Architectural risk assessment/analysis

- Architectural risk assessment is a risk management process that identifies flaws in a software architecture and determines risks to business information assets that result from those flaws.
- Through the process of architectural risk assessment, flaws are found that expose information assets to risk, risks are prioritized based on their impact to the business, mitigations for those risks are developed and implemented, and the software is reassessed to determine the efficacy of the mitigations.

- **Risk Analysis**
- Risk analysis is an activity geared towards assessing and analyzing system risks. Risk analysis can be conducted on a scheduled, event-driven, or as needed basis. Risk analysis can be implemented as an iterative process where information collected and analyzed during previous assessments are fed forward into future risk analysis efforts.

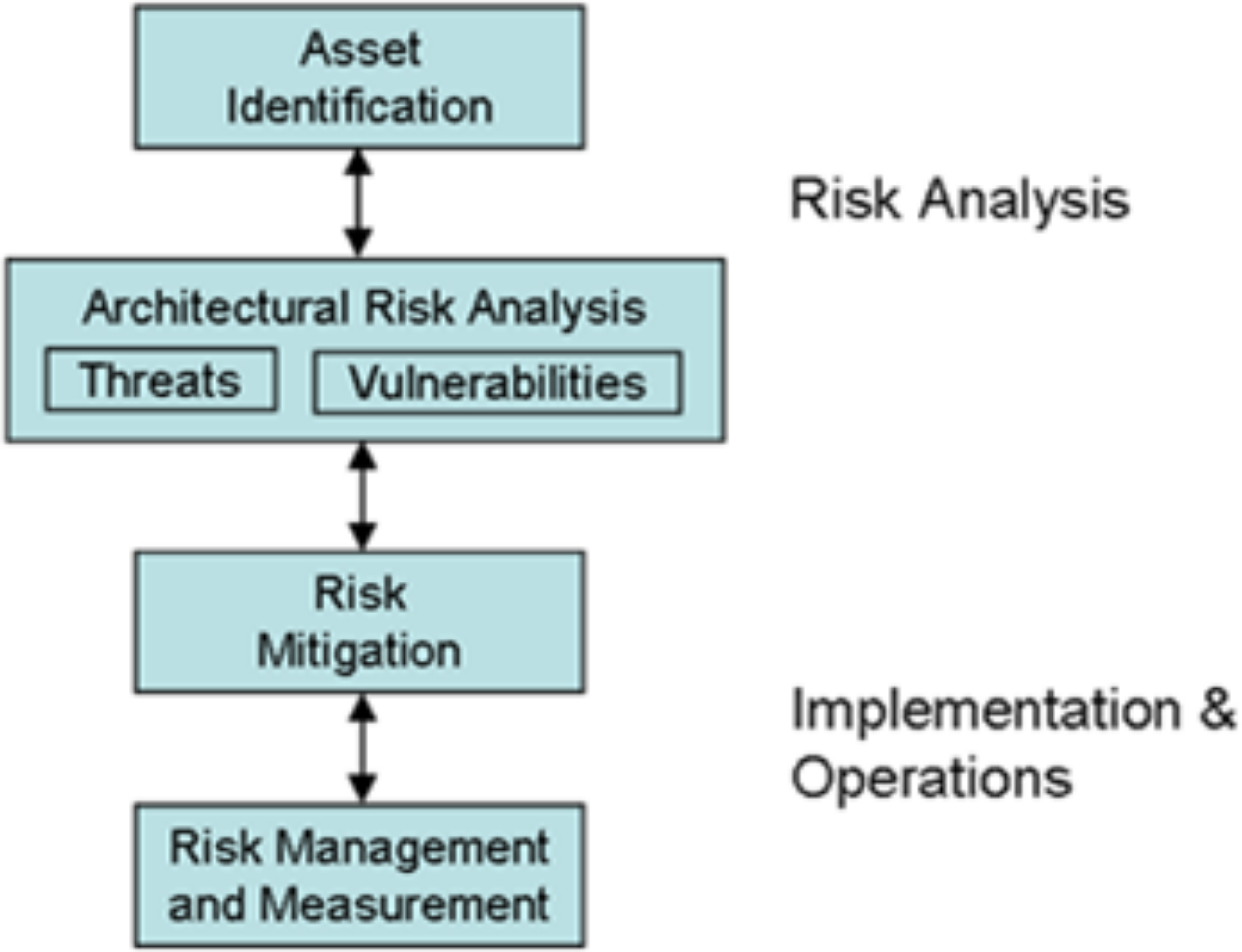
- **Risks**
- Risk is a product of the probability of a threat exploiting a vulnerability and the impact to the organization.
- The process of architecture risk management is the process of identifying those risks in software and then addressing them.
- Some complex risks spring to mind easily: a malicious attacker (threat) bypasses the authentication module (vulnerability) and downloads user accounts (information asset), thereby exposing the business to financial liability for the lost records (impact).
- It is important to note that the software architecture exists in a system context that includes risks in the physical, network, host, and data layers, and risks in those layers (including those generated outside the organization's perimeter) may cascade into the software architecture.

