

Starting Point

1. Resource Profiling

Describe the Resource and Rate Risk Sensitivity
(Business Owner)

2. Risk Assessment

Identify and Rate Threats, Vulnerabilities, and Risks
(Information Security)

3. Risk Evaluation

Decision to Accept, Avoid, Transfer, or Mitigate Risk
(Info Sec & Business Owner)

7. Monitoring & Audit

Conitually Track Changes to the System That May Affect the Risk Profile, and Perform Regular Audits
(Info Sec & Business Owner)

Information Security Risk Management Process

For an application, system, facility, environment, or vendor

4. Document

Document Risk Decisions Including Exceptions and Mitigation Plans
(Info Sec & Business Owner)

6. Validation

Test the Controls to Ensure the Actual Risk Exposure Matches the Desired Risk Levels
(Information Security)

5. Risk Mitigation

Implement Mitigation Plan with Specified Controls
(Resource Custodian)