چند رسانه ای
نگارستان

Information Security Risk Management

Based on
ISO/IEC 17799

Houman Sadeghi Kaji
Spread Spectrum Communication System PhD. ,
Cisco Certified Network Professional Security Specialist
BS7799 LA
info@houmankaji.net

Target Audience

This session is primarily intended for:

- ✓ Systems architects and planners
- ✓ Members of the information security team
- ✓ Security and IT auditors
- ✓ Senior executives, business analysts, and business decision makers
- ✓ Consultants and partners

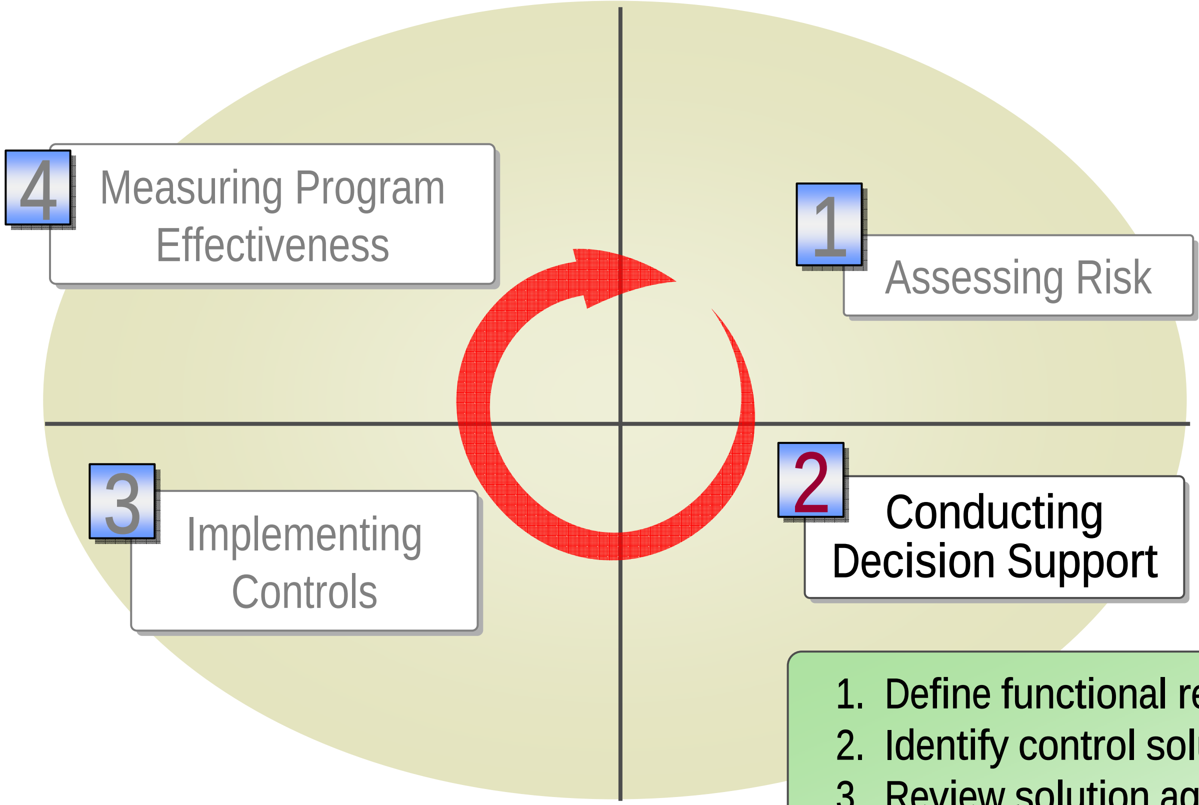
Motivation for this Presentation

- Security is a **process**, not a product. Security products will not save you.
- **Process** is composed of technology, people, and tools. This is important because processes involve time and interaction between entities and many of the hard problems in security stem from this inherent interaction.

