J. A. "Drew" Hamilton, Jr., Ph.D.

Chair, NSA Cyber Operations Community of Practice

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

This work funded by NSA Contract #H98230-19-1-0291

CCI
2 Research Blvd.
Starkville, MS 39759

Voice: (662) 325-2294
Fax: (662) 325-7692
drew@drew-hamilton.com

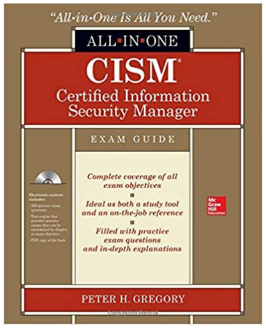
Domain 2
Information Risk Management

References:

Drew Hamilton Lecture Notes

CISM Review Manual, 15th Edition

CISM All-in-One Exam Guide, 1st Edition


"All-in-One Is All You Need."
ALL•IN•ONE
CISM
Certified Information Security Manager
EXAM GUIDE
Complete coverage of all exam objectives
Ideal as both a study tool and an on-the-job reference
Filled with practice exam questions and in-depth explanations
PETER H. GREGORY

Domain 1 Outline

- Risk Management Overview
- Risk Management Strategy
- Effective Information Risk Management
- Implementing Risk Management
- Risk Assessment
- Information Asset Classification
- Operational Risk Management
- Security Control Baselines
- Risk Monitoring and Communication

Risk Management Overview

Domain 2
Information Risk Management

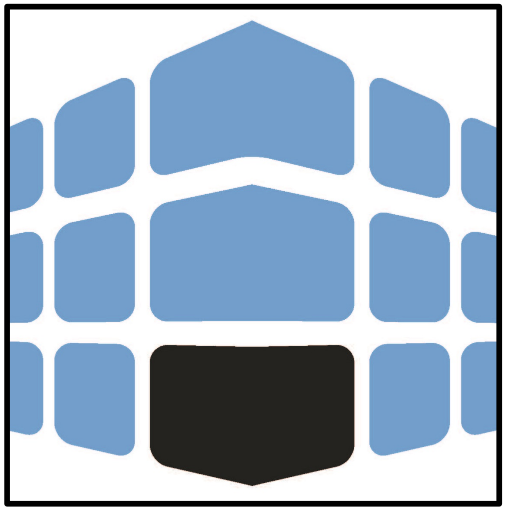
Risk Management Concepts

Risk Management is being reasonably aware of the risks to your organization that could cause unexpected harm and managing those risks

The goal for risk management is to identify threats to your organization and decide on the best way to handle those threats

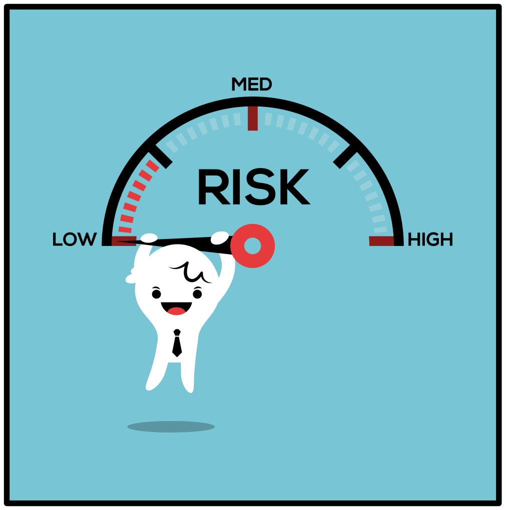
Organizations with proper risk management programs have experienced fewer security incidents and the organization is better prepared for those incidents that do happen, lowering the impact of security incidents

The Importance of Risk Management



Risk Management is the cornerstone of any information security program

Risk Management provides key information that enables the security managers and organization's executives to prioritize scarce resources in away that results in the greatest possible risk reduction



The Importance of Risk Management

Risk Management implements methods and techniques that:

- Identify risks
- Helps those responsible judge the probability of those risks occurring
- Understand the potential impact of those risks
- Measure key attributes of security and risk for long-term trending and for reporting to executive management

The Importance of Risk Management

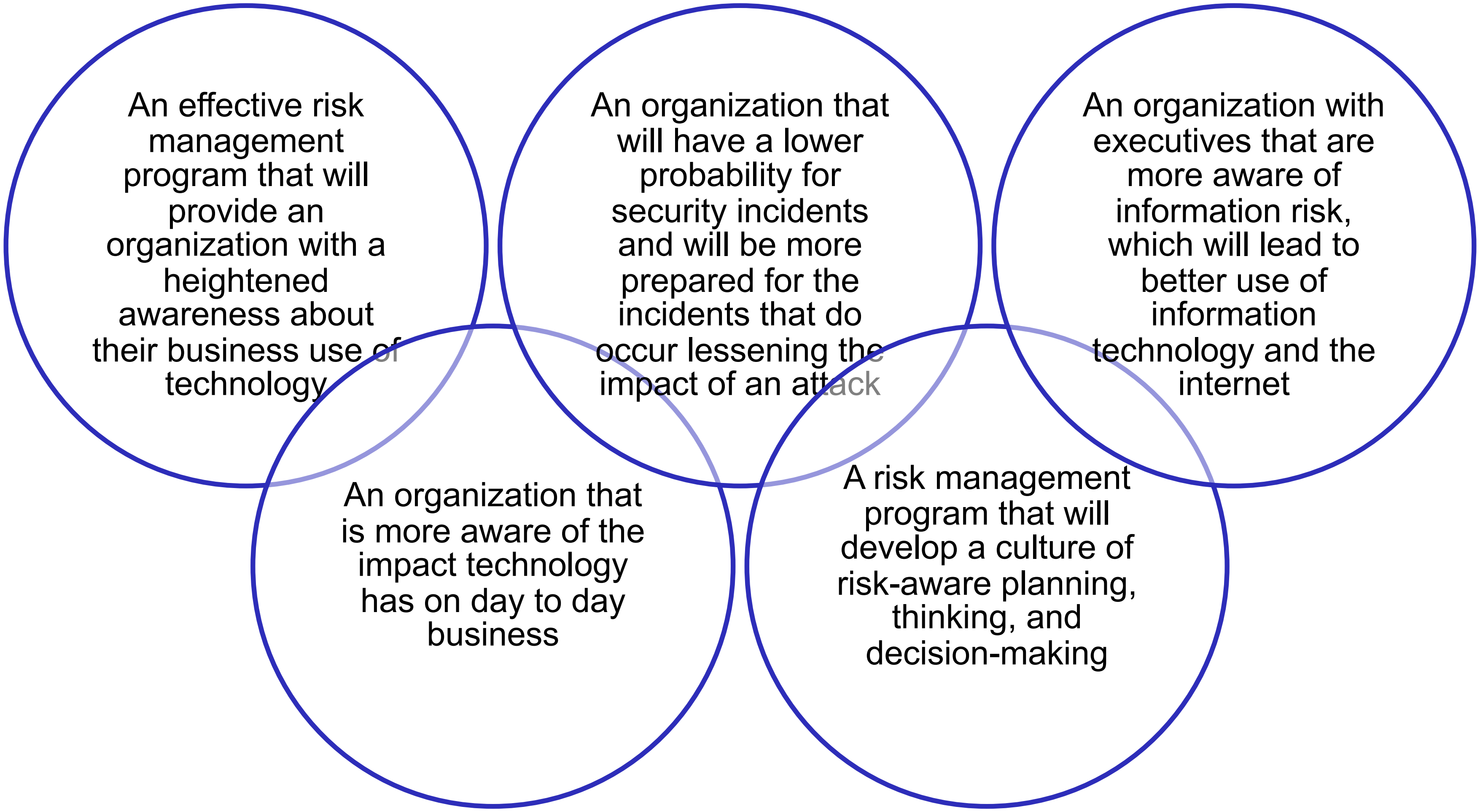
The effectiveness of risk management depends on two factors:

- Executive Management Support
- An Organization's culture that has respect for security awareness and accountability

Each risk management program is different based on several factors:

- Culture
- Mission, objectives, and goals
- Management structure
- Management support
- Industry sector
- Market conditions
- Applicable laws, regulations, and other legal obligations
- Stated or unstated risk tolerance
- Financial health

Outcomes of Risk Management



An effective risk management program that will provide an organization with a heightened awareness about their business use of technology

An organization that will have a lower probability for security incidents and will be more prepared for the incidents that do occur lessening the impact of an attack

An organization with executives that are more aware of information risk, which will lead to better use of information technology and the internet

An organization that is more aware of the impact technology has on day to day business

A risk management program that will develop a culture of risk-aware planning, thinking, and decision-making

Risk Management Strategy

Domain 2
Information Risk Management

Risk Management Strategy

Risk Management Strategy is the plan to meet the goals of the risk management objectives

The goals of the risk management objectives are to recognize all possible risks and reduce those risks to an acceptable level

An acceptable level of risk is often related to these factors:

- The ability to absorb losses, as well as the ability to build defenses
- Management's risk appetite
- The costs to develop acceptable risk levels
- The risk-benefit ratios

Risk Management Strategy

Risk Tolerance is an organization's acceptable level of risk

Establishing a level of risk tolerance will drive the implementation and refinement of the controls

- Controls are the primary means for mitigating risks

There is a negative stigma toward most IT teams within an organization

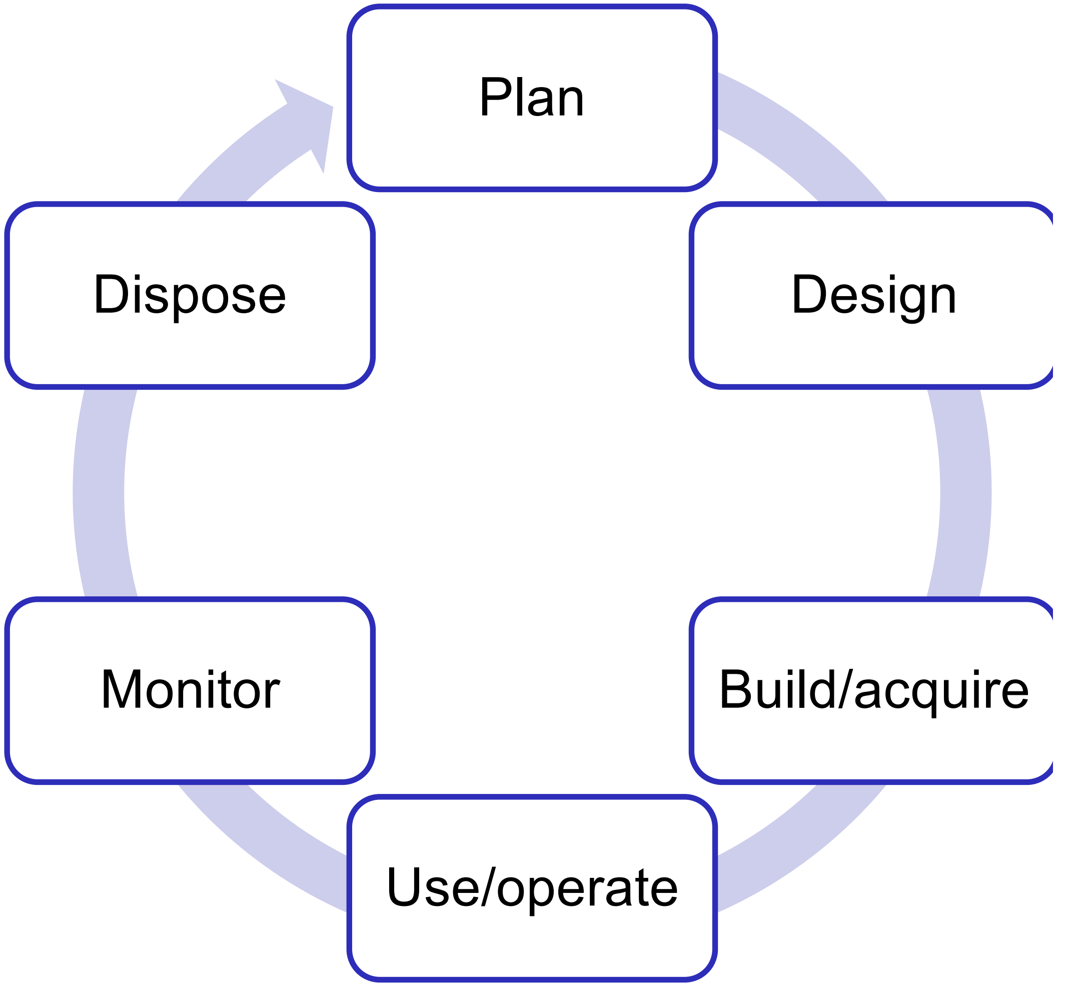
Risk Management originates from the IT group in most cases

Foster a relationship with business leaders and the IT team

Risk Communication

Risk Communication Plan

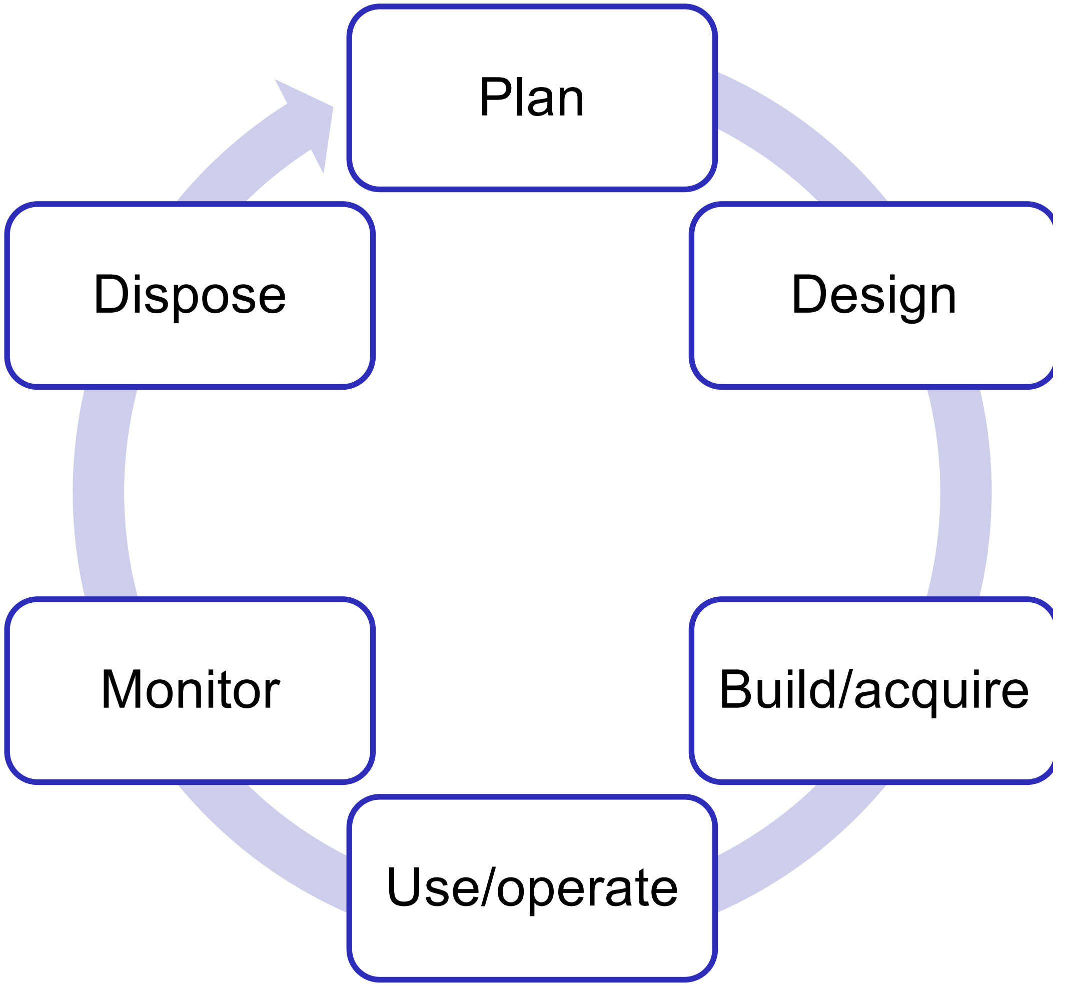
- Its purpose is to define information about risk without causing an overload of non-relevant information
- Life Cycle
  - Plan:
    - Develop a plan were risks are communicated quickly and effectively
  - Design
    - Outline the different aspects of the risk communication plan to ensure risks and their impact are clearly communicated
  - Build/acquire
    - Develop details of each outlined aspect of the risk communication plan
  - Use/operate
    - Effectively using the risk communication plan to ensure risks are communicated correctly and concisely to the stakeholder



Risk Communication

Risk Communication Plan

- Its purpose is to define information about risk without causing an overload of non-relevant information
- Life Cycle
  - Monitor
    - Monitor the status of risks to ensure actions are being taken in a timely manner
    - Validate the risk communication plan regularly
  - Dispose
    - Securely dispose of information in a timely manner to avoid potential risks



Risk Awareness

Risk awareness is shaping the ethical culture of an organization.

- Knowing what should be done
- Knowing why it should be done
- Knowing how it should be done

Changing the culture of an organization starts with upper management understanding the need for risk awareness and being a good example

- Provide annual risk awareness training
- Judge the level of risk awareness with quizzes or surveys

Risk Awareness

Risk and security awareness programs should have periodic testing to judge the level of awareness

Testing employees knowledge

Receiving feed back from employees on possible risk and security issues

More often than not, employees of an organization are aware of the issues

Make it possible for employees to communicate their concerns

If everyone is working to identify and report risks and security issues this will make risk management a team approach

This will enable faster response of risks and the ability to more quickly contain the risk

Risk Awareness

Not all risks can be avoided or eliminated but:

Risks can be understood and identifiable

Employees can be made aware of the effect an organization at risk can have on them personally

Upper management can acknowledge and utilizes means to manage risks to the organization

Risk Awareness program can and should be made for each individual group

The accounting department will see risks at a different level than those that work in IT

Do not disclose your organizations vulnerabilities or ongoing investigation

Instead describe resolved problems your organization and other organizations have experienced in the past

This will reinforce the need for each individual to do their own part when addressing risks

Risk Awareness

Senior management should be aware that they are responsible for the risks and knowing the acceptable level of risk

Managers are responsible for monitoring the actions of their employees and ensuring compliance with defined policy and procedures

Employees cannot be held responsible for not following policies or procedures they are not aware of

- Ensure employees take risk awareness training annually
- Test employees to measure the effectiveness of the risk awareness training

Risk Consulting

Security managers can be viewed as security and risk consultants

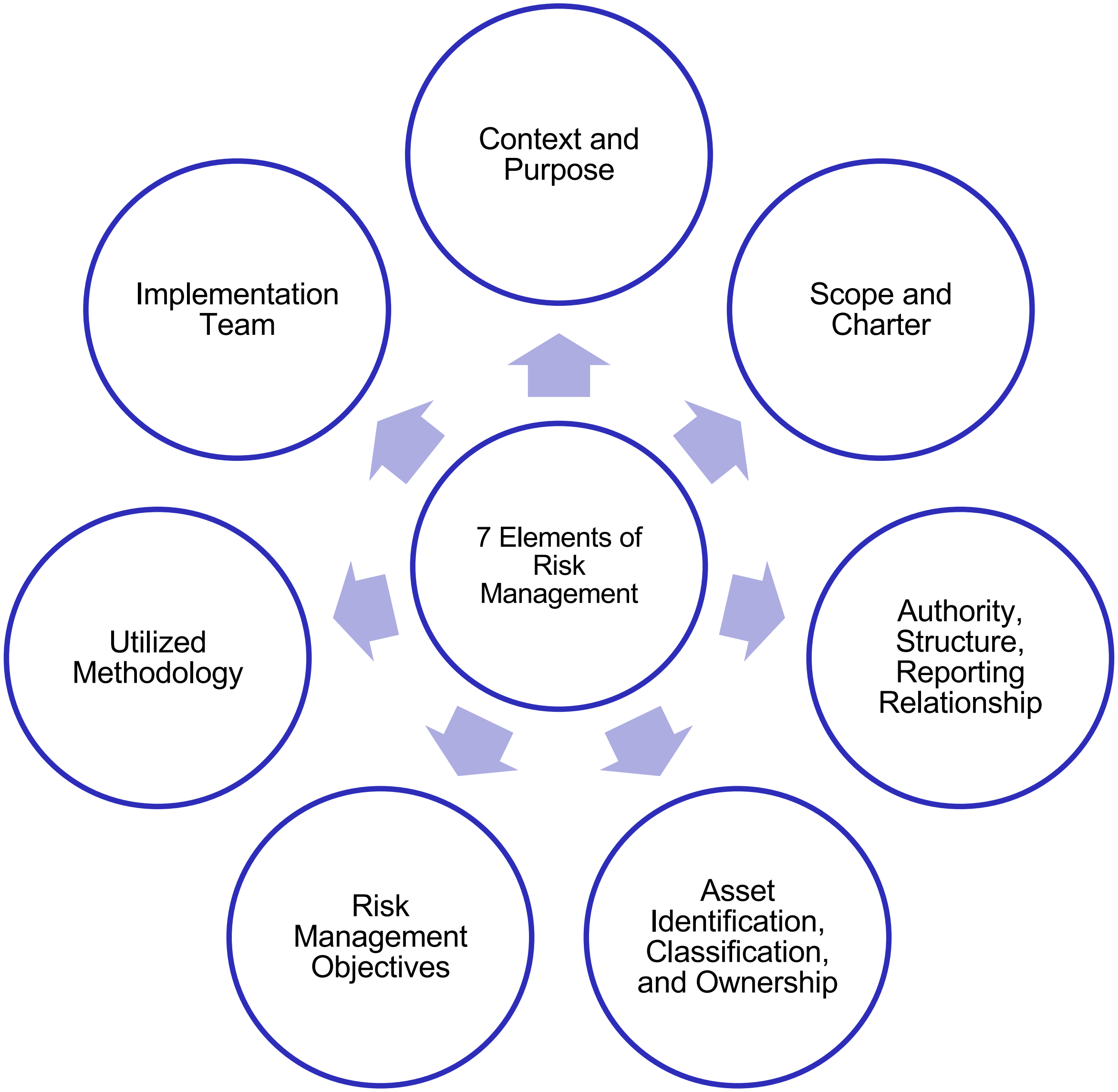
Good information security and risk consultants should:

- Have the ability to talk with upper management
- Have the ability to take information from upper management and effectively identify the impact of the information and other issues it may cause
- Be knowledgeable of the organization not just the supporting technology within the organization

Effective Information Risk Management

Domain 2
Information Risk Management

Developing A Risk Management Program



7 Elements of Risk Management

Context and Purpose

Scope and Charter

Authority, Structure, Reporting Relationship

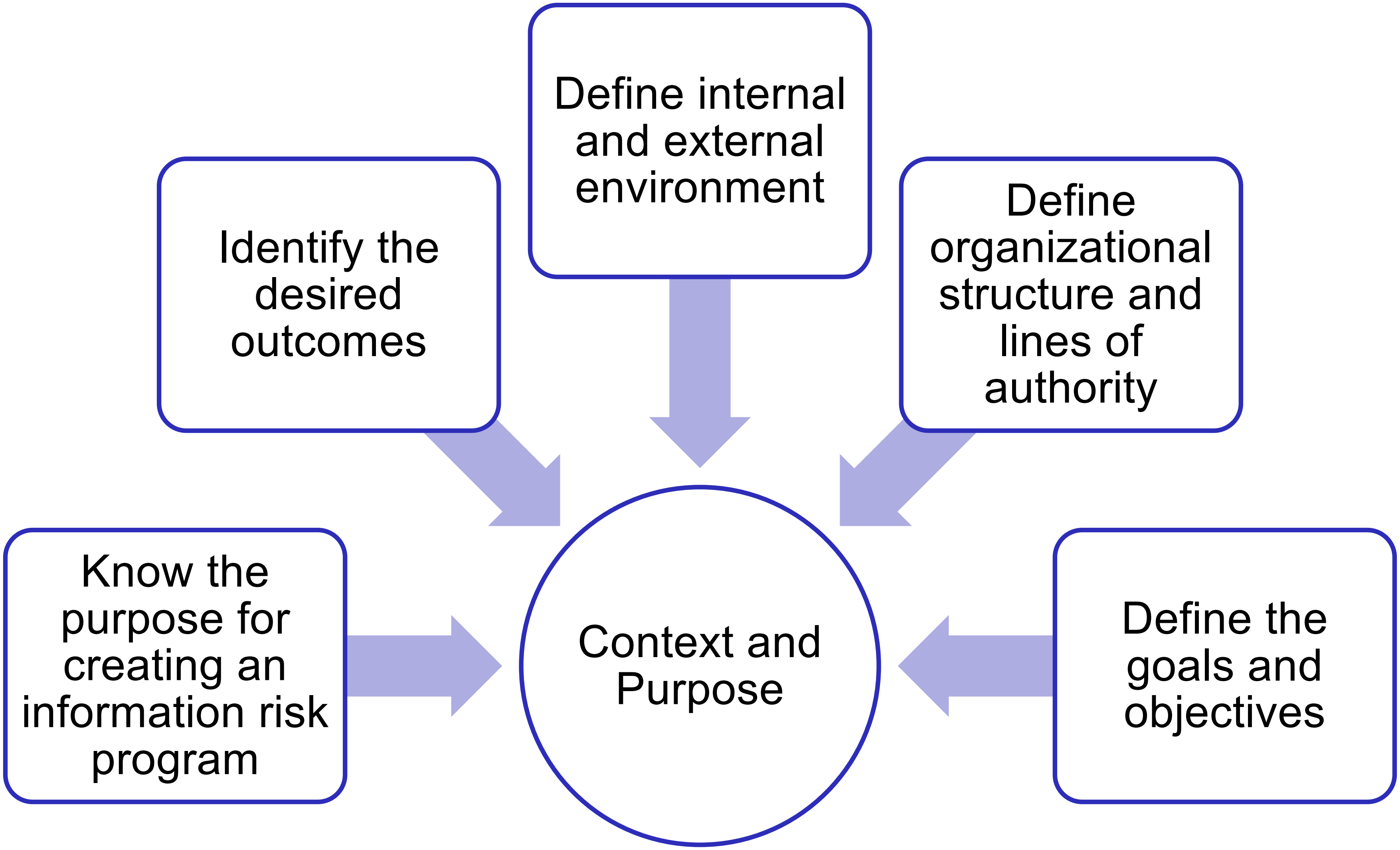
Asset Identification, Classification, and Ownership

