CA032810 - 532039
SL-2009-193

DEFENCE R&D DÉFENSE

Architectural Risk

Definitions

- **Vulnerabilities**: errors in the code which incorrectly implement the design or introduce unwanted behaviors.
  - May be difficult to detect but usually simple to correct.
- **Flaws**: fundamental failures in the design that mean that the software will always have a problem no matter how well it is implemented.
  - Significant redesign is usually necessary.
- **Attacks**: actions of a threat on information assets.

Definitions

- **Impacts**: consequences of a successful attack.
  - Loss of life, revenue, reputation, market share; increased development costs, maintenance costs, customer support costs, time to market; legal impacts, etc.
  - Depend on the criticality of information assets.
- **Risks**: P(threat exploiting flaw) x impact

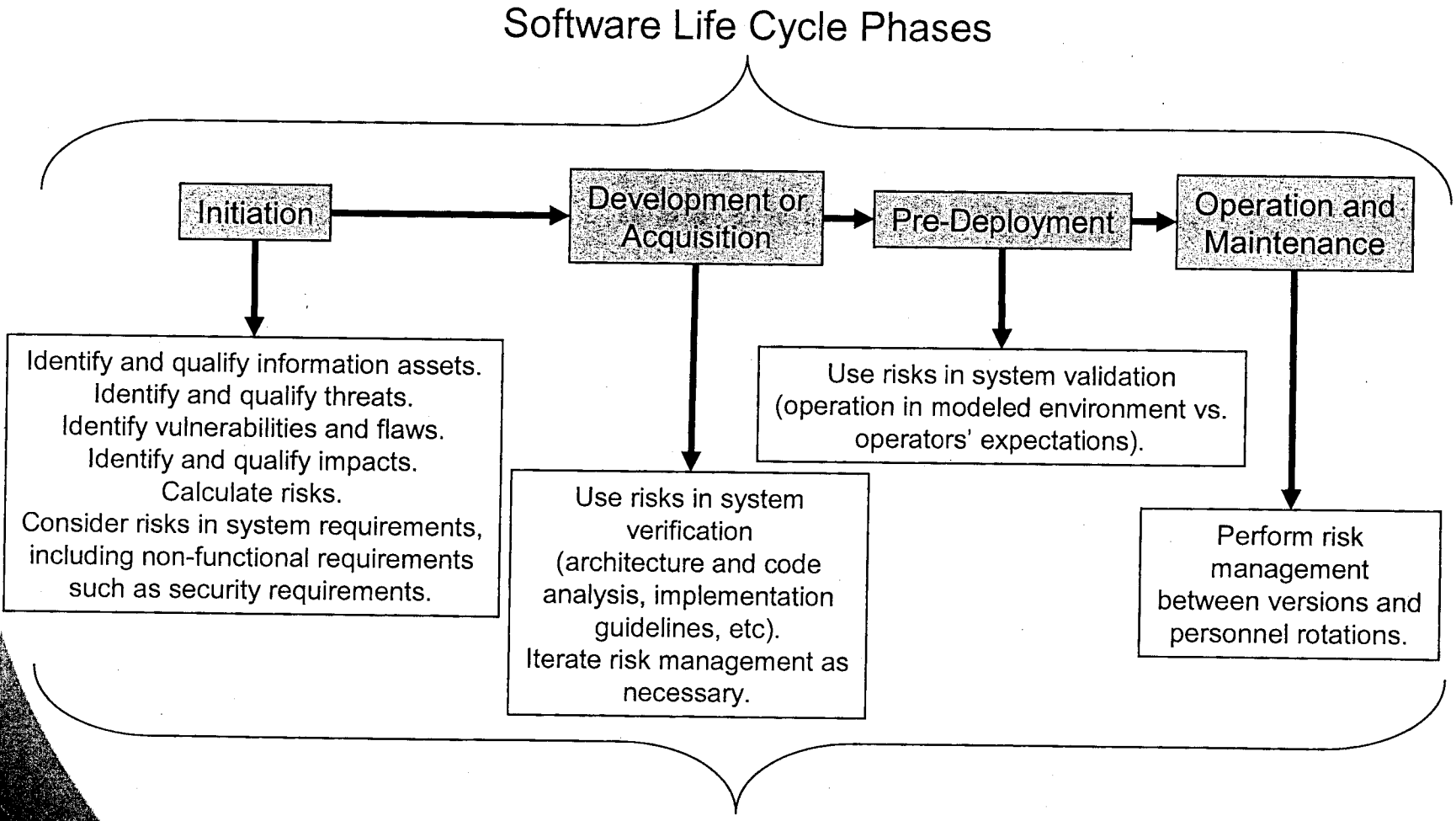
  OR

  P(successful attack) x impact.

Definitions

- **Risk analysis**: activity consisting in assessing and evaluating risks and proposing risk-reducing measures (controls).
  - Reduce *P(threat exploiting flaw)* and/or *impact*.
- **Risk mitigation**: process of prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from risk analysis.
- **Risk management**: ongoing process of information asset identification, risk analysis, and risk mitigation.

Software Risk Management



Particularities of Architectural Risk Management

- In Architectural Risk Analysis
  - Application characterization: scope/boundaries of the architecture.
  - Artifacts required or desired (not exhaustive!)
    - Next 2 slides…
    - Ultimate goal: describe "all" vital relationships between critical parts of the system.

Particularities of Architectural Risk Management

- Software business case
- Functional and non-functional requirements
- Enterprise architecture requirements
- Use case documents
- Misuse and abuse case documents
- Software architecture documents
- Data architecture documents
- Security architecture documents
- …
- Identity services (authentication) and management architecture documents
- Design documents
- Software development plan
- Quality assurance plan
- Test plan
- Risk management plan
- Software acceptance plan
- Problem resolution plan
- …

