ACTIVE CLEARANCE · MISSION: CERTIFICATION

FREE PREVIEW

CLEARED GOVTECH PARTNERS

CompTIA Security+ SY0-701

Exam Preparation Booklet — Free Preview

275 practice questions · full answer keys · acronym glossary
study plan · exam-day strategy · glossary quiz

Prepared for our transitioning servicemembers and veterans.
Aligned to the current SY0-701 (V7) exam objectives. · This free preview contains a sample of the full 275-question booklet.

CONTENTS

What’s in this preview

In the full booklet — not in this preview

WELCOME

The Credential the Cleared Market Asks For First.

Security+ is the baseline. For most cleared cybersecurity roles it is the credential that gets your resume past the filter — it meets the DoD 8140/8570 IAT Level II requirement and is the single most widely required cert in the cleared market. If you earn one certification on your way out of uniform, make it this one.

The exam is broad and foundational: core security concepts, the threats and mitigations you will actually defend against, secure architecture, day-to-day operations, and the governance that ties it together. None of it is exotic. All of it is the language a security team speaks every day, and the discipline you already built in service maps onto it cleanly.

We built this booklet to read the way the exam thinks. The questions ahead are scenarios — a phone is lost, a backup is restored, a checksum doesn't match — and they ask what a professional does next. That is the judgment Security+ is testing, and it is the judgment that keeps a network safe.

— The team at Cleared GovTech Partners

BEFORE YOU BEGIN

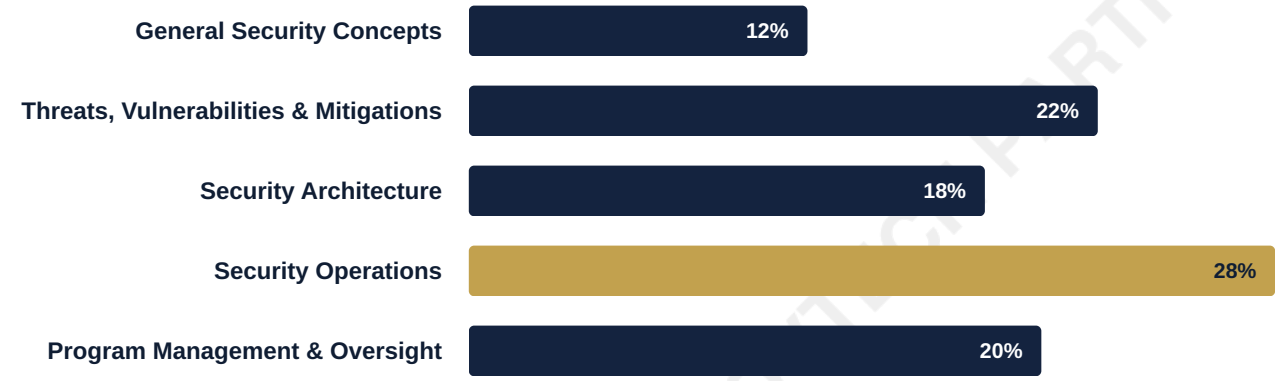
The Security+ (SY0-701) exam at a glance

Exam code	SY0-701 (CompTIA Security+)
Format	Up to 90 questions — multiple-choice and performance-based (PBQs)
Time limit	90 minutes
Passing score	750 on a scale of 100–900
Structure	Five domains — General Security Concepts (12%), Threats, Vulnerabilities & Mitigations (22%), Security Architecture (18%), Security Operations (28%), Security Program Management & Oversight (20%)
Eligibility	No required prerequisite; CompTIA Network+ and ~2 years of security or systems-administration experience are recommended
Renewal	Valid 3 years; renew with 50 CEUs (or re-take the current exam)
DoD value	DoD 8140/8570 approved — meets the IAT Level II baseline and is the most widely required credential in the cleared market.
Style	Broad and foundational — core security concepts, threats and mitigations, architecture, day-to-day operations, and governance

A note on price. A Security+ voucher runs roughly $425 in the U.S. direct from CompTIA — budget around $425, and authorized resellers often sell for less. Confirm the current cost on CompTIA's site before you pay. See the funding page near the back, because you may not have to pay it yourself. SY0-701 replaced SY0-601; this booklet targets the current SY0-701 blueprint.

The Five Domains of Security+

Security+ spreads across five domains, and the weighting tells you where to spend your time. Operations and Threats together are half the exam.



DOMAIN 1

General Security Concepts

55 practice questions · exam weight 12%

OFFICIAL EXAM OBJECTIVES FOR THIS DOMAIN

- 1.1 Compare and contrast various types of security controls
- 1.2 Summarize fundamental security concepts
- 1.3 Explain the importance of change management processes
- 1.4 Explain the importance of using appropriate cryptographic solutions

Source: CompTIA Security+ SY0-701 exam objectives. These are the official objective statements for this domain; download the complete objectives, including every sub-point, directly from CompTIA at comptia.org/certifications/security.