Risk Management Objectives

Utilized Methodology

Implementation Team

Developing A Risk Management Program



Define internal and external environment

Identify the desired outcomes

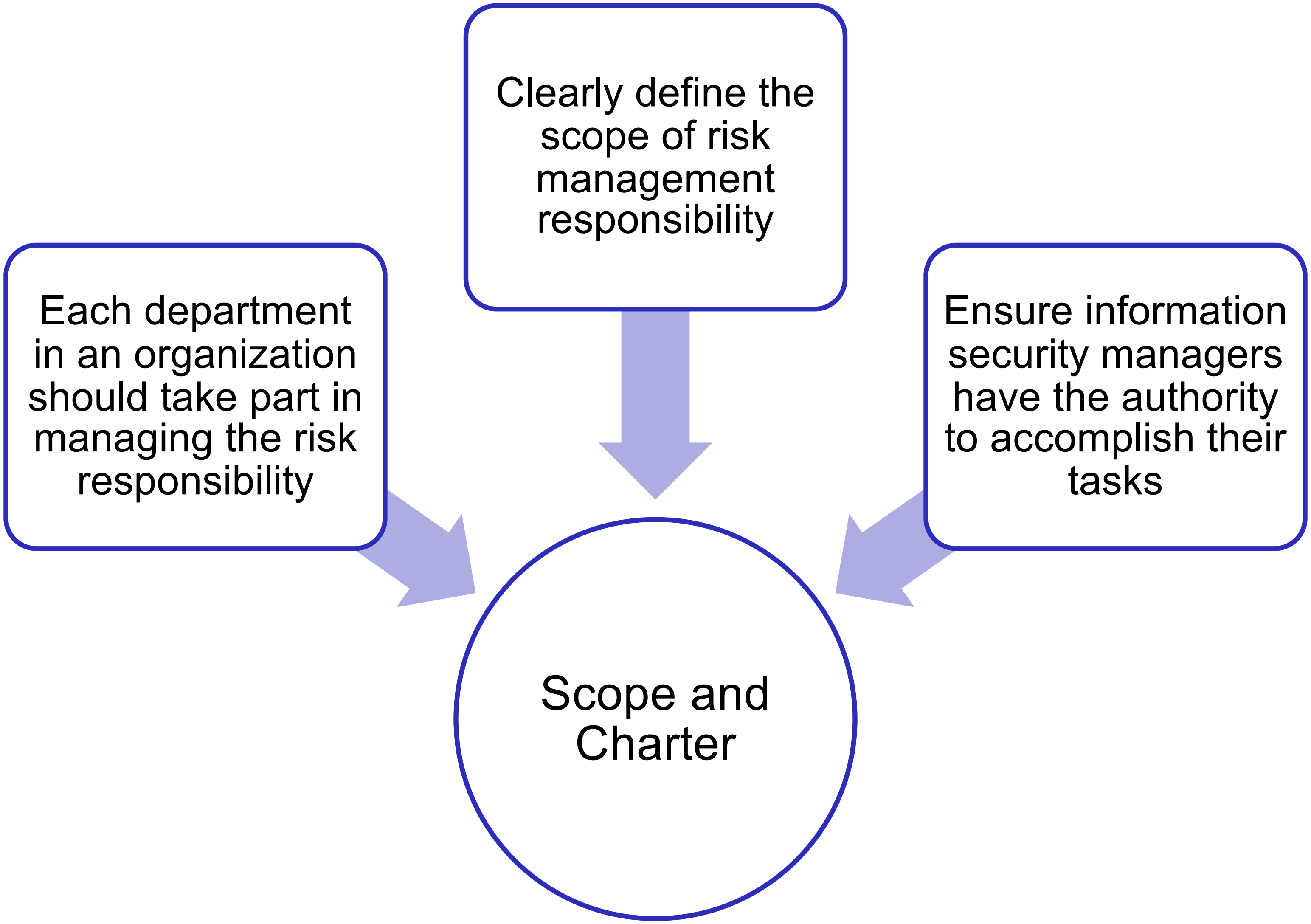
Define organizational structure and lines of authority

Know the purpose for creating an information risk program

Context and Purpose

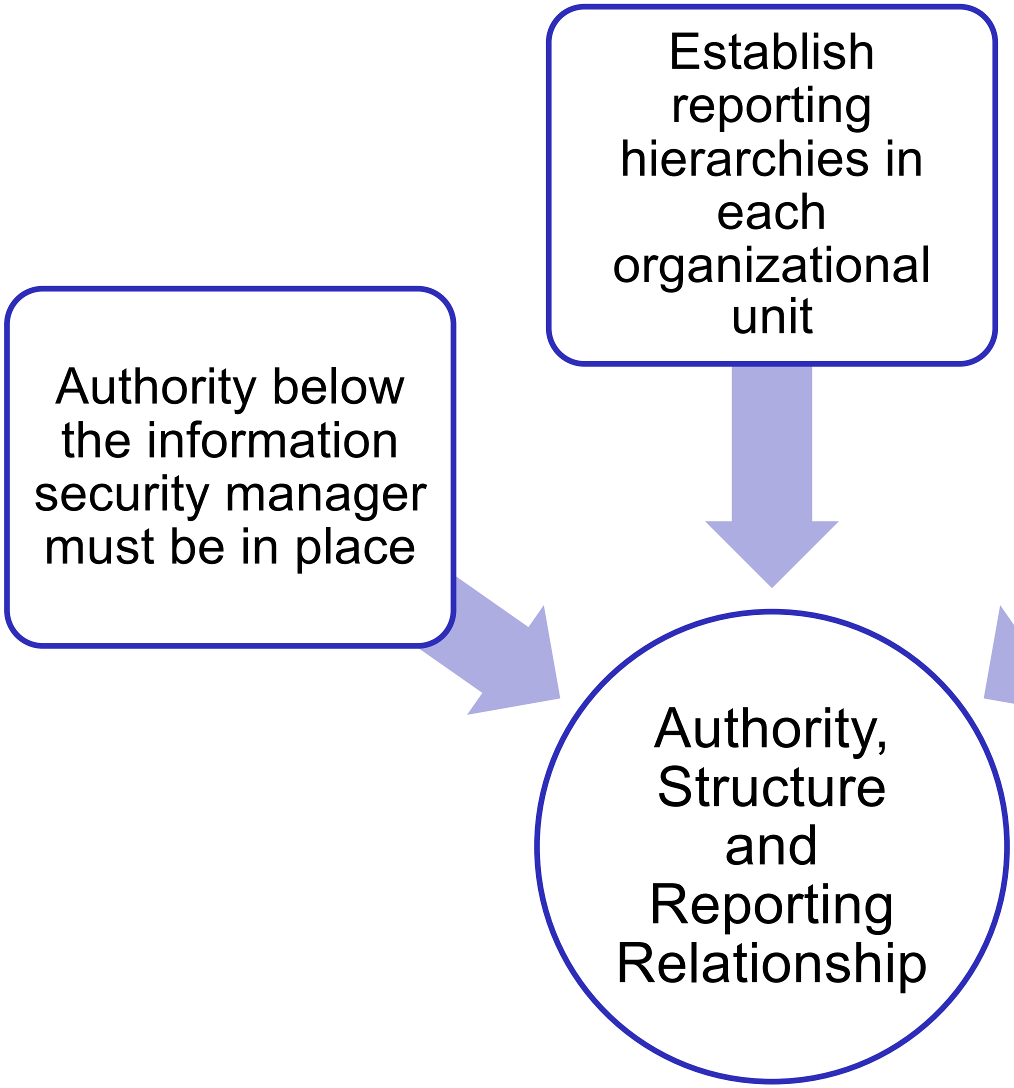
Define the goals and objectives

Developing A Risk Management Program



Clearly define the scope of risk management responsibility
Each department in an organization should take part in managing the risk responsibility
Ensure information security managers have the authority to accomplish their tasks
Scope and Charter

Developing A Risk Management Program

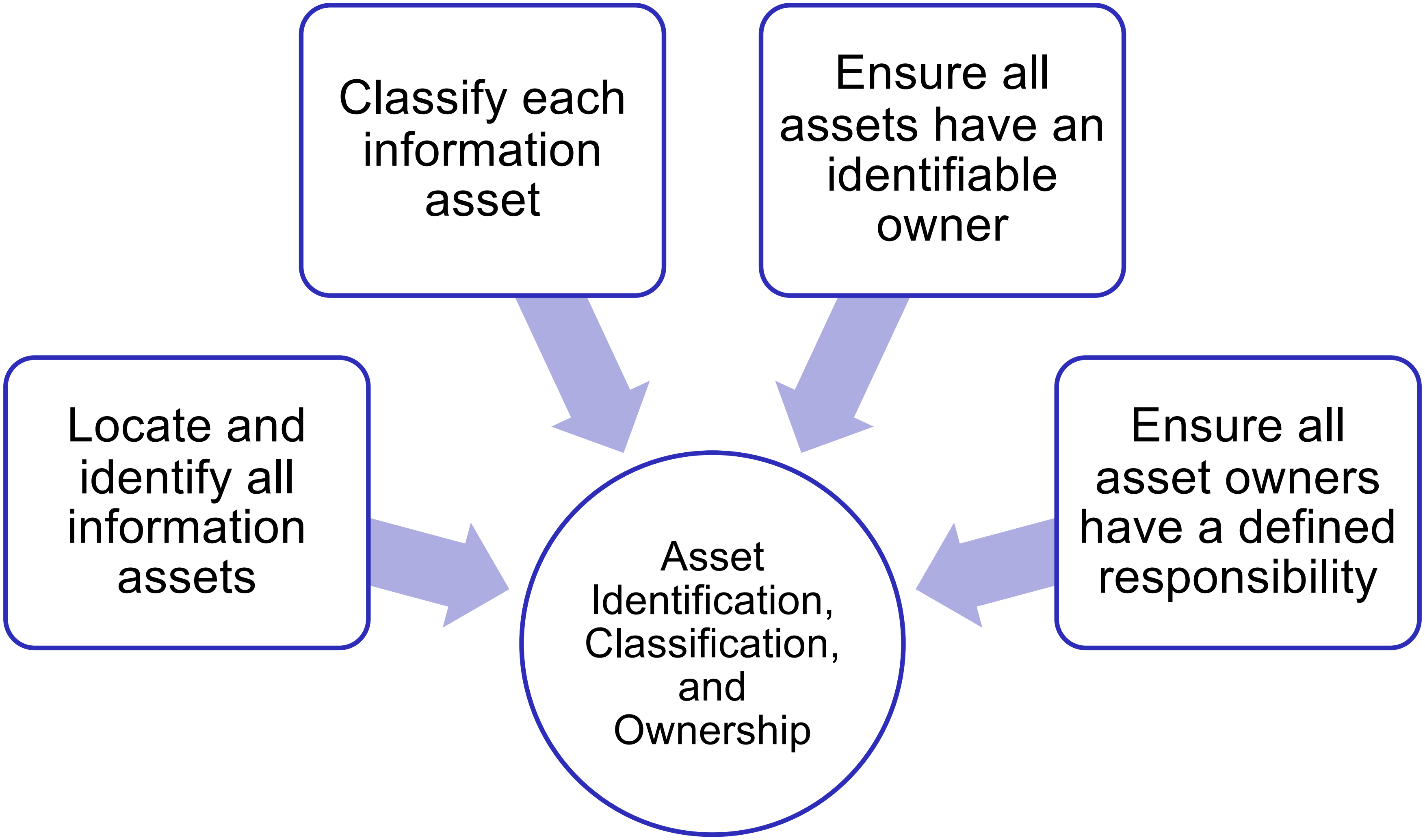

Establish reporting hierarchies in each organizational unit

Authority below the information security manager must be in place

Define those that will have the authority to take certain actions and make certain decisions

Authority, Structure and Reporting Relationship

Developing A Risk Management Program



Classify each information asset

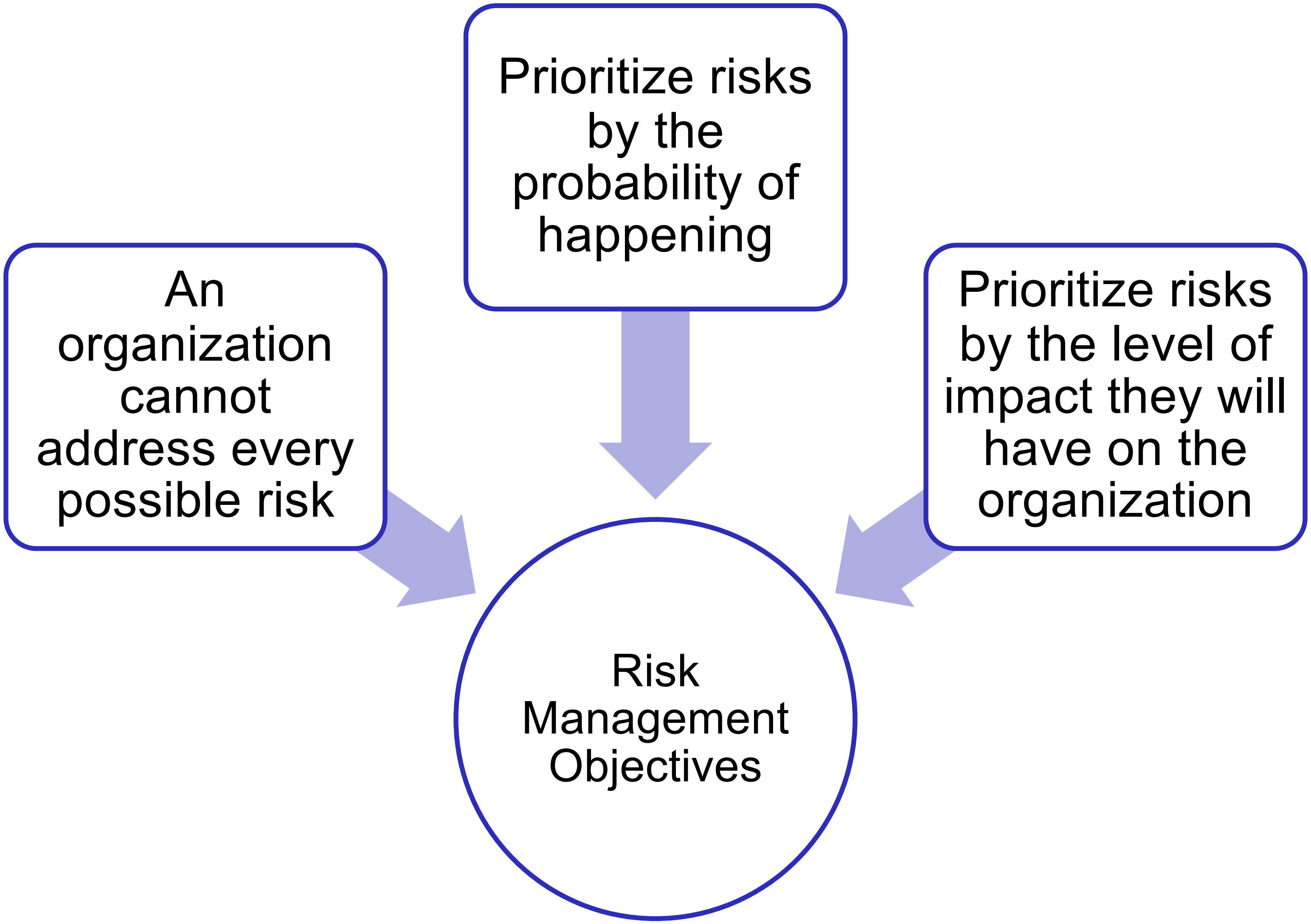
Ensure all assets have an identifiable owner

Locate and identify all information assets

Ensure all asset owners have a defined responsibility

Asset Identification, Classification, and Ownership

Developing A Risk Management Program



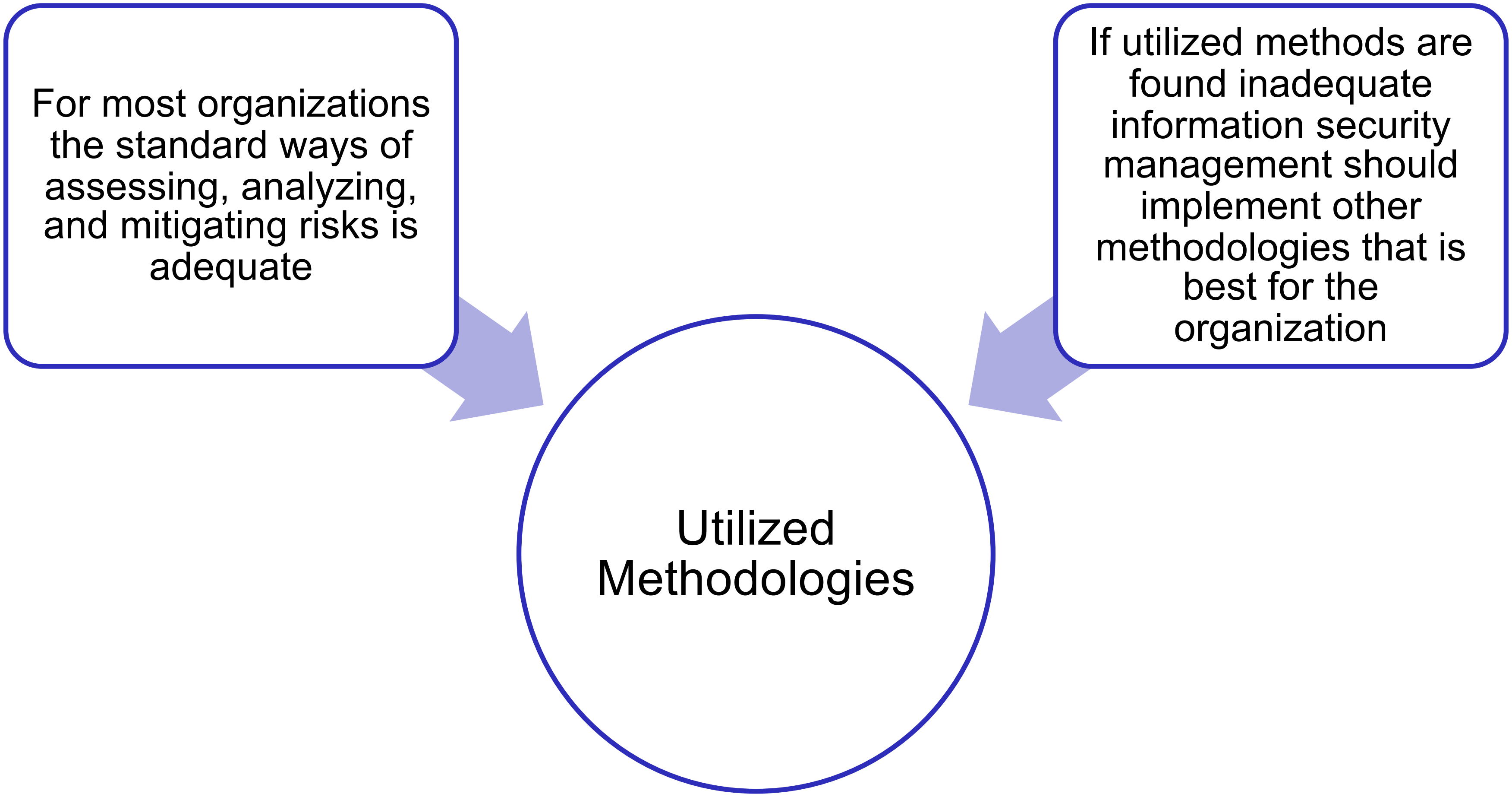
An organization cannot address every possible risk

Prioritize risks by the probability of happening

Prioritize risks by the level of impact they will have on the organization

Risk Management Objectives

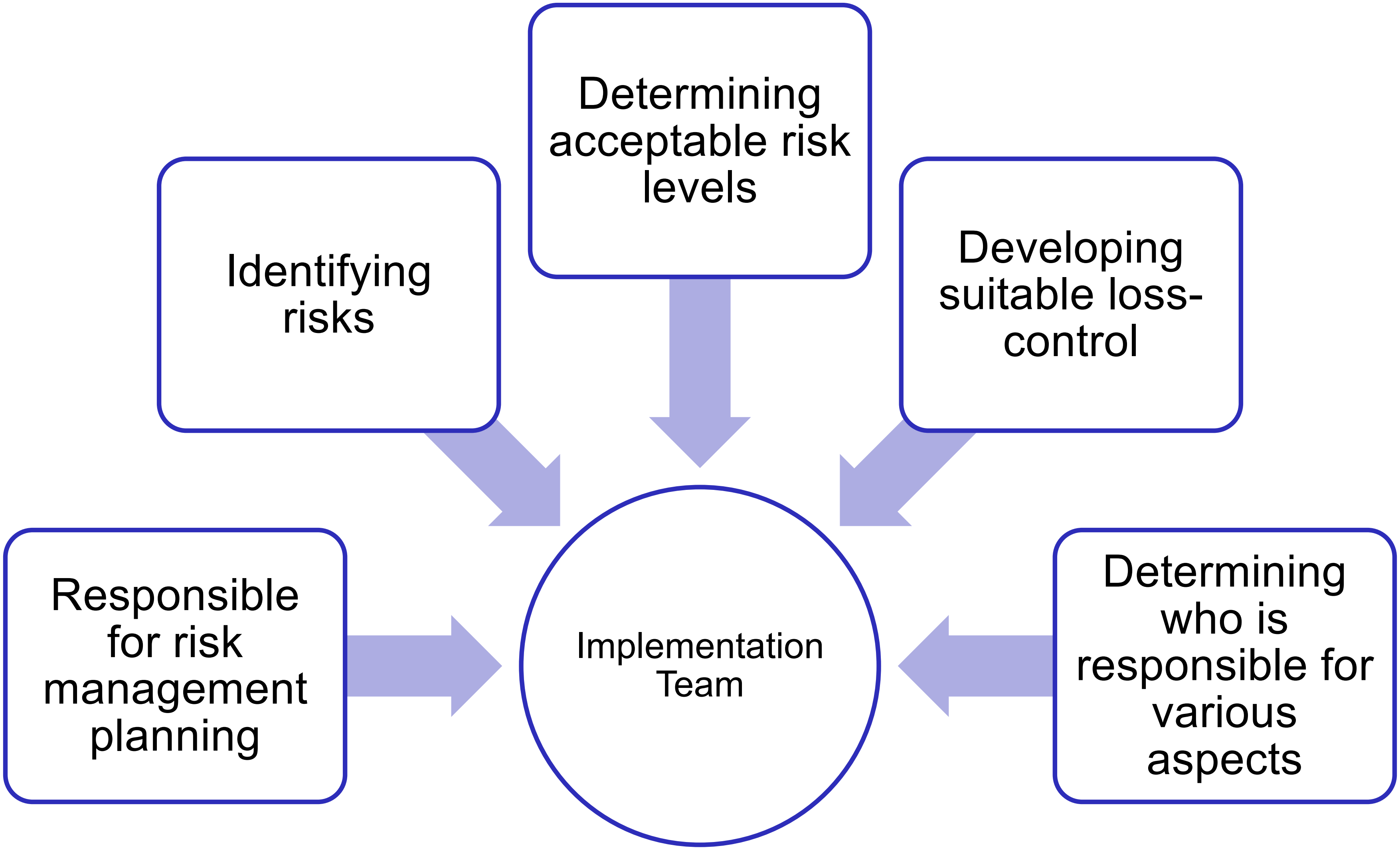
Developing A Risk Management Program


For most organizations the standard ways of assessing, analyzing, and mitigating risks is adequate

If utilized methods are found inadequate information security management should implement other methodologies that is best for the organization

Utilized Methodologies

Developing A Risk Management Program



Determining acceptable risk levels

Identifying risks

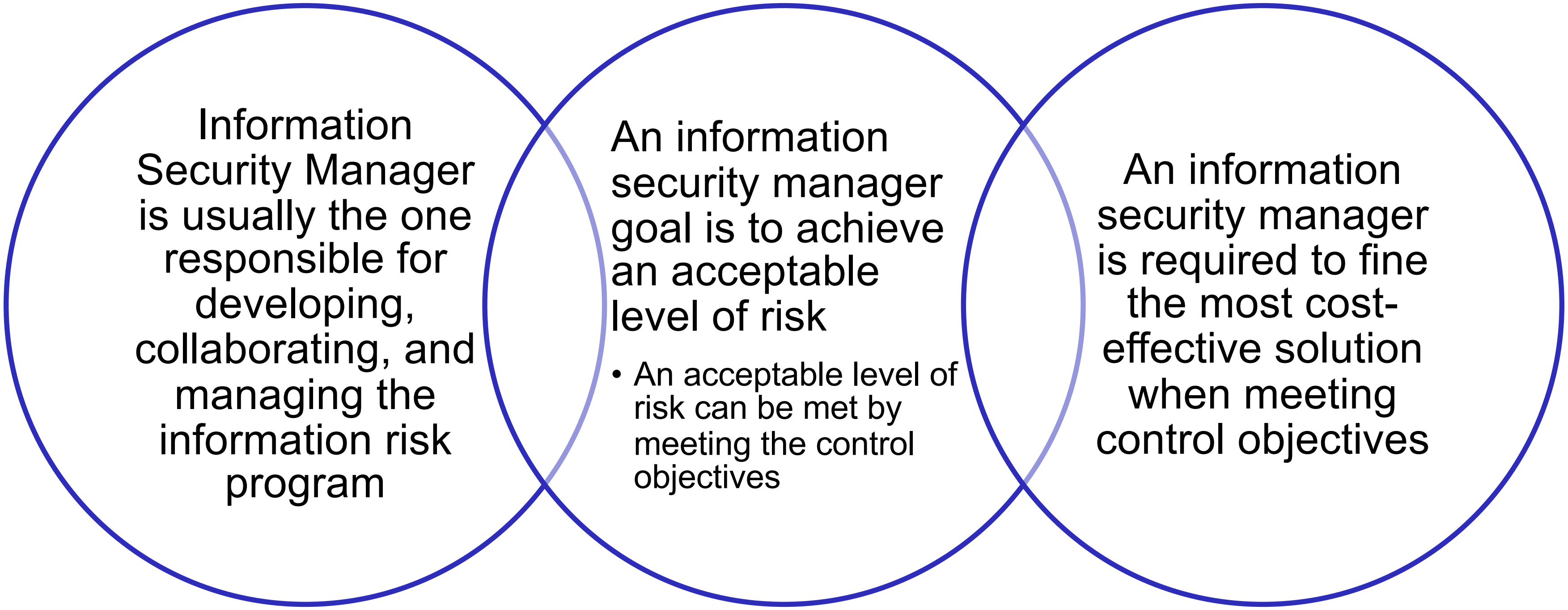
Developing suitable loss-control

Responsible for risk management planning

Implementation Team

Determining who is responsible for various aspects

Roles and Responsibilities



Information Security Manager is usually the one responsible for developing, collaborating, and managing the information risk program

An information security manager goal is to achieve an acceptable level of risk

- An acceptable level of risk can be met by meeting the control objectives

An information security manager is required to fine the most cost-effective solution when meeting control objectives