Particularities of Architectural Risk Management

- Risk list
- Issues list
- Project metrics
- Programming guidelines
- Configuration and change management plan
- Project management plan
- Disaster recovery plan
- System logs
- Operational guides
- …

- Documentation of the system and data criticality
- Documentation of the system and data sensitivity
- System security policies governing the software
- Management controls used for the software
- Information storage protection
- Flow of information in the software
- Technical controls used for the software
- …

Particularities of Architectural Risk Management

- In Architectural Risk Analysis (cont'd)
  - Models must be used to represent and analyze behavior, e.g.:
    - State diagrams for processes
    - Sequence diagrams for communication between processes
  - No tools for automatic ARA

Particularities of Architectural Risk Management

- In Architectural Risk Analysis (cont'd)
  - All this documentation is not always available or up-to-date
    - Architecture reconstruction is helpful
    - But tools are incomplete

Particularities of Architectural Risk Management

- In Architectural Risk Analysis (cont'd)
  - Three activities can guide ARA:
    - Known flaws analysis
      - Based on security patterns
    - Ambiguity analysis
      - Search for ambiguities in requirements and failures to resolve them in architecture and/or implementation.
    - Underlying platform vulnerability analysis
      - Windows, Linux, Java, WebLogic, WebSphere, PHP, ASP.net, Jakarta, etc.

Particularities of Architectural Risk Management

- In Architectural Risk Mitigation
  - Mitigations to architectural flaws are complicated
    - Different modules, subsystems, classes, teams
    - Early discovery and security in mind are key
  - But sometimes, little changes make a big difference
    - Authentication mechanisms, cryptography, etc.

Discussion

- When all documents are not available or up-to-date, regeneration tools are useful but actually incomplete.
- Which documents could be, at least partially, regenerated?
  - Use case documents
  - Misuse and abuse case documents
  - Software architecture documents
  - Data architecture documents
  - Design documents
  - Flow of information in the software
  - …