

Risk Management



Kevin Henry

CISM CISSP CCSP

kevin@kmhenrymanagement.com

Security Principles for the CCSM Certification

Agenda:

**Information Security Concepts
and Governance**

Risk Management

Security Controls

(ISC)² Code of Ethics

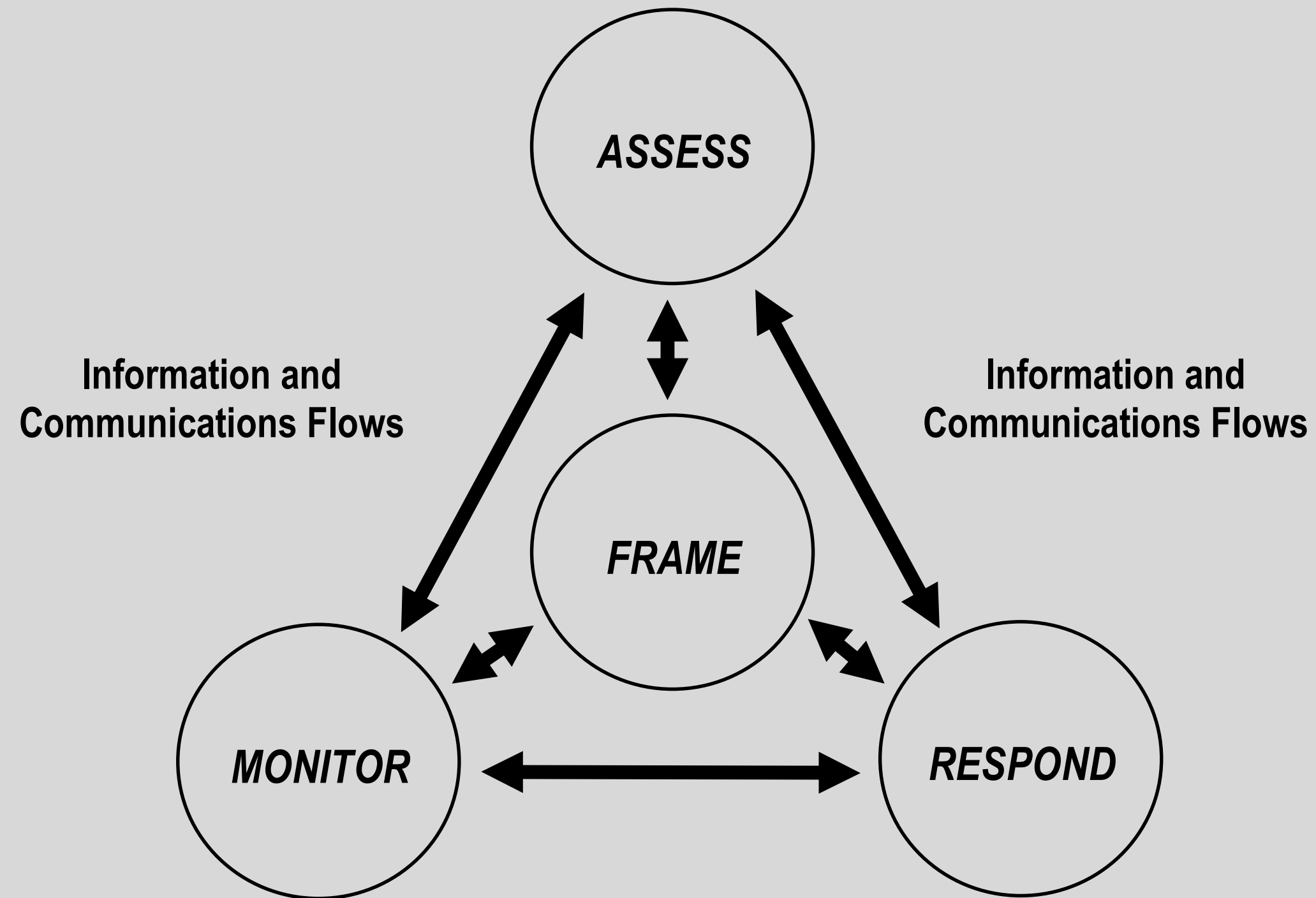
Risk

Risk is defined as the probability of an event and its consequence.

“Information security risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.”