Roles and Responsibilities

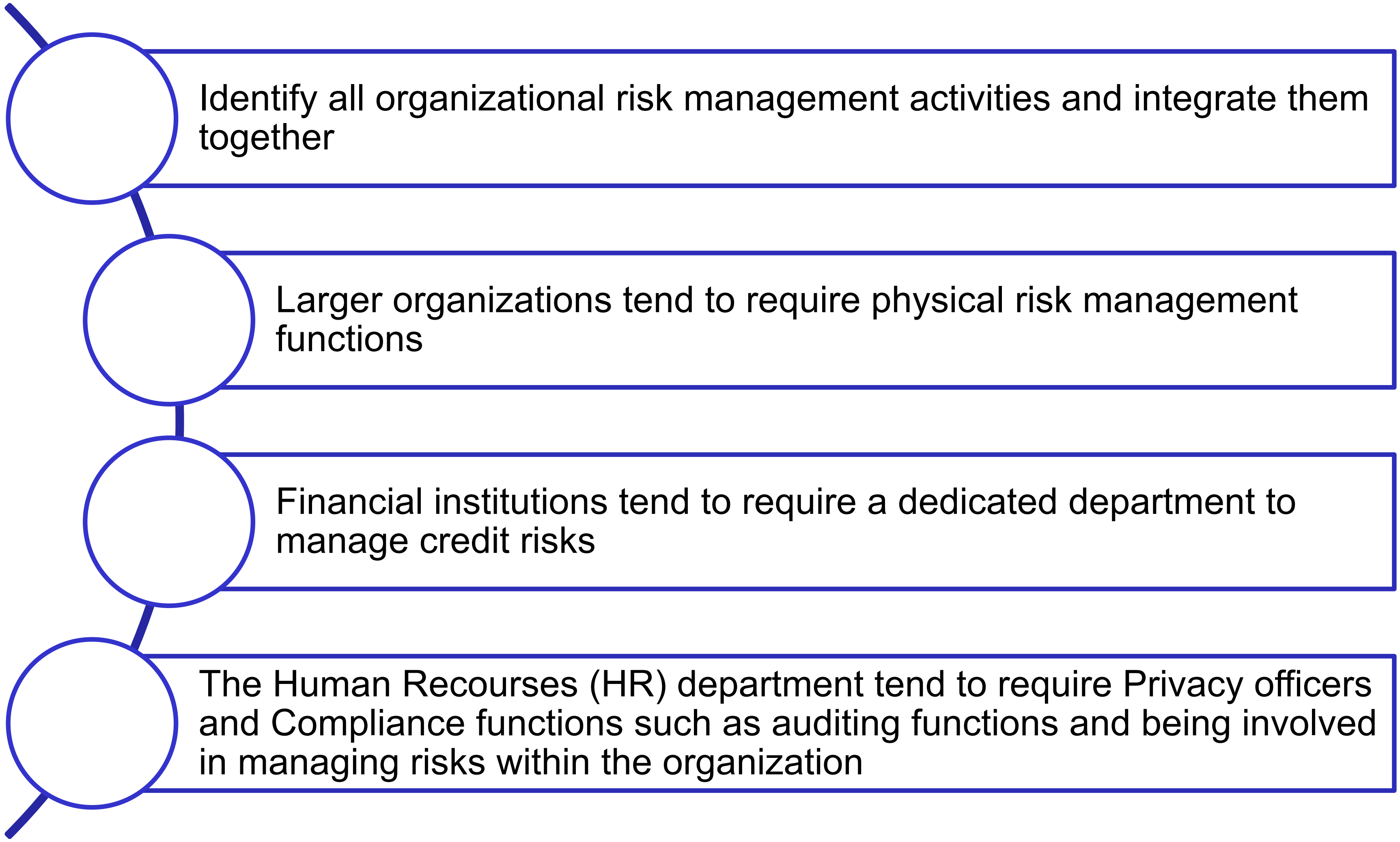
Anther important role an information security manager has is to prevent gaps in risk management by:

- Coordinating with other risk management teams
- Reducing duplication of effort
- Preventing working at cross purposes
- In general providing the most cost-effective implementation

Implementing Risk Management

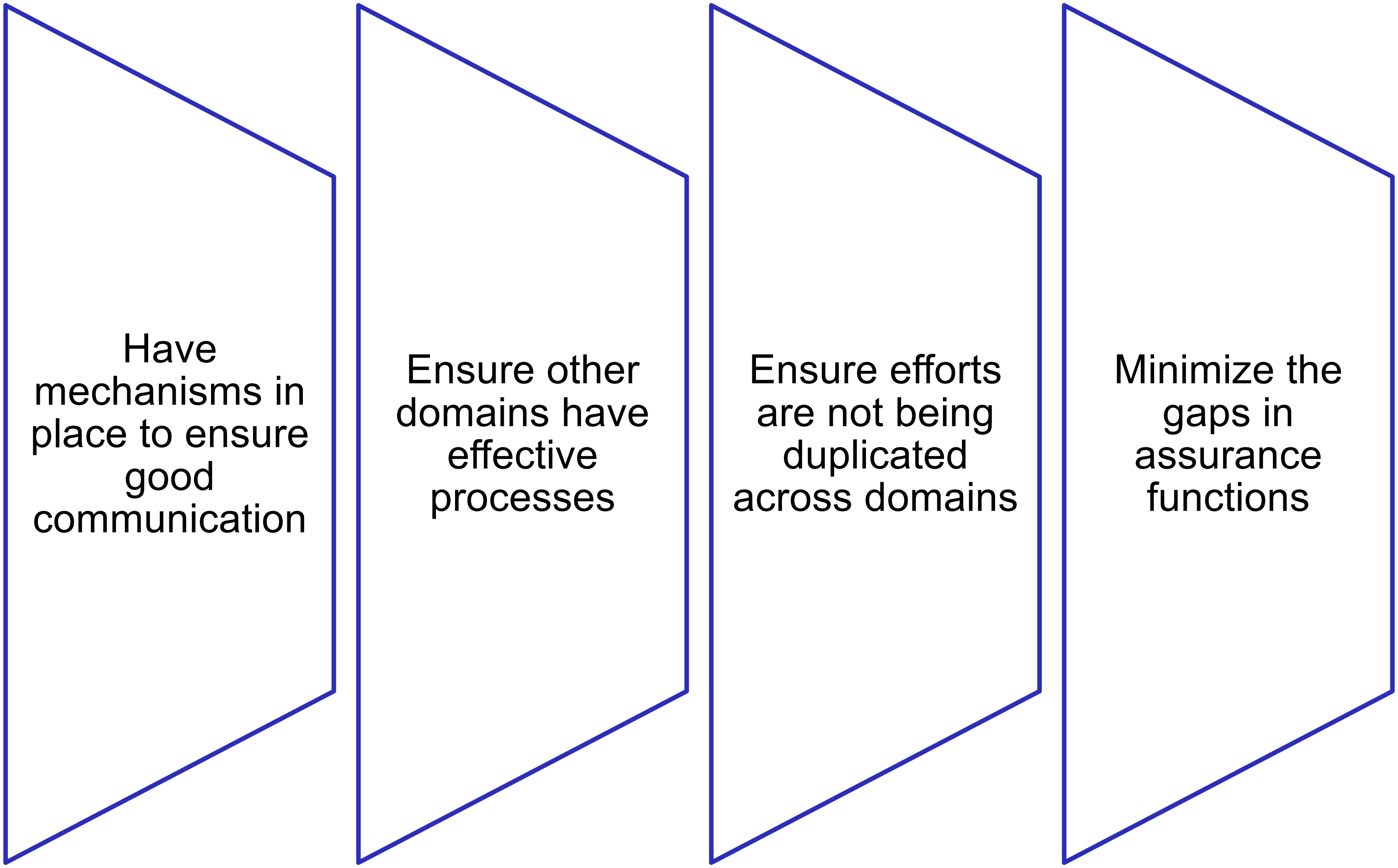
Domain 2
Information Risk Management

Planning a risk management program



- Identify all organizational risk management activities and integrate them together
- Larger organizations tend to require physical risk management functions
- Financial institutions tend to require a dedicated department to manage credit risks
- The Human Recourses (HR) department tend to require Privacy officers and Compliance functions such as auditing functions and being involved in managing risks within the organization

Being Effective



Have mechanisms in place to ensure good communication

Ensure other domains have effective processes

Ensure efforts are not being duplicated across domains

Minimize the gaps in assurance functions

Risk Management Processes

Establish scope and boundaries

Identify information assets and valuation

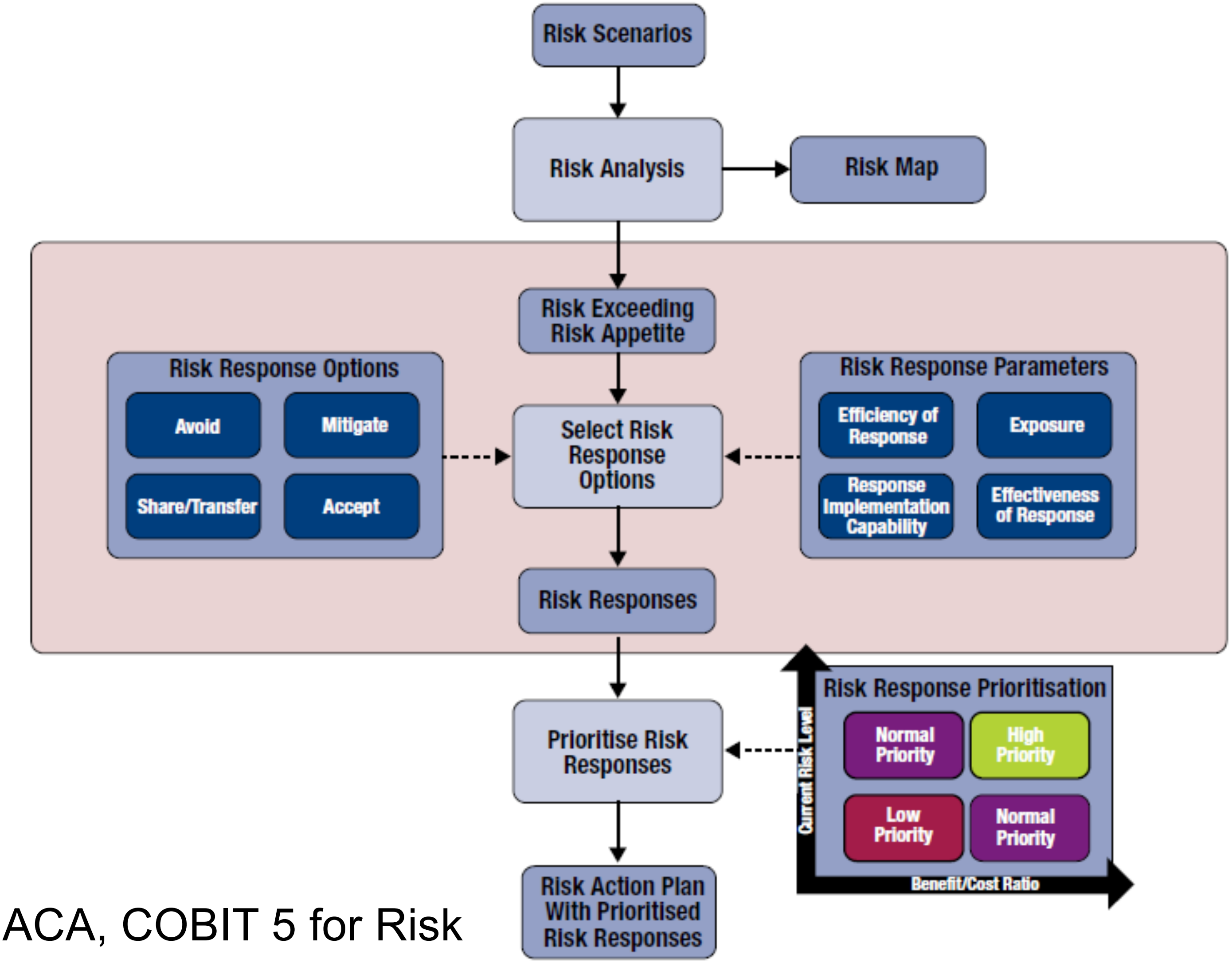
Perform risk assessments

Determine risk treatment or response

Accept residual risk

Communicate about and monitor risks

Risk Response Workflow

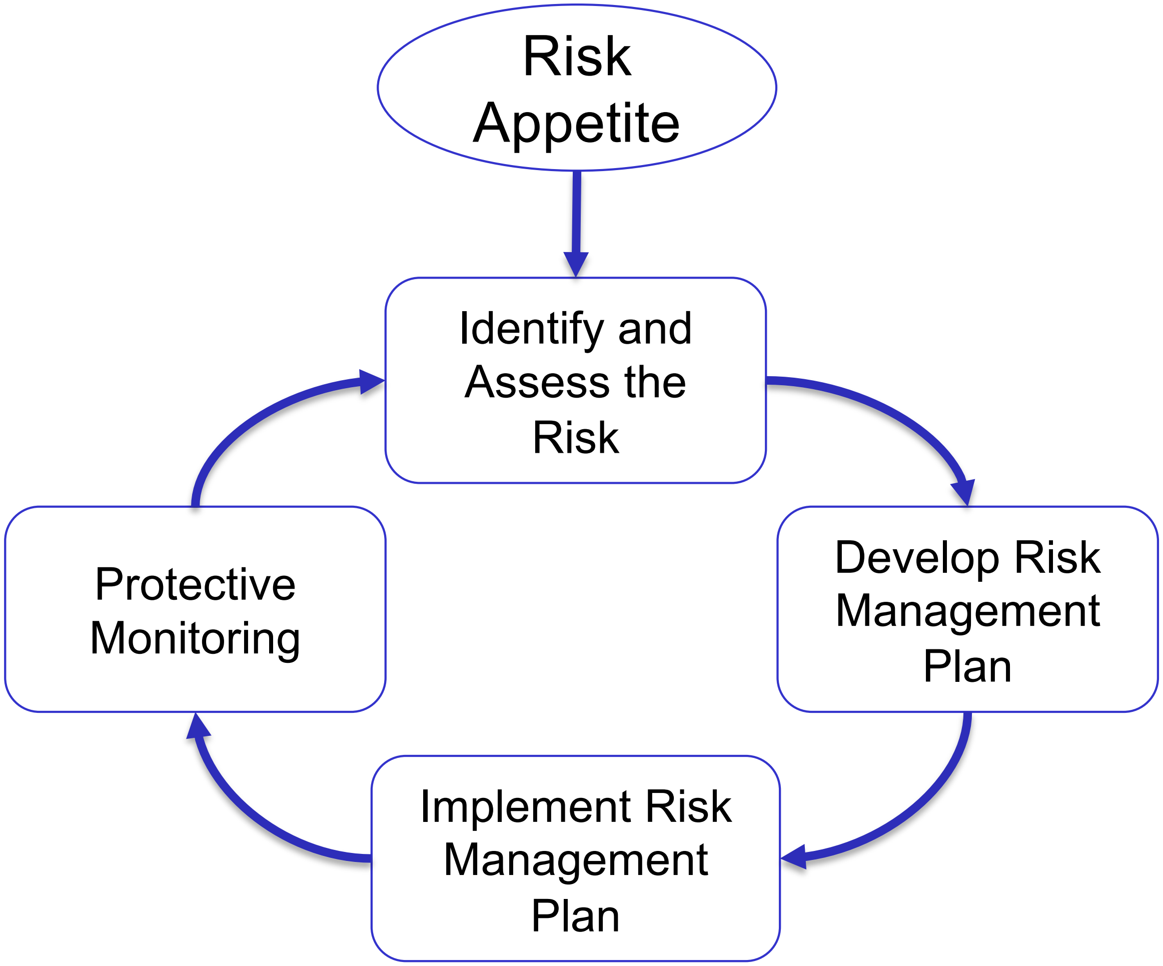


Source: ISACA, COBIT 5 for Risk

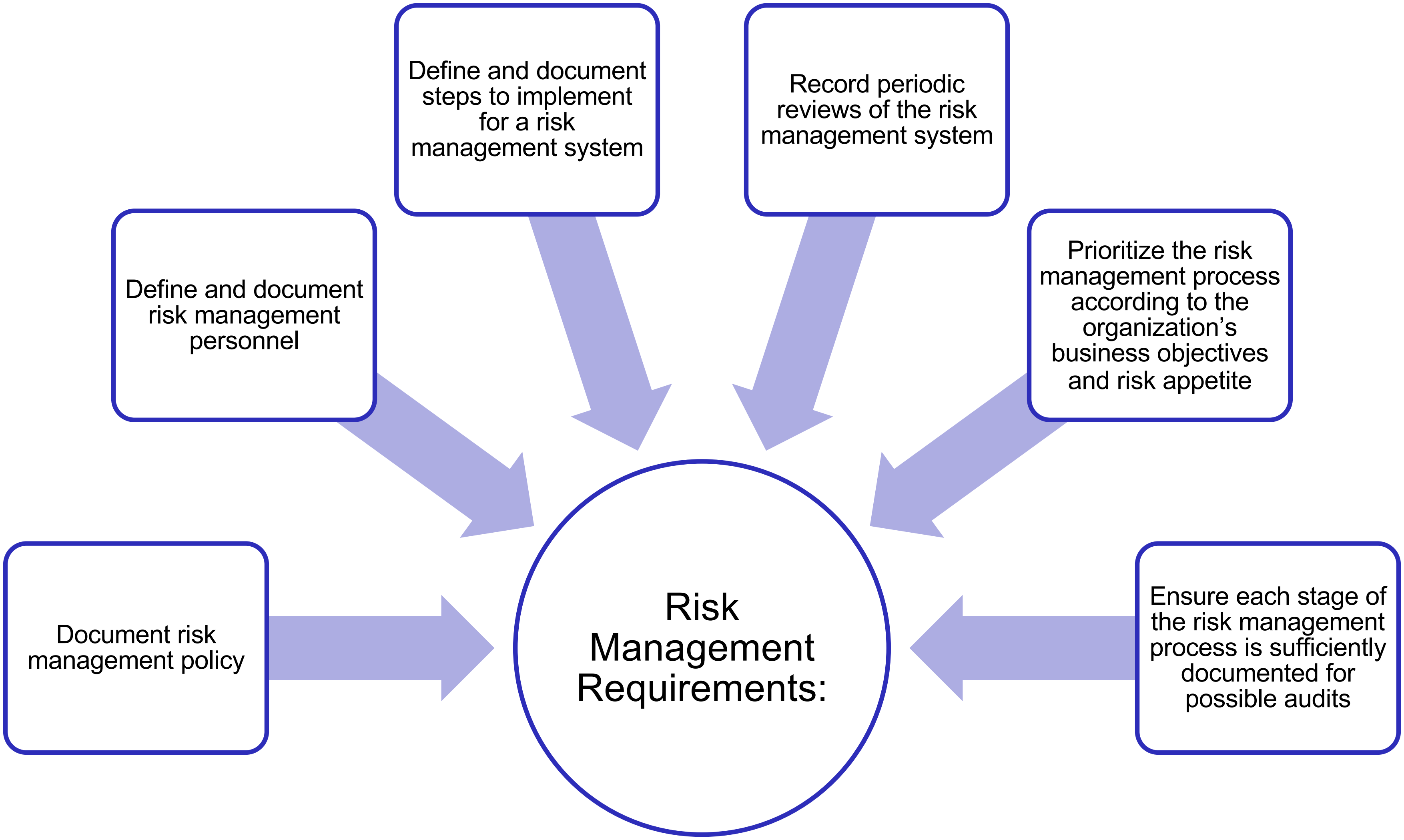
Continuous Risk Management Steps

Requiring Regular Reviews will ensure

- Changes in risks are being maintained
- Countermeasures are being followed
- Implemented countermeasures have not caused new risks


Risk Appetite
Identify and Assess the Risk
Develop Risk Management Plan
Implement Risk Management Plan
Protective Monitoring

Defining a Risk Management Framework


Define and document steps to implement for a risk management system
Record periodic reviews of the risk management system
Define and document risk management personnel
Prioritize the risk management process according to the organization's business objectives and risk appetite
Document risk management policy
Risk Management Requirements:
Ensure each stage of the risk management process is sufficiently documented for possible audits

Defining a Risk Management Framework

To establish an effective framework it is essential to

- Understand the organization and its risks
- Evaluate current risk management activities
- Evaluate the set standard for acceptable risk levels
- Develop sufficient control objectives that will help obtain acceptable risk levels

Defining the External Environment

External Environment Characteristically Include

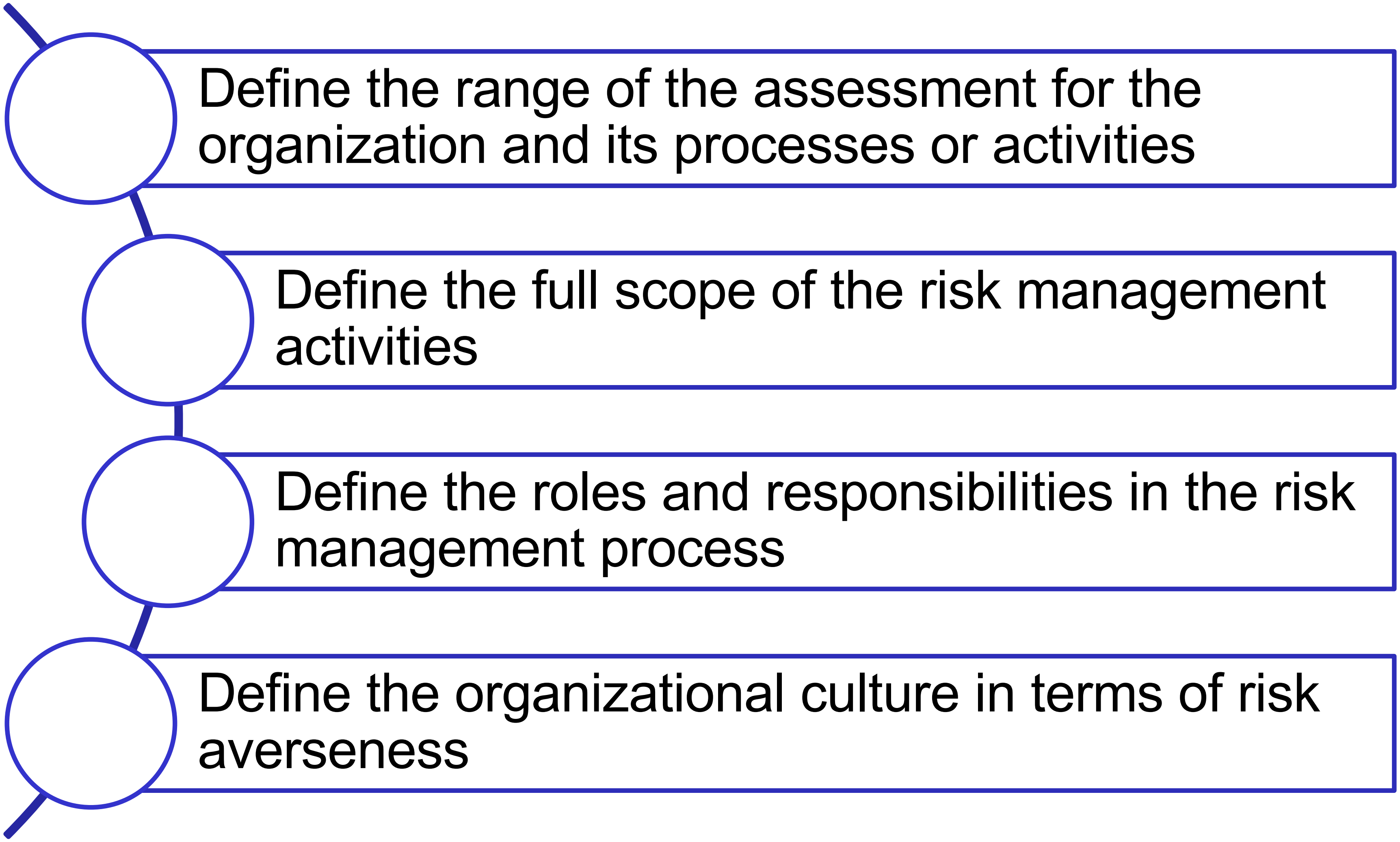
- The local market and business environment
- The law and regulatory environment
- Social and cultural conditions
- Stakeholders outside the organization

Defining the Internal Environment

Internal Environment Characteristically Include

- Key business drivers
- Strengths, weaknesses, opportunities, and threats of the organization
- Stakeholders within the company
- Culture and structure of the organization
- Resource assets
- Goals and objectives

Determining the Risk Management Context



- Define the range of the assessment for the organization and its processes or activities
- Define the full scope of the risk management activities
- Define the roles and responsibilities in the risk management process
- Define the organizational culture in terms of risk averseness

Determining the Risk Management Context

Determine the criteria by which risk will be evaluated such as

- The scale of impact a risk accruing could have
- The likelihood of a risk accruing
- The rules that determine the risk level