How this booklet helps you excel here

This is the vocabulary the rest of the exam is built on: the categories and types of security controls, the CIA triad, and the everyday concepts a practitioner reaches for first. Every question turns an abstract term into a real decision — which is exactly how the exam tests it.

Sample of 5 questions from this domain. The full booklet contains all 275.

1. A logistics company is rolling out a BYOD program so employees can check email on personal phones. Leadership wants to guarantee corporate data is protected if a phone is lost, but employees are worried the company will erase their personal photos and messages. Which approach BEST satisfies both concerns?

A. Enable remote wipe of the entire device through MDM
B. Require a 4-digit PIN to unlock the phone
C. Enforce full-disk encryption on enrolled devices through MDM and containerize corporate data
D. Perform a factory reset before installing corporate apps

2. A new CISO discovers the organization has no formal process for evaluating risk before adopting new technology. She introduces a written risk-assessment policy and an annual review cycle. These additions are an example of which control category?

A. Technical
B. Managerial
C. Physical
D. Operational

3. After several after-hours break-in attempts at a warehouse, the security manager installs bright floodlights and prominent ‘Area Under Video Surveillance’ signs at every entrance. The primary intent of these measures is to:

A. Restore systems after an incident

B. Discourage intruders from attempting entry in the first place

C. Provide an alternative when a primary control fails

D. Encrypt footage stored on the recorder

4. A hospital is hit with ransomware that encrypts patient scheduling data. The IT team wipes the affected servers and restores the data from the previous night’s clean backups to resume operations. Restoring from backup is BEST classified as which type of control?

A. Preventive

B. Deterrent

C. Corrective

D. Detective

5. A company policy requires badge readers on a sensitive lab, but the new biometric readers are on backorder for two months. To maintain protection in the interim, management stations a guard at the door to check IDs. The guard is functioning as which kind of control?

A. Directive

B. Detective

C. Compensating

D. Preventive

Reference

Answer Keys & Explanations

Detailed rationale for every question in the full booklet

DOMAIN 1 — ANSWER KEY

General Security Concepts

1. Correct answer: C — Enforce full-disk encryption on enrolled devices through MDM and containerize corporate data.

Mobile Device Management (MDM) is centrally managed software that lets an organization enforce security policy on phones and tablets, whether company-owned or personally owned under a BYOD program. In a BYOD scenario the core tension is ownership: the company needs to protect its data, but it has no claim on the employee's personal photos, messages, or apps, so the right control has to draw a clean line between the two.

Full-disk encryption (FDE) scrambles everything stored on the device so a lost or stolen phone is useless without the key, protecting corporate data at rest. Pairing FDE with containerization — which isolates corporate email and files inside a separate managed container — lets the company encrypt, control, and selectively wipe only the work container while never touching the employee's personal space.

2. Correct answer: B — Managerial.

Security controls are grouped by how they work. Managerial (also called administrative) controls direct how the security program is run through policy, governance, and risk decisions rather than through technology or physical barriers. A written risk-assessment policy and an annual review cycle are governance mechanisms that tell the organization how to evaluate risk, which makes them managerial by definition.

3. Correct answer: B — Discourage intruders from attempting entry in the first place.

Controls are also classified by the function they serve. A deterrent control aims to discourage an attacker from acting at all by making the attempt seem risky or not worth it. Bright floodlights and visible "Area Under Video Surveillance" signage do not physically stop anyone — they influence the would-be intruder's decision before any action is taken, which is the textbook purpose of a deterrent.

4. Correct answer: C — Corrective.

A corrective control acts after an incident has occurred to repair the damage and return operations to normal. Restoring encrypted data from a known-good backup is a classic corrective action: the harm has already happened, and the control's job is recovery.

5. Correct answer: C — Compensating.

A compensating control is an alternative measure put in place temporarily when the intended control cannot yet be implemented, providing equivalent protection in the interim. The biometric readers are on backorder, so the stationed

guard fills the gap until the real control is available — that “stand-in for a missing control” role is precisely what compensating means.

YOU'VE SEEN THE SAMPLE

Unlock the full Security+ booklet

This preview is a taste. The complete 275-question booklet takes you through every domain with the same scenario-driven questions and plain-language explanations — built to match how the real SY0-701 exam thinks.

- ✓ All 275 scenario questions across every domain
- ✓ Full answer keys with exam cues for every question
- ✓ 8-week study schedule & recommended resources
- ✓ Career roadmap, acronym glossary & glossary quiz
- ✓ Exam-day quick reference & funding guide

You may not have to pay for this yourself.

Transitioning servicemembers and veterans can often fund the exam fee and training through Credentialing Assistance (Army CA / COOL), the GI Bill, or VET TEC. The full booklet includes a step-by-step funding guide. Ask us how to get your voucher covered before you pay out of pocket.