**ISO/IEC 27005 – Information Technology –
Security Techniques – Information Security Risk Management**

Risk Management



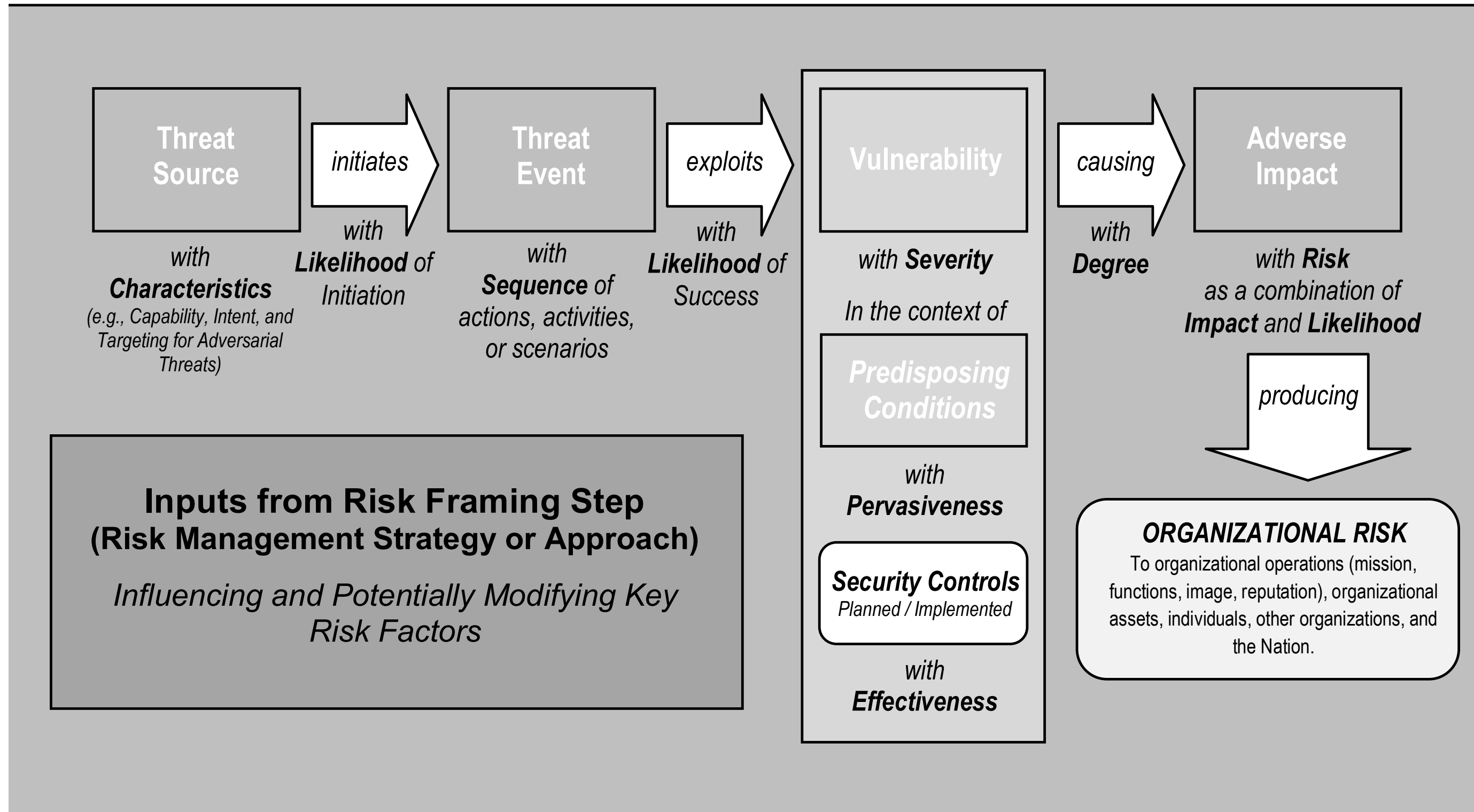


Risk Identification

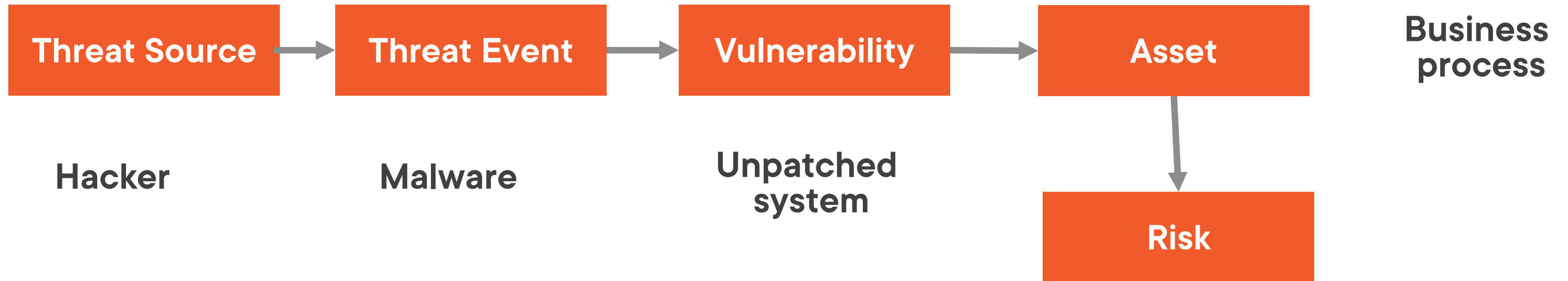
To identify the risk is to:

- Determine:
 - Asset value
 - Threats
 - Vulnerabilities
- Document controls
- Understand the consequences of risk events

NIST SP800-30r1



Risk Identification



Risk Identification/Assessment Requirements

Identify Risk

Assets

Threats

Vulnerabilities

Likelihood/probability

Impact/consequence

Risk Assessment/Analysis Results

Assess Risk

Prioritization

**Recommended actions
(response)**

Determine risk owner

**Generate Risk
Assessment Report**

Update risk register

Key Points Review

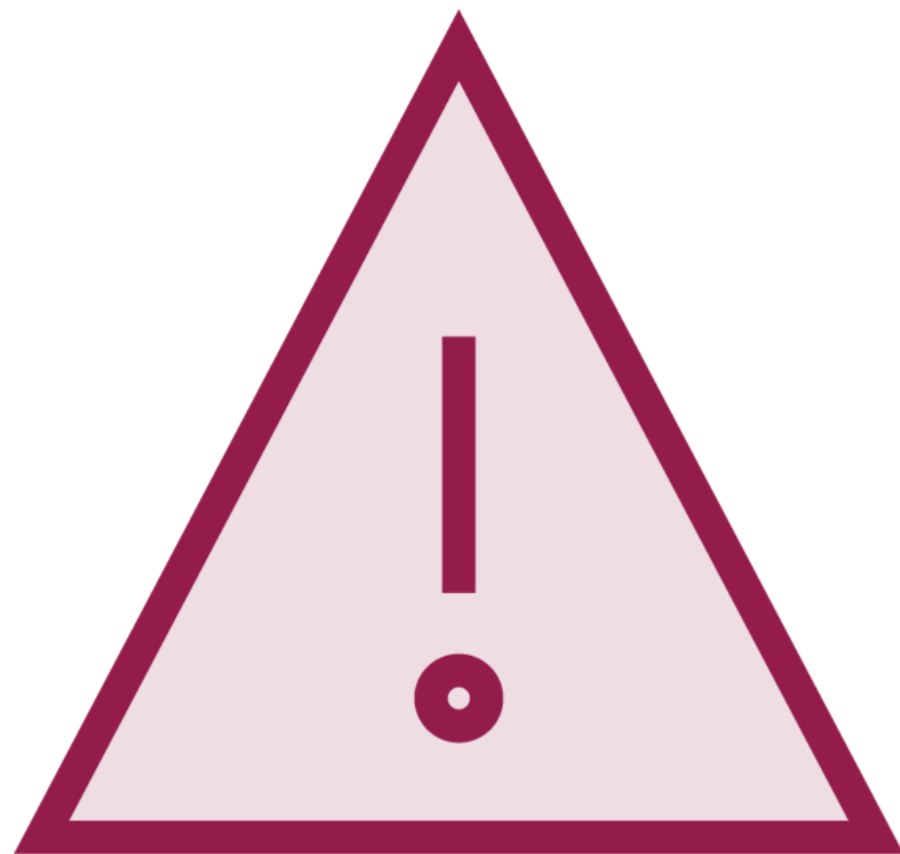


Risk management consists of several activities that may happen concurrently and consecutively

- Establishing context seeks to understand the organization
- Risk assessment identifies and prioritizes risk
- IT risk is a subset of organizational risk

Threat Modelling

Threats



Any circumstance or event with the potential to adversely impact:

- Organizational operations: including mission, functions, image, or reputation
- Organizational assets
- Individuals
- Other organizations
- Or the nation

Through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

Threat Source

Element which alone, or in combination, has the potential to give rise to risk.