Gap Analysis

Gap Analysis is the gap between the current controls and the control objectives

Regularly analyze the gap between controls and control objectives

Other Organizational Support

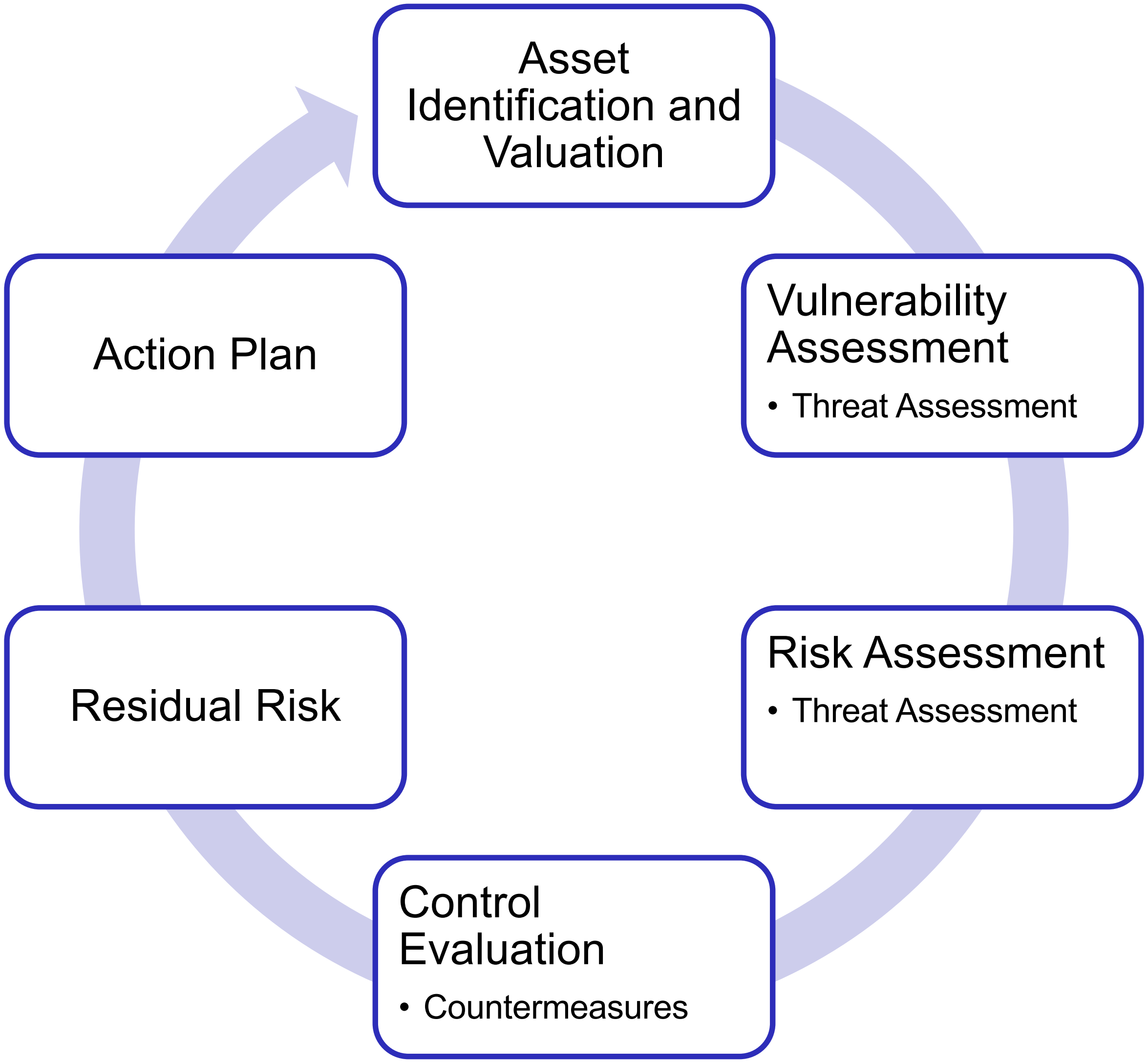
The information security manager should stay informed of any new information

- Good practices published by trusted organizations
- Security networking roundtables
- Security news organizations
- Security related studies
- Security training organizations
- Vulnerability alerting serivies

Risk Assessment

Domain 2
Information Risk Management

Risk Analysis Cycle



Asset Identification and Valuation

Vulnerability Assessment

- Threat Assessment

Risk Assessment

- Threat Assessment

Control Evaluation

- Countermeasures

Residual Risk

Action Plan

Information Asset Identification and Valuation

First step in Risk Assessment has two parts

- Locate and inventory all information assets
- Determine an approximate value for all information assets
  - Risk = Likelihood x Consequences

Typical Information Assets

- Proprietary information and processes
- Financial records and future projections
- Acquisition or merger plans
- Strategic marketing plans
- Trade secrets
- Patent-related information
- Personally Identifiable Information (PII)

Information Asset Valuation Strategy

The problems with resource valuation

Can be hard to obtain an accurate list of assets

Can be difficult to categorize each assets

Can be challenging to give each asset an exact value

Information Asset Valuation Strategy

A Manageable Solution

Loss Scenario Matrix

Scenario	Type of Data	Size of Loss	Reputation Loss	Lawsuit Loss	Fines/Reg Loss	Market Loss	Expected Loss per year	Notes
Data Breach	Client Data	50k records	$10M	$20M	$30M	$6M	$10M	Approximately 2 years of regulatory losses
Data is stolen and sold to a competitor	Strategic plan	4-year plan	Minimal	Minimal	Minimal	$30M	$3M	Competitor has a competitive edge in the Market

Information Asset Valuation Methodologies

Asset Valuation

Identifying the value of the asset

Without the value of an asset the risk of loss is difficult to calculate

Without a calculated valuation the impact of loss is unknown

Information Asset Valuation Methodologies

Some variables of asset valuation methodologies are

- Level of technical complexity
- Level of potential direct financial loss
- Level of potential consequential financial loss

Information Asset Valuation Methodologies

Quantitative Valuation Methodology

- Currency value such as replacement cost of the asset, the book value, or net present value (NPV)
- Useful for mature organizations
- It is clearer to see the actual cost of loss events

Qualitative Valuation Methodology

- Numeric scale such as 1 to 10 or low-medium-high
- Can be used for organizations that have a large number of assets.
- It is clearer to see which assets have high-value and which have low-value

Risk Assessment and Management Approaches

Here are a few of the serval risk management and assessment approaches available

COBIT 5

- Process for identifying risks and risk analysis

ISO/IEC 31010

- Risk management and risk assessment techniques

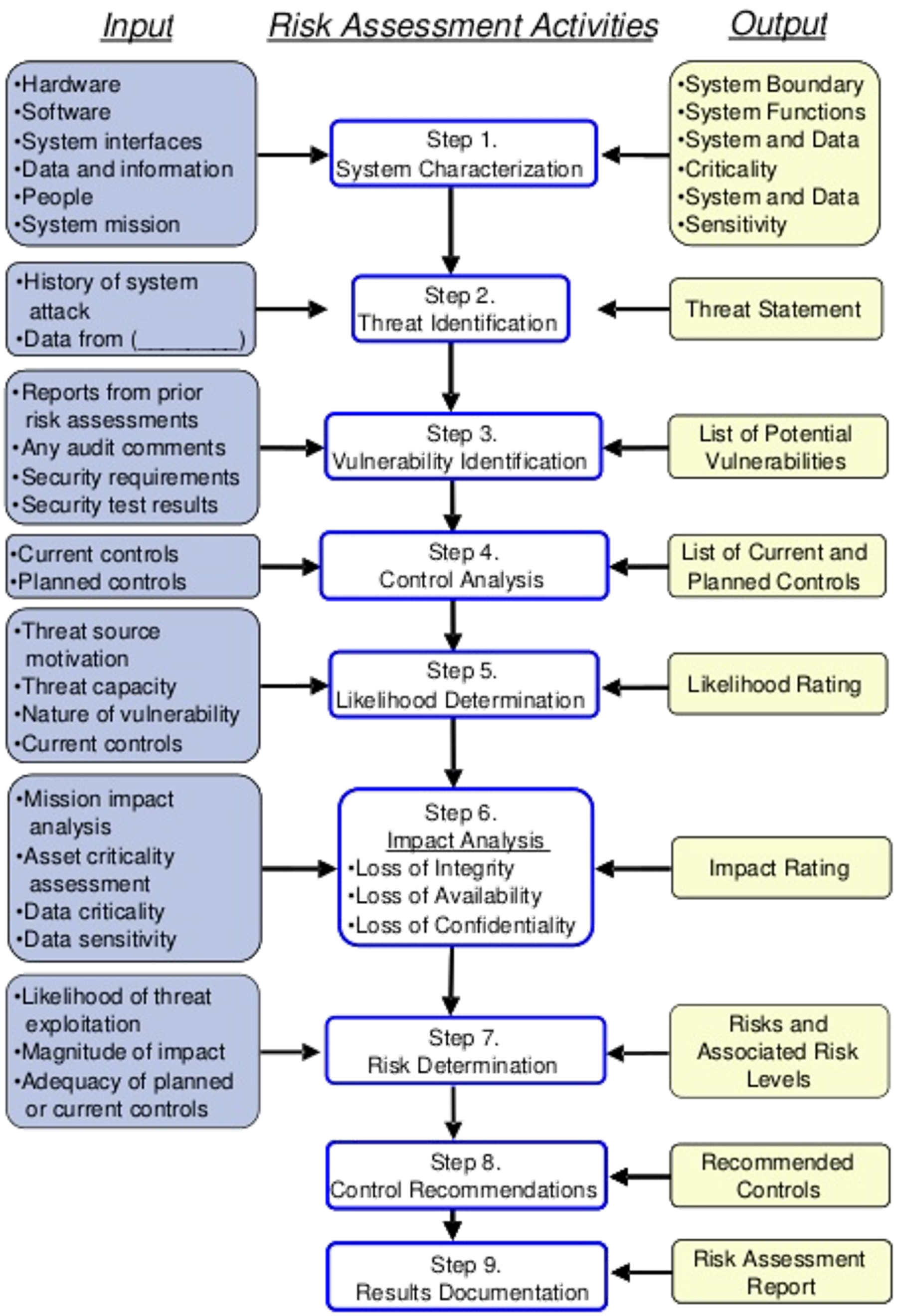
Factor Analysis of Information Risk (FAIR)

- Method of analysis to help management clearly see the factors that contribute to risk

NIST 800-39

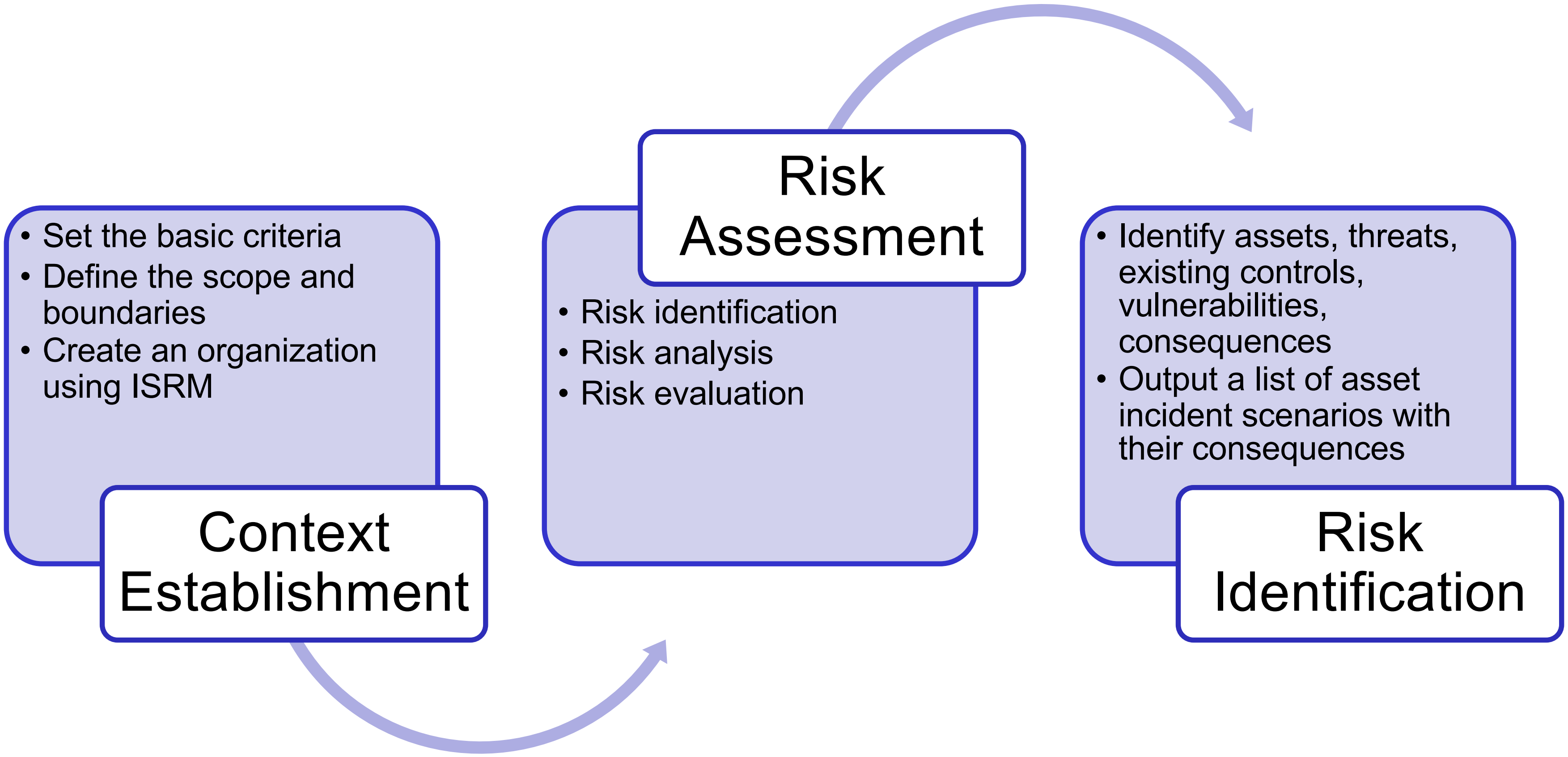
- Managing Information Security Risk

NIST Risk Assessment Methodology



Input	*Risk Assessment Activities*	*Output*
•Hardware •Software •System interfaces •Data and information •People •System mission	Step 1. System Characterization	•System Boundary •System Functions •System and Data •Criticality •System and Data •Sensitivity
•History of system attack •Data from (________)	Step 2. Threat Identification	Threat Statement
•Reports from prior risk assessments •Any audit comments •Security requirements •Security test results	Step 3. Vulnerability Identification	List of Potential Vulnerabilities
•Current controls •Planned controls	Step 4. Control Analysis	List of Current and Planned Controls
•Threat source motivation •Threat capacity •Nature of vulnerability •Current controls	Step 5. Likelihood Determination	Likelihood Rating
•Mission impact analysis •Asset criticality assessment •Data criticality •Data sensitivity	Step 6. Impact Analysis •Loss of Integrity •Loss of Availability •Loss of Confidentiality	Impact Rating
•Likelihood of threat exploitation •Magnitude of impact •Adequacy of planned or current controls	Step 7. Risk Determination	Risks and Associated Risk Levels
	Step 8. Control Recommendations	Recommended Controls
	Step 9. Results Documentation	Risk Assessment Report

ISO/IEC Process Steps



Context Establishment

- Set the basic criteria
- Define the scope and boundaries
- Create an organization using ISRM

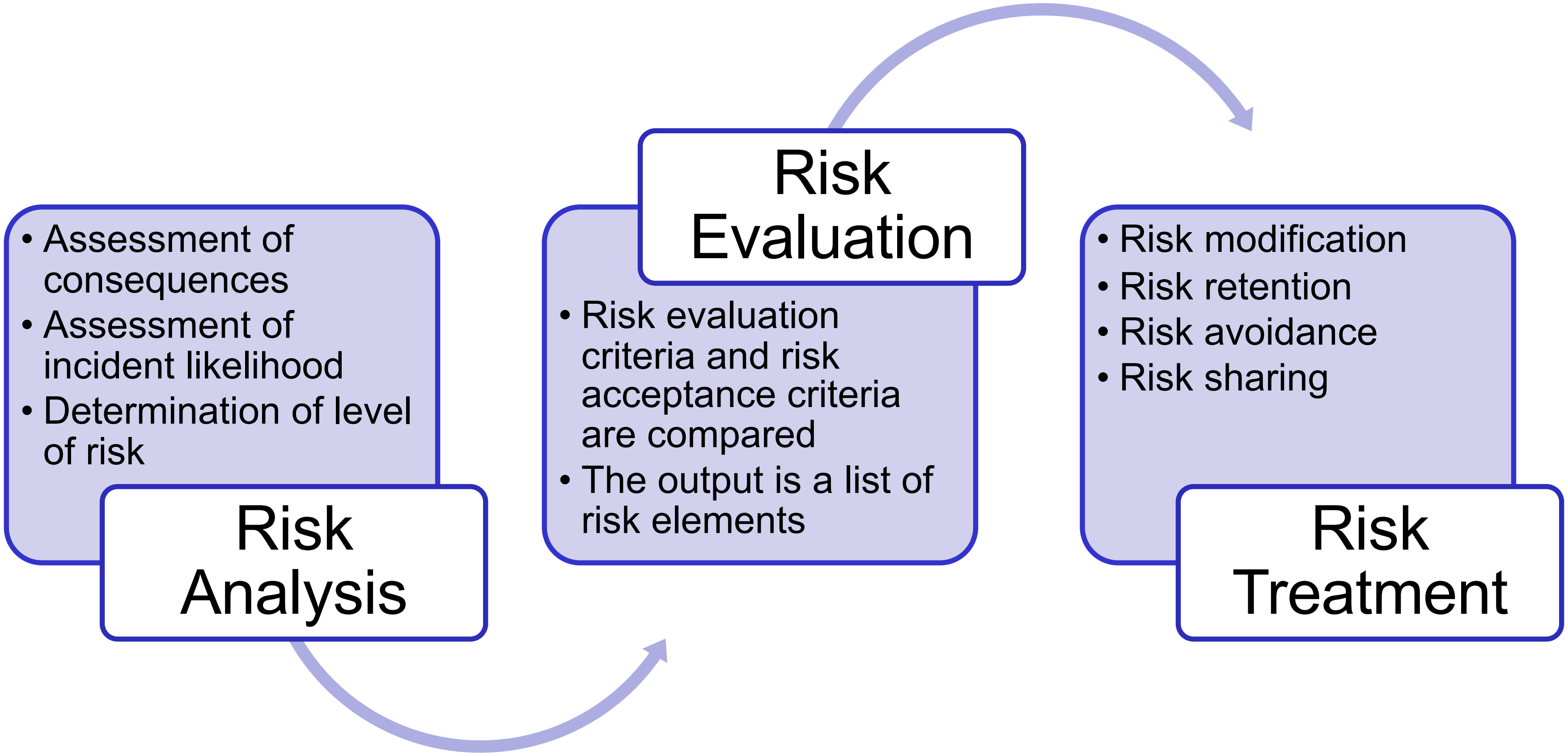
Risk Assessment

- Risk identification
- Risk analysis
- Risk evaluation

Risk Identification

- Identify assets, threats, existing controls, vulnerabilities, consequences
- Output a list of asset incident scenarios with their consequences

ISO/IEC Process Steps



- Assessment of consequences
- Assessment of incident likelihood
- Determination of level of risk

Risk Analysis

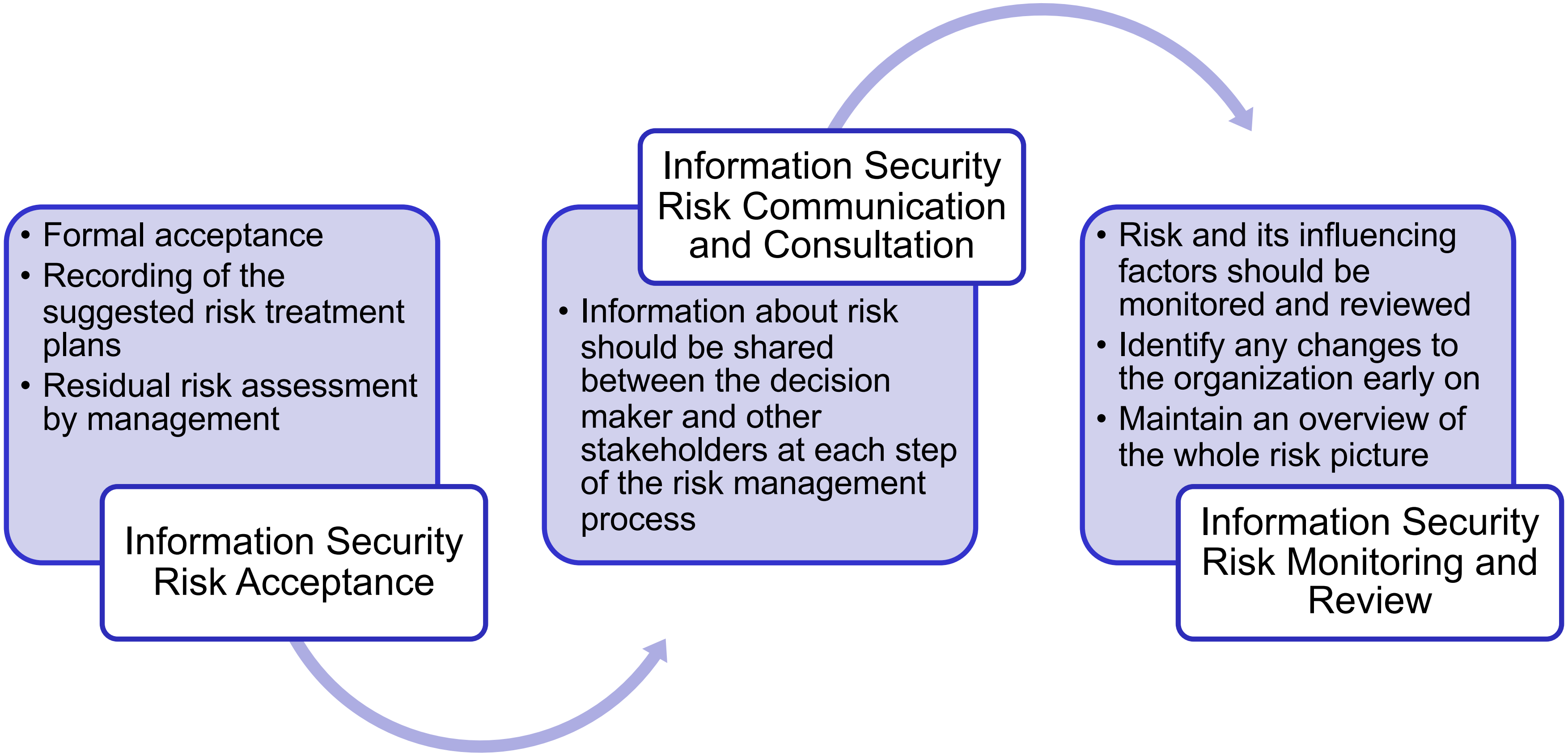
Risk Evaluation

- Risk evaluation criteria and risk acceptance criteria are compared
- The output is a list of risk elements

- Risk modification
- Risk retention
- Risk avoidance
- Risk sharing

Risk Treatment

ISO/IEC Process Steps



Information Security Risk Acceptance

- Formal acceptance
- Recording of the suggested risk treatment plans
- Residual risk assessment by management

Information Security Risk Communication and Consultation

- Information about risk should be shared between the decision maker and other stakeholders at each step of the risk management process

Information Security Risk Monitoring and Review

- Risk and its influencing factors should be monitored and reviewed
- Identify any changes to the organization early on
- Maintain an overview of the whole risk picture

Aggregated And Cascading Risk

Aggregated Risk

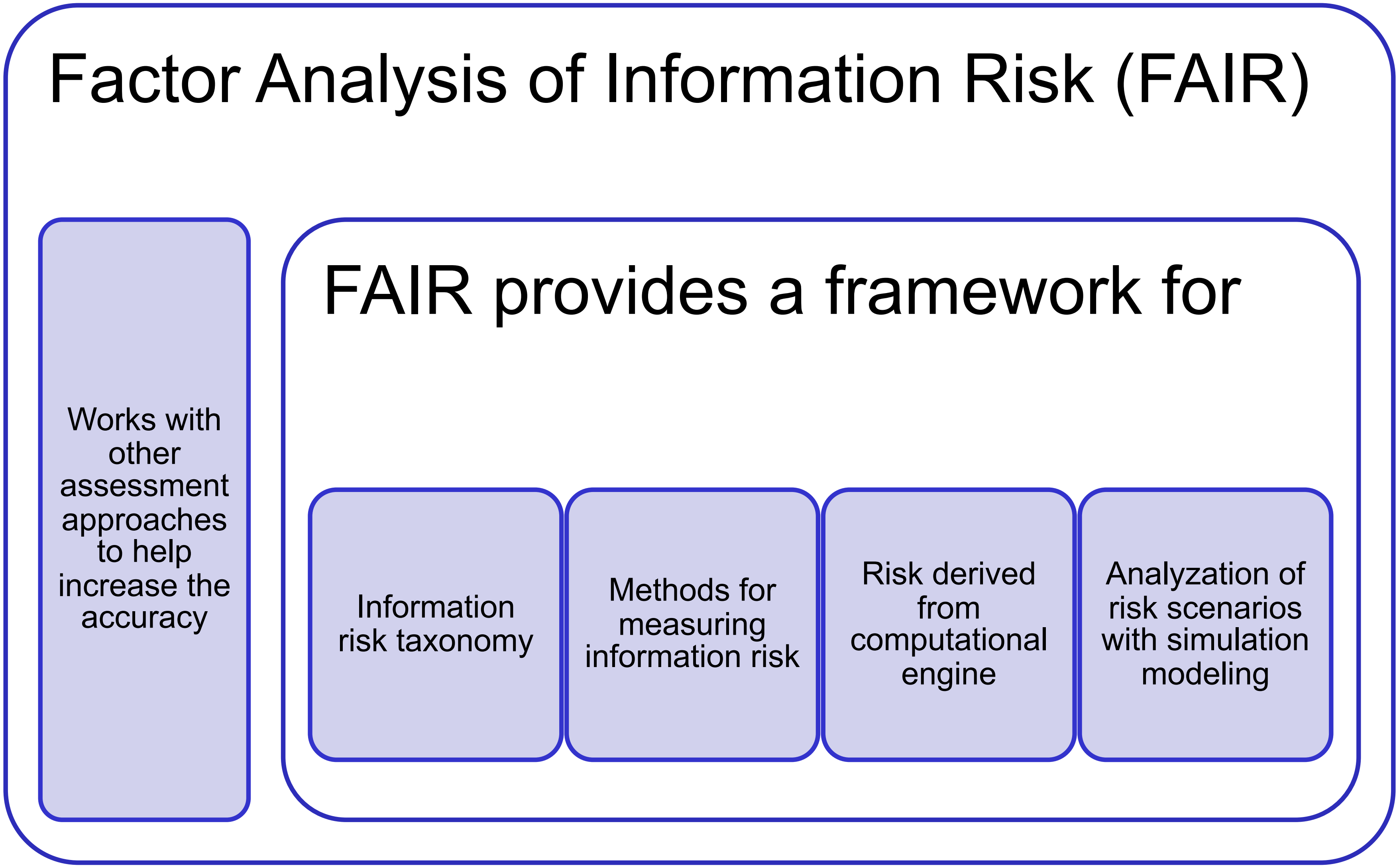
Can happen when a particular threat affects a large number of low-risk vulnerabilities causing significant impact

Can also exist when several threats affect a number of low-risk vulnerabilities that results in catastrophic impact

Cascading Risk

Can exist when one failure leads to a chain reaction that cause one failure after another

Other Risk Assessment Approaches



Factor Analysis of Information Risk (FAIR)

Works with other assessment approaches to help increase the accuracy

FAIR provides a framework for

- Information risk taxonomy
- Methods for measuring information risk
- Risk derived from computational engine
- Analyzation of risk scenarios with simulation modeling

Other Risk Assessment Approaches

Probabilistic Risk Assessment (PRA)

A systematic and comprehensive methodology to evaluate risk

This approach is complex and time-consuming

Typically applied in cases where high network security is required

PRA works to answer three questions

What can go wrong?

