Ron Shuck, CISSP, CISM, CISA, GCIA
Infrastructure Security Architect
Spirit AeroSystems

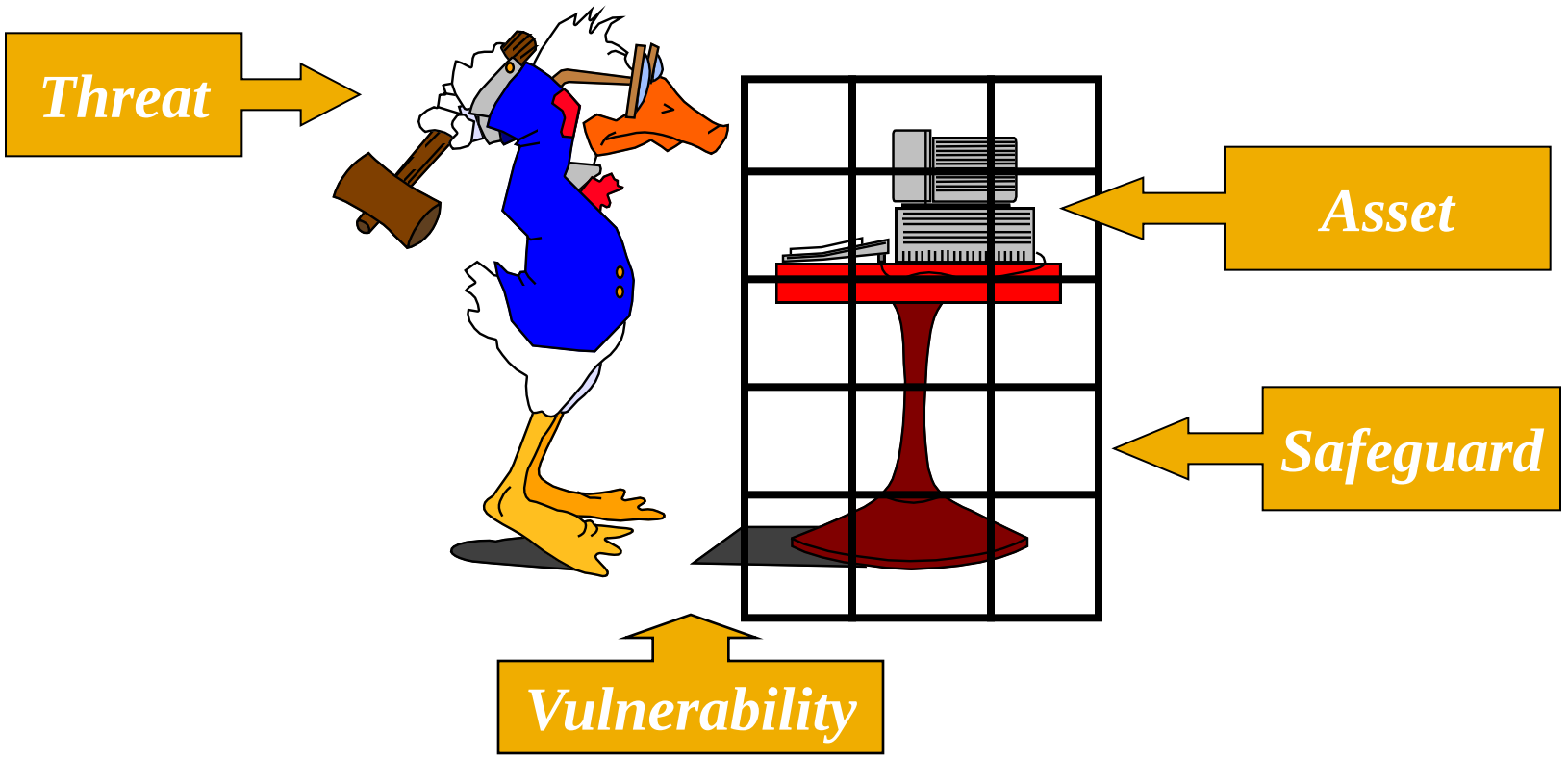
ISC² CBK Roundtable: Risk Management

February 5, 2010

Overview

- What is Risk
- Identification of Risk
- Management of Risk
- Risk Management Framework
- Risk Analysis
- Risk Assessment Process
- Risk Mitigation Process