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

Man-Made Threat Sources / Agents

Hostile actions

Understand the motivation, capabilities,
intent of the attacker

Know the techniques tactics and
procedures used by the adversary

Errors of omission or commission



Threat Sources



Environmental

Natural events
Power failure
Telecommunications failure
DNS failure



Structural

Equipment
Software

Threat Modelling: Attack Vectors

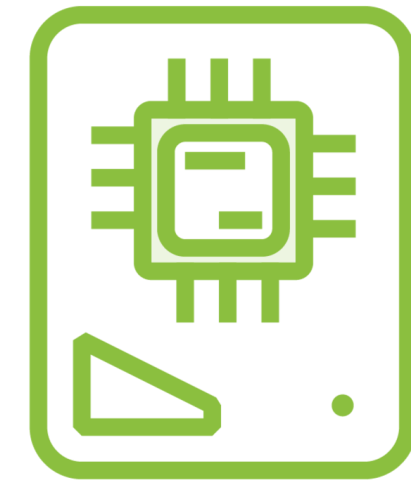
Attack surface



Facility



Network



Hardware



User inputs



Administrator interfaces



Social engineering

Key Points Review

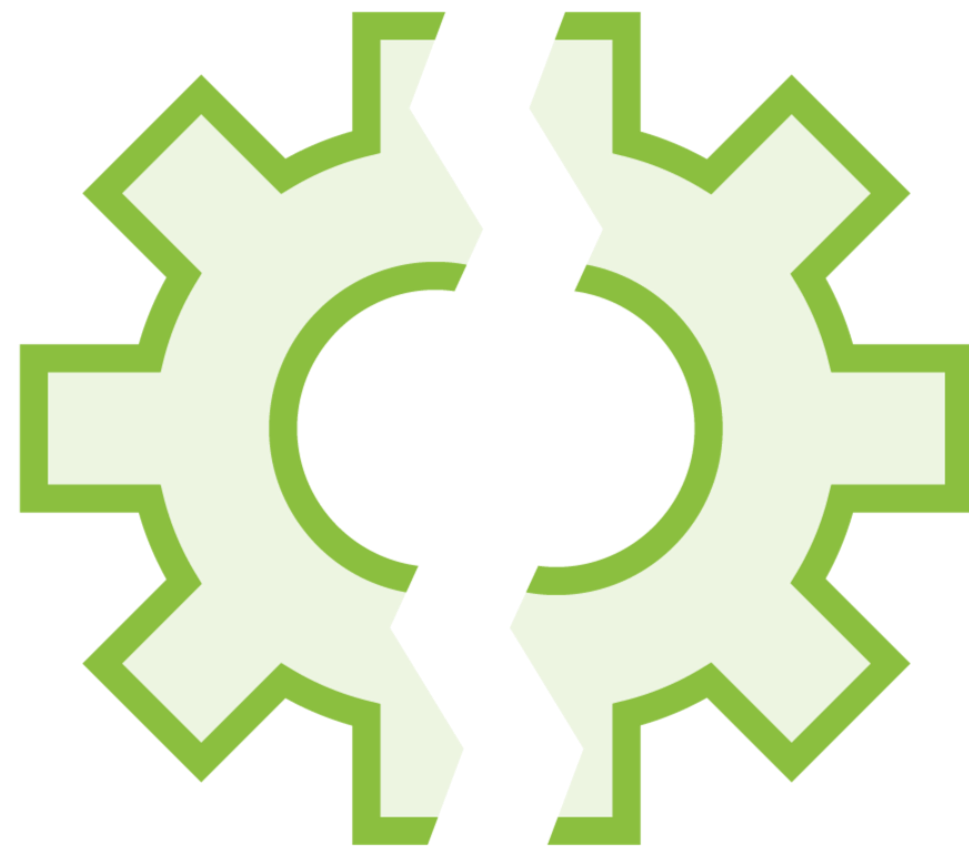


Risk Identification is a methodical, step-by-step process

- Identify assets and their value
- Perform threat modelling
- Do vulnerability assessment
- Determine likelihood and impact
- Calculate risk level
- Consider appropriate response to risk
- Communicate results

Vulnerability Assessment

Vulnerability



A weakness in

- An information system
- System security procedures
- Internal controls
- Or implementation

That could be exploited by a threat source

Vulnerability Assessment



**The process of discovering
potential points of compromise
of an IT system**

Internal or external review



**Most IT system compromises
would have been prevented if the
organization had identified and
fixed vulnerabilities that were
already known and documented**

Known Vulnerabilities

**CVSS – common vulnerability
scoring system**

**CWE – common weakness
and enumeration**

**CIS controls –
Critical security controls**

**Use of standards
Payment Card Industry**

Vulnerability Assessment

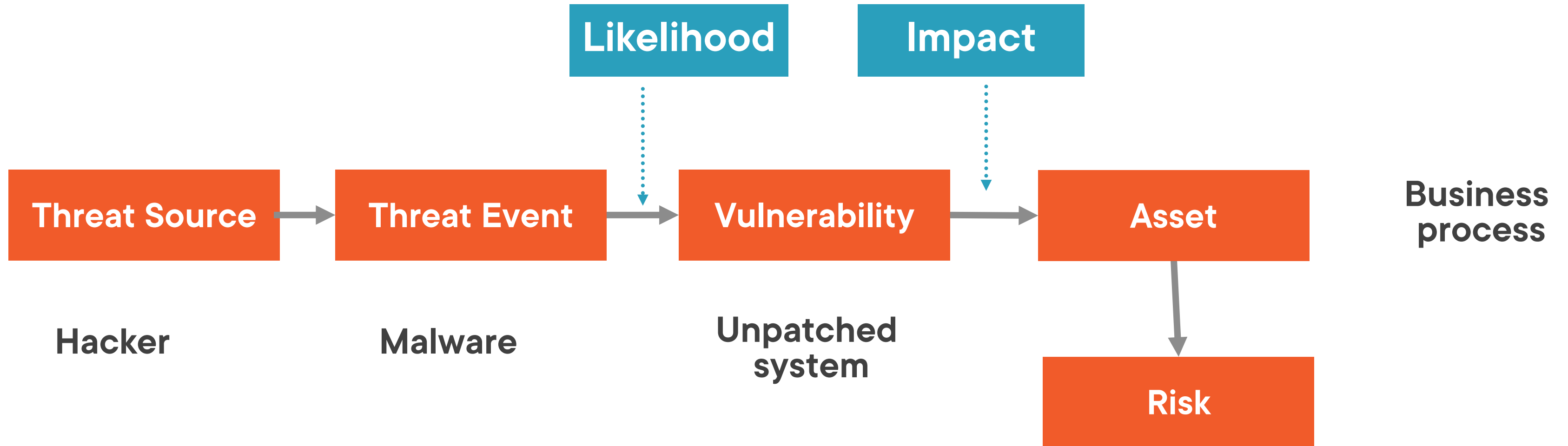


To use a military analogy, a vulnerability assessment is like the actions of a General that is going to defend a city

- First, the General should review the status of the defenses
 - Awake, alert, adequate?
- Second approach the city from the perspective of a potential attacker
 - How would an attack be conducted?
 - Threat modelling

Risk Likelihood and Impact

Risk Identification



Car Accident



Likelihood

- Risk factors and predisposing conditions
 - Condition of:
 - Tires
 - Roads (icy)
 - Driver experience and attentiveness
 - Other vehicles

Car Accident

Impact:

Ditch

Tree

Other vehicle

Risk Identification Output

A list of incident scenarios with their consequences related to assets and business processes

Key Points Review



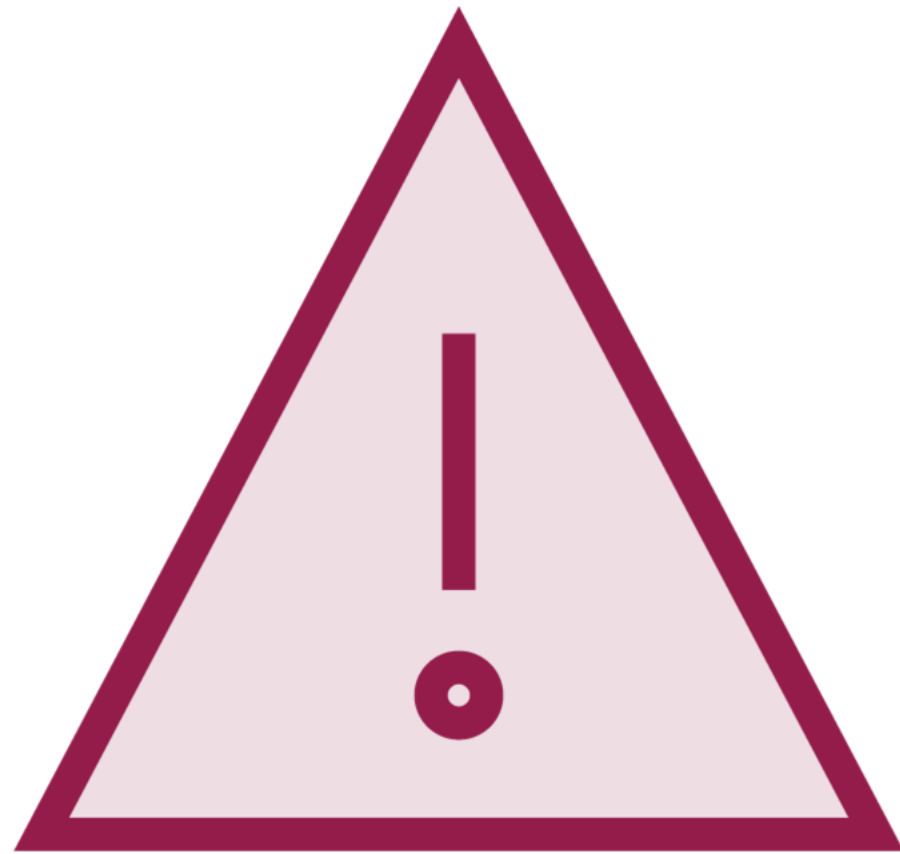
Risk assessment is the foundation of good IT security

