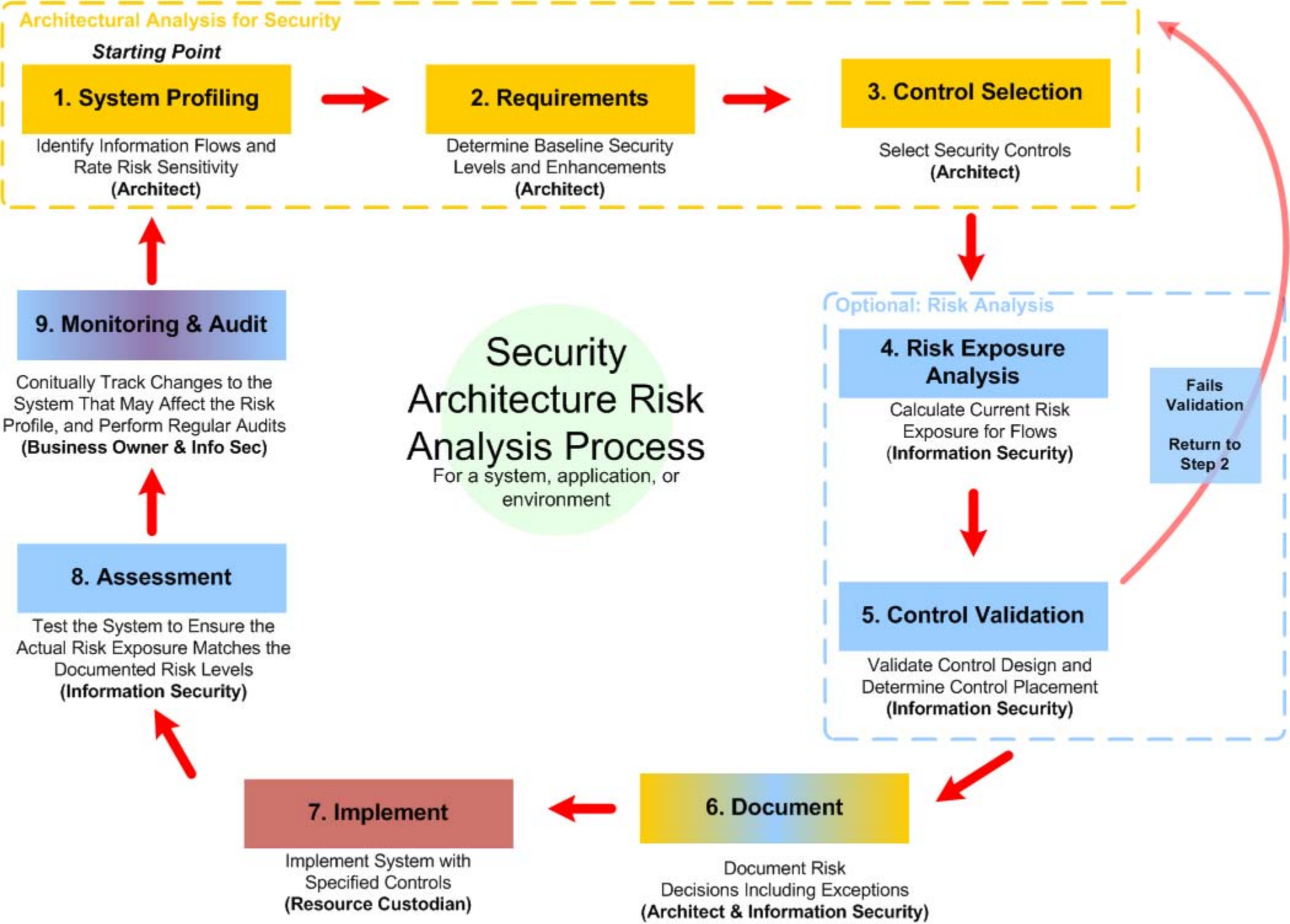
Architectural Analysis for Security
Starting Point
1. System Profiling
Identify Information Flows and Rate Risk Sensitivity (Architect)
2. Requirements
Determine Baseline Security Levels and Enhancements (Architect)
3. Control Selection
Select Security Controls (Architect)
Optional: Risk Analysis
4. Risk Exposure Analysis
Calculate Current Risk Exposure for Flows (Information Security)
Fails Validation
Return to Step 2
5. Control Validation
Validate Control Design and Determine Control Placement (Information Security)
6. Document
Document Risk Decisions Including Exceptions (Architect & Information Security)
7. Implement
Implement System with Specified Controls (Resource Custodian)
8. Assessment
Test the System to Ensure the Actual Risk Exposure Matches the Documented Risk Levels (Information Security)
9. Monitoring & Audit
Conitually Track Changes to the System That May Affect the Risk Profile, and Perform Regular Audits (Business Owner & Info Sec)
Security Architecture Risk Analysis Process
For a system, application, or environment