CompTIA Security+ Exam SY0-701

Lesson 1

Summarizing Fundamental Security Concepts

Objectives

- Summarize information security concepts
- Compare and contrast security control types
- Describe security roles and responsibilities

Lesson 1

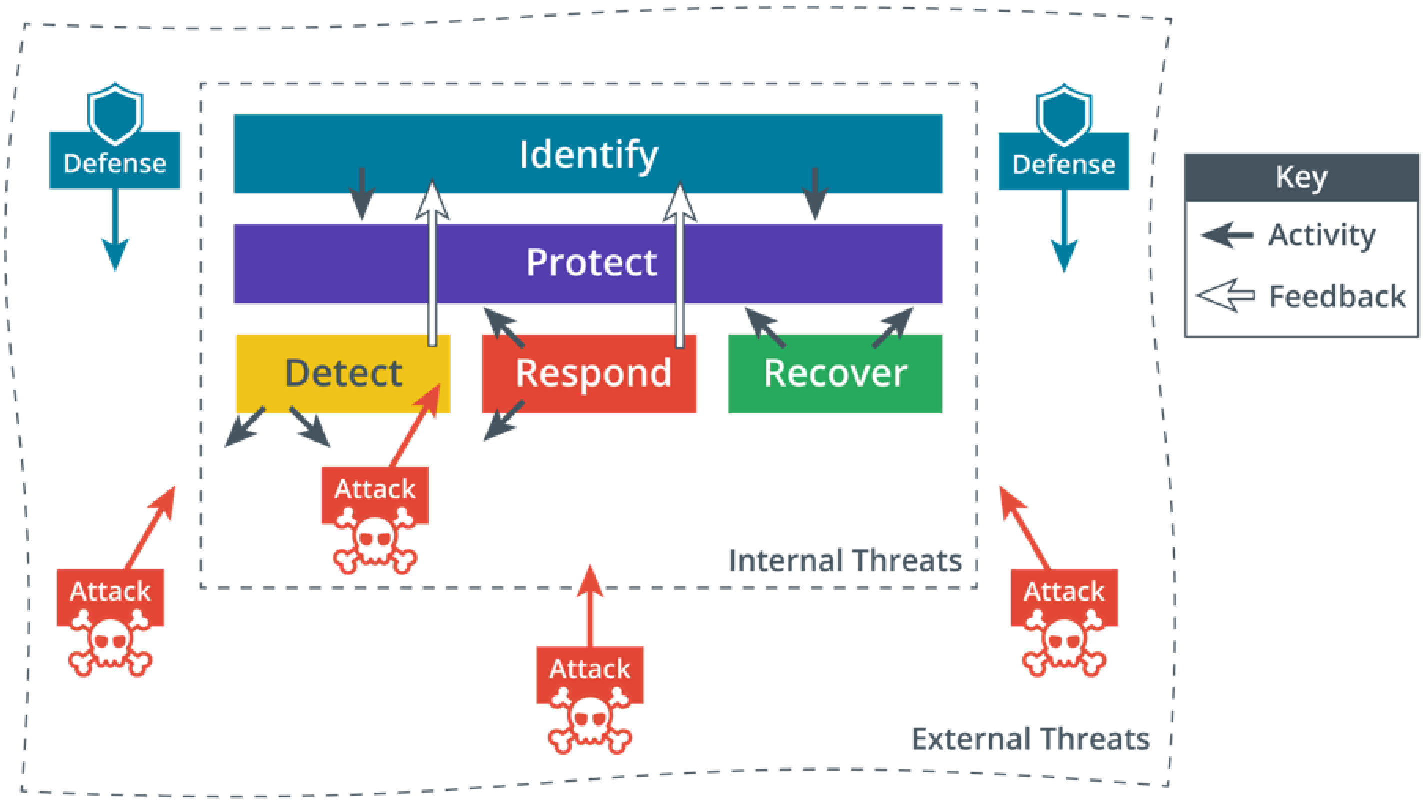
Topic 1A

Security Concepts

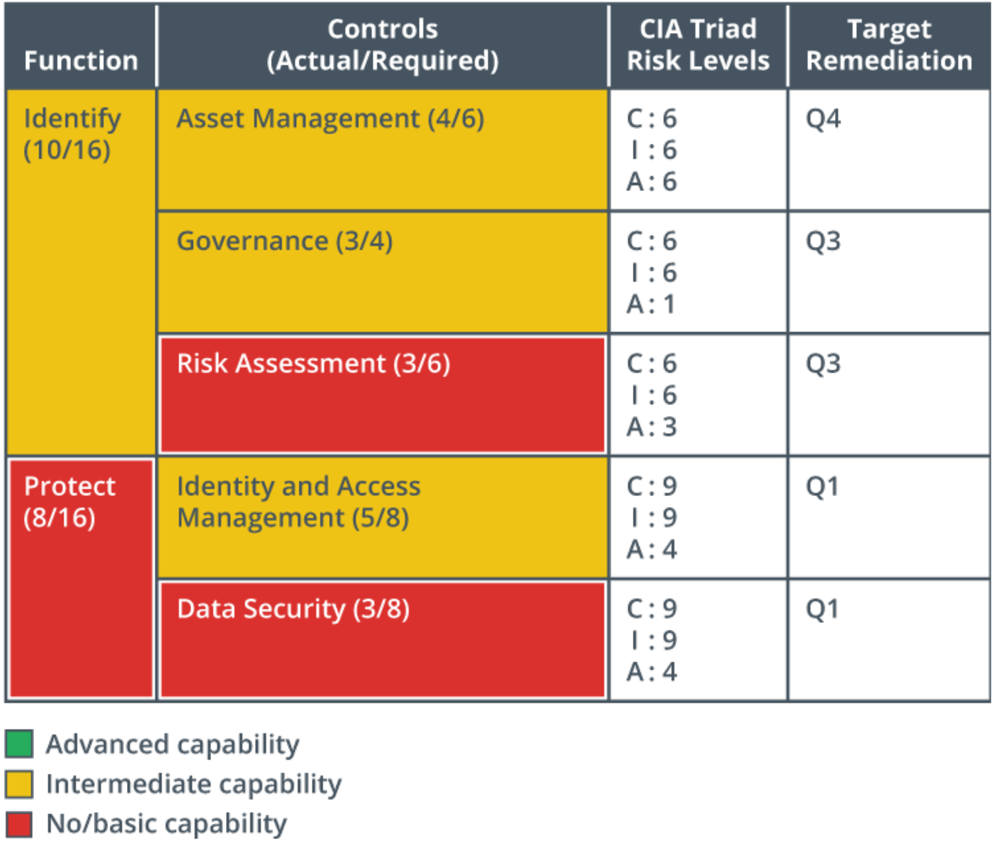
Information Security

- Confidentiality
  - Information should only be read by authorized persons
- Integrity
  - Data is stored and transferred as intended and any modification is authorized
- Availability
  - Information is accessible to those authorized to view or modify it
- Non-repudiation
  - Persons cannot deny creating or modifying data