- Justifies controls
- Informs management
- Demonstrates/measures compliance

The results of the risk assessment are the foundation of risk treatment or risk response

Risk Treatment / Risk Response Options

Risk Response



Risk Acceptance

Risk Avoidance

Risk Transference

Risk Mitigation / Reduction

Risk Ownership

**“If it’s nobody’ job,
nobody does it”**

**Each risk should be
communicated to
management and a
risk owner identified**

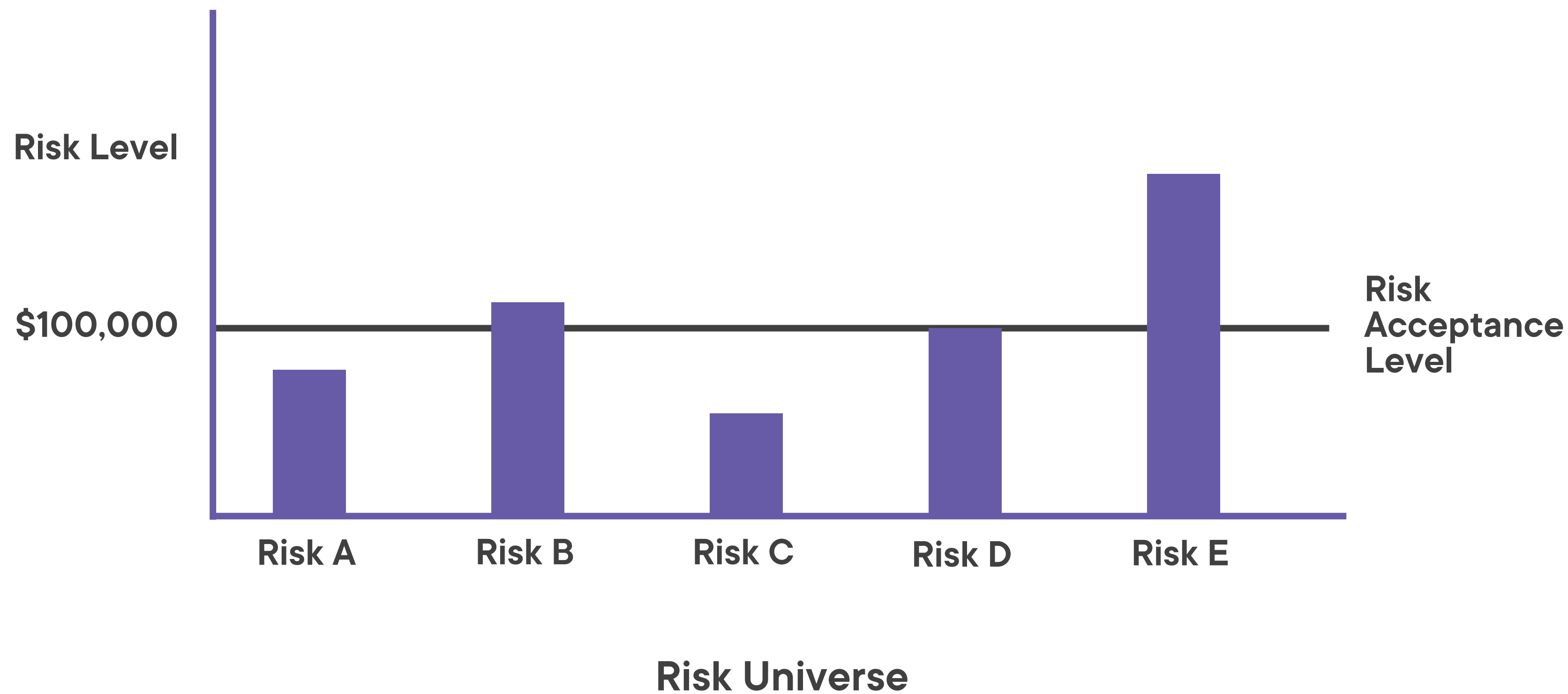
**The risk owner
determines the
appropriate response
to the risk**