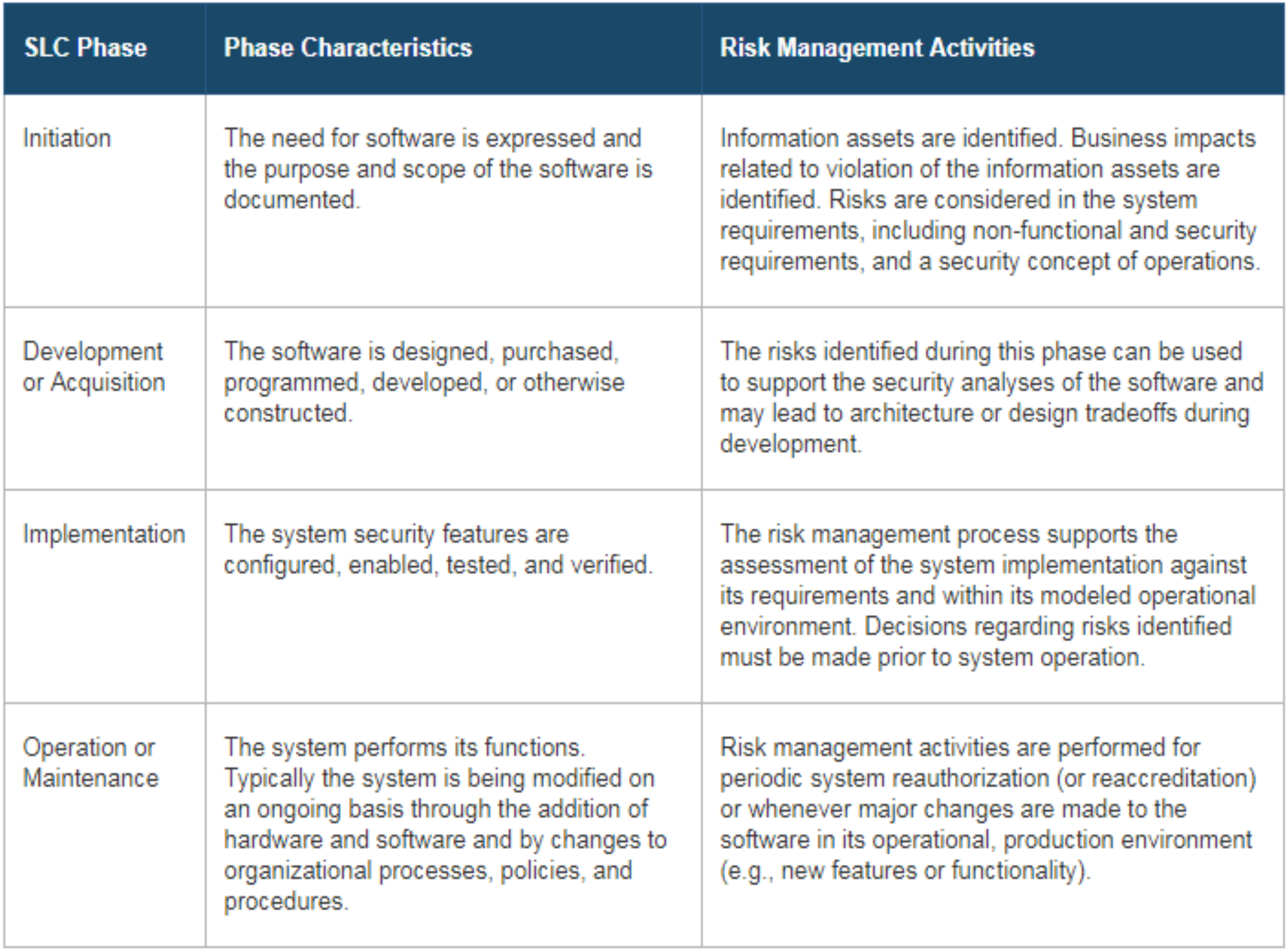
- **Mitigations**
- Risk mitigation refers to the process of prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk analysis process.
- Mitigating a risk means changing the architecture of the software or the business in one or more ways to reduce the likelihood or the impact of the risk.
- A mitigation consists of one or more *controls* whose purpose is to prevent a successful attack against the software architecture’s confidentiality, integrity, and availability