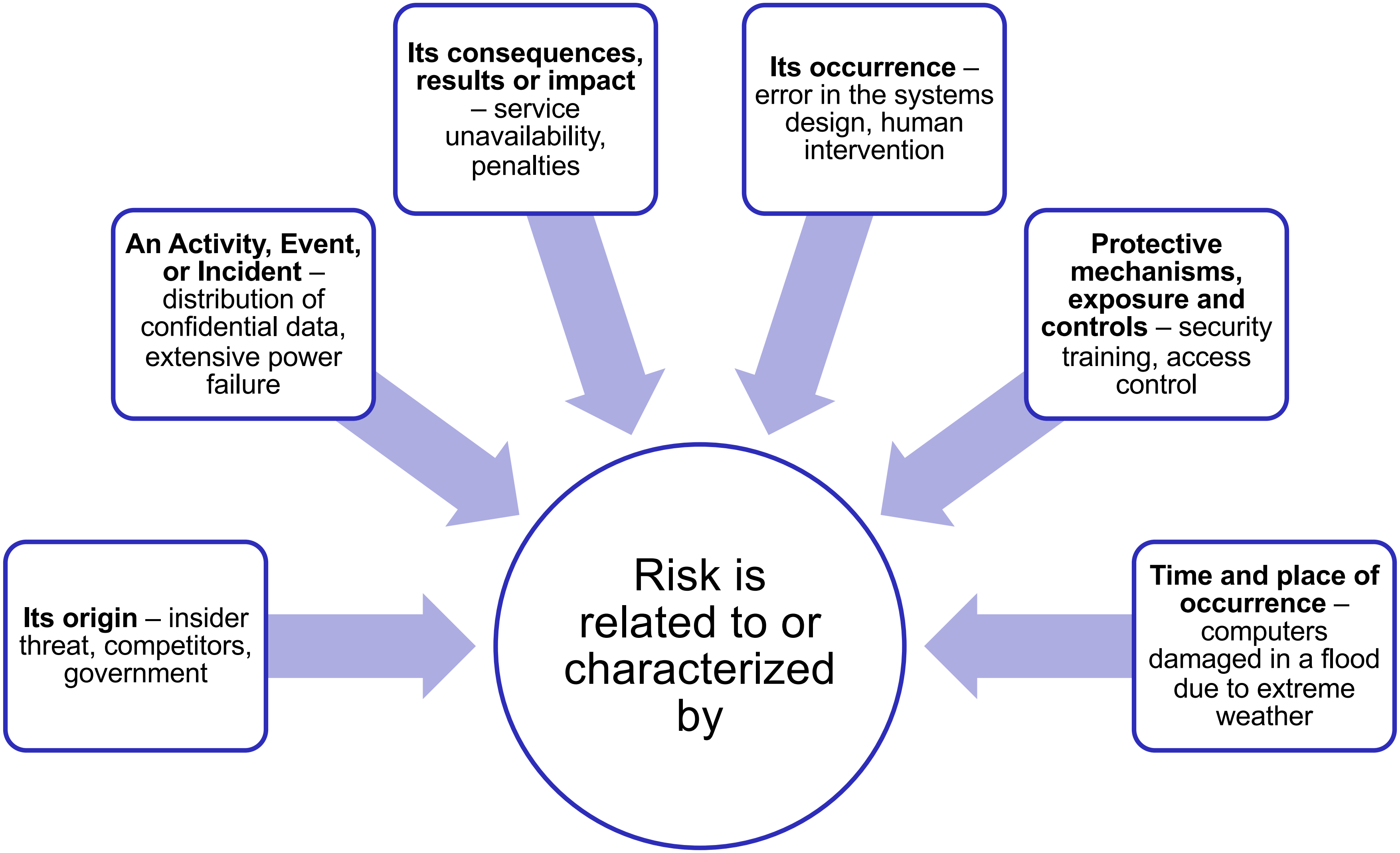
What is the likelihood something will go wrong?

What are the consequence if something does go wrong?

Identification Of Risk

- Risk identification is the process of determining viable threats to the organization
- It is important to identify all information assets such as contractors or service providers
- Typically risk identification is a group effort that develop a variety of risk scenarios
- Identified vulnerabilities are evaluated to determine the likelihood of the threat and the potential impact

Identification Of Risk



Risk is related to or characterized by

Its origin – insider threat, competitors, government

An Activity, Event, or Incident – distribution of confidential data, extensive power failure

Its consequences, results or impact – service unavailability, penalties

Its occurrence – error in the systems design, human intervention

Protective mechanisms, exposure and controls – security training, access control

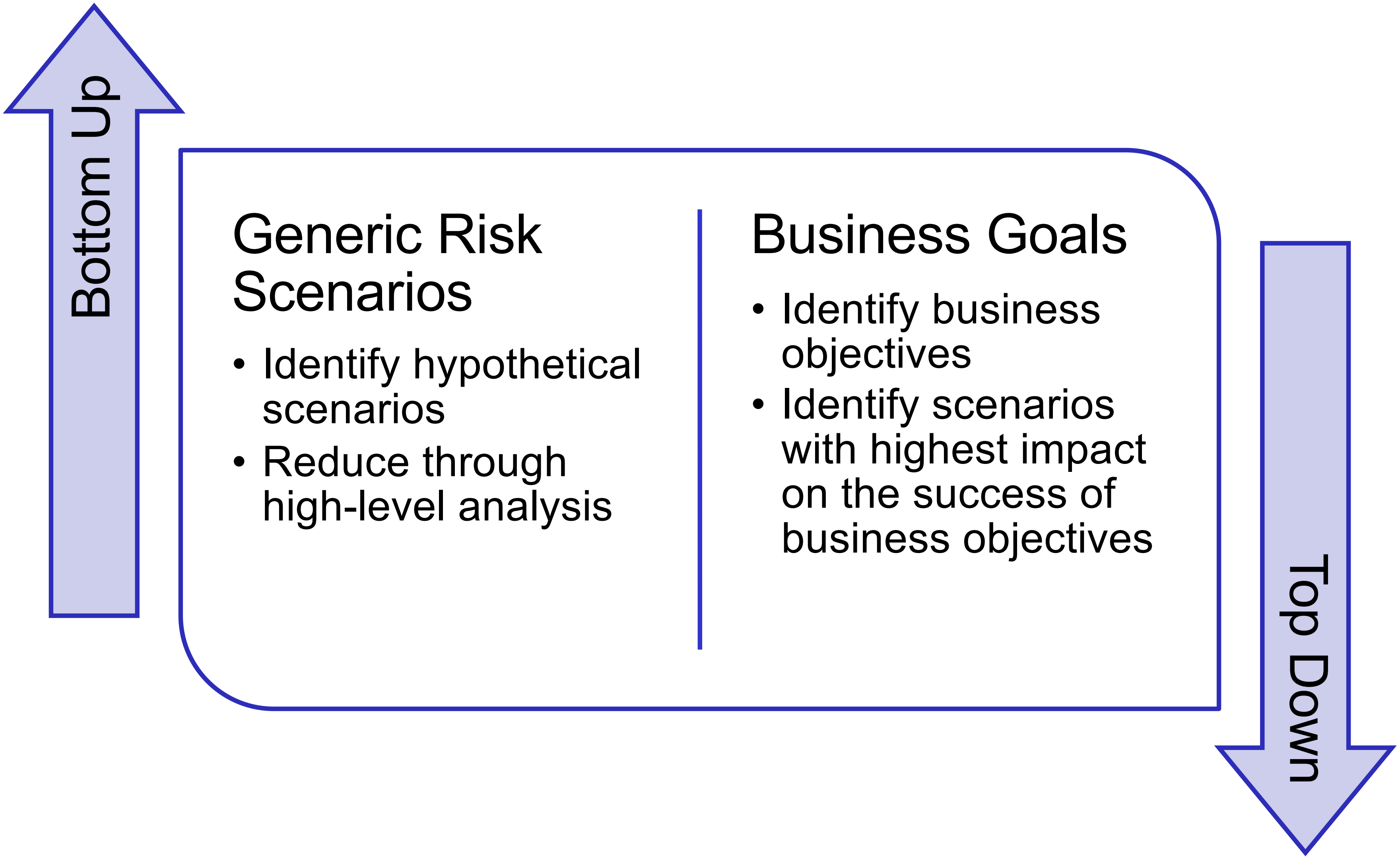
Time and place of occurrence – computers damaged in a flood due to extreme weather

Identification Of Risk

Techniques to be considered when selecting a risk identification methodology

- Team-based brainstorming
- Structured techniques for example operational modeling
- Scenario analysis
- Mapping identified internal and external threats

Risk Scenario Approaches



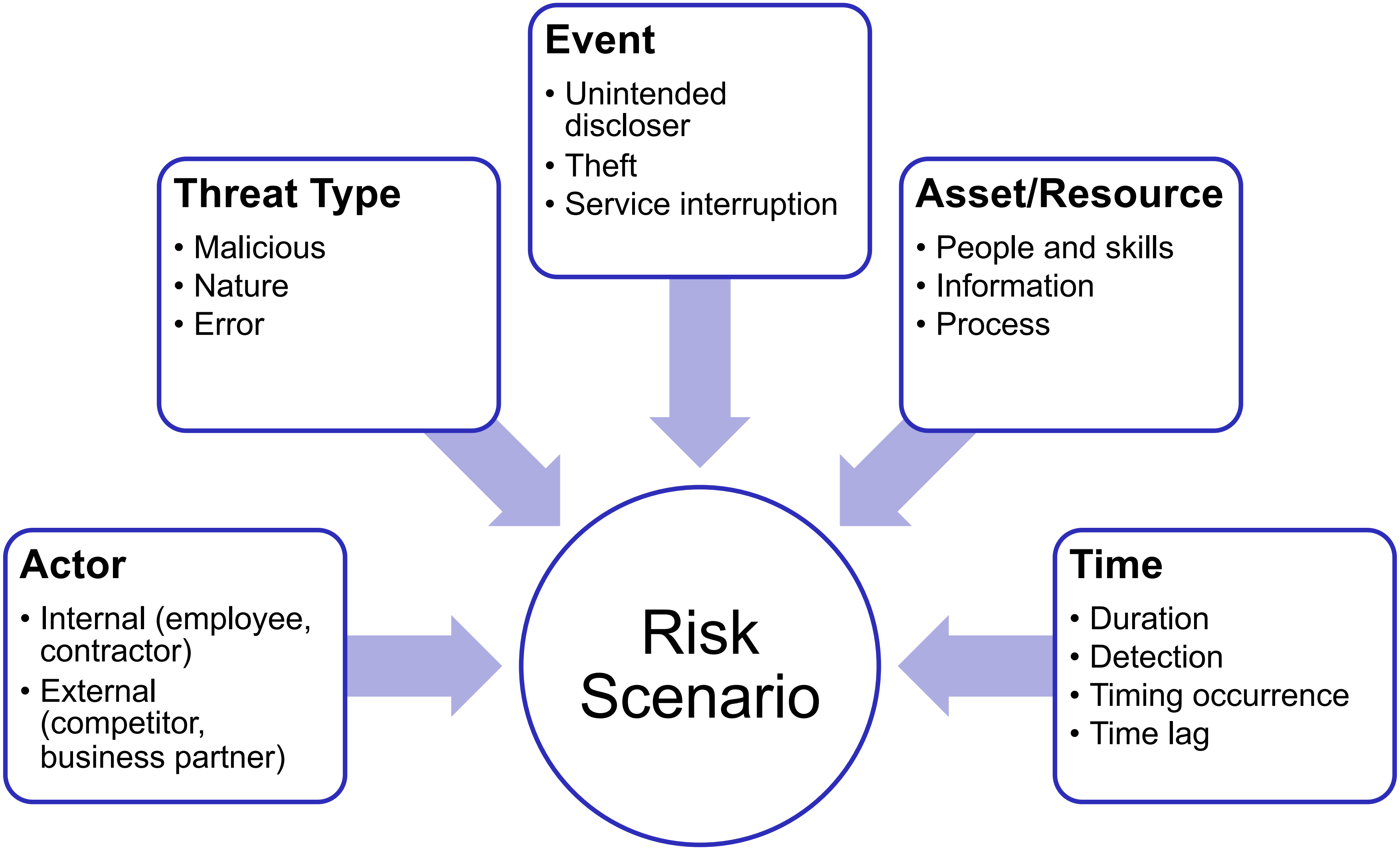
Generic Risk Scenarios

- Identify hypothetical scenarios
- Reduce through high-level analysis

Business Goals

- Identify business objectives
- Identify scenarios with highest impact on the success of business objectives

Risk Scenario Structure



Event

- Unintended discloser
- Theft
- Service interruption

Threat Type

- Malicious
- Nature
- Error

Asset/Resource

- People and skills
- Information
- Process

Actor

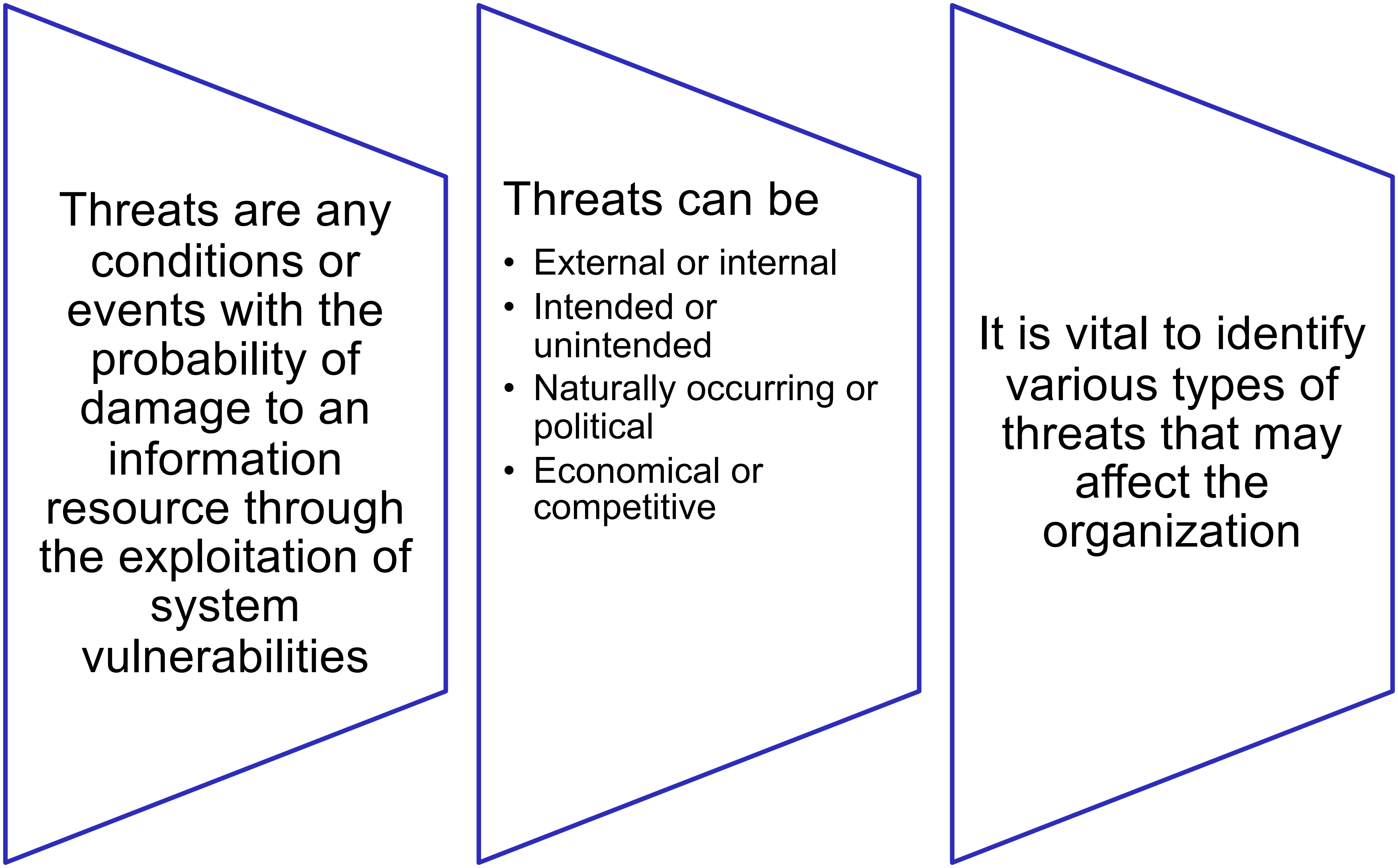
- Internal (employee, contractor)
- External (competitor, business partner)

Risk Scenario

Time

- Duration
- Detection
- Timing occurrence
- Time lag

Threats



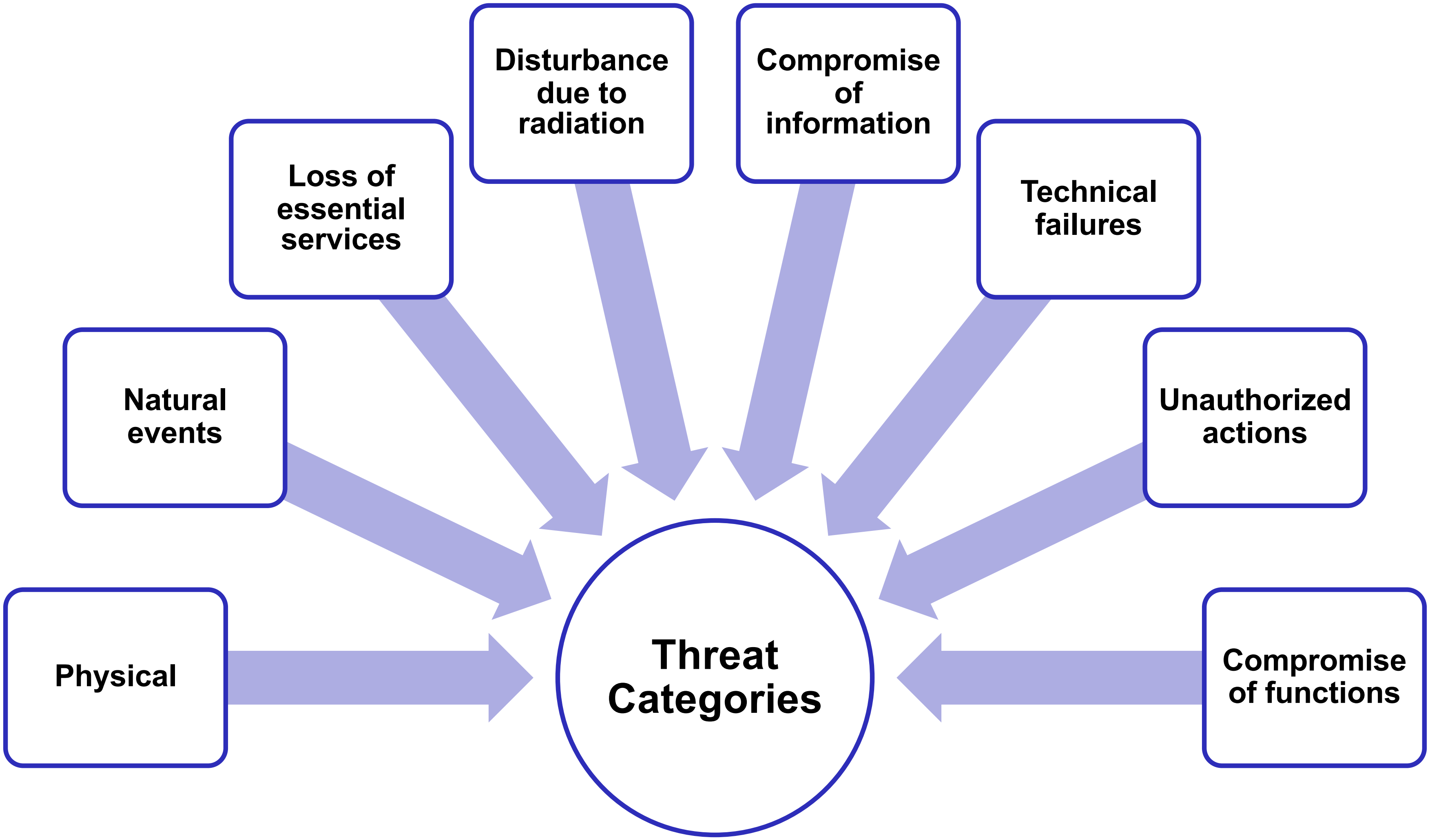
Threats are any conditions or events with the probability of damage to an information resource through the exploitation of system vulnerabilities

Threats can be

- External or internal
- Intended or unintended
- Naturally occurring or political
- Economical or competitive

It is vital to identify various types of threats that may affect the organization

Threats



Physical

Natural events

Loss of essential services

Disturbance due to radiation

Compromise of information

Technical failures

Unauthorized actions

Compromise of functions

Threat Categories

Threats

Internal Threats

- Unhappy employees may intentionally compromise systems or release confidential data
- Inadequately trained employees may unintentionally compromise systems or release confidential data
- Loss of key personnel that cause knowledge gaps

Mitigating internal threats

- Apply need-to-know or least-privilege methods
- Training sessions on ethics and policies
- Employees should sign a non-discloser agreement
- Ensure employees return all organization assets

Threats

External Threats

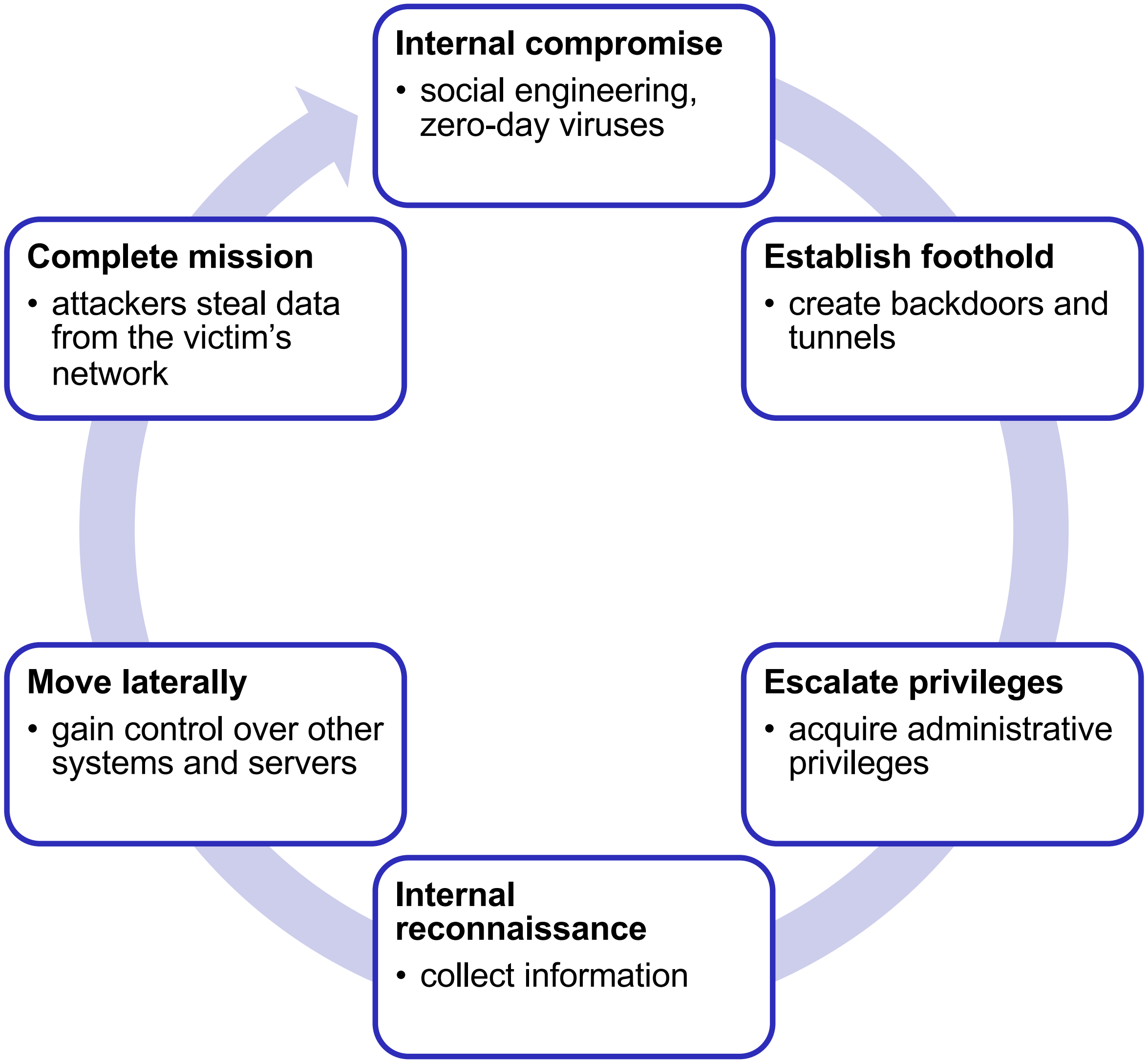
- Network environment stored offsite
- Cloud service providers
- Criminal acts or Espionage
- Flooding or Fire
- Power surge or utility failure
- Supply chain interruptions

Threats

Advanced Persistent Threat (APT)

- A skilled attacker that is determined to exploit the organization’s networks and systems