**Accept, avoid,
transfer, reduce**

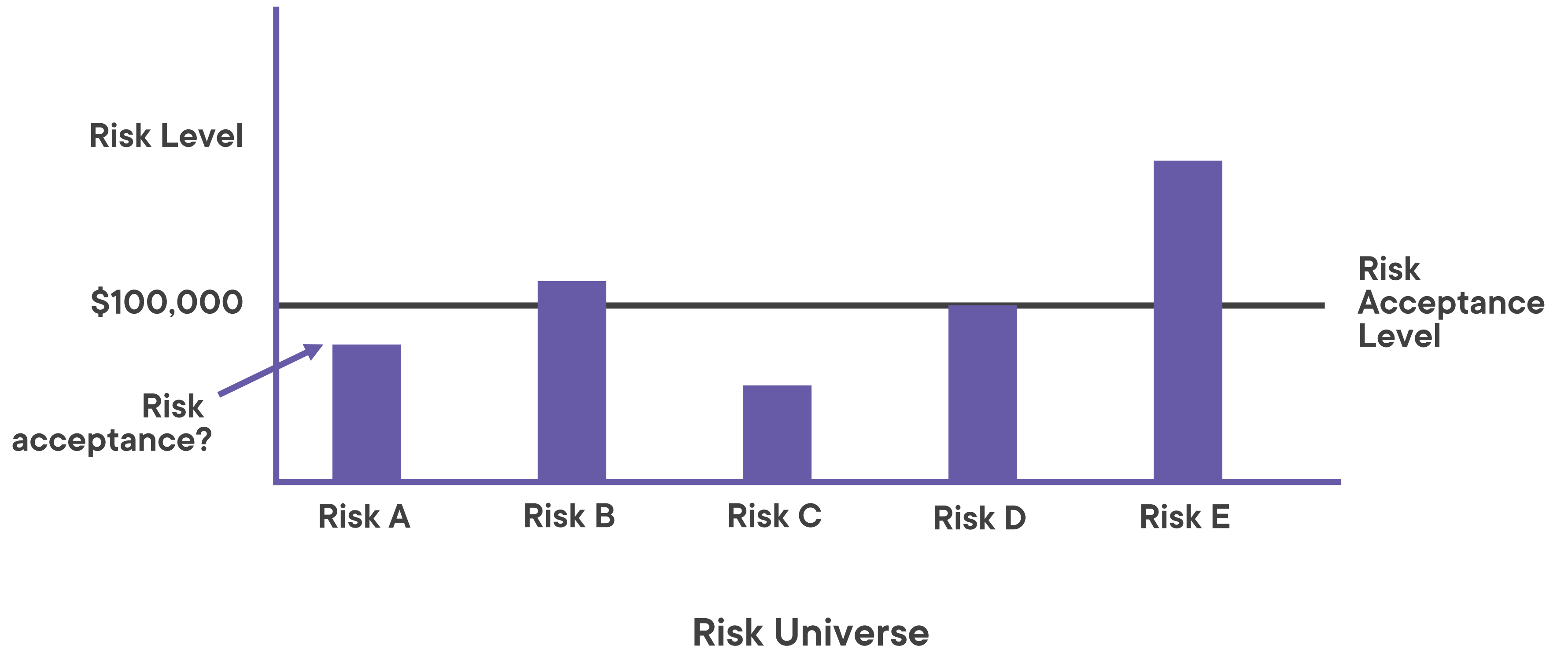
Risk Acceptance

The level of risk senior management (the risk owner) is willing to tolerate

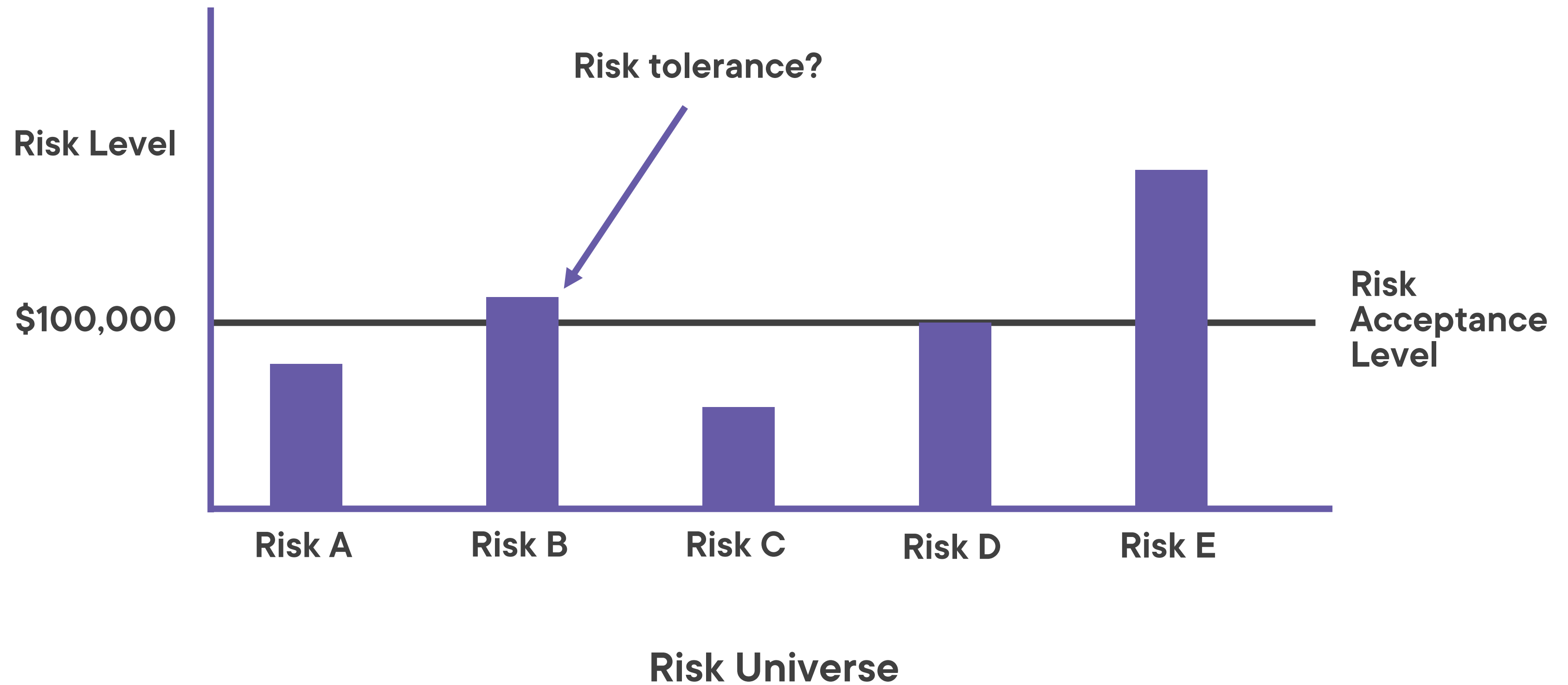