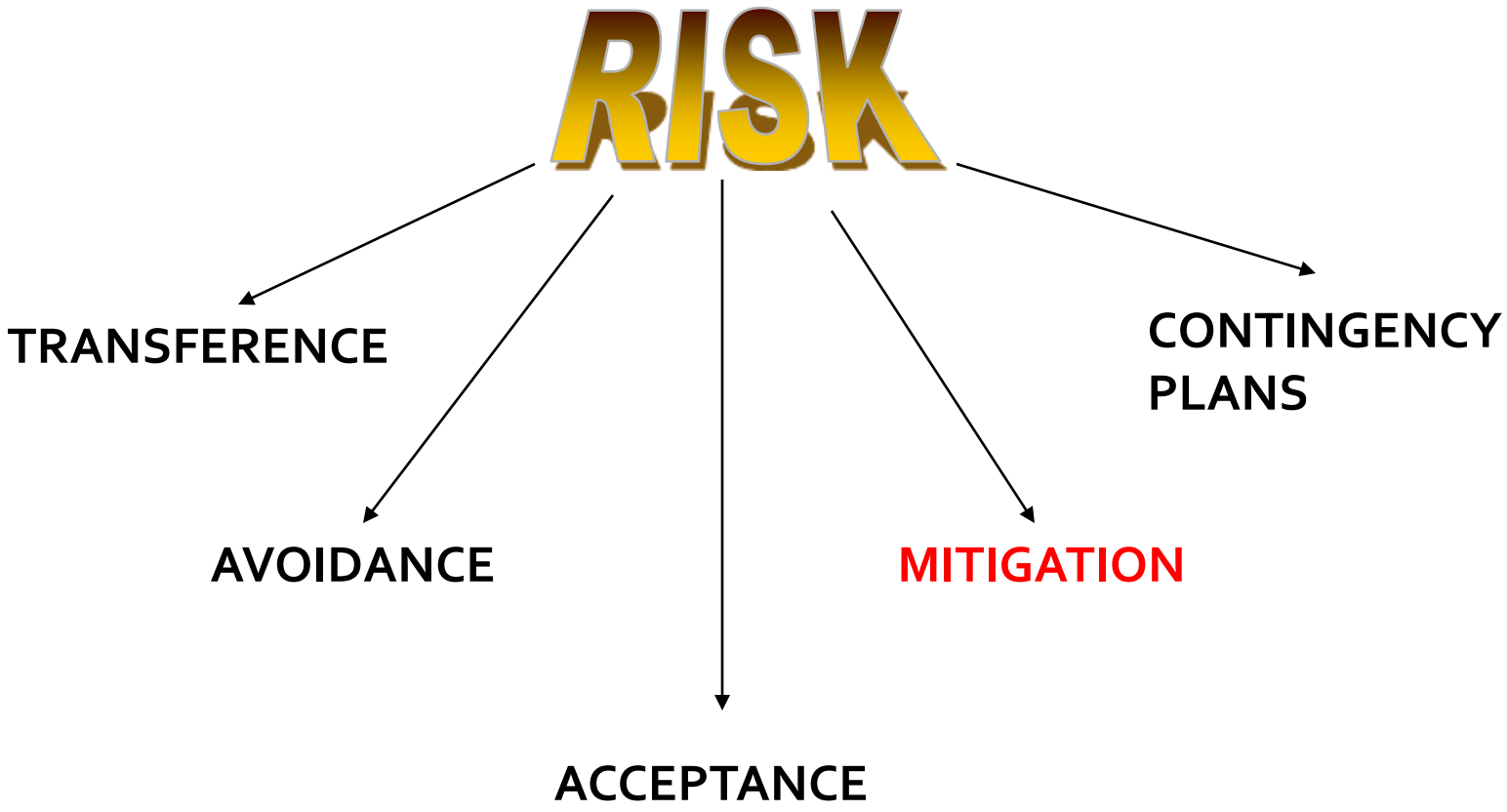
Risk



Identification of Risk

- Actual Threat
- Possible Consequences
- Occurrence Frequency of threat
- Confidence in occurrence of threat

Management of Risk



Risk Management Framework

NIST Special Publication 800-37 rev1 Guide for Applying the Risk Management Framework to Federal Information Systems

