COURSE: SECURITY+ SY0-401

MODULE 2: COMPLIANCE AND OPERATION SECURITY
• Explain the importance of security related awareness and training
• Compare and contrast physical security and environmental controls
• Summarize risk management best practices
• Given a scenario, select the appropriate control to meet the goals of security
Information Classification

- High
- Medium
- Low
- Confidential
- Private
- Public
Security Awareness Training

• Security policy training and procedures
• Role-based training
• Personally identifiable information
• Data labeling, handling and disposal
• Compliance with laws, best practices and standards
• Security policy training and procedures
• Role-based training
• Personally identifiable information
• Data labeling, handling and disposal
• Compliance with laws, best practices and standards
Security Awareness Training

User Habits

- Password behaviors
- Data handling
- Clean desk policies
- Prevent tailgating
- Personally owned devices
New Threats and New Security Trends/Alerts

- New viruses
- Phishing attacks
- Zero-day exploits
Environmental Controls

- HVAC
- Fire suppression
- EMI shielding
- Hot and cold aisles
- Environmental monitoring
- Temperature and humidity controls
Physical and Environmental Security

- Hardware locks
- Mantraps
- Video Surveillance
- Fencing
- Proximity readers
- Access list
- Proper lighting
- Signs
- Guards
- Barricades
- Biometrics
- Protected distribution (cabling)
- Alarms
- Motion detection
Physical and Environmental Security

Control Types

- Deterrent
- Preventive
- Detective
- Compensating
- Technical
- Administrative
Risk Management

Business Continuity Concepts

- Identification of critical systems and components
- Business continuity planning and testing
  Business impact analysis
- Risk assessment
- Continuity of operations
- Disaster recovery
- IT contingency planning
- Succession planning
- High availability
- Redundancy
- Tabletop exercises
- Removing single points of failure
Fault Tolerance

What is fault tolerance?

Achieving fault tolerance

- Hardware
- RAID
- Clustering
- Load balancing
- Servers
Risk Management

Disaster Recovery Concepts

What is disaster recovery?

Disaster recovery measures

- Backup plans/policies
- Backup execution/frequency
- Cold site
- Hot site
- Warm site
Appropriate Security Controls

Confidentiality

What is confidentiality?

Protecting confidentiality

- Encryption
- Access controls
- Steganography
Appropriate Security Controls

Integrity

What is integrity?

Protecting integrity
- Hashing
- Digital signatures
- Certificates
- Non-repudiation
Appropriate Security Controls

Availability

What is availability?

Protecting availability

• Redundancy
• Fault tolerance
• Patching
Appropriate Security Controls

Safety

• Fencing
• Lighting
• Locks
• CCTV
• Escape plans
• Drills
• Escape routes
• Testing controls
THANK YOU