Risk Acceptance



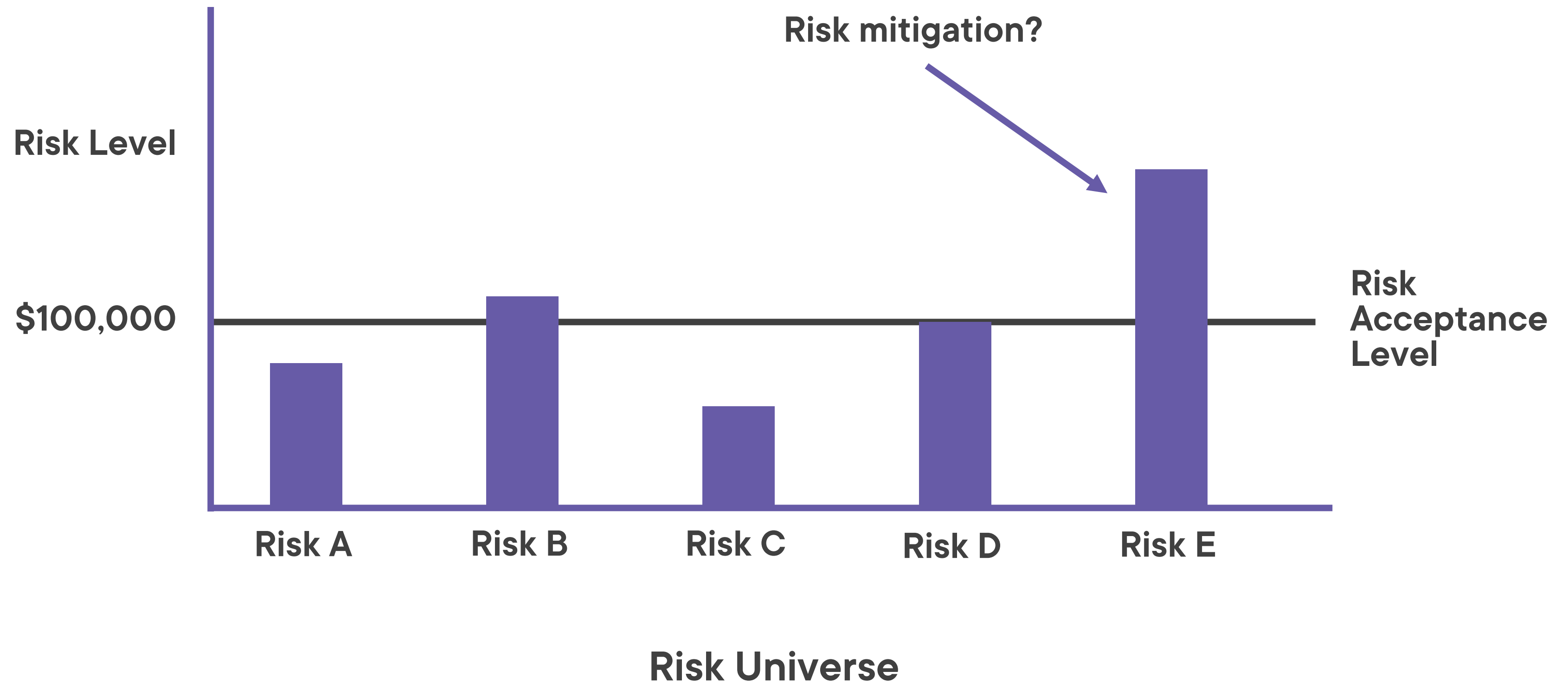
Risk Acceptance



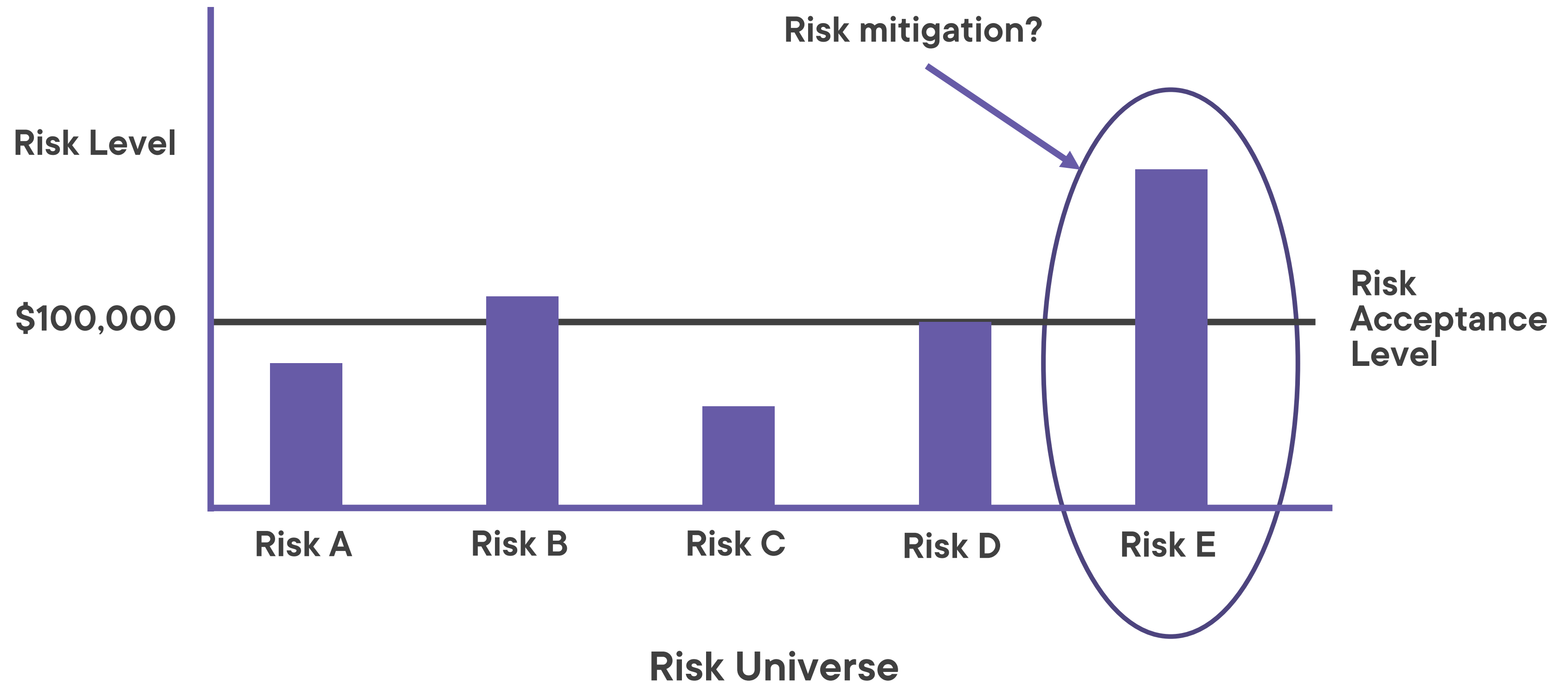
Risk Tolerance



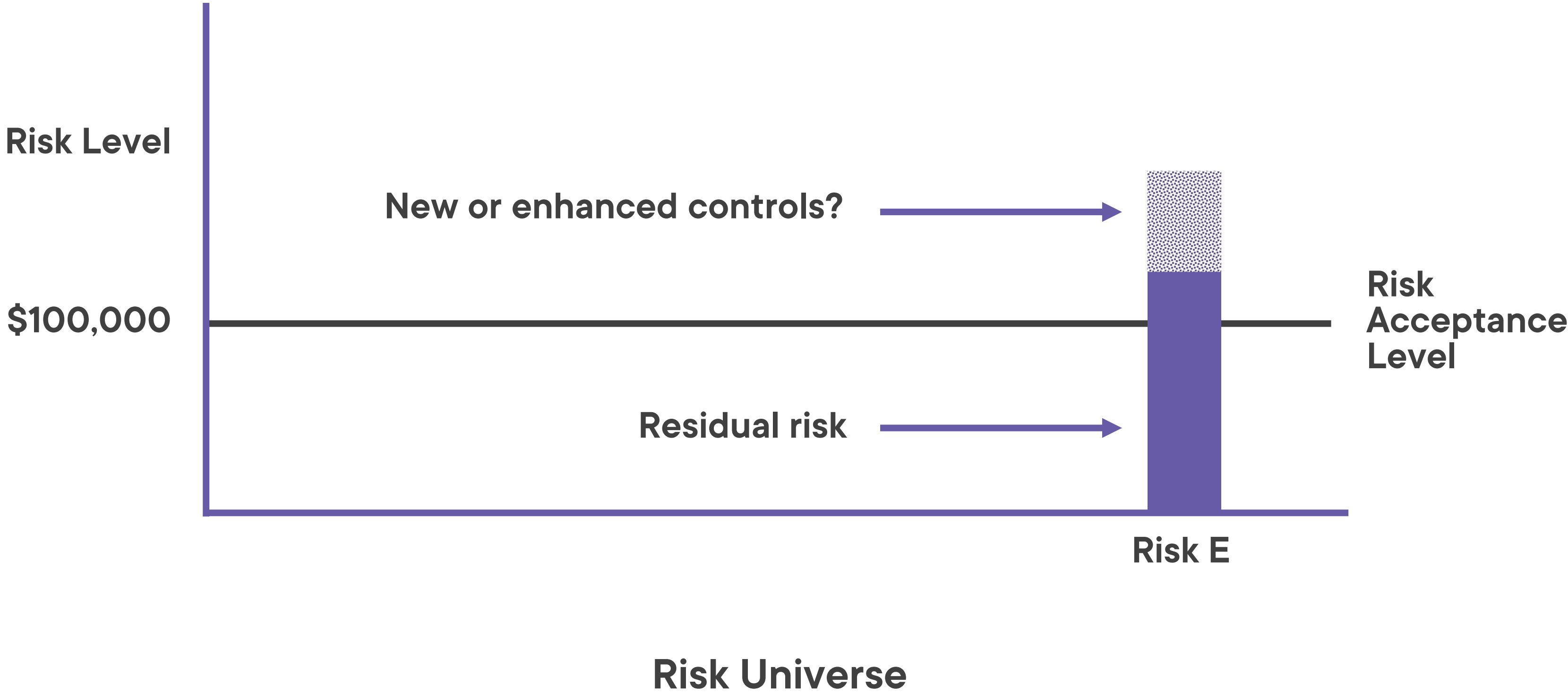
Risk Acceptance



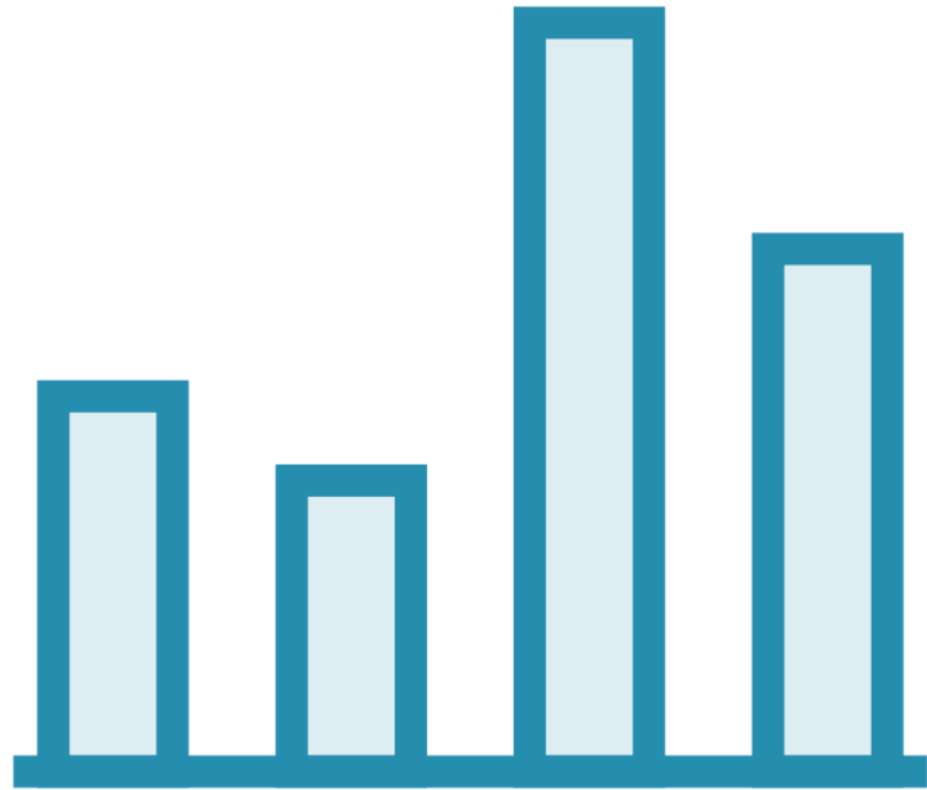