APT Life Cycle



Internal compromise

- social engineering, zero-day viruses

Establish foothold

- create backdoors and tunnels

Escalate privileges

- acquire administrative privileges

Internal reconnaissance

- collect information

Move laterally

- gain control over other systems and servers

Complete mission

- attackers steal data from the victim's network

Threats

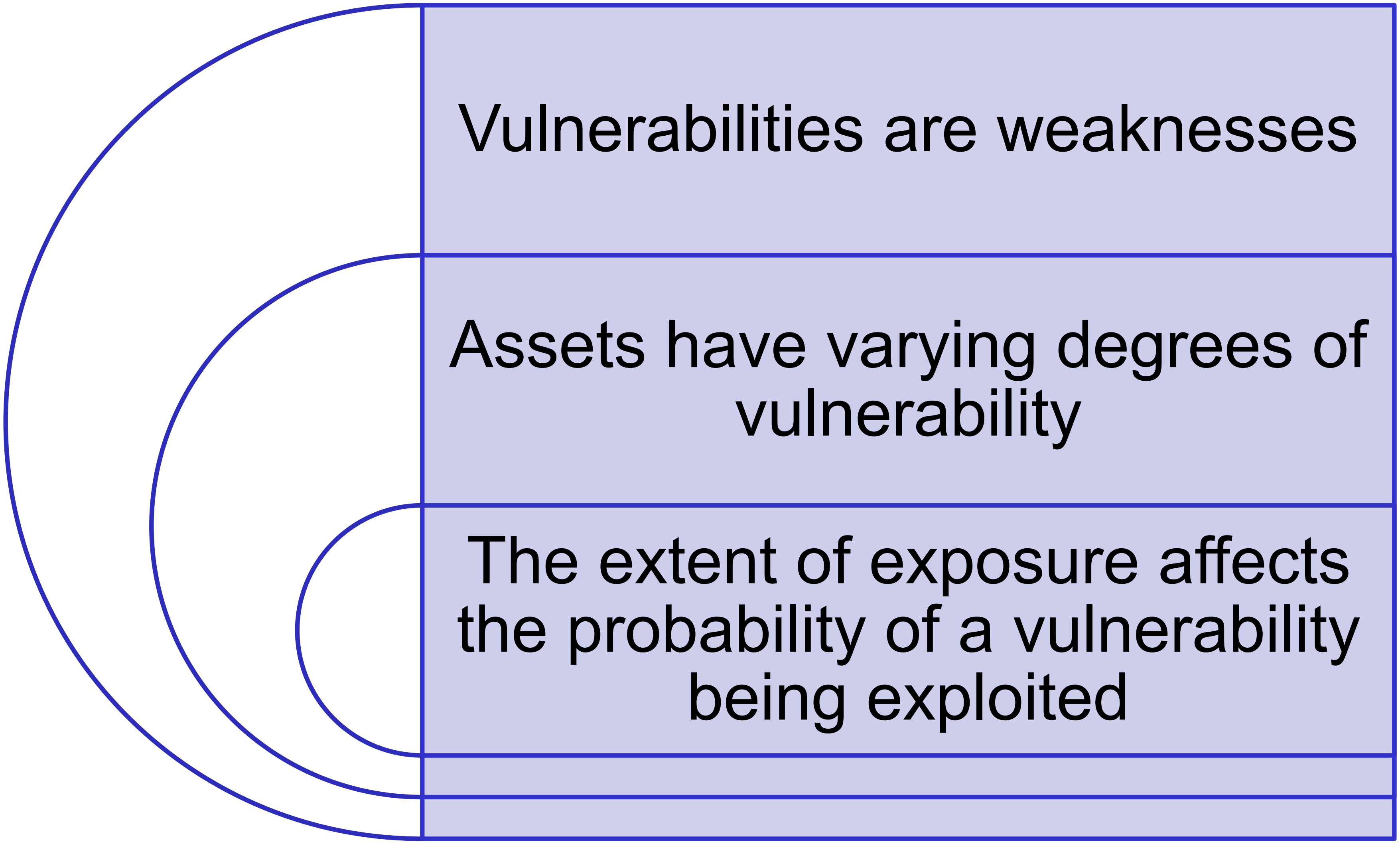
Emerging threat indicators

- Unusual activity on a system
- Repeated alarms
- Slow system and network performance

Emerging Threats

- New technology or software can have many vulnerabilities
- Bring your own device (BYOD) can be a threat but the benefit out weights the cost

Vulnerabilities



Vulnerabilities are weaknesses

Assets have varying degrees of vulnerability

The extent of exposure affects the probability of a vulnerability being exploited

Vulnerabilities

Estimating the degree of vulnerability can be quantitative or qualitative

- Estimating is imprecise in nature and it is important to communicate this to management

A control can be weak but it combined with other controls could be robust

- It is important to have a good understanding of controls

Vulnerabilities in IT systems can be identified using scanning tools

Vulnerabilities in processes and performances can be identified through careful review and analysis

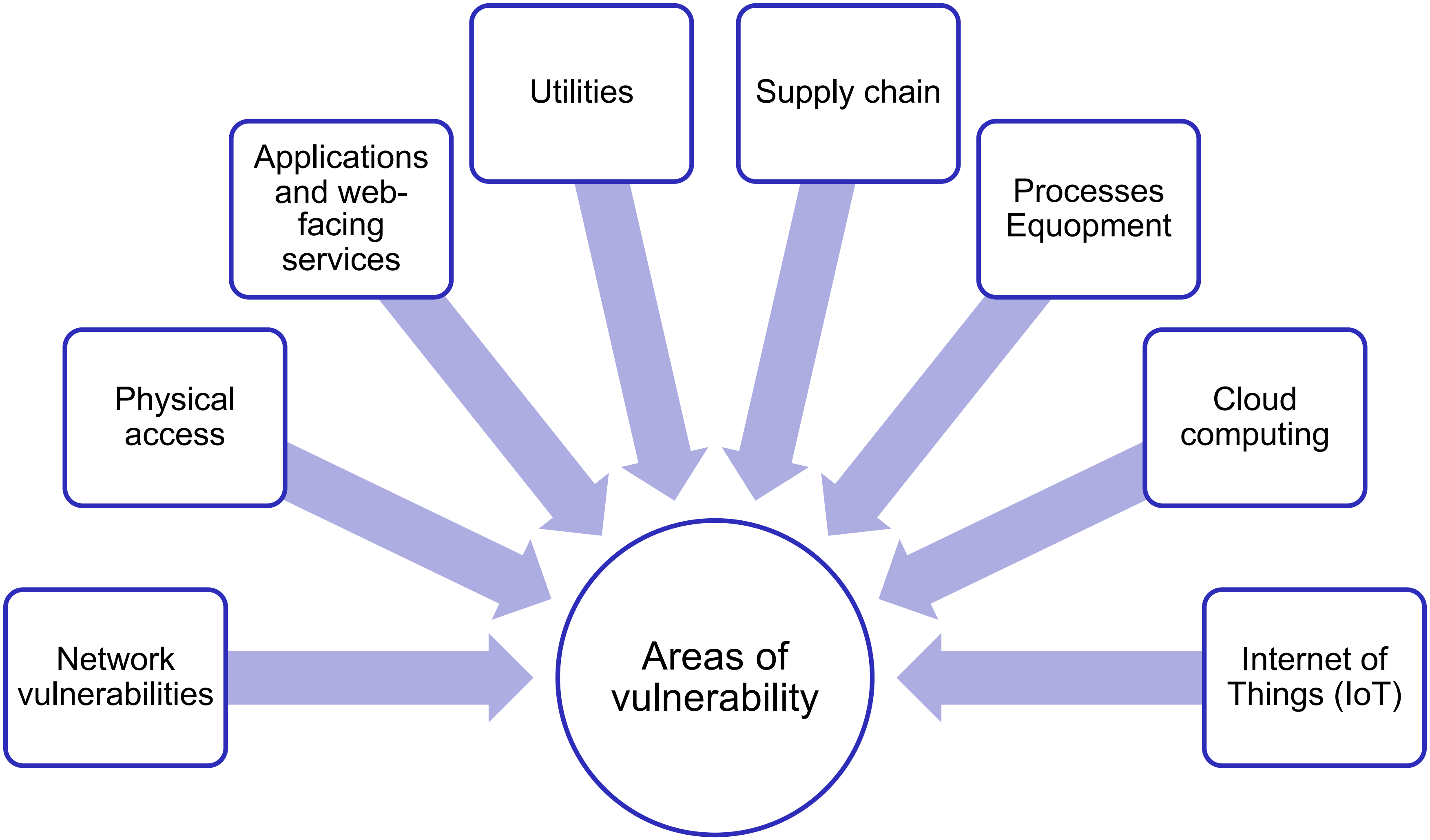
Vulnerabilities

Security training and awareness programs are very important to the security health of an organization

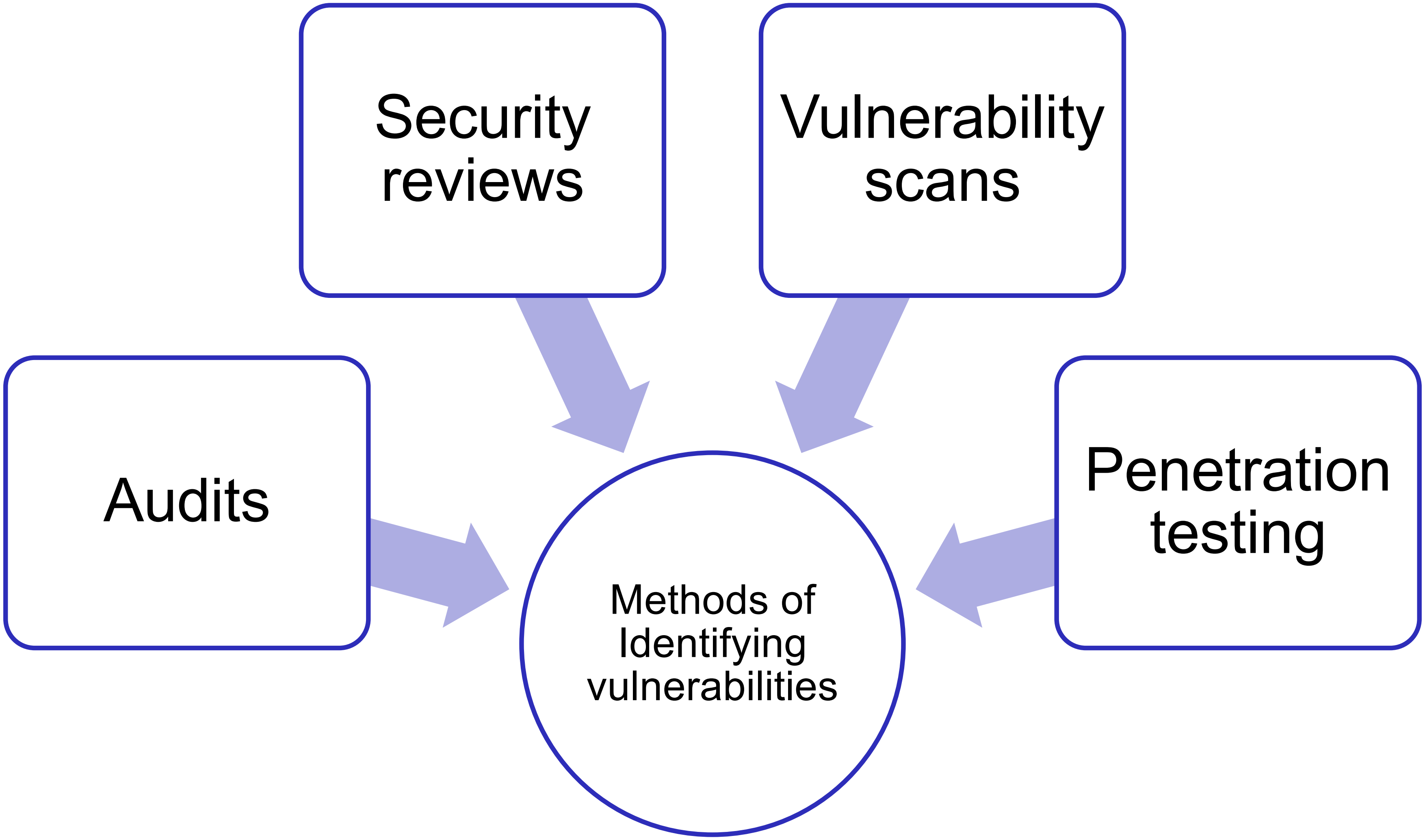
Employees that are unaware of security standers, policies, and guidelines are a high-risk vulnerability

- This can cause weak controls
- Poor ethics
- Technical issues
- Countless human errors

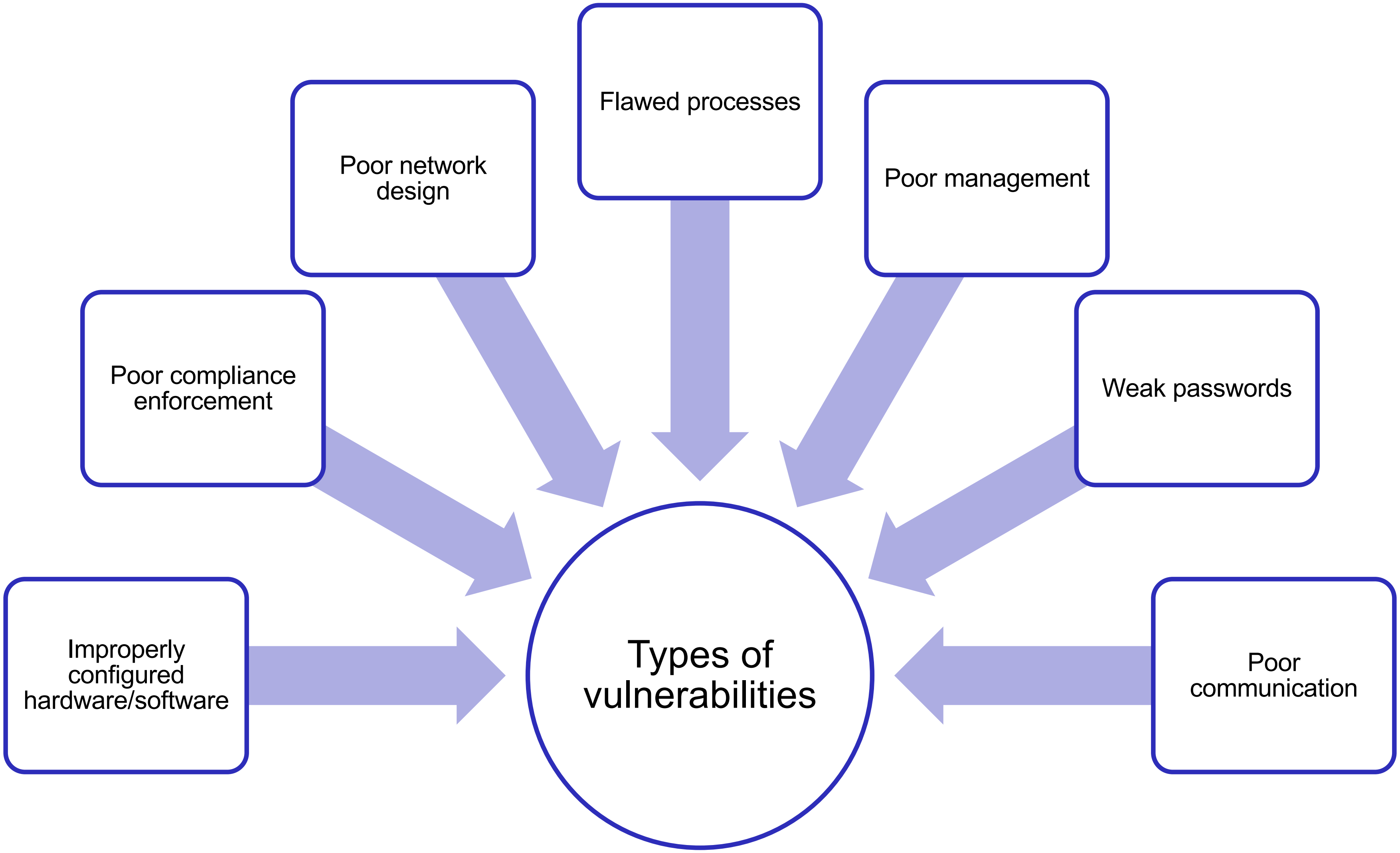
Vulnerabilities



Vulnerabilities



Vulnerabilities



Risk, Likelihood And Impact

Risk can be expressed as

- Threat × Vulnerability = Risk

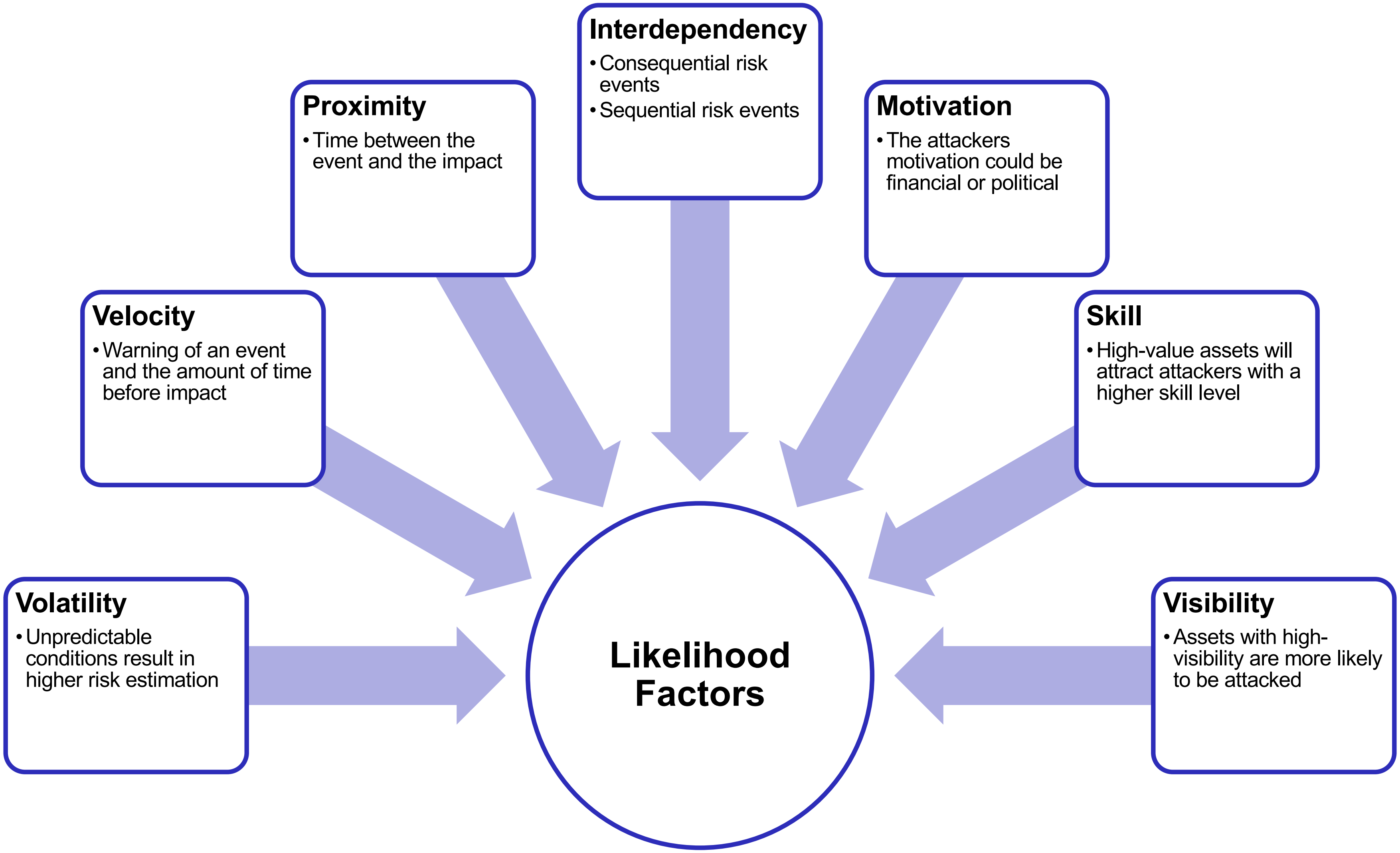
The likelihood of an event occurring is a measurement of its frequency of occurring

- The greater the frequency, the greater the likelihood, and therefore the greater the risk

It can be view that if there are no consequences (impact) there are no risks

- Threat × Vulnerability × Consequence = Risk

Risk, Likelihood And Impact



Interdependency
- Consequential risk events
- Sequential risk events

Proximity
- Time between the event and the impact

Motivation
- The attackers motivation could be financial or political

Velocity
- Warning of an event and the amount of time before impact

Skill
- High-value assets will attract attackers with a higher skill level

Volatility
- Unpredictable conditions result in higher risk estimation

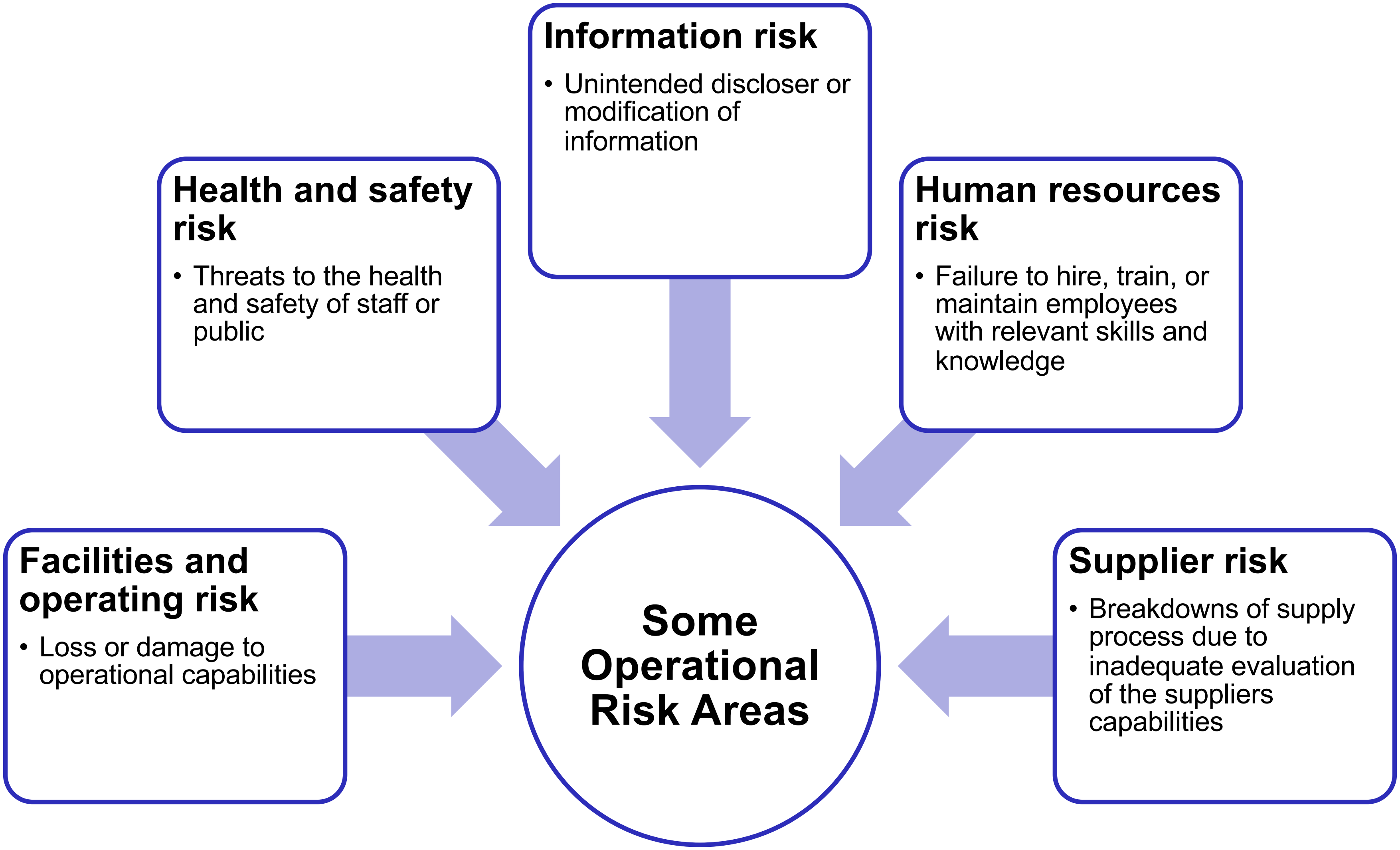
Visibility
- Assets with high-visibility are more likely to be attacked

Likelihood Factors

Risk, Likelihood And Impact

- Categorize possible risk areas of an organization
- Develop cost-effective risk treatment approaches that are relevant to the organization
- It is impossible to eliminate all risks therefore it is only practical to categorize risk at a high-level

Risk, Likelihood And Impact



Some Operational Risk Areas

Information risk

- Unintended discloser or modification of information

Health and safety risk

- Threats to the health and safety of staff or public

Human resources risk

- Failure to hire, train, or maintain employees with relevant skills and knowledge

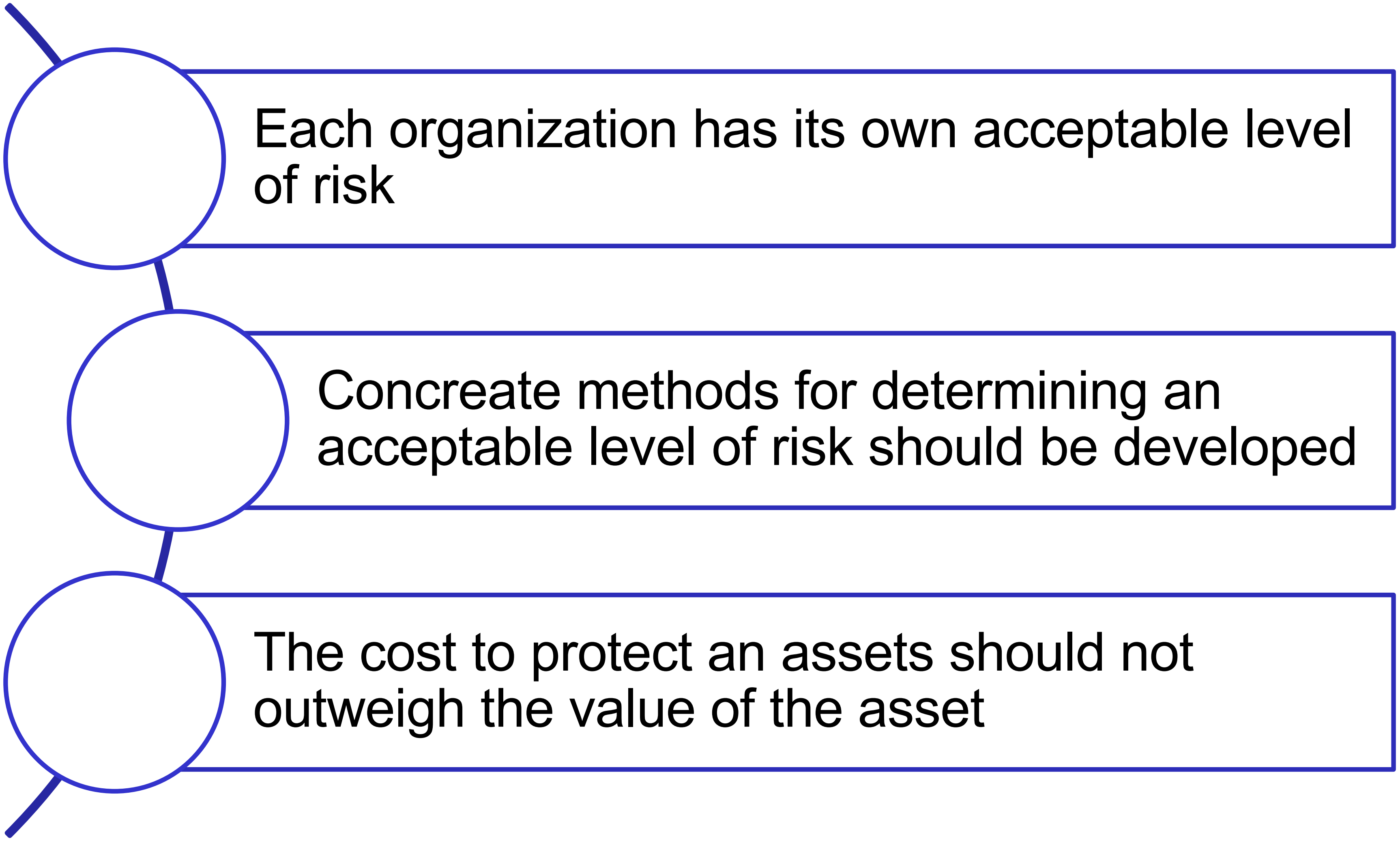
Facilities and operating risk

- Loss or damage to operational capabilities

Supplier risk

- Breakdowns of supply process due to inadequate evaluation of the suppliers capabilities

