

# CompTIA Security+: CompTIA Security+ (SY0-701)

Official Body: CompTIA | Syllabus: SY0-701 (2024-2026)

Free 10-Q Diagnostic ->

**Passing Standard: 750 on a scale of 100-900**

Format & Timing: Up to 90 questions (MCQ + performance-based). 90 minutes. (Pearson VUE)

Testing Windows: On-demand, year-round

## 1. OFFICIAL 2026 BLUEPRINT DOMAINS & WEIGHTINGS

### SEC-1: General Security Concepts

Weight: 12%

Security Control Categories (Technical, Managerial, Operational, Physical) and Types (Preventive, Detective, Corrective, Deterrent, Compensating, Directive), Fundamental Security Principles: CIA Triad, Non-Repudiation, AAA (Authentication, Authorization, Accounting), Zero Trust Architecture, and Deception/Disruption

### SEC-2: Threats, Vulnerabilities, and Mitigations

Weight: 22%

Threat Actors and Motivations: Nation-States, Unskilled Attackers, Hacktivists, Insider Threats, Shadow IT, and Organized Crime, Threat Vectors and Attack Surfaces: Phishing/Vishing/Smishing, Business Email Compromise (BEC), Supply Chain Attacks, and Social Engineering, Types of Vulnerabilities: Application

### SEC-3: Security Architecture

Weight: 18%

Architecture Models: Cloud (IaaS, PaaS, SaaS, Shared Responsibility), Serverless, Microservices, Infrastructure as Code (IaC), IoT, and ICS/SCADA, Enterprise Infrastructure Security: Network Appliances (Jump Servers, Proxy, IDS/IPS, NGFW, WAF), Port Security (802.1X), and Secure Communication (VPN, TLS, IPSec,

### SEC-4: Security Operations

Weight: 28%

Computing Resource Security Baselines, Mobile Device Management (MDM, COPE, BYOD), Wireless Security (WPA3, SAE, RADIUS), and Application Security (Sandboxing, Secure Coding), Asset Management Lifecycle: Acquisition, Assignment, Monitoring, Inventory, Enumeration, and Disposal/Decommissioning,

### SEC-5: Security Program Management and Oversight

Weight: 20%

Information Security Governance: Policies (AUP, Password, Data Retention), Standards, Procedures, Roles/Responsibilities (Owners, Controllers, Processors, Custodians), Risk Management Processes: Risk Identification, Quantitative vs. Qualitative Analysis (SLE, ARO, ALE), Risk Register, Risk Appetite/Tolerance, and

## 2. PRIMARY STATUTORY & REGULATORY AUTHORITIES TESTED

### \* NIST Cybersecurity Framework (CSF) - NIST CSF 2.0

Identify/Protect/Detect/Respond/Recover functions referenced throughout

### \* NIST SP 800-53 - NIST SP 800-53 Rev. 5

Security and privacy controls catalog

## 3. EXAMINER TRAPS & HIGH-YIELD PASS STRATEGY

Key Challenge: Broad coverage plus scenario-based questions across cryptography, architecture, and incident response.

Pass the CompTIA Security+ on your first try with VoraPrep's complete 6-pillar interactive course:

1. Full CompTIA Security+ Course ->

2. Free 10-Q Diagnostic ->

3. Score & Hours Calculator ->