Risk Acceptance



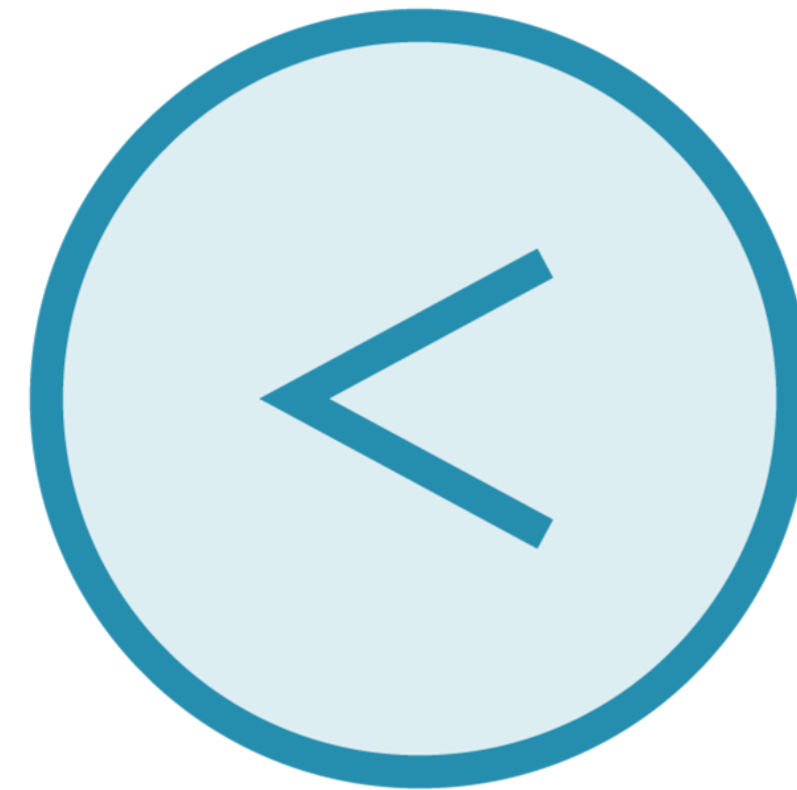
Risk Reduction



Residual Risk

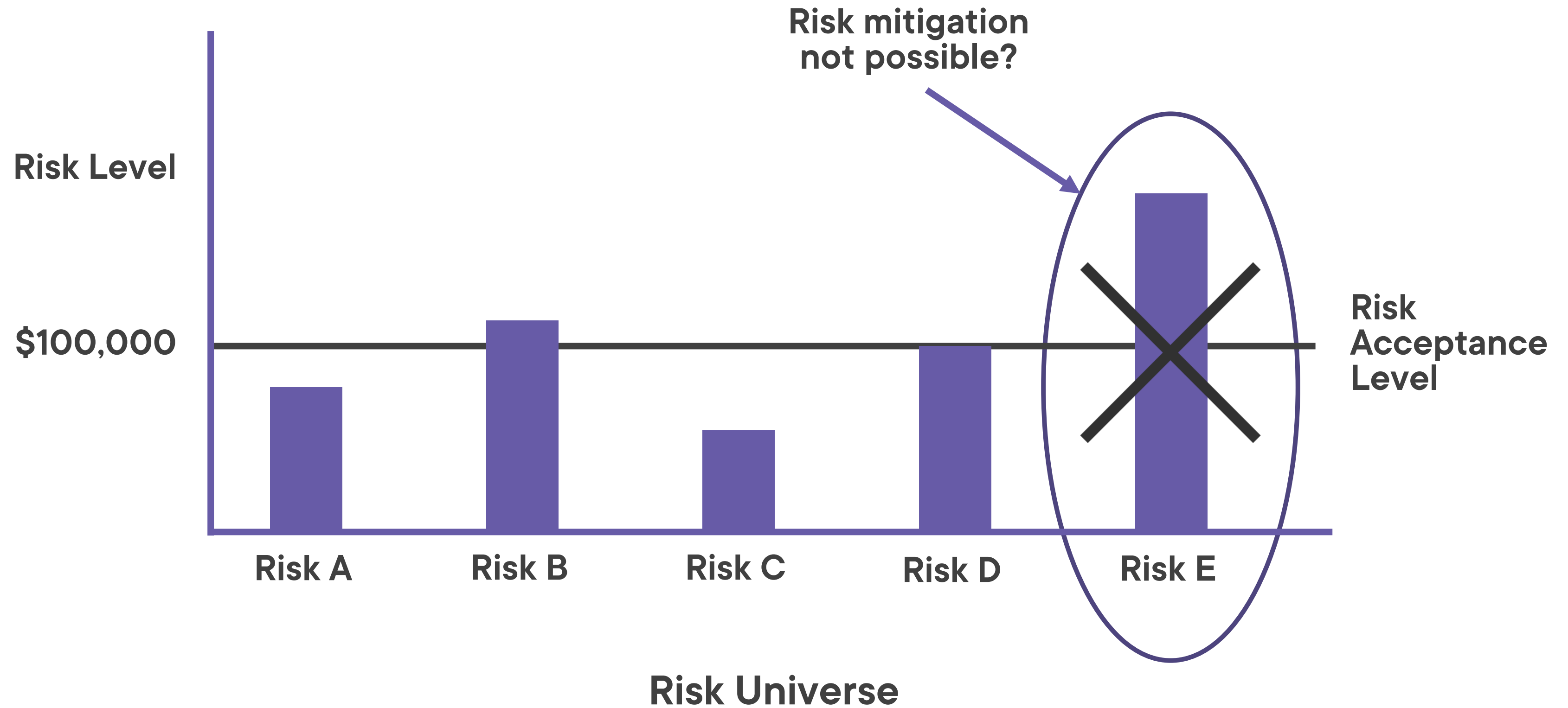


The level of risk that remains after the implementation of control(s)