Conducting Decision Support

- Security Risk Management Concepts
- Identifying Security Risk Management Prerequisites
- Assessing Risk
- Conducting Decision Support
- Implementing Controls and Measuring Program Effectiveness

Overview of the Decision Support Phase



1. Define functional requirements
2. Identify control solutions
3. Review solution against requirements
4. Estimate degree of risk reduction
5. Estimate cost of each solution
6. Select the risk mitigation strategy

Identifying Output for the Decision Support Phase

Key elements to gather include:

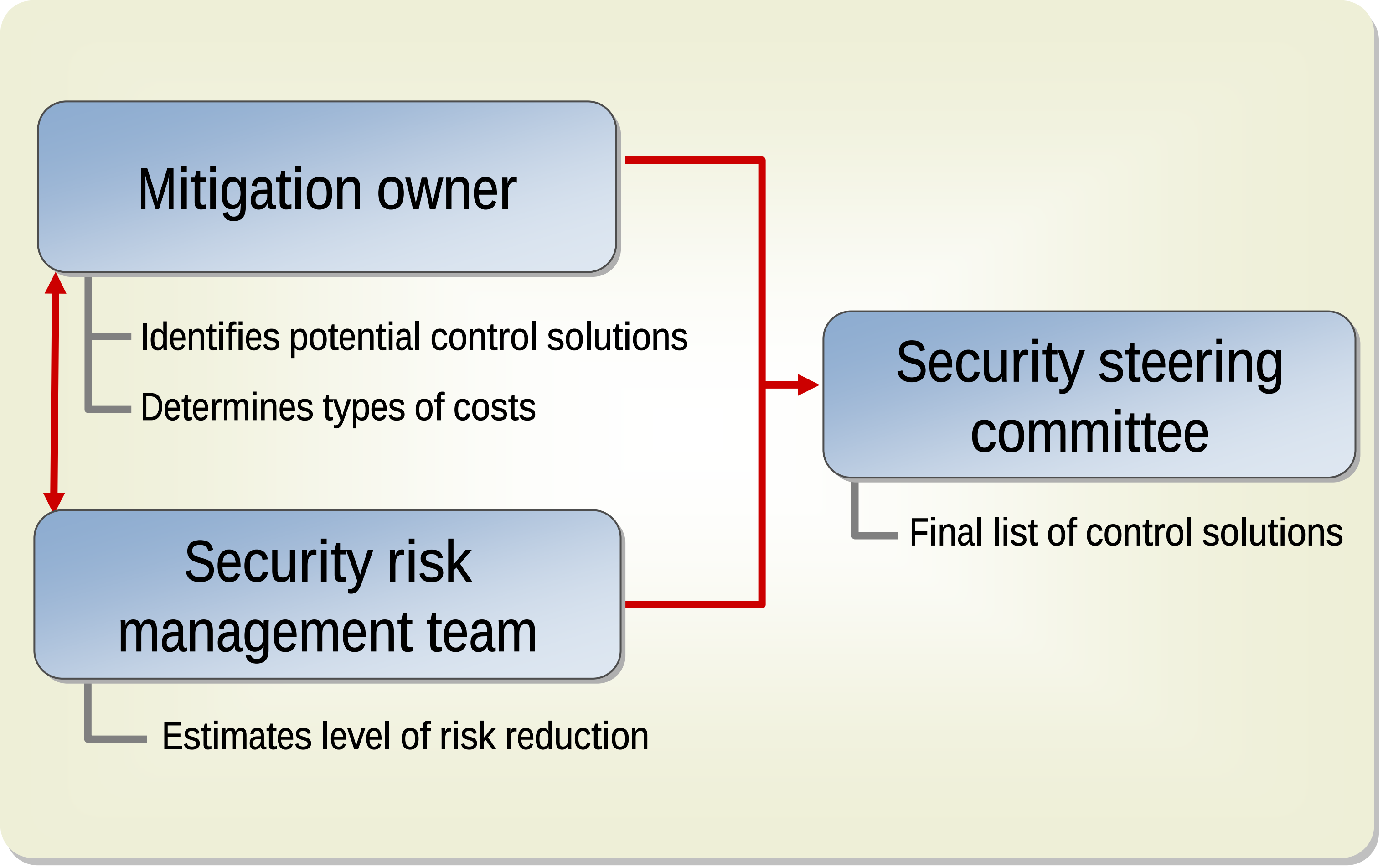
- Decision on how to handle each risk
- Functional requirements
- Potential control solutions
- Risk reduction of each control solution
- Estimated cost of each control solution
- List of control solutions to be implemented

Considering the Decision Support Options

Options for handling risk:

- ☑ Accepting the current risk
- ☑ Implementing controls to reduce risk

Overview of the Identifying and Comparing Controls Process


Mitigation owner

- Identifies potential control solutions
- Determines types of costs

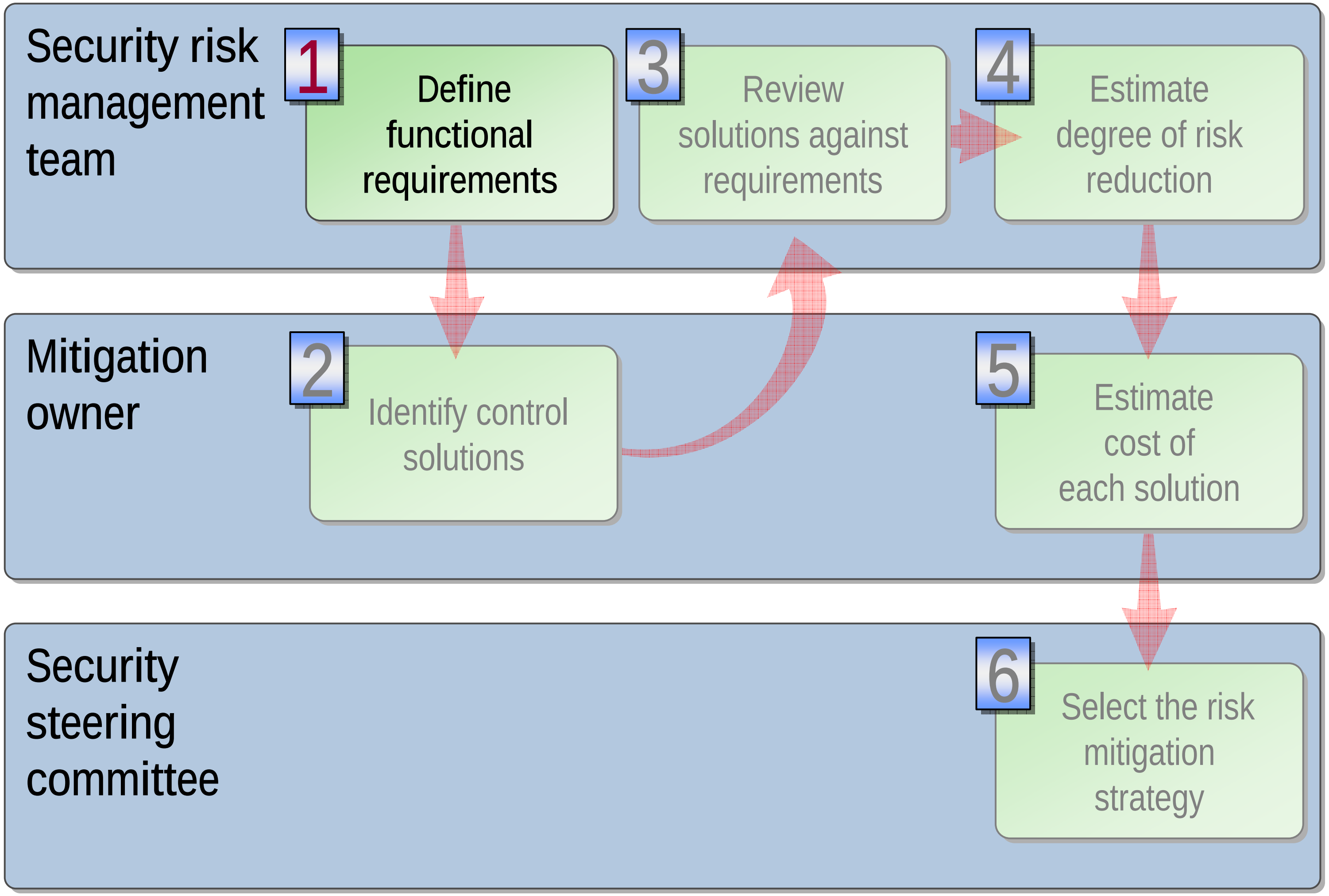
Security risk management team

- Estimates level of risk reduction

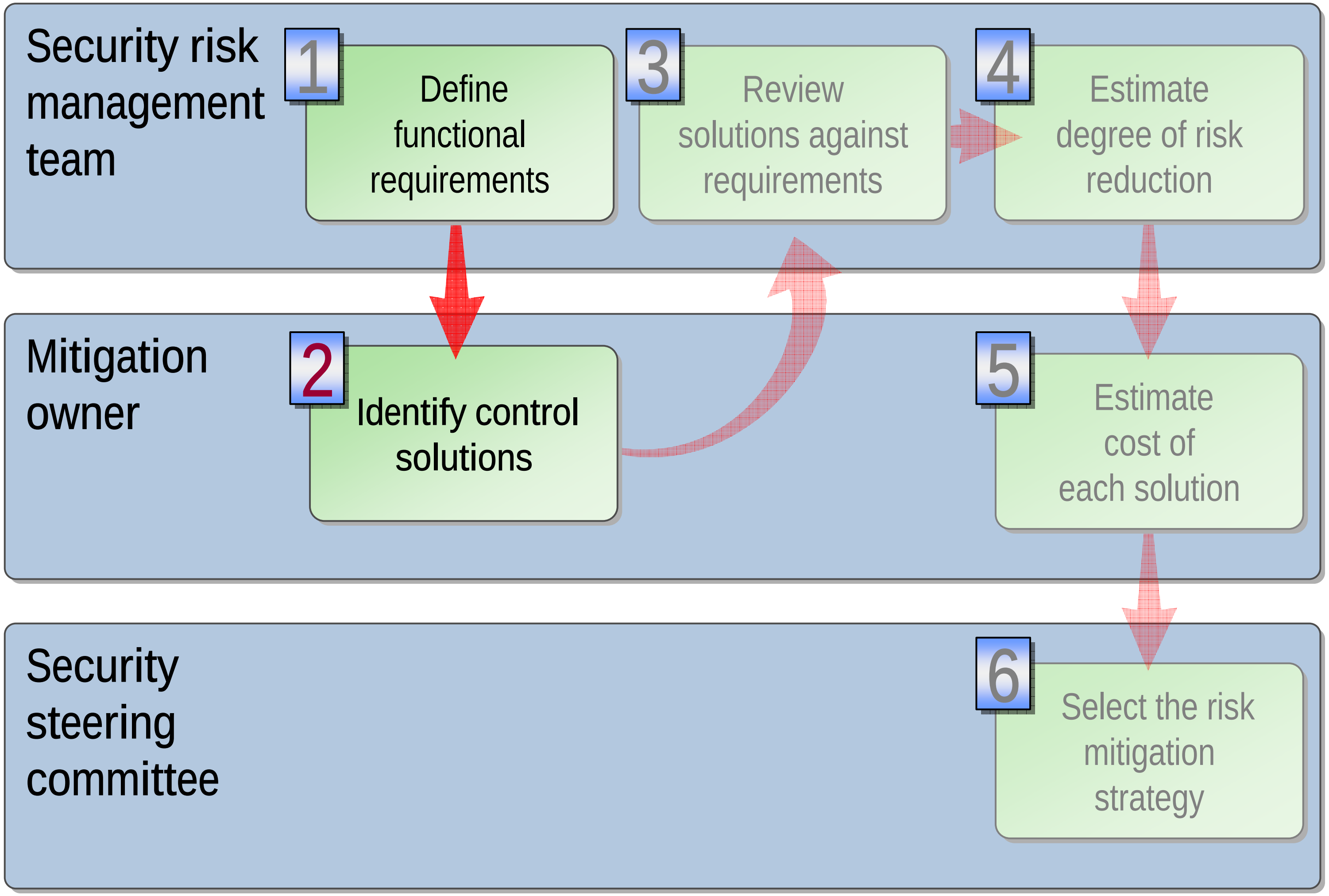
