Exam Objectives that do NOT Exist in Security+ SY0-401 but ARE in SY0-501

Click here for the practice tests and exam simulations

**OBJ/Sub-OBJ** NEW in 501

### 5.0 Risk Management

#### 5.1 Explain the importance of policies, plans and procedures related to organizational security.
- System administrator NEW
- System owner NEW
- User NEW
- Privileged user NEW
- Executive user NEW
  - Continuing education NEW
  - Adverse actions NEW
- General security policies
  - Personal email NEW

#### 5.2 Summarize business impact analysis concepts.
- Mission-essential functions NEW
  - Life NEW
  - Property NEW
  - Safety NEW
  - Finance NEW
  - Reputation NEW
- Privacy impact assessment NEW
- Privacy threshold assessment NEW

#### 5.3 Explain risk management processes and concepts.
- Threat assessment
  - Environmental NEW
  - Manmade NEW
  - Internal vs. external NEW
- Risk assessment
  - Asset value NEW
  - Risk register NEW
  - Supply chain assessment

#### 5.4 Given a scenario, follow incident response procedures.
- Incident response plan
  - Cyber-incident response team: NEW

#### 5.5 Summarize basic concepts of forensics.
- Legal hold NEW
5.6 Explain disaster recovery and continuity of operation concepts.
- Order of restoration
- Geographic considerations
  - Off-site backups
  - Distance
  - Location selection
  - Legal implications
  - Data sovereignty
- Continuity of operation planning
  - Failover

5.7 Compare and contrast various types of controls.
- Physical

5.8 Given a scenario, carry out data security and privacy practices.
- Data destruction and media sanitization
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Purging
- Data sensitivity labeling and handling
  - PII
  - PHI
- Data roles
  - Owner
  - Steward/custodian
  - Privacy officer
- Change management

5.4 Given a scenario, follow incident response procedures.
- Incident response plan
  - Documented incident types/category definitions
  - Roles and responsibilities
  - Reporting requirements/escalation
  - Cyber-incident response teams
  - Exercise
- Incident response process
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned
5.5 Summarize basic concepts of forensics.
- Order of volatility
- Chain of custody
- Legal hold
- Data acquisition
  - Capture system image
  - Network traffic and logs
  - Capture video
  - Record time offset
  - Take hashes
  - Screenshots
  - Witness interviews
- Preservation
- Recovery

5.6 Explain disaster recovery and continuity of operation concepts.
- Recovery sites
- Order of restoration
- Geographic considerations
  - Off-site backups
  - Distance
  - Location selection
  - Legal implications
  - Data sovereignty
- Continuity of operation planning
  - Failover

5.7 Compare and contrast various types of controls.
- Physical

5.8 Given a scenario, carry out data security and privacy practices.
- Data destruction and media sanitization
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Purging
- Data sensitivity labeling and handling
  - PII
  - PHI
- Data roles
  - Owner
  - Steward/custodian
  - Privacy officer