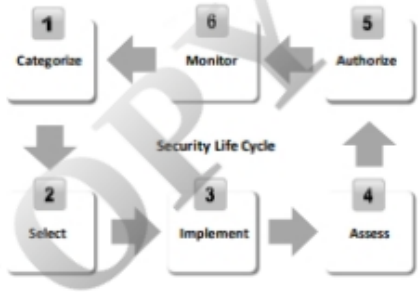
Risk Management Framework: NIST Risk Management Framework

- The NIST Risk Management Framework is a **structured and continuous process** that integrates information security and risk management activities into the system development life cycle (SDLC)

- **Categorize**: Define criticality or sensitivity of an information system according to the potential worst-case adverse impact to the mission or business
- **Select**: Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment
- **Implement**: Implement security controls within enterprise architecture using sound system engineering practices; apply security configuration changes
- **Assess**: Determine security control effectiveness (i.e. that controls are implemented correctly, operating as intended, and meeting security requirements for information system)
- **Authorize**: Determine risk to organizational operations and assets, individuals, other organizations, and the nation; if acceptable, authorize operation
- **Monitor**: Continuously track changes to the information system that may affect security controls and reassess control effectiveness



http://csrc.nist.gov

Risk Management Framework: COSO ERM Framework

- COSO ERM Framework defines essential components, suggests a common language, and provides **clear direction and guidance** for enterprise risk management
- It emphasizes that ERM involves those elements of the management process that enable management to make **genuine risk-based decisions**

http://www.coso.org

Notes:

Risk Management Framework: COBIT Framework

- **COBIT** Framework is an IT governance framework and supporting **toolset** that allows **managers** to bridge the gap between control requirements, technical issues, and business risks
- It **emphasizes** regulatory compliance, helps organizations to **increase** the value attained from IT, and enables alignment and simplifies implementation of the enterprise's IT governance and **control framework**

Enterprise Network Risk Management Policy

- Risk Management Policy assists in **developing** and **establishing** essential processes and procedures to address and minimize **information** security risks
- It outlines different aspects of risk and identifies people to manage the risk in the organization

Objectives:

- Equip the organization with the required skills to identify and treat risks
- Provide a consistent risk management framework
- Provide the overall direction and purpose for performing risk management
- Manage the risks with adequate risk mitigation techniques
- Combat the existing and emerging risks
- Integrate operational risks into the risk management process
- Accomplish the strategic and operational goals of the organization
- Facilitate assistance in taking strategic management decisions
- Meet legal and regulatory requirements

Notes: _____