Security steering committee

- Final list of control solutions

Step 1: Define Functional Requirements

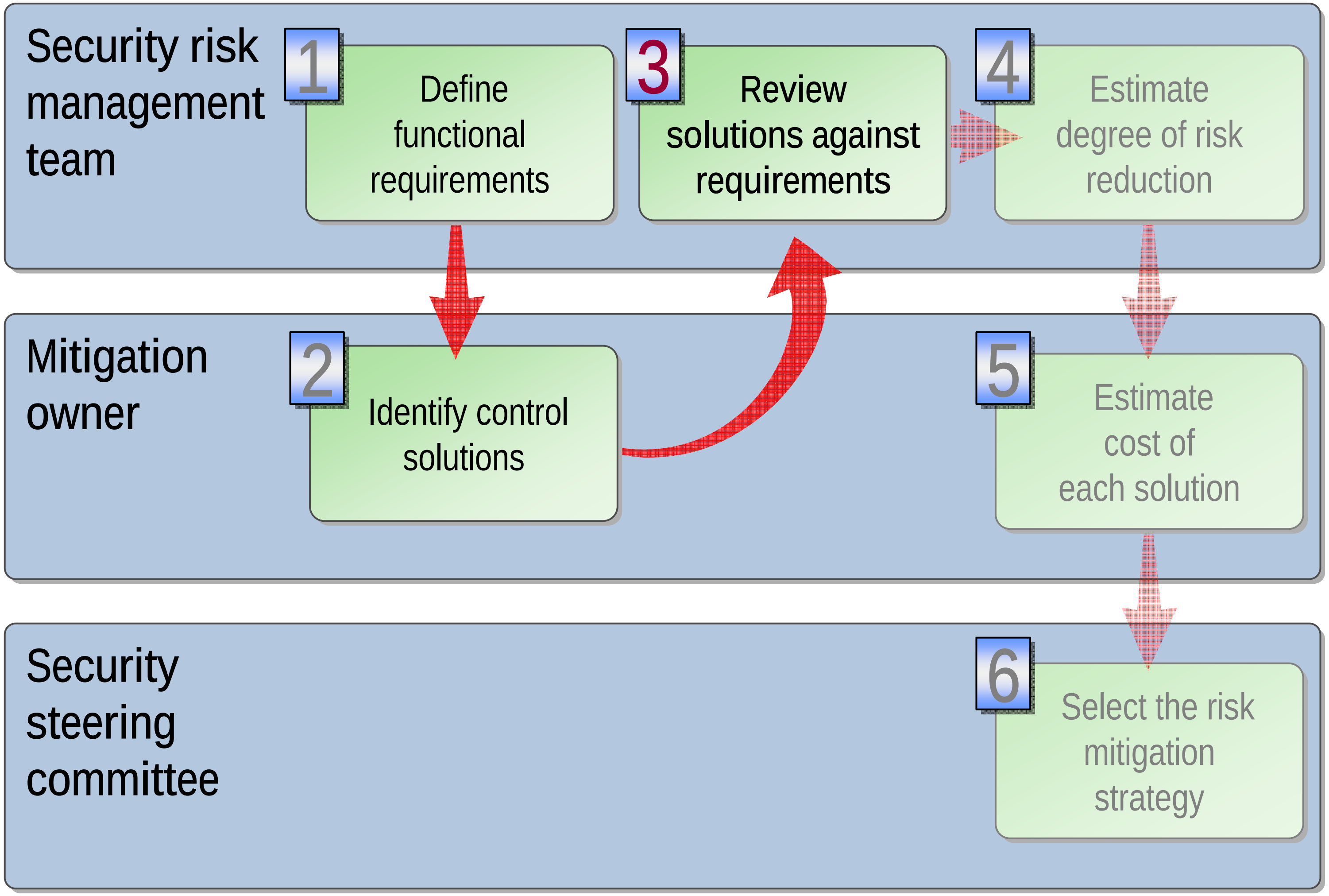

Security risk management team
Mitigation owner
Security steering committee
1
Define functional requirements
2
Identify control solutions
3
Review solutions against requirements
4
Estimate degree of risk reduction
5
Estimate cost of each solution
6
Select the risk mitigation strategy

Step 2: Identify Control Solutions



Security risk management team
1
Define functional requirements
3
Review solutions against requirements
4
Estimate degree of risk reduction
Mitigation owner
2
Identify control solutions
5
Estimate cost of each solution
Security steering committee
6
Select the risk mitigation strategy

