



# SEC+

## Lesson 14:

# Summarize Security Governance Concepts

Lesson 14

# Topic 14A

Policies, Standards,  
and Procedures



# Policies

- Vital in establishing effective governance and ensuring organizational compliance
- Form the framework for operations, decision-making, and behaviors, and rules for a compliant and ethical corporate culture
- Align the organization around common goals, prevent misconduct, and remove inefficiencies
- Common Policies
  - Acceptable Use Policy (AUP)
  - Information Security Policies
  - Business Continuity & Continuity of Operations Plans (COOP)
  - Disaster Recovery
  - Incident Response
  - Software Development Life Cycle (SDLC) Policy
  - Change Management

# Guidelines

- Recommendations that steer actions in a particular job role or department
- They are more flexible than policies and
- Allow flexibility for their implementation

# Procedures

- Define step-by-step instructions and checklists
- Ensure a task is completed in a compliant and repeatable way
- Playbooks
  - Collection of critical actions generally associated with Security Operations (SOC)

# Procedures

- Examples
  - Onboarding/Offboarding
  - Background Checks
  - Service/Software Provisioning
  - Desktop Deployment
  - Patching and updating
  - “Go-Live” actions
  - After hours support
  - Ticket management

# Standards

- Define a set of best practices and include specific details
  - Often associated with regulations and policies
  - Regulations and policies use standards to offload details
  - Standard can change often while policy remains the same
  - Standard can be managed by subject matter experts
- Industry Standards
  - ISO 27k series, NIST 800 series Special Publications, PCI-DSS, FIPS, many others...
- Internal Standards
  - Encryption, coding Practices, audit, many others...

# Legal Environment

- Governance committees ensure their organizations abide by all applicable cybersecurity laws and regulations to protect them from legal liability
- Frameworks, benchmarks, and configuration guides may be used to demonstrate compliance with legal/regulatory requirements
- Global Law
- National Law
- State/Local Law
- Industry Regulations
- Privacy Legislation

# Legal Environment

- Privacy
  - GDPR
  - CCPA
  - Many others
- Energy
  - North American Electric Reliability Corporation (NERC) (United States and Canada)
- Education & Children
  - Family Educational Rights and Privacy Act (FERPA) (United States)
  - Children's Internet Protection Act (CIPA) (United States)
  - Children's Online Privacy Protection Act (COPPA) (United States)

# Legal Environment

- Healthcare
  - Health Insurance Portability and Accountability Act (HIPAA) (United States)
- Financial Services
  - Gramm-Leach-Bliley Act (GLBA) (United States)
  - Payment Card Industry Data Security Standard (PCI DSS) (Contractual obligation)
- Government
  - Federal Information Security Modernization Act (FISMA) (United States)
  - Criminal Justice Information Services Security Policy (CJIS) (United States)
  - The Government Security Classifications (GSC) (United Kingdom)

# Governance and Accountability

- Governance practices ensure organizations abide by all applicable cybersecurity laws and regulations to protect them from legal liability.
- Governance Boards
- Committees
- Centralized vs Decentralized
- Managing Risk and Revising Policies

- Data Governance Roles
  - Owner
  - Controller
  - Processor
  - Custodian

# Policies, Standards, and Procedures

- Policies
- Procedures
- Standards
- Legal Environment
- Governance and Accountability

Lesson 14

# Topic 14B

## Change Management



# Change Management Programs

- Systematic approach that manages all changes made to a product or system
- Ensures that methods and procedures are used to handle changes efficiently and effectively
- Helps minimize risks associated with changes
- Ensure changes do not negatively impact security, availability, or performance

# Change Management Programs

- Stakeholder Input
- Change Review Board
- Impact Analysis
- Test Results
- Rollout Plans
- Backout Plans
- Maintenance Windows
- Standard Operating Procedures (SOPs)

# Restarts, Dependencies, and Downtime

- Typically have a direct impact on business operations
- Dependencies complicate changes because a service restart in one area may significantly impact another
- Primary goal of change management is to minimize these disruptions
- Processes include communication requirements designed to inform/update stakeholders
- Legacy Systems and Applications
  - Often critical to business operations and difficult to manage
  - Legacy features often have compatibility issues when implementing changes

# Documentation and Version Control

- Assessing how a change impacts existing policies, procedures, documentation and diagrams is essential, and change management plans should include provisions requiring updates to these documents as part of the implementation
- Version control
  - Tracking and controlling changes to documents, diagrams, code, or other important data
  - Historical record of changes

# Change Management

- Change Management Programs
- Allowed and Blocked Changes
- Restarts, Dependencies, and Downtime
- Documentation and Version Control

Lesson 14

# Topic 14C

Automation and  
Orchestration



# Automation and Scripting

- Critical tools in modern IT operations
- Streamline processes
- Enhance security
- Improve efficiency
- Enforce security policies
- Reduce the risk of human error
- Reduce implementation time
- Provide clear audit trails

# Automation and Orchestration Implementation

- Enhance efficiency by enabling repetitive tasks to be performed quickly and consistently
- Mitigate operator fatigue
- Orchestration enhances the impact of automation by coordinating automated tasks across different systems and software tools

# Automation and Orchestration Implementation

- Security Automation
- DevOps
- Important Considerations
  - Complexity
  - Cost
  - Single Point of Failure
  - Technical Debt
  - Ongoing Support

# Automation and Orchestration

- Automation and Scripting
- Automation and Orchestration Implementation

CompTIA Security+ Exam SY0-701

# Lesson 14



## Summary