Risk, Likelihood And Impact

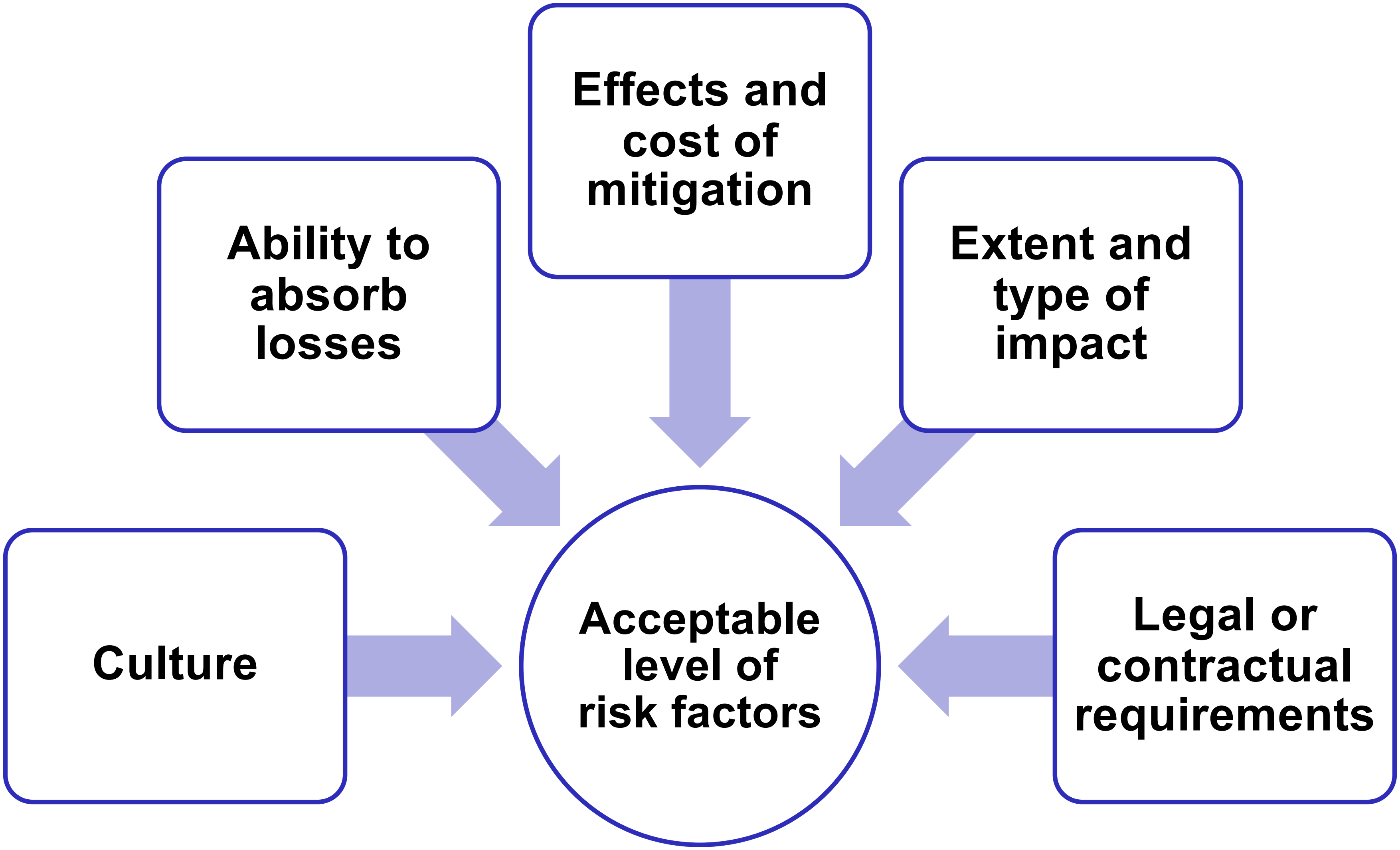


Each organization has its own acceptable level of risk

Concreate methods for determining an acceptable level of risk should be developed

The cost to protect an assets should not outweigh the value of the asset

Risk, Likelihood And Impact


Effects and cost of mitigation
Ability to absorb losses
Extent and type of impact
Culture
Acceptable level of risk factors
Legal or contractual requirements

Risk, Likelihood And Impact

- Adequately identify, analyze, evaluate, and respond to risks
- Properly allocate risk management efforts toward areas that pose the greatest risk and impact
- Reduce organizational risk by having strong access controls, limiting privileges, network segmentation, and good monitoring

Risk Register

Risk Register

- Should be the central source for all security risk information
- Should serve as the organization’s risk profile
- Should also serve as the reference point for all risk management activities

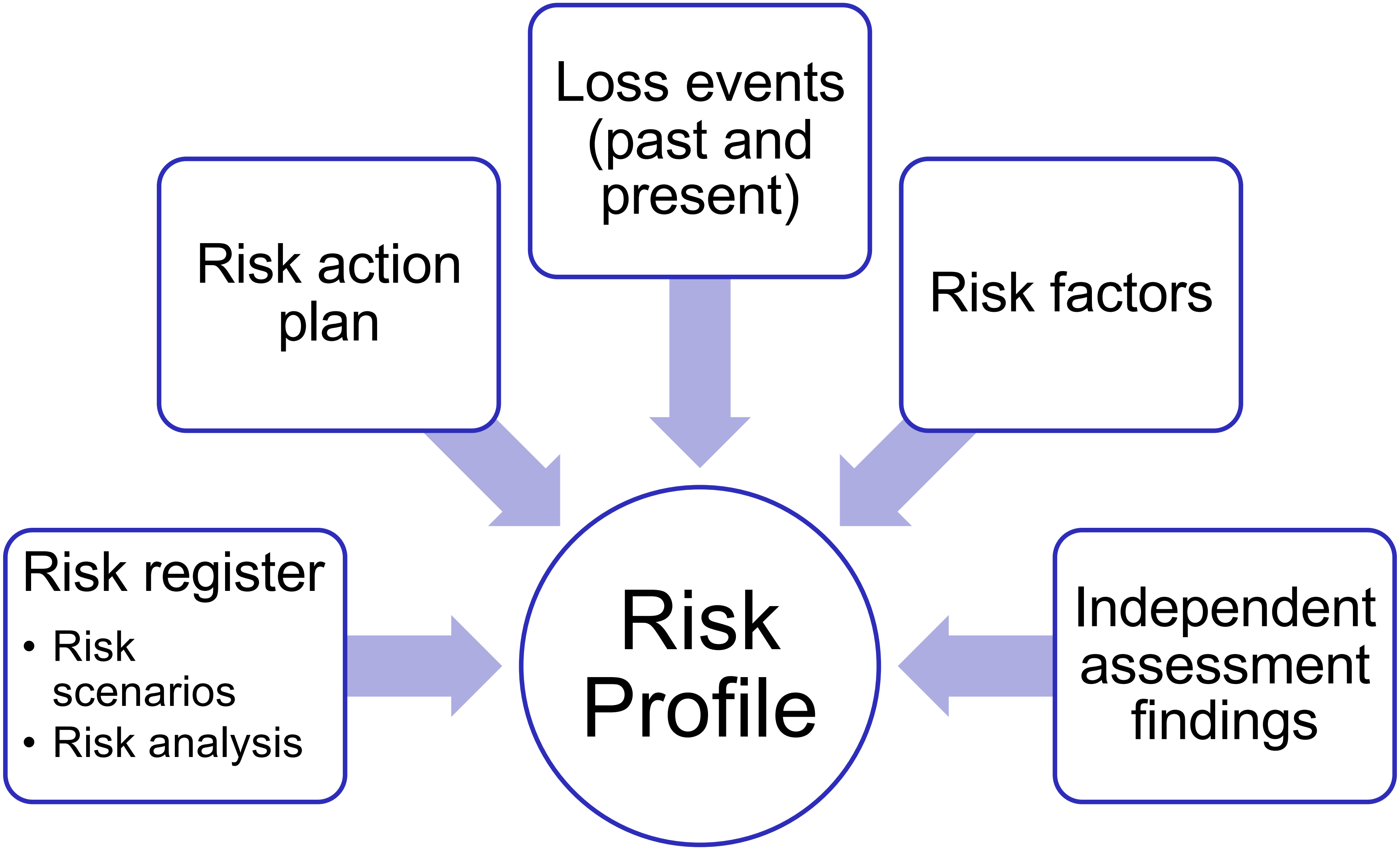
Risk Profile

- Vital for effective information risk management
- Provides an overview of all known risks

COBIT 5 Approach

- Has an effective, detailed process for creating a risk profile

Risk Register



Loss events (past and present)

Risk action plan

Risk factors

Risk register

- Risk scenarios
- Risk analysis

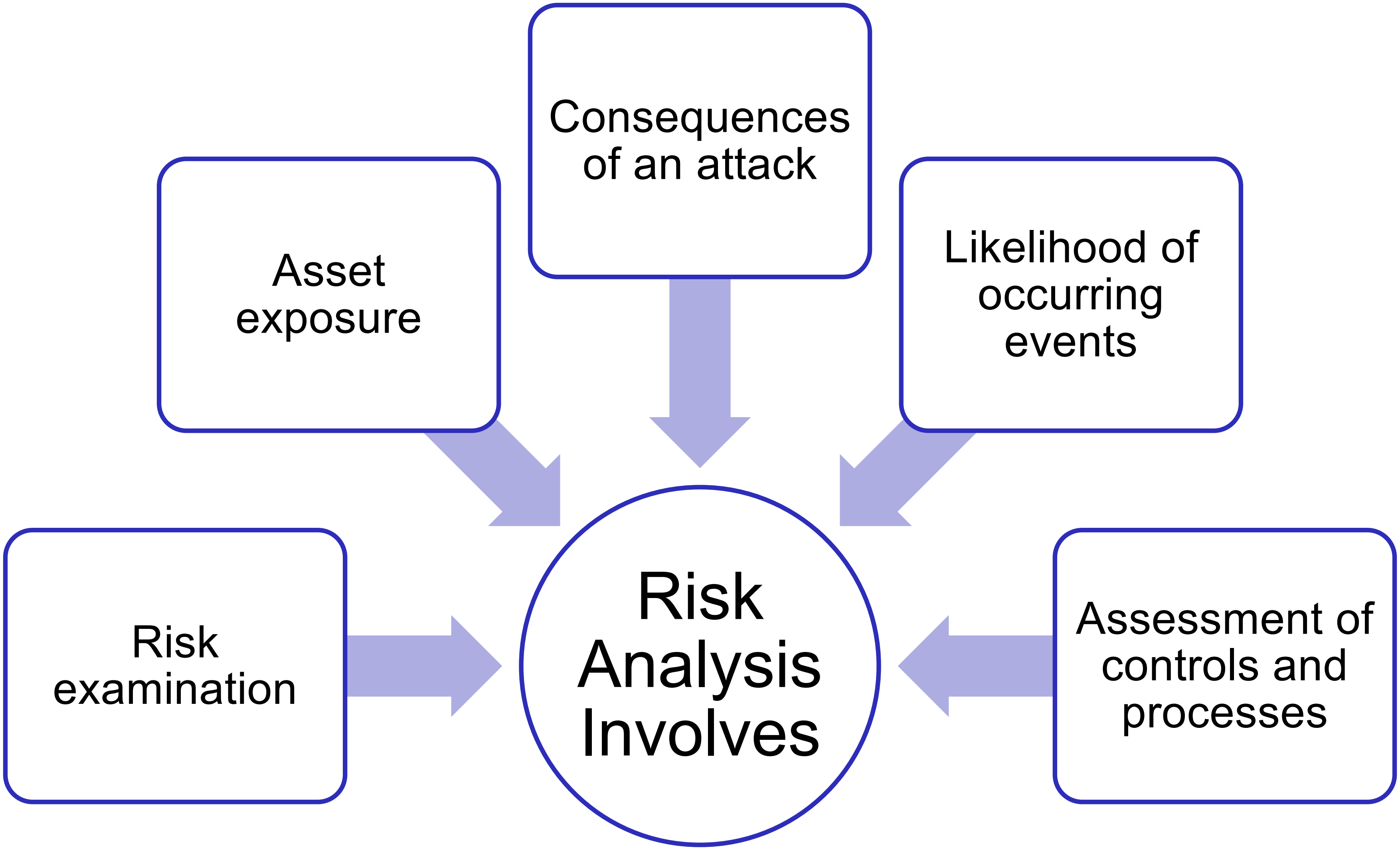
Risk Profile

Independent assessment findings

Risk Register

RISK REGISTER WORKSHEET EXAMPLE

Analysis Of Risk



Risk Analysis Involves

Asset exposure

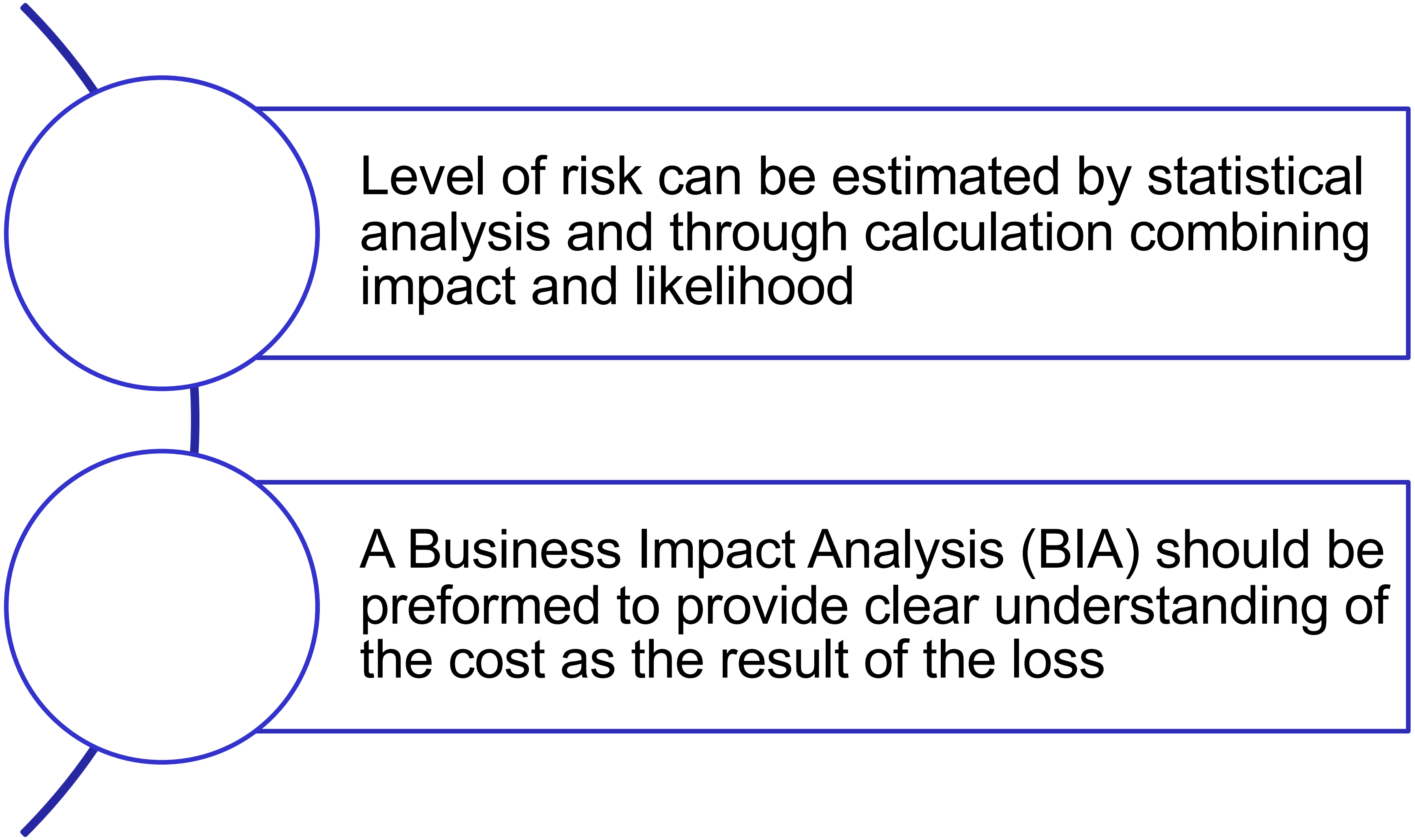
Consequences of an attack

Likelihood of occurring events

Risk examination

Assessment of controls and processes

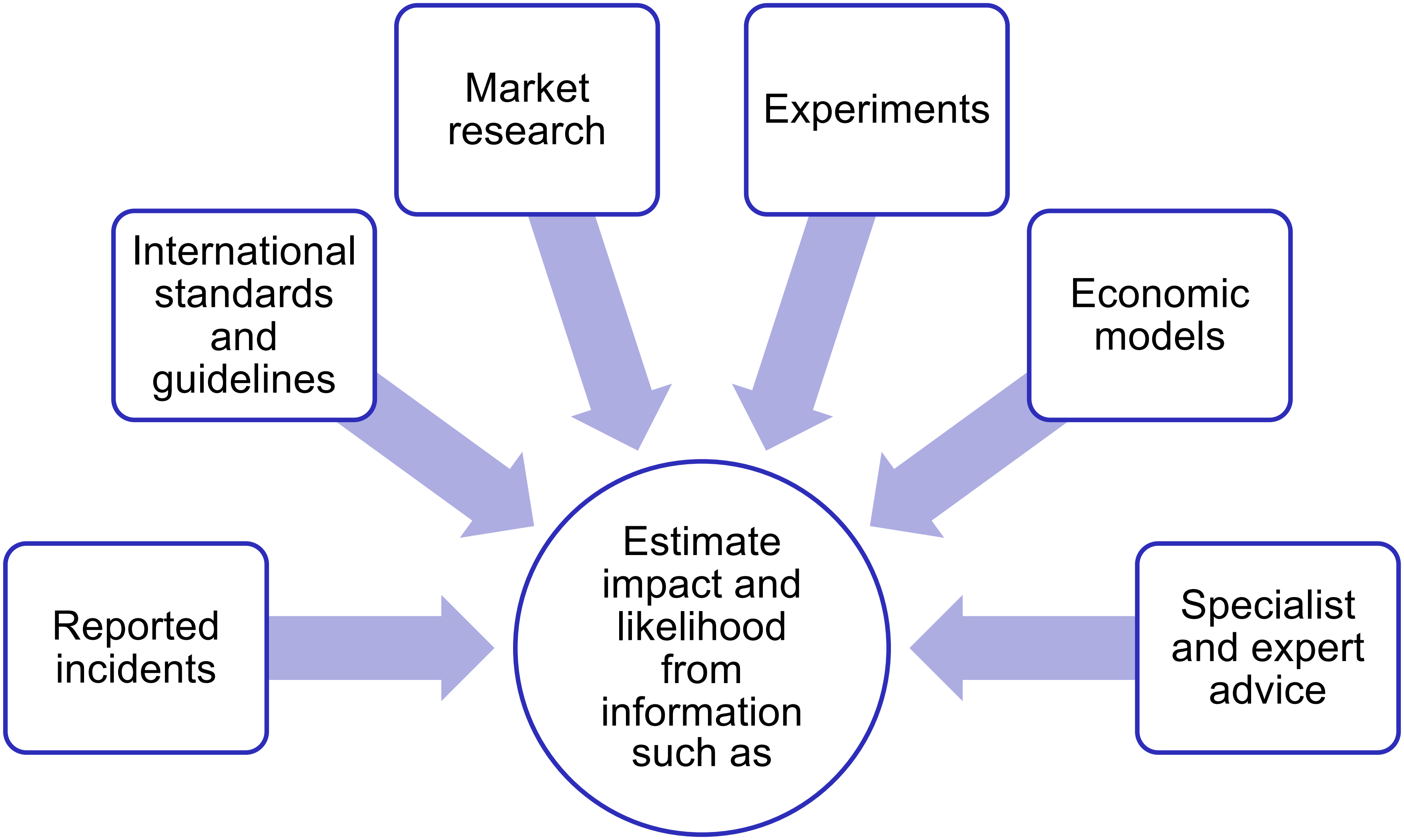
Analysis Of Risk



Level of risk can be estimated by statistical analysis and through calculation combining impact and likelihood

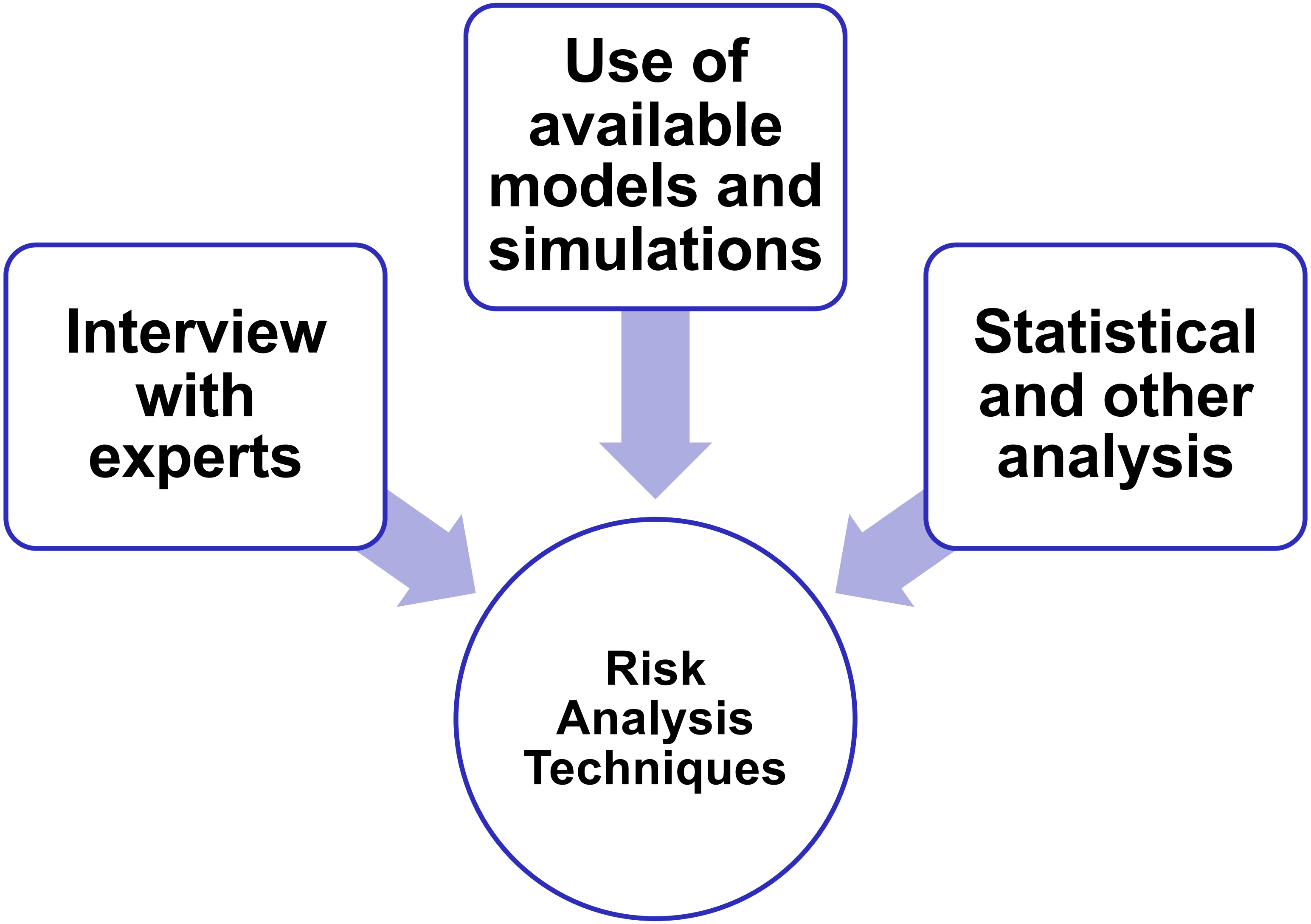
A Business Impact Analysis (BIA) should be preformed to provide clear understanding of the cost as the result of the loss

Analysis Of Risk



Market research
Experiments
International standards and guidelines
Economic models
Reported incidents
Estimate impact and likelihood from information such as
Specialist and expert advice

Analysis Of Risk



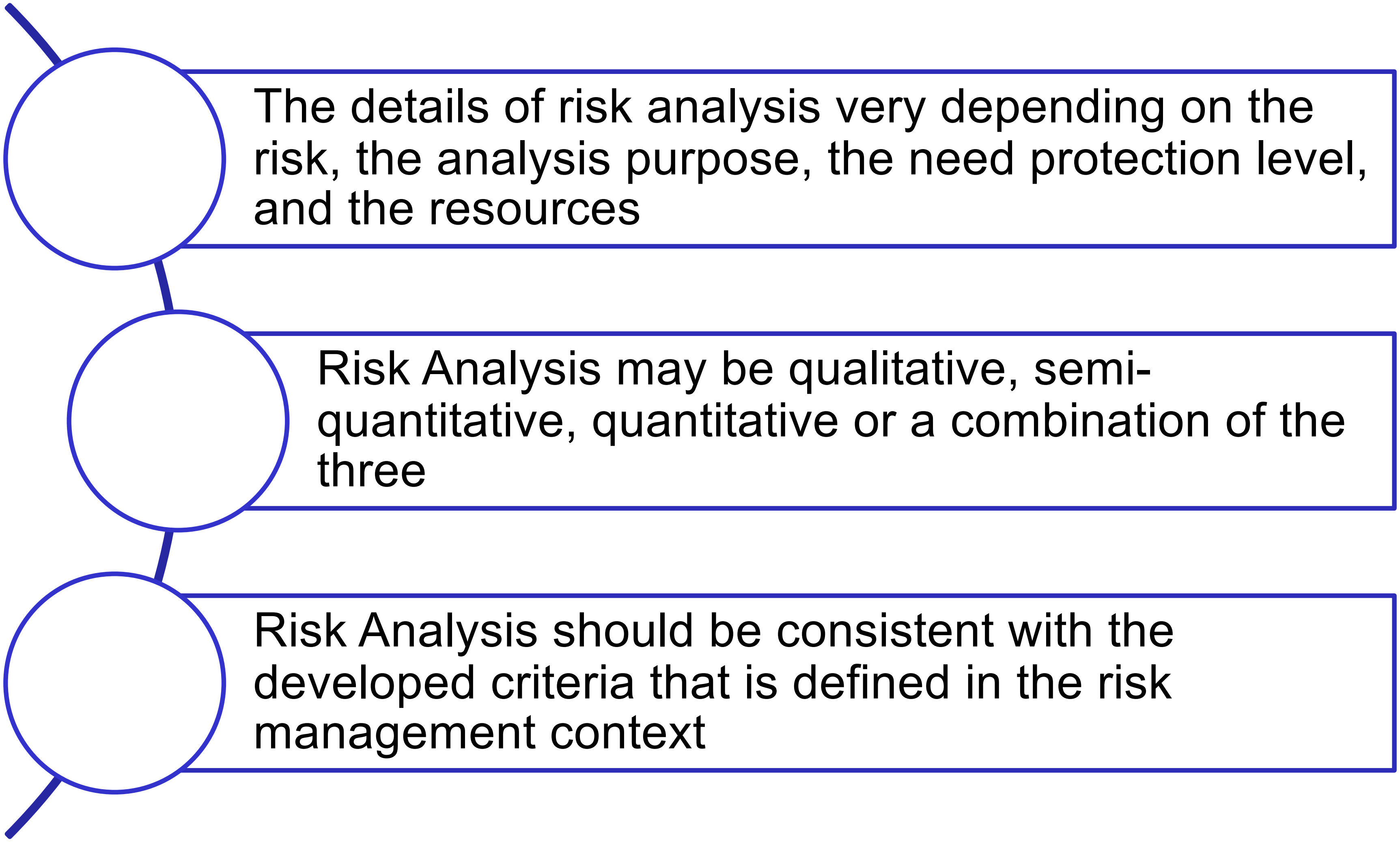
Use of available models and simulations

Interview with experts

Statistical and other analysis

Risk Analysis Techniques

Analysis Of Risk



The details of risk analysis very depending on the risk, the analysis purpose, the need protection level, and the resources