Cybersecurity Framework



Gap Analysis



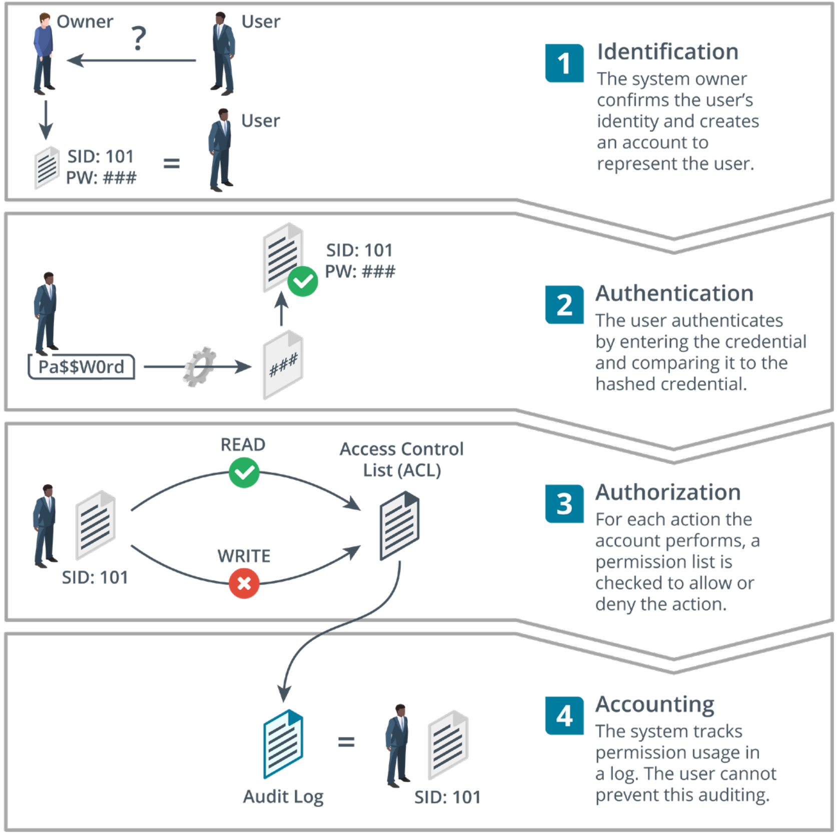
Function	Controls (Actual/Required)	CIA Triad Risk Levels	Target Remediation
🟨 Identify (10/16)	🟨 Asset Management (4/6)	C : 6 I : 6 A : 6	Q4
	🟨 Governance (3/4)	C : 6 I : 6 A : 1	Q3
	🟥 Risk Assessment (3/6)	C : 6 I : 6 A : 3	Q3
🟥 Protect (8/16)	🟨 Identity and Access Management (5/8)	C : 9 I : 9 A : 4	Q1
	🟥 Data Security (3/8)	C : 9 I : 9 A : 4	Q1

🟩 Advanced capability

🟨 Intermediate capability

🟥 No/basic capability

Access Control



1 Identification

The system owner confirms the user's identity and creates an account to represent the user.

2 Authentication

The user authenticates by entering the credential and comparing it to the hashed credential.

3 Authorization

For each action the account performs, a permission list is checked to allow or deny the action.

4 Accounting

The system tracks permission usage in a log. The user cannot prevent this auditing.

Review Activity: Security Concepts

- Information security
  - CIA triad
- Cybersecurity framework
- Gap analysis
- Access control
  - IAM and AAA

Lab Activity

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Perform System Configuration Gap Analysis