ISSA™ Information Systems Security Association — CENTRAL PLAINS CHAPTER

Risk Analysis Terms

- Exposure Factor (**EF**)
  - % loss to asset if threat realized
- Single Loss Expectancy (**SLE**)
  - $Asset\ Value \times EF$
- Annualized Rate of Occurrence (**ARO**)
  - Expected frequency of threat
- Annualized Loss Expectancy (**ALE**)
  - $SLE \times ARO$

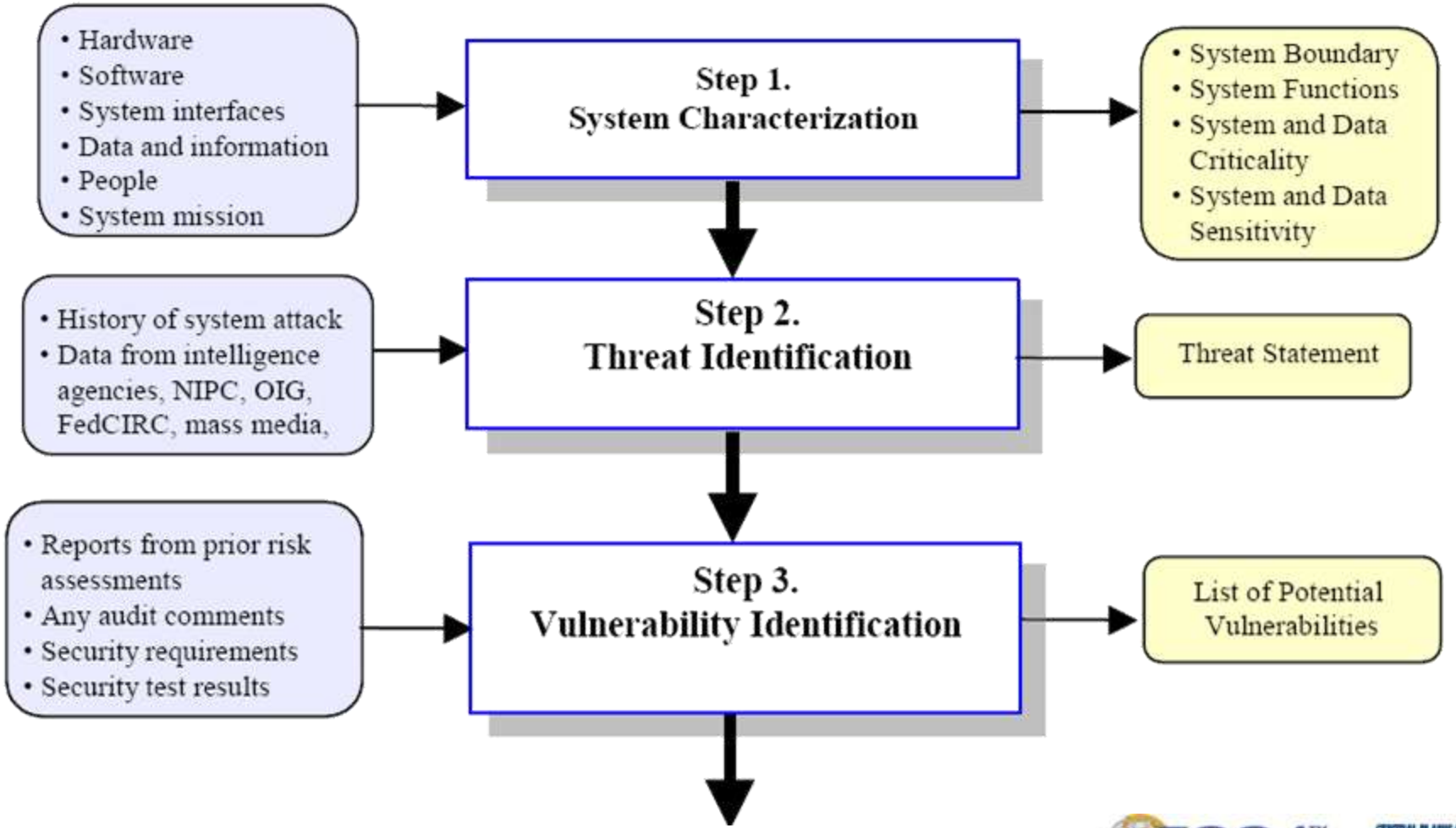
Quantitative Risk Analysis

- Preliminary Security Examination (PSE)
- Steps
  - Determine Asset Value
  - Analyze Potential threats
  - Define ALE
- Remedies
  - Risk Reduction
  - Risk Transference – Insurance
  - Risk Acceptance

