: Implement Authentication Technologies Lesson 7D: Summarize Biometrics Authentication Concepts **TOPIC 8: IMPLEMENTING IDENTITY AND ACCOUNT MANAGEMENT CONTROLS** Lesson 8A: Implement Identity and Account Types Lesson 8B: Implement Account Policies Lesson 8C: Implement Authorization Solutions Lesson 8D: Explain the Importance of Personnel Policies **TOPIC 9: IMPLEMENTING SECURE NETWORK DESIGNS** Lesson 9A: Implement Secure Network Designs Lesson 9B: Implement Secure Switching and Routing Lesson 9C: Implement Secure Wireless Infrastructure Lesson 9D: Implement Load Balancers **TOPIC 10: IMPLEMENTING NETWORK SECURITY APPLIANCES** Lesson 10A: Implement Firewalls and Proxy Servers Lesson 10B: Implement Network Security Monitoring Lesson 10C: Summarize the Use of SIEM **TOPIC 11: IMPLEMENTING SECURE NETWORK PROTOCOLS** Lesson 11A: Implement Secure Network Operations Protocols Lesson 11B: Implement Secure Application Protocols Lesson 11C: Implement Secure Remote Access Protocols

	TOPIC 12: IMPLEMENTING HOST SECURITY SOLUTIONS Lesson 12A: Implement Secure Firmware Lesson 12B: Implement Endpoint Security Lesson 12C: Explain Embedded System Security Implications **TOPIC 13: IMPLEMENTING SECURE MOBILE SOLUTIONS** Lesson 13A: Implement Mobile Device Management Lesson 13B: Implement Secure Mobile Device Connections **TOPIC 14: SUMMARIZING SECURE APPLICATION CONCEPTS** Lesson 14A: Analyze Indicators of Application Attacks Lesson 14B: Analyze Indicators of Web Application Attacks Lesson 14C: Summarize Secure Coding Practices Lesson 14D: Implement Secure Script Environments Lesson 14E: Summarize Deployment and Automation Concepts **TOPIC 15: IMPLEMENTING SECURE CLOUD SOLUTIONS** Lesson 15A: Summarize Secure Cloud and Virtualization Services Lesson 15B: Apply Cloud Security Solutions Lesson 15C: Summarize Infrastructure as Code Concepts **TOPIC 16: EXPLAINING DATA PRIVACY AND PROTECTION CONCEPTS** Lesson 16A: Explain Privacy and Data Sensitivity Concepts Lesson 16B: Explain Privacy and Data Protection Controls **TOPIC 17: PERFORMING INCIDENT RESPONSE** Lesson 17A: Summarize Incident Response Procedures Lesson 17B: Utilize Appropriate Data Sources for Incident Response Lesson 17C: Apply Mitigation Controls **TOPIC 18: EXPLAINING DIGITAL FORENSICS** Lesson 18A: Explain Key Aspects of Digital Forensics Documentation Lesson 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition

	TOPIC 19: SUMMARIZING RISK MANAGEMENT CONCEPTS Lesson 19A: Explain Risk Management Processes and Concepts **TOPIC 20: IMPLEMENTING CYBERSECURITY RESILIENCE** Lesson 20A: Implement Redundancy Strategies Lesson 20B: Implement Backup Strategies Lesson 20C: Implement Cybersecurity Resiliency Strategies **TOPIC 21: EXPLAINING PHYSICAL SECURITY** Lesson 21A: Explain the Importance of Physical Site Security Controls Lesson 21B: Explain the Importance of Physical Host Security Controls