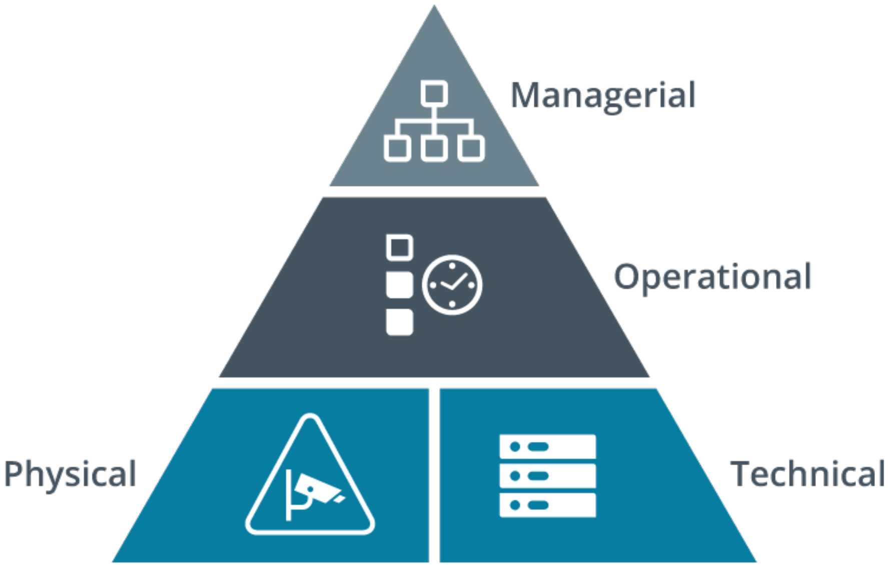
Lesson 1

Topic 1B

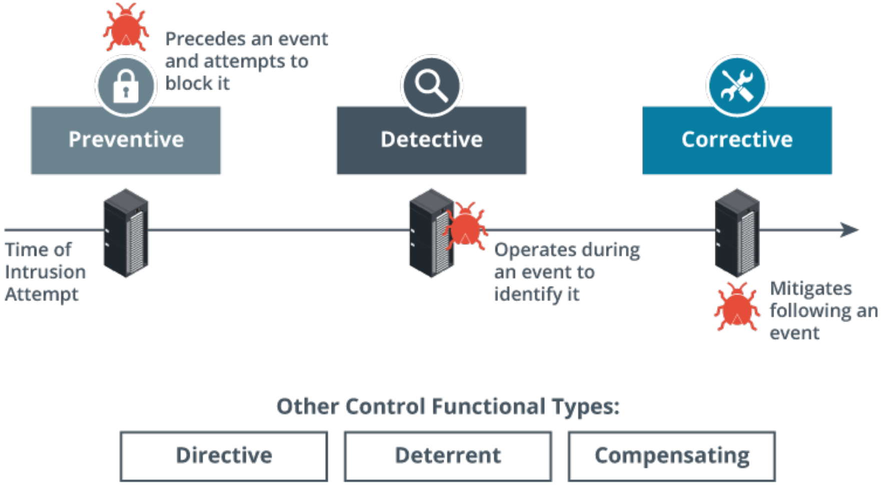
Security Controls

Security Control Categories

- Managerial
  - Give oversight of system
- Operational
  - Relies on a person for implementation
- Technical
  - Implemented in operating systems, software, and security appliances
- Physical
  - Devices that mediate access to premises and hardware



Security Control Functional Types (1)



Precedes an event and attempts to block it
Preventive
Detective
Corrective
Time of Intrusion Attempt
Operates during an event to identify it
Mitigates following an event
Other Control Functional Types:
Directive
Deterrent
Compensating

Images © 123rf.com.

- Preventive
  - Physically or logically restricts unauthorized access
  - Operates before an attack
- Detective
  - Identifies attempted or successful intrusions
  - Operates during an attack
- Corrective
  - Responds to and fixes an incident and may prevent its reoccurrence
  - Operates after an attack

Security Control Functional Types (2)

- Directive
  - Enforces a rule of behavior
- Deterrent
  - Psychologically discourages intrusions
- Compensating
  - Substitutes for a principal control
  - Associated with framework compliance measures

Information Security Roles and Responsibilities

Image credit: Shannon Fagan © 123rf.com.

- Overall responsibility
  - Chief Information Officer (CIO)
  - Chief Security Officer (CSO)
- Managerial
- Technical
  - Information Systems Security Officer (ISSO)
- Non-technical
- Due care/liability

Information Security Competencies

- Risk assessments and testing
- Specifying, sourcing, installing, and configuring secure devices and software
- Access control and user privileges
- Auditing logs and events
- Incident response and reporting
- Business continuity and disaster recovery
- Security training and education programs

Information Security Business Units

- Security Operations Center (SOC)
- DevSecOps
  - Development, security, and operations
- Incident response
  - Cyber incident response team (CIRT)

Image © gorodenkoff 123RF.com

Review Activity: Security Controls

- Security control categories
  - Managerial, operational, technical, physical
- Security control functional types
  - Preventive, detective, corrective plus directive, deterrent, compensating
- Information security roles and responsibilities
- Information security competencies
- Information security business units
  - SOC, DevSecOps, and CIRT

Lab Activity

- Assisted Lab: Configuring Examples of Security Control Types

CompTIA Security+ Exam SY0-701

Lesson 1

Summary