Qualitative Risk Analysis

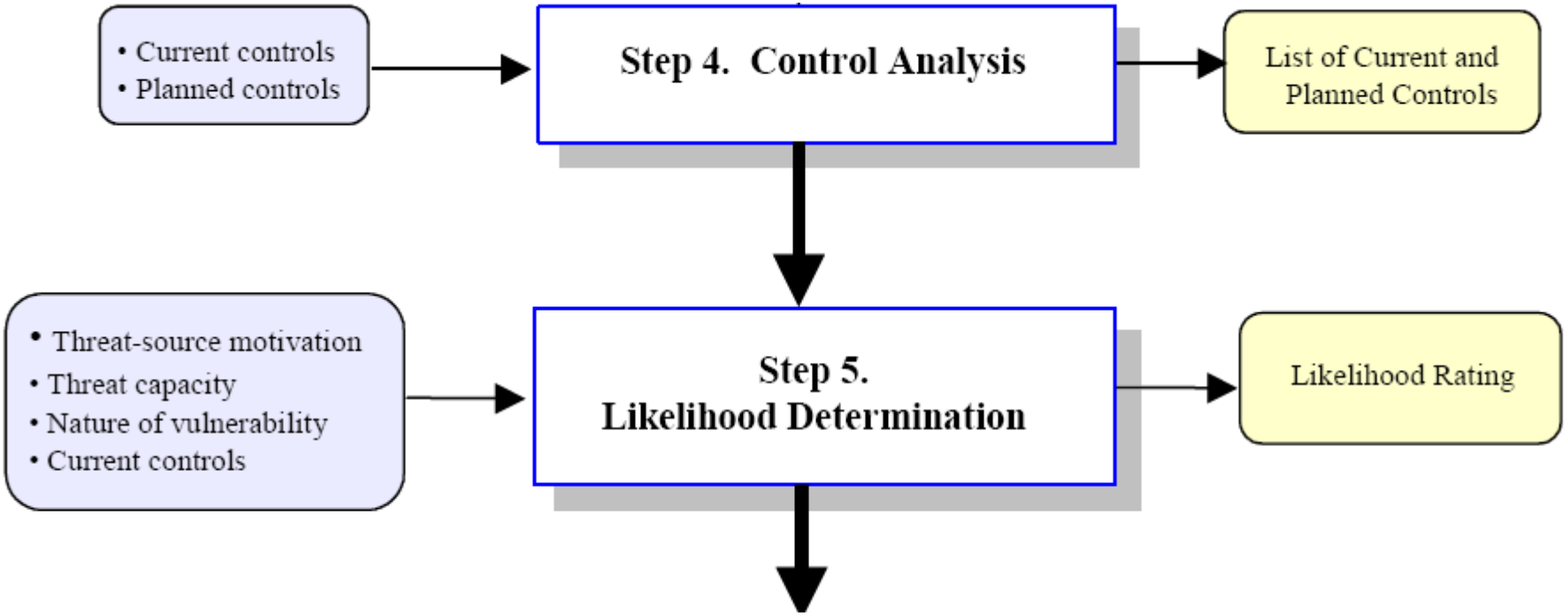
- Scenario Procedure
- Asset Valuation Process
- Safeguard Selection
  - Cost/Benefit
  - Manual operations
  - Audit/Accountability
  - Recovery
  - Vendor