Step 3: Review Solutions Against Requirements



Security risk management team

1 Define functional requirements

3 Review solutions against requirements

4 Estimate degree of risk reduction

Mitigation owner

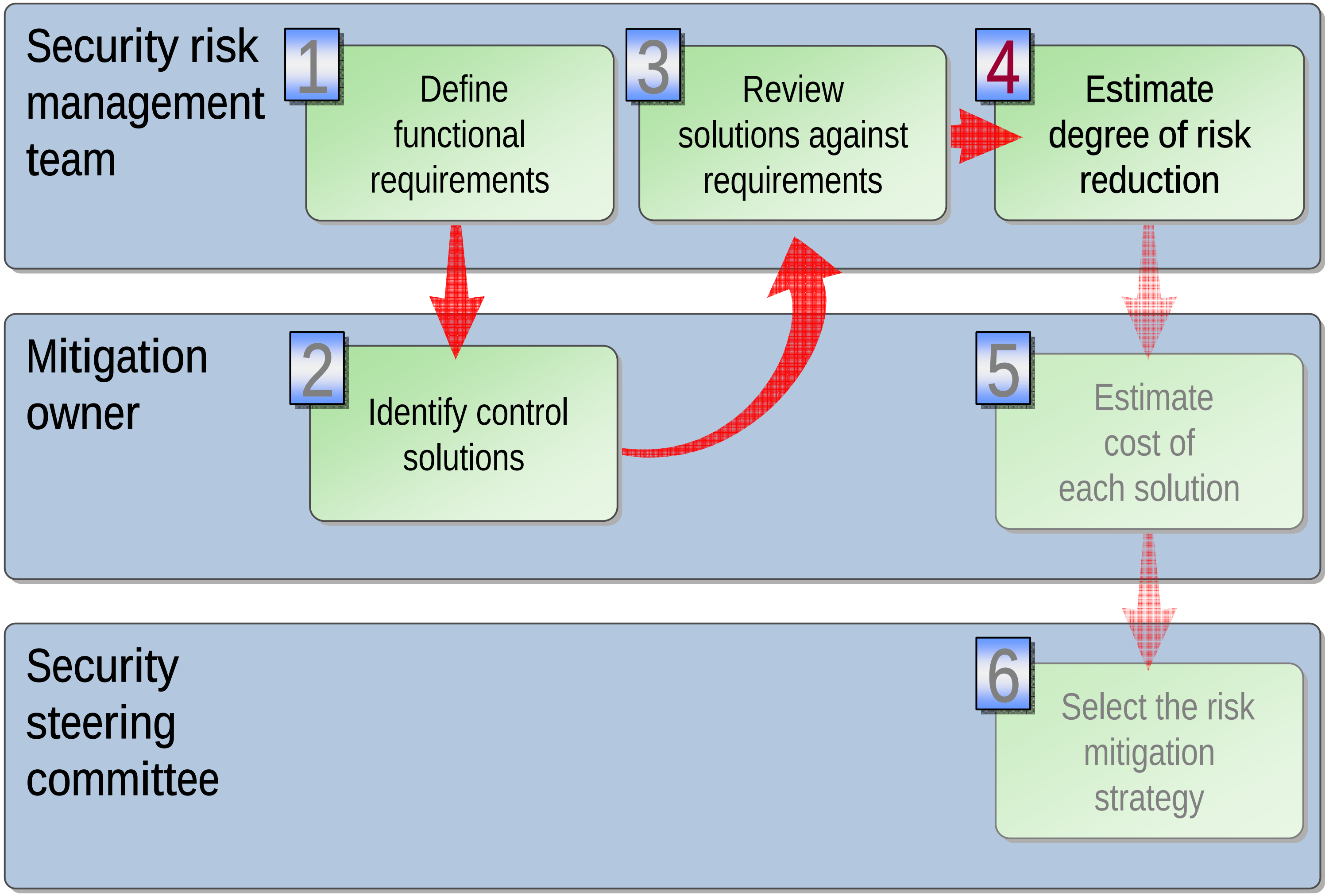
2 Identify control solutions

5 Estimate cost of each solution

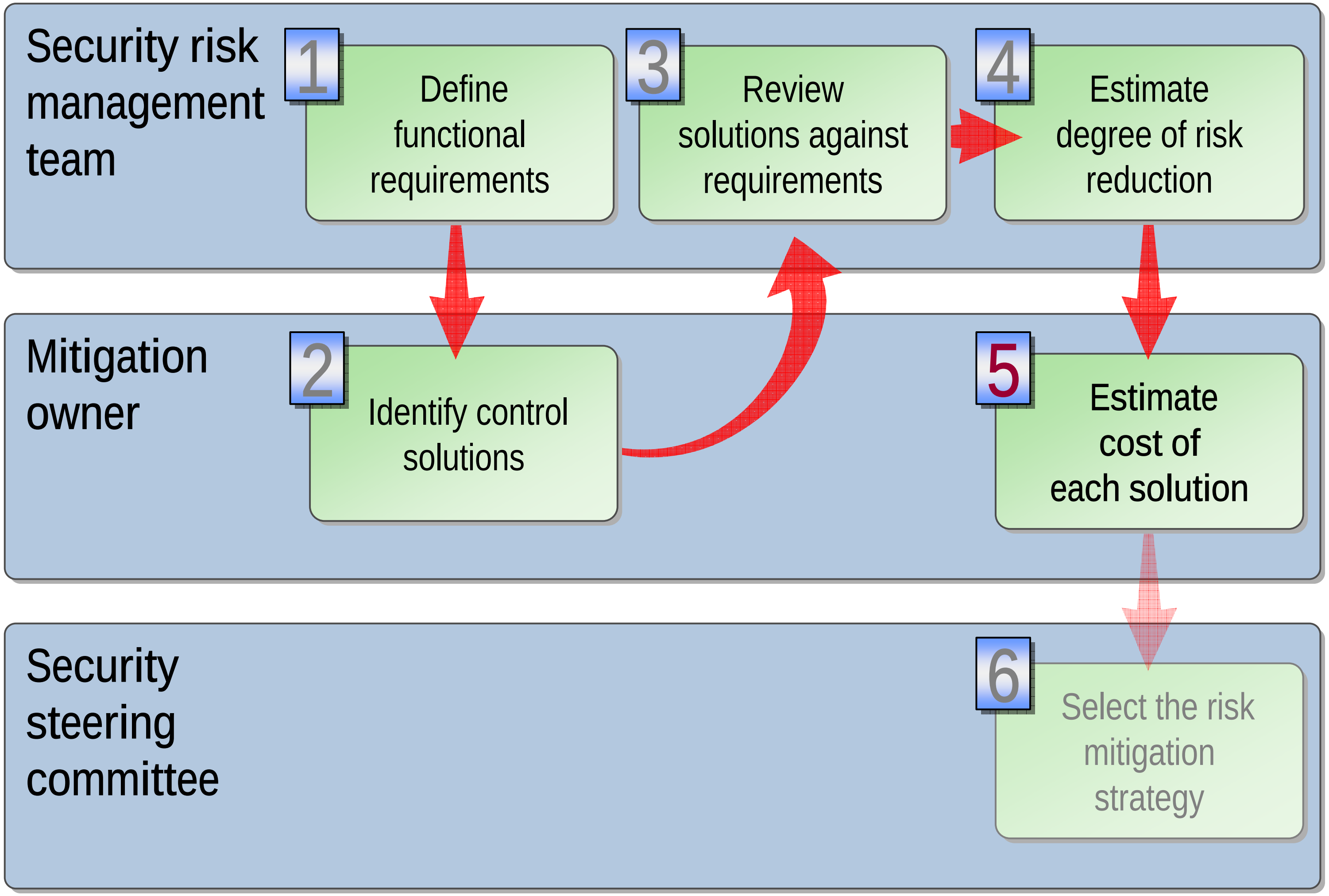
Security steering committee

6 Select the risk mitigation strategy

Step 4: Estimate Degree of Risk Reduction


Security risk management team
1
Define functional requirements
3
Review solutions against requirements
4
Estimate degree of risk reduction
Mitigation owner
2
Identify control solutions
5
Estimate cost of each solution
Security steering committee
6
Select the risk mitigation strategy

