Security Program Management and Oversight

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

14% of the exam · 6 exam objectives · SY0-801

Domain 5 is about running a security programme: the documents that govern it, how risk is identified, analyzed and treated, how vendors are chosen and watched, what compliance requires, how audits and tests are done, and how staff are trained. Expect judgement questions that ask which document, agreement, treatment or test fits a situation, and short risk calculations.

You should be able to: A $10,000 asset would lose 40% of its value in an incident expected twice a year. What are the SLE and the ALE?

Every exam objective: the key point and the trap

5.1 Explain the importance of governance, risk, and compliance artifacts.

Guidelines are advisory: benchmarks, advisories, implementation guides and reference architectures recommend how to do something.

Trap: Treating a benchmark or reference architecture as mandatory. They are guidelines until the organization adopts them into a baseline or standard.

5.2 Explain the impact of risk management processes on the security of the organization.

Risk identification starts with asset identification and gives each risk a stakeholder owner.

Trap: Confusing SLE with ALE, or entering the years between events as the ARO instead of its reciprocal.

5.3 Explain the assessment and management processes associated with third-party risk.

Vendor selection uses an RFI to explore the market, an RFQ for prices, an RFP for full proposals, and an EOI to gauge interest, with due diligence and conflict of interest checks.

Trap: Choosing an SLO when the question asks for a commitment with consequences. The SLA is the agreement; the SLO is only the target.

5.4 Summarize elements of effective security compliance.

Compliance training covers data handling, AML/CTF and anti-bribery.

Trap: Mixing up attestation and acknowledgement. Staff acknowledge a policy; management or an assessor attests that controls comply.

5.5 Explain concepts associated with audit and assessment activities.

Data gathering uses sampling, questionnaires and surveys, interviews, testing assertions, and reference sources such as MITRE ATT&CK, the Cyber Kill Chain and the Diamond Model of Intrusion Analysis.

Trap: Confusing benchmarking with a gap analysis. Benchmarking compares with peers; a gap analysis compares with a required standard.

5.6 Given a scenario, apply security awareness concepts to improve organizational security.

Training types are initial or onboarding, ongoing, targeted (for high-risk roles) and corrective (after a failure).

Trap: Measuring completion only. A course completed by everyone proves nothing unless behavior metrics improve.

Key terms

ALE: Annualized Loss Expectancy

ARO: Annualized Rate of Occurrence

SLE: Single Loss Expectancy

AUP: Acceptable Use Policy

SOP: Standard Operating Procedure

RFP: Request for Proposal

MOU: Memorandum of Understanding

SOW: Statement of Work

AML/CTF: Anti-money Laundering/Counter-terrorism Financing

LMS: Learning Management System

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.