Architectural Risk Management

- Risk management is the process of continually assessing and addressing risk throughout the life of the software.
- It encompasses four processes: (1) asset identification, (2) risk analysis, (3) risk mitigation, and (4) risk management and measurement.
- During each of these phases, business impact is the guiding factor for risk analysis. The architectural risk analysis process includes identification and evaluation of risks and risk impacts and recommendation of risk-reducing measures

The diagram below shows the process view of risk analysis and risk management areas.


Asset Identification
Risk Analysis
Architectural Risk Analysis
Threats
Vulnerabilities
Risk Mitigation
Implementation & Operations
Risk Management and Measurement



SLC Phase	Phase Characteristics	Risk Management Activities
Initiation	The need for software is expressed and the purpose and scope of the software is documented.	Information assets are identified. Business impacts related to violation of the information assets are identified. Risks are considered in the system requirements, including non-functional and security requirements, and a security concept of operations.
Development or Acquisition	The software is designed, purchased, programmed, developed, or otherwise constructed.	The risks identified during this phase can be used to support the security analyses of the software and may lead to architecture or design tradeoffs during development.
Implementation	The system security features are configured, enabled, tested, and verified.	The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation.
Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures.	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to the software in its operational, production environment (e.g., new features or functionality).

Risk management

- Process of: assessing risk, taking steps to reduce it to an acceptable level, and maintaining that level of risk
- Five principle:
  - **I. Assess risk and determine needs**
    - Recognize the importance of protecting information resource assets
    - Develop risk assessment procedures that link IA to business needs
    - Hold programs and managers accountable
    - Manage risk on a continuing basis
  - **II. Establish a central management focus**
    - Designate a central group for key activities
    - Provide independent access to senior executives to the group
    - Designate dedicated funding and staff
    - Periodically, enhance staff technical skills

- III. **Implement appropriate policies and related controls**
    - Link policies to business risks
    - Differentiate policies and guidelines
    - Support polices via the central IA group
- **IV Promote awareness**
  - Educate user and others on risks and related policies
  - Use attention-getting and user-friendly techniques
- **V Monitor and evaluate policy and control effectiveness**
  - Monitor factor that affect risk and indicate IA effectiveness
  - Use results to direct future efforts and hold managers accountable
  - Be on the lookout for new monitoring tools and techniques