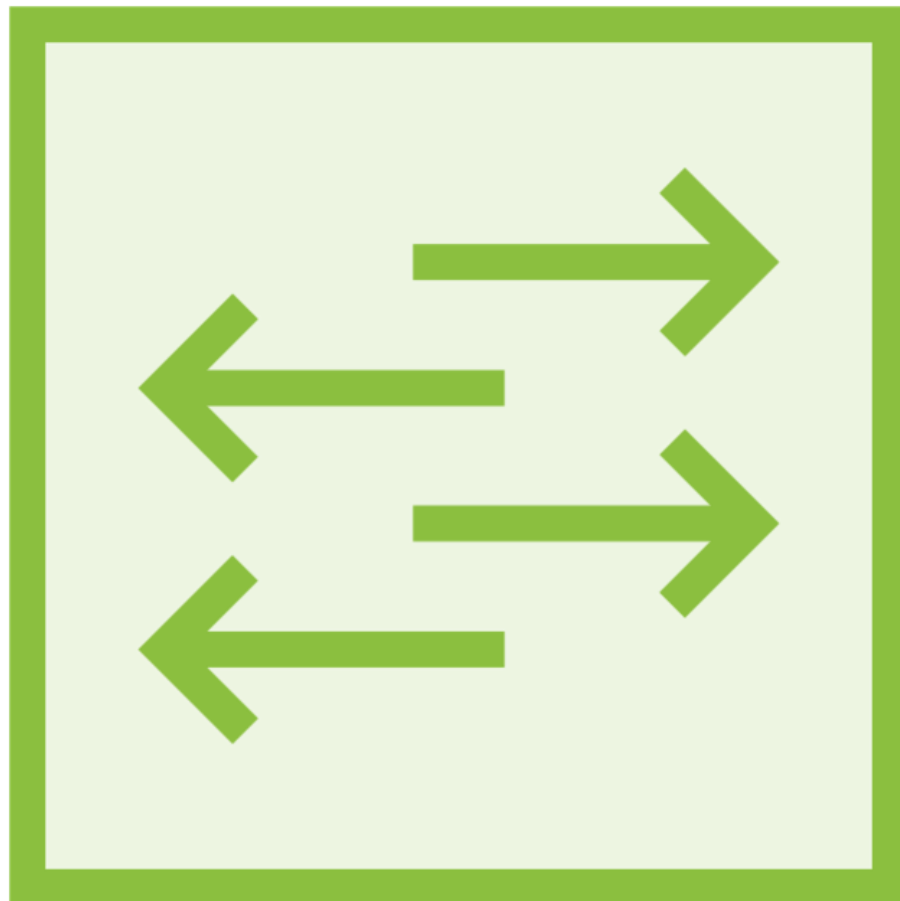


The goal is that residual risk is less than or equal to risk acceptance

Risk Avoidance



Risk Transference



To transfer some of the risk to another party

- Insurance

To share the risk with another party

- Joint venture
- Financial investment

Monitoring Risk



Logs:

- System monitoring
 - Security Information and Event Management (SIEM) tools
- Threat intelligence feeds
- Vulnerability Assessments
- Penetration Testing
- Alerts and Alarms

Key Points Review



The level of risk acceptance sets out the baseline for the appropriate level of risk

A goal of risk management is to ensure that residual risk is less than or equal to the risk acceptance level set by the risk owner

Learning Objectives

**Information Security Risk
Assessment**

**Information Security Risk
Response**

Key Risk Management Points Review

Key Points



**Information Security
Risk is a subset of
business risk**



**Align with business'
risk management
program**



**Use Risk Management to
protect Information,
Information Systems
and Business Operations**

Risk Assessment

Identify Risk

Prioritize Risk

Risk Assessment



Threat modeling

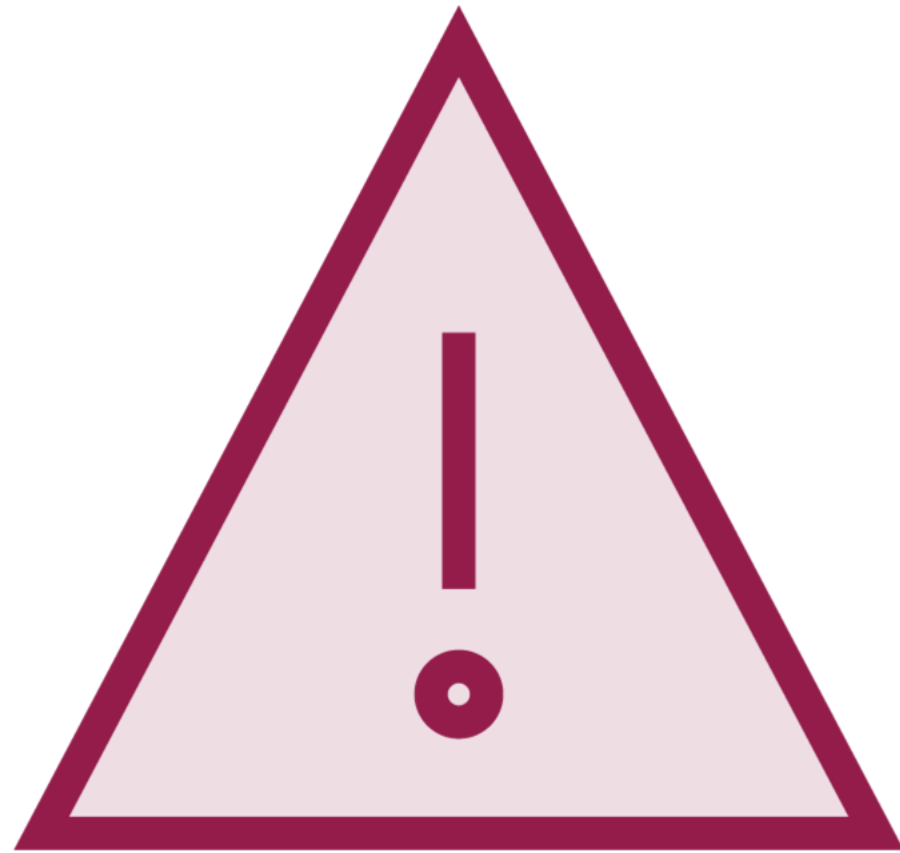


**Vulnerability
Identification**



**Assess Control
Effectiveness**

Risk Response



Risk Acceptance

Risk Avoidance

Risk Transference

Risk Mitigation / Reduction

Communicate Risk



Risk Register

Risk Monitoring

Emerging risk

Control Effectiveness