General Security Concepts

CompTIA Security+ certification exam, SY0-801 (V8)

16% of the exam · 3 exam objectives · SY0-801

Domain 1 is the vocabulary of security: the goals controls serve, how controls are grouped and what they do, how change management keeps changes from creating risk, and how to choose the right cryptography for each need.

You should be able to: A system cannot use multifactor authentication, so the team adds extra log review for it. What control type is the log review, and which change management element would record how to undo the change if it failed?

Every exam objective: the key point and the trap

1.1 Explain security concepts and controls.

Defense in depth layers controls so that one failure does not expose an asset. The core goals those controls serve are confidentiality (only the right people read data), integrity (data is not changed without authorization) and availability (systems work when needed): CIA.

Trap: Mixing up category and type, for example calling a security guard detective when the question asks for the category (operational), or calling a fence physical when it asks for the type (preventive or deterring).

1.2 Given a scenario, demonstrate the impact of change management processes on security.

The change advisory board (CAB) runs the approval process. A change needs a named owner who is accountable and identified stakeholders who are affected.

Trap: Treating backout planning and failing forward as the same thing: backout reverts to the earlier state, failing forward applies a new fix to the changed state.

1.3 Explain the importance of using appropriate cryptographic solutions.

Public key infrastructure (PKI) binds public keys to identities. The private key stays with its owner; the public key is shared. Key escrow keeps copies of keys with a trusted party for recovery.

Trap: Confusing which key signs and which key encrypts: you sign with your own private key, and you encrypt for someone with their public key.

Key terms

CIA: Confidentiality, Integrity, and Availability

AAA: Authentication, Authorization, and Accounting

CAB: Change Advisory Board

SOP: Standard Operating Procedure

PKI: Public Key Infrastructure

CSR: Certificate Signing Request

CRL: Certificate Revocation List

OCSP: Online Certificate Status Protocol

TLS: Transport Layer Security

IPSec: Internet Protocol Security

ExamDragon, examdragon.com/secplus. Independent exam preparation, not affiliated with or endorsed by CompTIA; written in our own words to the SY0-801 exam objectives. CompTIA and Security+ are trademarks of CompTIA, Inc.