Step 5: Estimate Cost of Each Solution



Security risk management team

1 Define functional requirements

3 Review solutions against requirements

4 Estimate degree of risk reduction

Mitigation owner

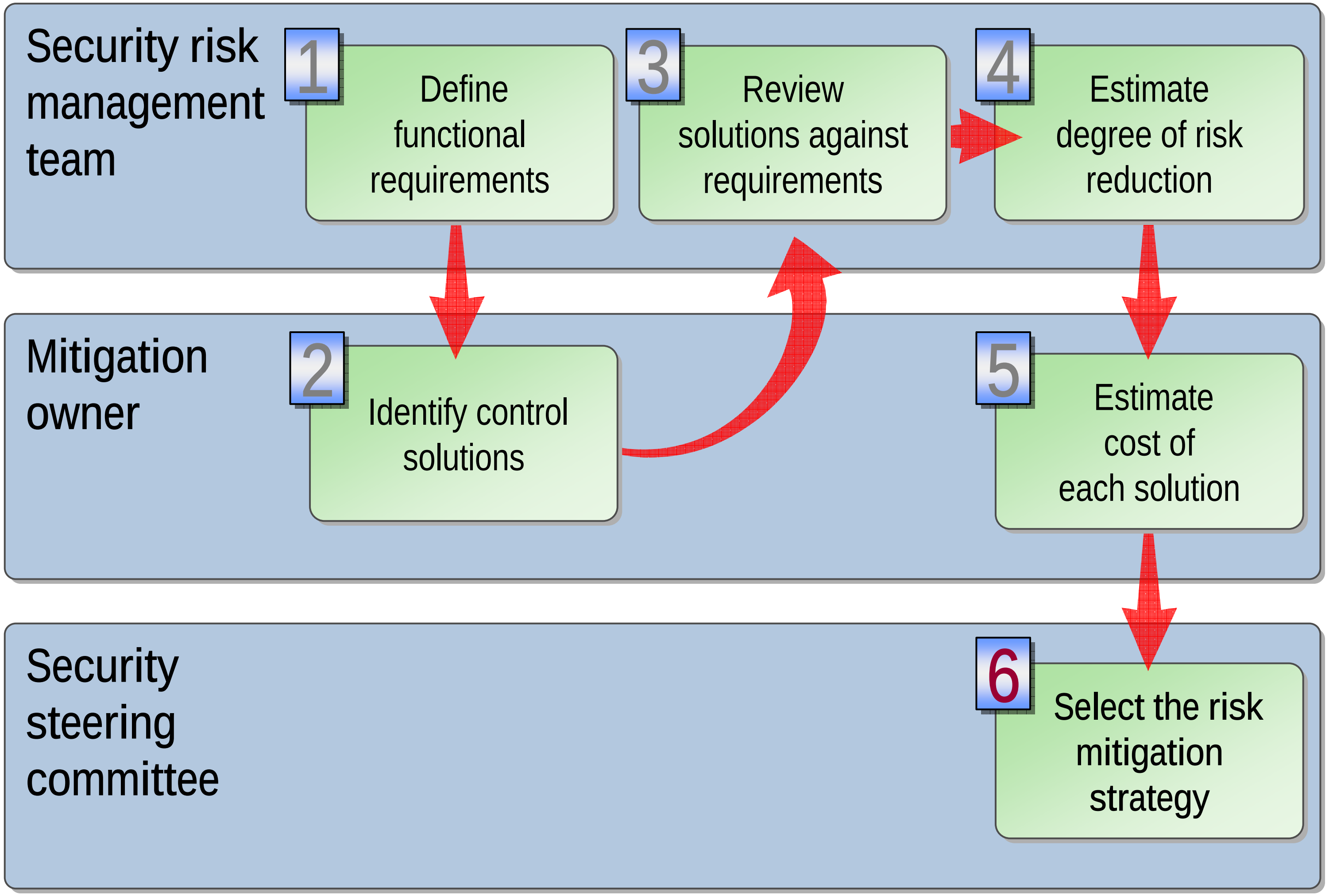
2 Identify control solutions

5 Estimate cost of each solution

Security steering committee

6 Select the risk mitigation strategy

Step 6: Select the Risk Mitigation Strategy



Security risk management team

1 Define functional requirements

3 Review solutions against requirements

4 Estimate degree of risk reduction

Mitigation owner

2 Identify control solutions

5 Estimate cost of each solution

Security steering committee

6 Select the risk mitigation strategy

Conducting Decision Support: Best Practices

- ✓ Consider assigning a security technologist to each identified risk
- ✓ Set reasonable expectations
- ✓ Build team consensus
- ✓ Focus on the amount of risk after the mitigation solution