Risk Assessment Process

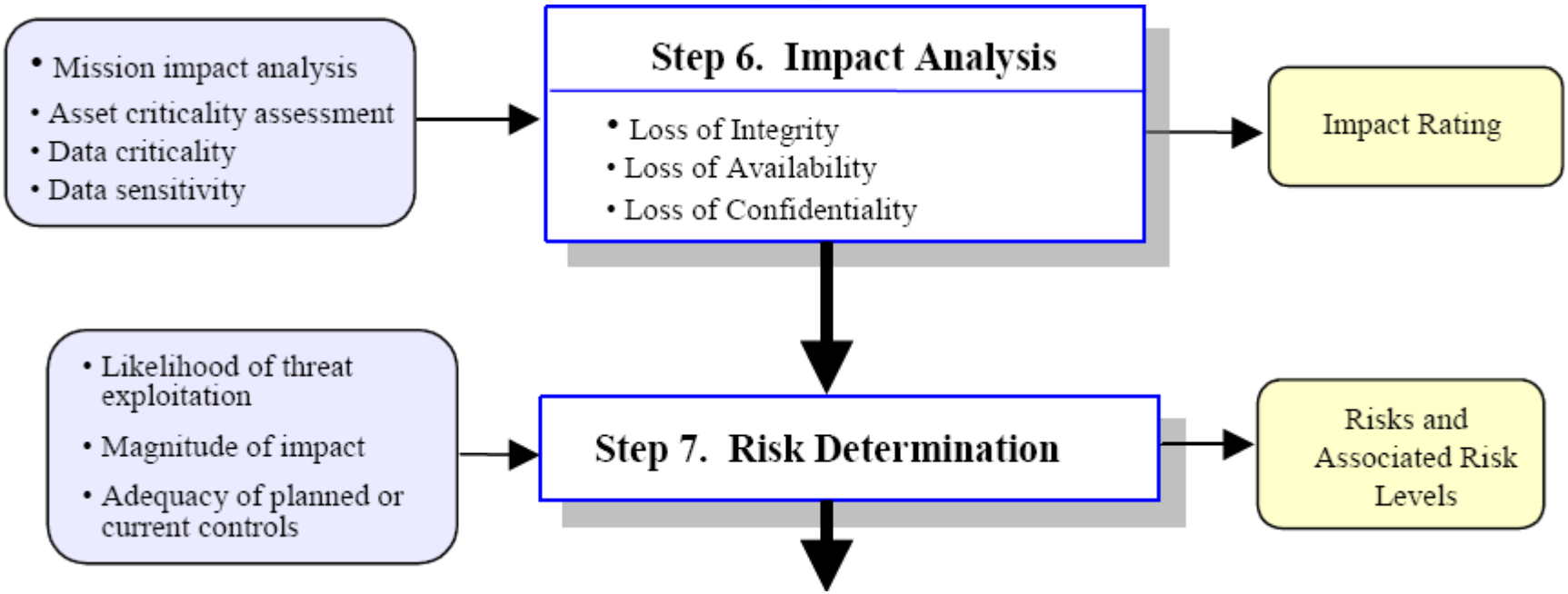


NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems

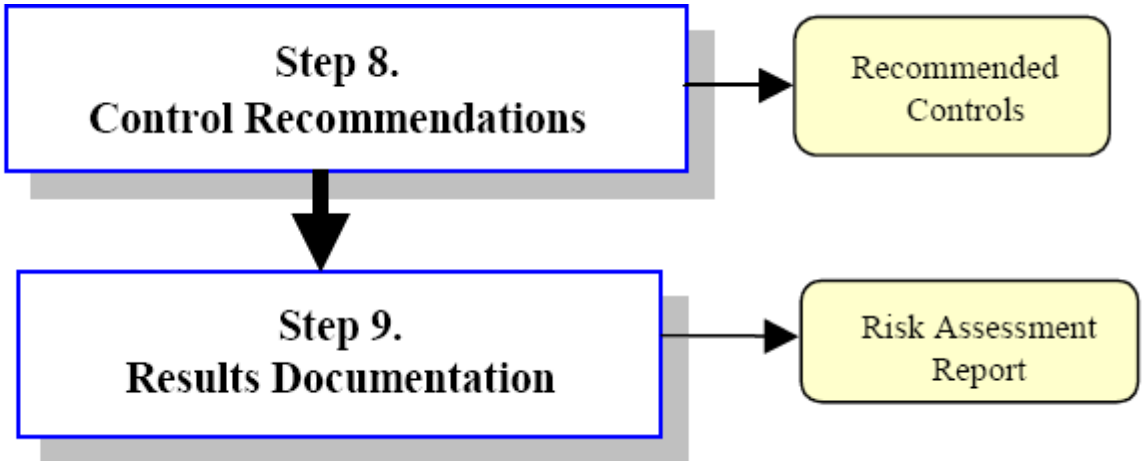
Risk Assessment Process



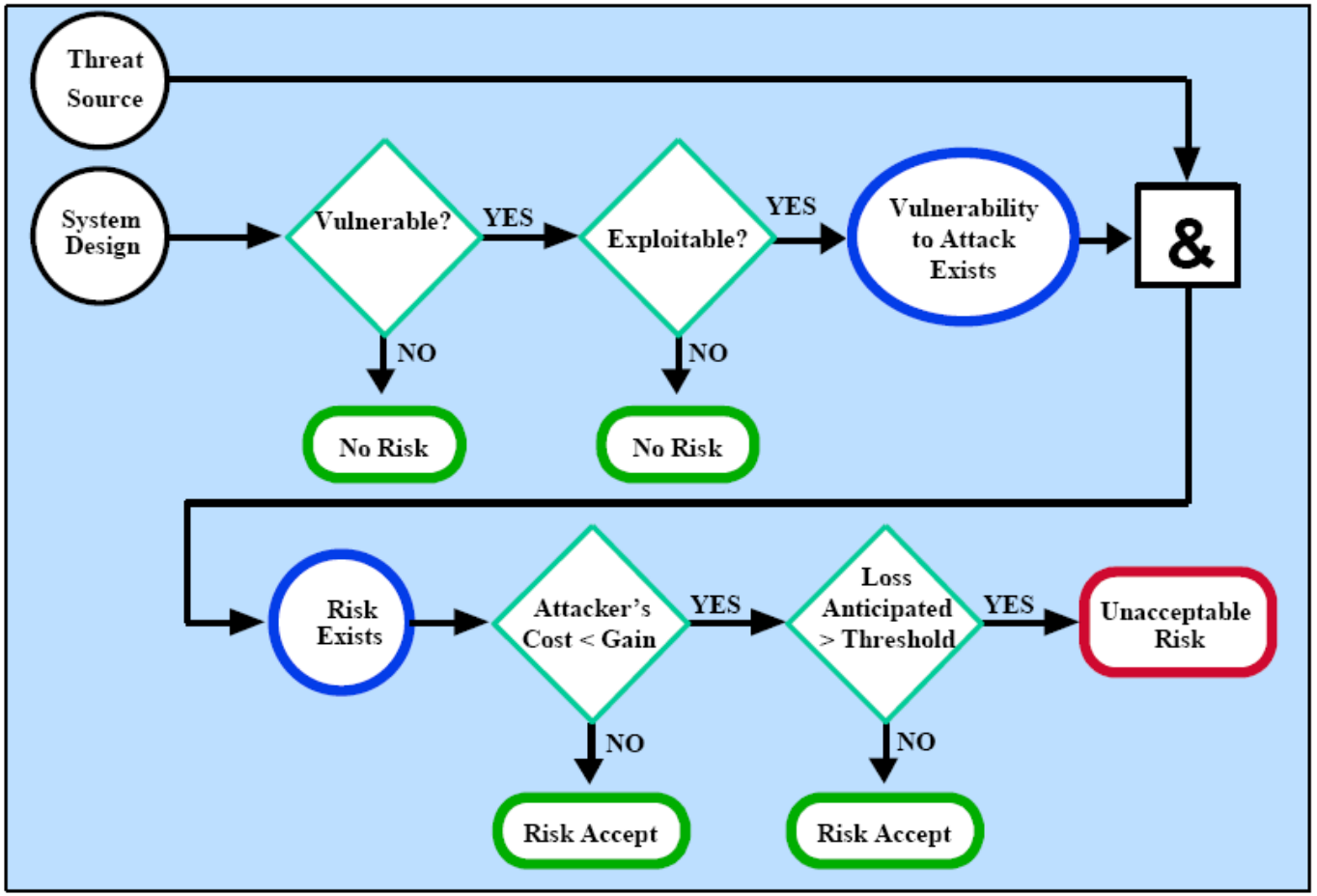
Risk Assessment Process



Risk Assessment Process



Risk Mitigation Process



NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems

ISSA™ Information Systems Security Association — Central Plains Chapter

Risk Management

Questions