2.0 Risk Management and Incident Response

2.1 Interpret business and industry influences and explain associated security risks.

- **Risk management of new products, new technologies and user behaviors**
- **New or changing business models/strategies**
    - Partnerships
    - Outsourcing
    - Cloud
    - Merger and demerger/divestiture
- **Security concerns of integrating diverse industries**
    - Rules
    - Policies
    - Regulations
    - Geography
- **Ensuring third-party providers have requisite levels of information security**
- **Internal and external influences**
    - Competitors
    - Auditors/audit findings
    - Regulatory entities
    - Internal and external client requirements
    - Top level management
- **Impact of de-perimeterization (e.g., constantly changing network boundary)**
    - Telecommuting
    - Cloud
    - BYOD
    - Outsourcing

2.2 Given a scenario, execute risk mitigation planning, strategies and controls.

- **Classify information types into levels of CIA based on organization/industry**
- **Incorporate stakeholder input into CIA decisions**
- **Implement technical controls based on CIA requirements and policies of the organization**
- **Determine aggregate score of CIA**
- **Extreme scenario planning/ worst case scenario**
- **Determine minimum required security controls based on aggregate score**
- **Conduct system specific risk analysis**
- **Make risk determination**
    - Magnitude of impact
        - ALE
        - SLE
    - Likelihood of threat
        - Motivation
        - Source
        - ARO
        - Trend analysis
    - Return On Investment (ROI)
    - Total cost of ownership
- **Recommend which strategy should be applied based on risk appetite**
    - Avoid
    - Transfer
    - Mitigate
    - Accept
- **Risk management processes**
    - Exemptions
    - Deterrance
    - Inherent
    - Residual
- **Enterprise security architecture frameworks**
- **Continuous improvement/monitoring**
- **Business continuity planning**
- **IT governance**

2.3 Compare and contrast security, privacy policies and procedures based on organizational requirements.

- **Policy development and updates in light of new business, technology, risks and environment changes**
- **Process/procedure development and updates in light of policy, environment and business changes**
- **Support legal compliance and advocacy by partnering with HR, legal, management and other entities**
- **Use common business documents to support security**
  - Risk assessment (RA)/ Statement Of Applicability (SOA)
  - Business Impact Analysis (BIA)
  - Interoperability Agreement (IA)
  - Interconnection Security Agreement (ISA)
  - Memorandum Of Understanding (MOU)
  - Service Level Agreement (SLA)
  - Operating Level Agreement (OLA)
  - Non-Disclosure Agreement (NDA)
  - Business Partnership Agreement (BPA)
- **Use general privacy principles for sensitive information (PII)**
- **Support the development of policies that contain**
  - Separation of duties
  - Job rotation
  - Mandatory vacation
  - Least privilege
  - Incident response
  - Forensic tasks
  - Employment and termination procedures
  - Continuous monitoring
  - Training and awareness for users
  - Auditing requirements and frequency

2.4 Given a scenario, conduct incident response and recovery procedures.

- **E-discovery**
  - Electronic inventory and asset control
  - Data retention policies
  - Data recovery and storage
  - Data ownership
  - Data handling
  - Legal holds
- **Data breach**
  - Detection and collection
    - Data analytics
  - Mitigation
    - Minimize
    - Isolate
  - Recovery/reconstitution
  - Response
  - Disclosure
- **Design systems to facilitate incident response**
  - Internal and external violations
    - Privacy policy violations
    - Criminal actions
    - Insider threat
    - Non-malicious threats/ misconfigurations
  - Establish and review system, audit and security logs
- **Incident and emergency response**
  - Chain of custody
  - Forensic analysis of compromised system
  - Continuity Of Operation Plan (COOP)
  - Order of volatility