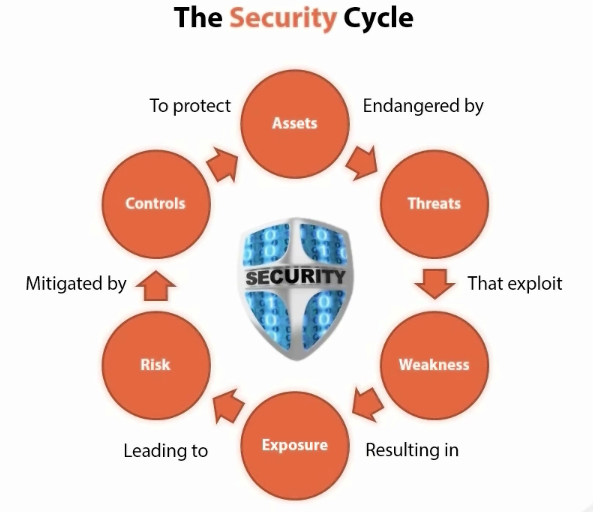
# CompTia Notes: Compliance and Operational Security

* Module Overview
  + Importance of Risk, risk calculation, loss, etc.
  + Managing risk, annual loss, single event loss
  + NIST Special Publication 800-53:
    - National Institute of Standards has recommended security controls for federal information systems
    - Protects “CIA triad”:
      * Confidentiality
      * Integrity
      * Availability
  + The Security Cycle 
  + Control Types
    - Important that organizations have a written security policy
    - Important to have contingency planning and incident response
    - Physical and personnel security
    - Awareness and training
    - Change/configuration management in place to make sure changes don’t create any problems where a change in one area affects another
  + Creating Incident Response plan
    - Preparation, detection and analysis, Containment Eradication and Recovery, Post-Incident activity
    - Average time to contain a cyber-attack is 31 days
    - Average cost of cyber-crimes is 7.6 million per year
  + Important policies to have
    - Privacy policy
    - Acceptable use policy
    - Security policy
    - Mandatory vacations
    - Job rotation(make sure people that get rotated don’t retain their previous privlidges
    - Separation of duties (separation of powers-> checks and balances)
    - Least privilege
  + Why mandatory vacations
    - Keeps personnel away from company assets for a period of time (allows companies to see anomalies) doesn’t allow people who are doing fraud, theft, etc to cover their tracks
    - Allows another person to step in to do things the right way and see if the other person was really doing their job correctly
  + Risk Calculation
    - How often will the issue occur?
    - How much will it cost?
    - What is the likelihood that it will happen?
    - Quantitative analysis assigns an exact monetary value to assets, attempts to give expected yearly loss in dollars for any given risk, enables prioritization based on cost
    - ALE: Annual Loss Expectancy
    - SLE: Single Loss Expectancy = asset value x Exposure factor
    - Annualized rate of Occurrence
  + Other terms
    - MTTF: Mean time between failures, statistical average a device lasts between failures
    - MTTR: Mean time to failure, statistical average of how long a component lasts, referring to things that will be replaced rather than repaired
    - MTBF: Mean time to repair
  + Risk Management Concepts
    - Risk Transference by using a hosted provider or insurance company
    - Risk Acceptance: what is the cost of removing the risk vs. dealing with the issue if/when it occurs “juice isn’t worth the squeeze”
    - Risk Mitigation/deterrence
    - Risk Avoidance: Opting not to do something because the risk is too high