# 5.0 Risk Management

## 5.1 Explain the importance of policies, plans and procedures related to organizational security.

- **Standard operating procedure**
- **Agreement types**
  - BPA
  - SLA
  - ISA
  - MOU/MOA
- **Personnel management**
  - Mandatory vacations
  - Job rotation
  - Separation of duties
  - Clean desk
  - Background checks
  - Exit interviews
  - Role-based awareness training
    - Data owner
    - System administrator
    - System owner
    - User
    - Privileged user
    - Executive user
  - NDA
  - Onboarding
  - Continuing education
  - Acceptable use policy/rules of behavior
  - Adverse actions
- **General security policies**
  - Social media networks/applications
  - Personal email

## 5.2 Summarize business impact analysis concepts.

- **RTO/RPO**
- **MTBF**
- **MTTR**
- **Mission-essential functions**
- **Identification of critical systems**
- **Single point of failure**
- **Impact**
  - Life
  - Property
  - Safety
  - Finance
  - Reputation
- **Privacy impact assessment**
- **Privacy threshold assessment**

## 5.3 Explain risk management processes and concepts.

- **Threat assessment**
  - Environmental
  - Manmade
  - Internal vs. external
- **Risk assessment**
  - SLE
  - ALE
  - ARO
  - Asset value
  - Risk register
  - Likelihood of occurrence
  - Supply chain assessment
  - Impact
  - Quantitative
  - Qualitative
  - Testing
    - Penetration testing authorization
    - Vulnerability testing authorization
  - Risk response techniques
    - Accept
    - Transfer
    - Avoid
    - Mitigate
- **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**
- **Strategic intelligence/ counterintelligence gathering**
  - Active logging
- **Track man-hours**

## 5.6 Explain disaster recovery and continuity of operation concepts.

- **Recovery sites**
  - Hot site
  - Warm site
  - Cold site
- **Order of restoration**
- **Backup concepts**
  - Differential
  - Incremental
  - Snapshots
  - Full
- **Geographic considerations**
  - Off-site backups
  - Distance
  - Location selection
  - Legal implications
  - Data sovereignty
- **Continuity of operation planning**
  - Exercises/tabletop
  - After-action reports
  - Failover
  - Alternate processing sites
  - Alternate business practices

## 5.7 Compare and contrast various types of controls.

- **Deterrent**
- **Preventive**
- **Detective**
- **Corrective**
- **Compensating**
- **Technical**
- **Administrative**
- **Physical**

## 5.8 Given a scenario, carry out data security and privacy practices.

- **Data destruction and media sanitization**
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Purging
  - Wiping
- **Data sensitivity labeling and handling**
  - Confidential
  - Private
  - Public
  - Proprietary
  - PII
  - PHI
- **Data roles**
  - Owner
  - Steward/custodian
  - Privacy officer
- **Data retention**
- **Legal and compliance**