Risk Analysis may be qualitative, semi-quantitative, quantitative or a combination of the three

Risk Analysis should be consistent with the developed criteria that is defined in the risk management context

Qualitative Analysis Of Risk

In qualitative analysis the scale of impact and the likelihood of impact are shown and described in detail on the scale

Available scales can be adjusted to suit the given circumstances

Use qualitative analysis

- As an internal assessment to identify risk,
- On nontangible assets (culture, reputation)
- Where there is not enough data or resources to develop an acceptable quantitative approach

Qualitative Analysis Of Risk

Impact

Catastrophic	🟨	🟧	🟥	🟥	🟥
Material	🟨	🟨	🟧	🟥	🟥
Major	🟩	🟨	🟨	🟧	🟥
Minor	🟩	🟨	🟨	🟨	🟧
Insignificant	🟩	🟩	🟩	🟨	🟨
	Rare	Unlikely	Moderate	Likely	Frequent

Likelihood

Semiquantitative Analysis Of Risk

- In Semiquantitative Analysis the goal is to assign values to the scales used
- The values used are usually not real values and do not show the actual magnitude of the consequences
- The values used must be used with a formula that accounts for the limitations and the assumptions made in the scale's description
- This type of analysis has some inconsistencies due to the values used may not appropriately reflect comparisons between risks
- The values chosen should be generic enough to prioritize one risk before another risk
- Define a common understanding for values chosen

Semiquantitative Analysis Of Risk

Similarly to Qualitative Analysis

Can use this common analysis approach and add values to the calculate risk priority

The probability of risk can be calculated as

- Risk = impact × likelihood

Example

- Risk = 4(material) × 3(moderate) = 12

Impact

Catastrophic 5	🟨	🟧	🟥	🟥	🟥
Material 4	🟨	🟨	🟧	🟥	🟥
Major 3	🟩	🟨	🟨	🟧	🟥
Minor 2	🟩	🟨	🟨	🟨	🟧
Insignificant 1	🟩	🟩	🟩	🟨	🟨
	Rare 1	Unlikely 2	Moderate 3	Likely 4	Frequent 5

Likelihood

Quantitative Analysis Of Risk

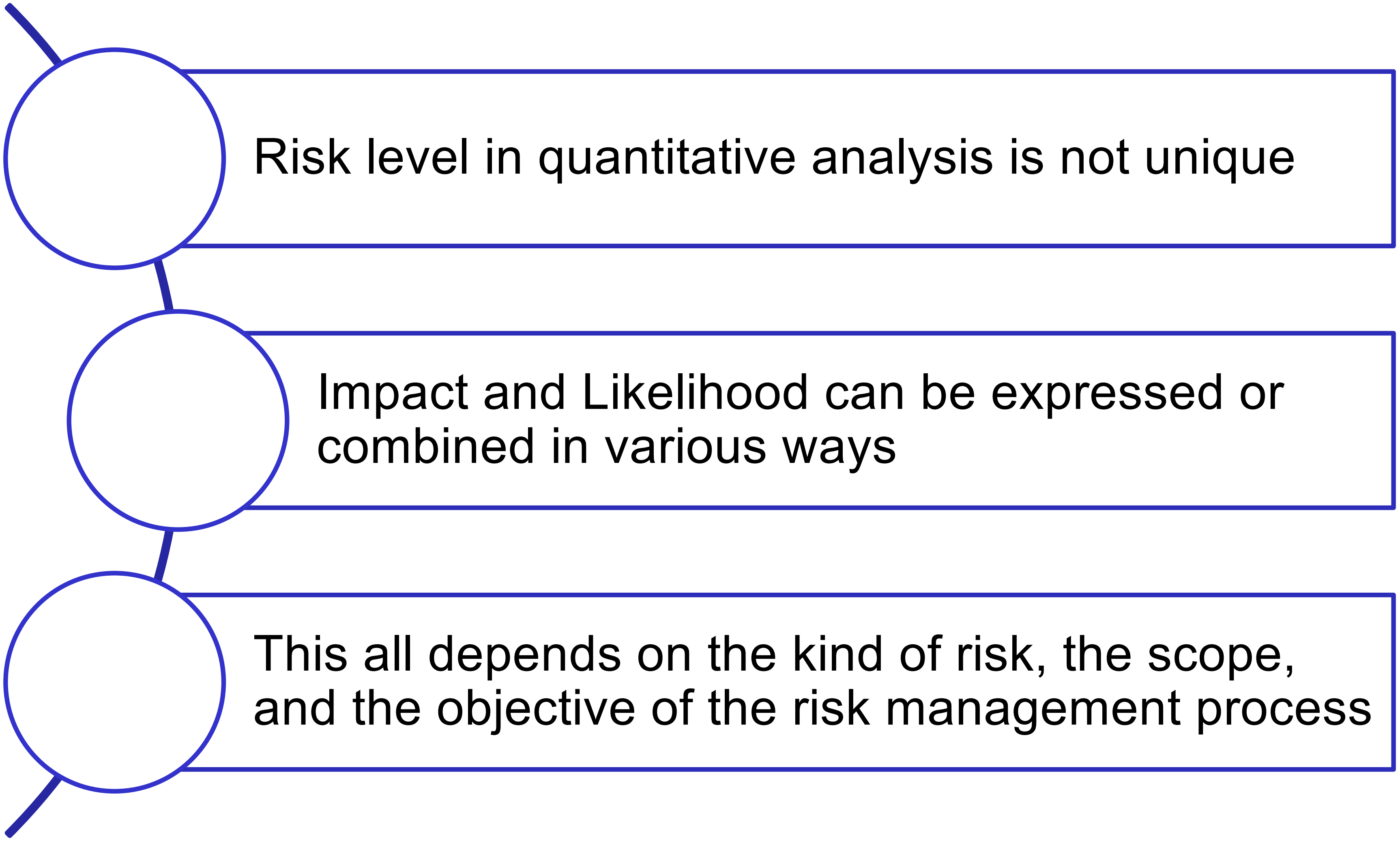
In Quantitative Analysis it is important to assign numerical values to both impact and likelihood

This analysis depends on the accuracy of the assigned values and the validity of the used statistical model

Determine impact by evaluating the results of an event or by extrapolation from experimental data or studies

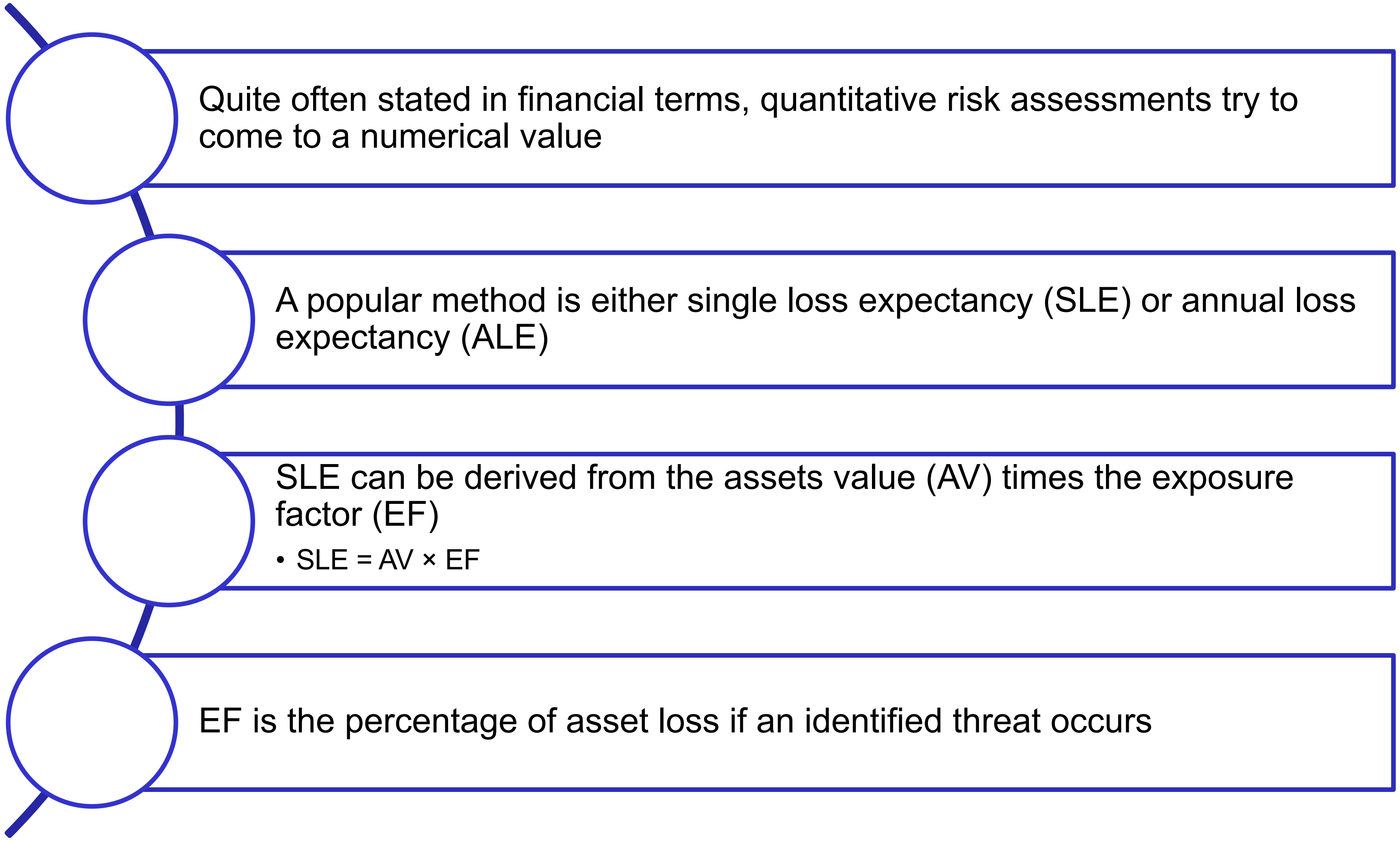
Consequences are expressed in terms of monetary, technical, operational, or human impact criteria

Quantitative Analysis Of Risk



- Risk level in quantitative analysis is not unique
- Impact and Likelihood can be expressed or combined in various ways
- This all depends on the kind of risk, the scope, and the objective of the risk management process

Annual Loss Expectancy



Quite often stated in financial terms, quantitative risk assessments try to come to a numerical value

A popular method is either single loss expectancy (SLE) or annual loss expectancy (ALE)

SLE can be derived from the assets value (AV) times the exposure factor (EF)

- SLE = AV × EF

EF is the percentage of asset loss if an identified threat occurs

Annual Loss Expectancy

ALE expresses that the more occurrences of an event will cause the probable losses to be greater

Annualized rate of occurrence (ARO) is added to the ALE equation

- ALE = SLE × ARO

ARO is the number of times a threat is projected to occur on a single asset

The level of risk associated with the threat equally effects the ARO

- The higher the risk the higher the ARO will be

Value At Risk

- Value at risk (VAR) is used in some financial sectors, which can also be useful in risk management
- For a given period of time VAR uses the probability distribution of loss from past data in that period with a certainty factor around 95 or 99 percent
- Monte Carlo simulations run through thousands of iterations with arbitrary variables based on the past data to generate the probability distribution

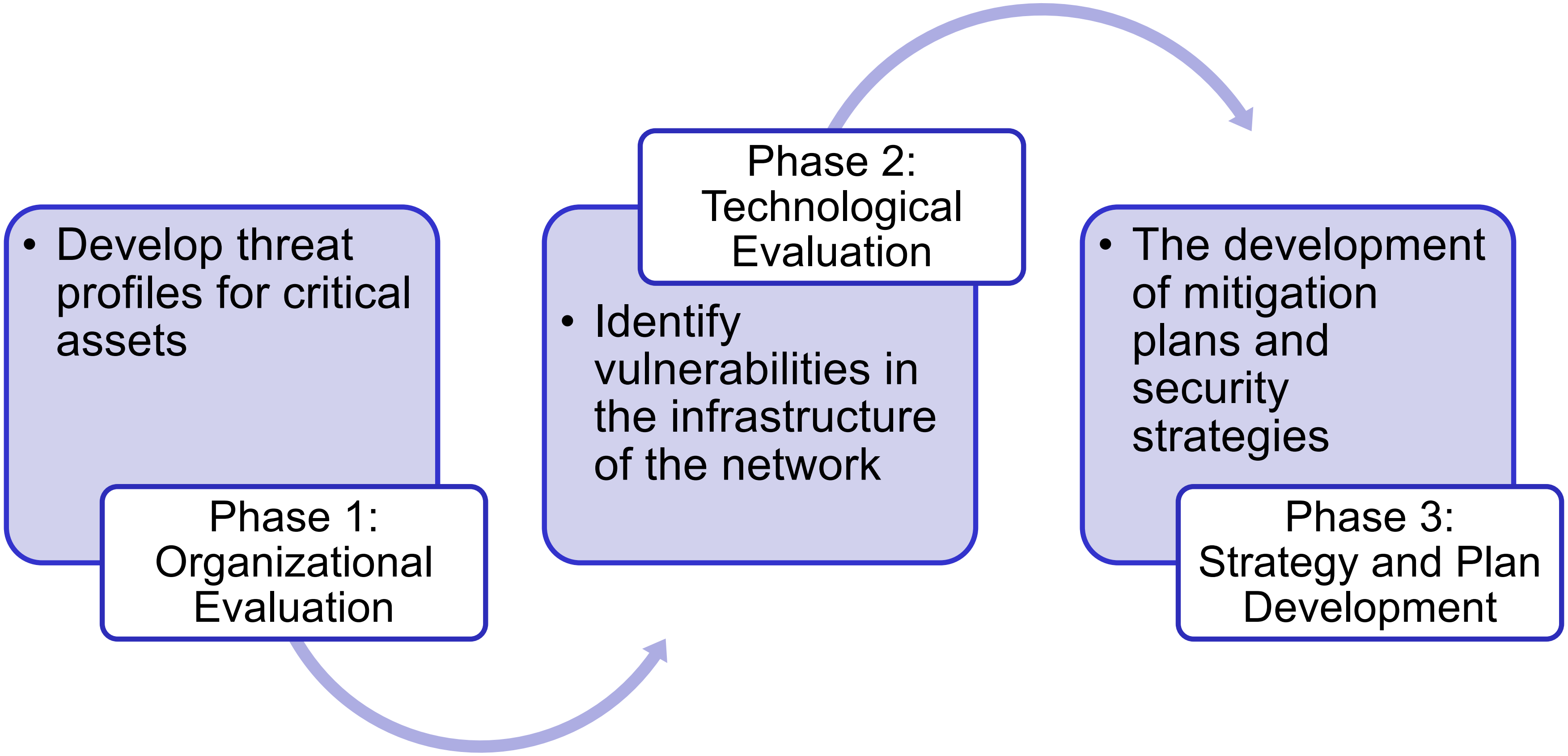
Analysis Of Risk

Operationally critical threat asset and vulnerability evaluation (OCTAVE)

A risk assessment and ranking approach that helps an organization understand, assess, and address its information security risk

Its methodology is process-driven and is utilized in identifying, prioritizing, and managing information security risk

OCTAVE Phases



- Develop threat profiles for critical assets

Phase 1: Organizational Evaluation

Phase 2: Technological Evaluation

- Identify vulnerabilities in the infrastructure of the network

- The development of mitigation plans and security strategies

Phase 3: Strategy and Plan Development

Other Risk Analysis Methods

Bayesian Analysis

A statistical inference method that utilizes past distribution data to calculate the probability of the result

Event Tree Analysis

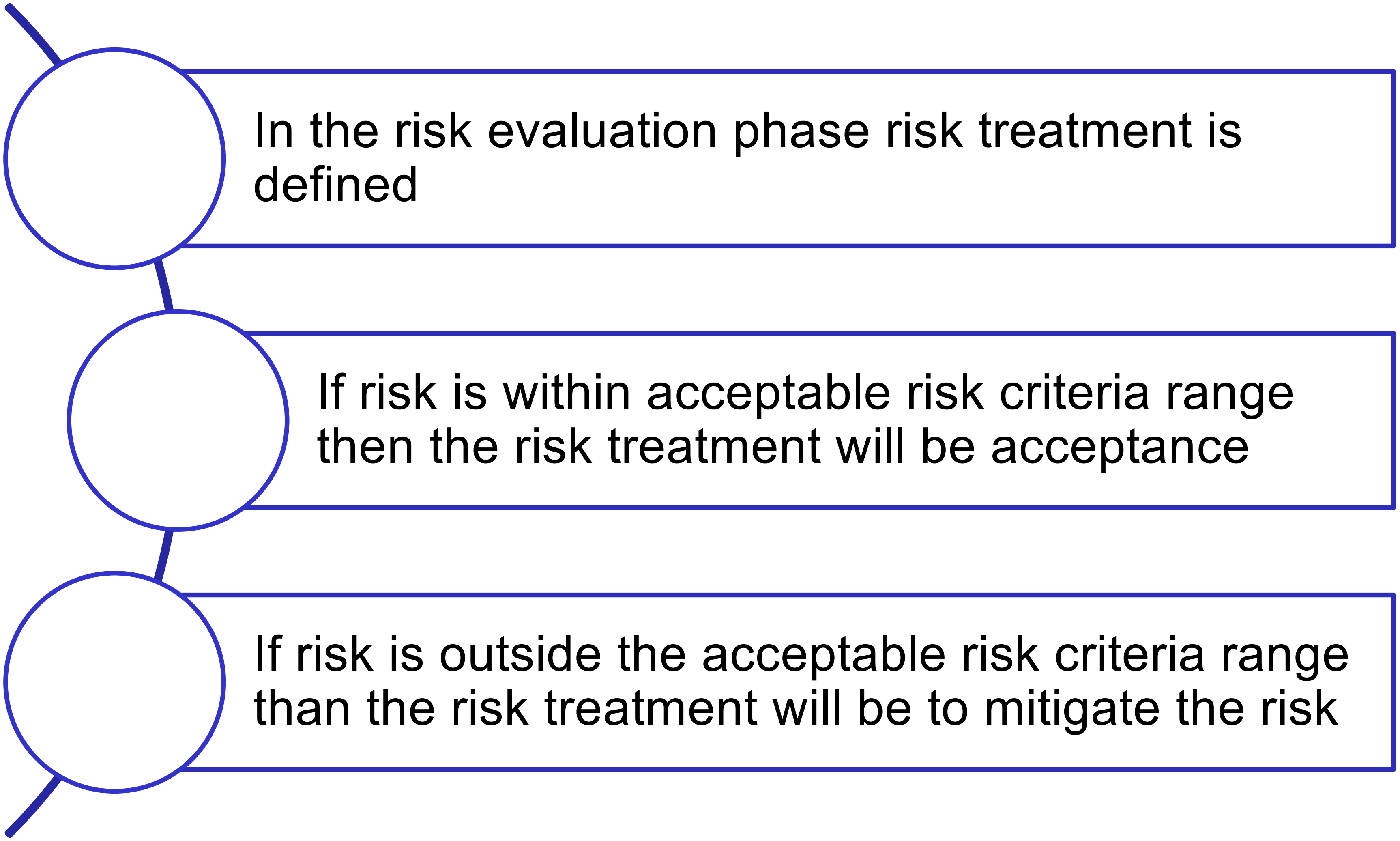
Forward-looking, bottom-up model that utilizes inductive reasoning to measures the probability of different events resulting in potential outcomes

Markov Analysis

Analyzes systems that can be in multiple states at one time

It is assumed that future events and past events are independent of each other

Evaluation Of Risk



In the risk evaluation phase risk treatment is defined

If risk is within acceptable risk criteria range then the risk treatment will be acceptance

If risk is outside the acceptable risk criteria range than the risk treatment will be to mitigate the risk

Evaluation Of Risk

It is important to find the most cost-effective mitigation option

Mitigation options include

- Adding/modifying controls or process
- Redesigning the system to reduce technical risk
- Transfer or share the risk

Risk transfer can be more cost-effective

- Tends to be for risks that have low likelihood and high impact

If mitigation cost is too high management could decide to accept the risk

Evaluation Of Risk

Acceptable risk criteria must consider

- The organization’s objectives
- The views of the stakeholders
- The scope and objective of the risk management process
- Any possible margins of error

The deciding factor is usually risk but other possible factors are

- Consequences
- The likelihood of events
- The impact of a series of simultaneous events
- The impact of cascading risk
- Cost of risk treatment
- The ability to absorb losses

Risk Ranking

From the results of a risk assessment, risk is arranged in an order that best guides risk response efforts

Risk Ranking is shown through combining of all the risk components

Risk ranking shows the level of risk associated with a threat

Risk Ownership And Accountability

A manager in the organization must identify the owner of the risk

- This concept work to create an environment where risk is addressed through proper treatment

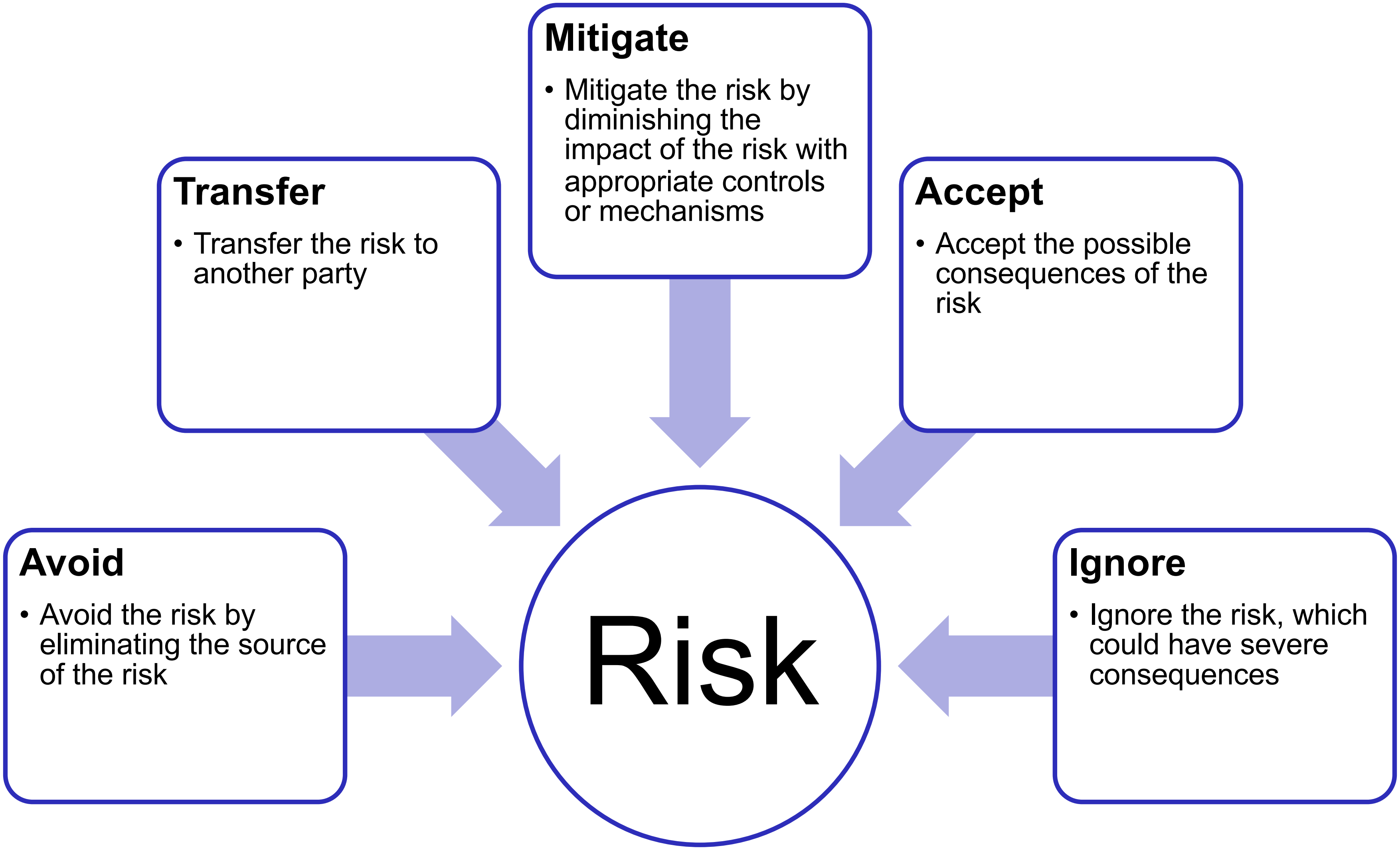
The risk owner is accountable for

- Accepting risk based on the organization's risk appetite
- Selecting the best risk response based on guidance from the information security manager
- Approving controls when the risk response is mitigation

The risk owner is also responsible for

- Any controls connected to risk
- Monitoring the controls
- Documenting risk elements

Risk Treatment Options



Mitigate

- Mitigate the risk by diminishing the impact of the risk with appropriate controls or mechanisms

Transfer

- Transfer the risk to another party

Accept

- Accept the possible consequences of the risk

Avoid

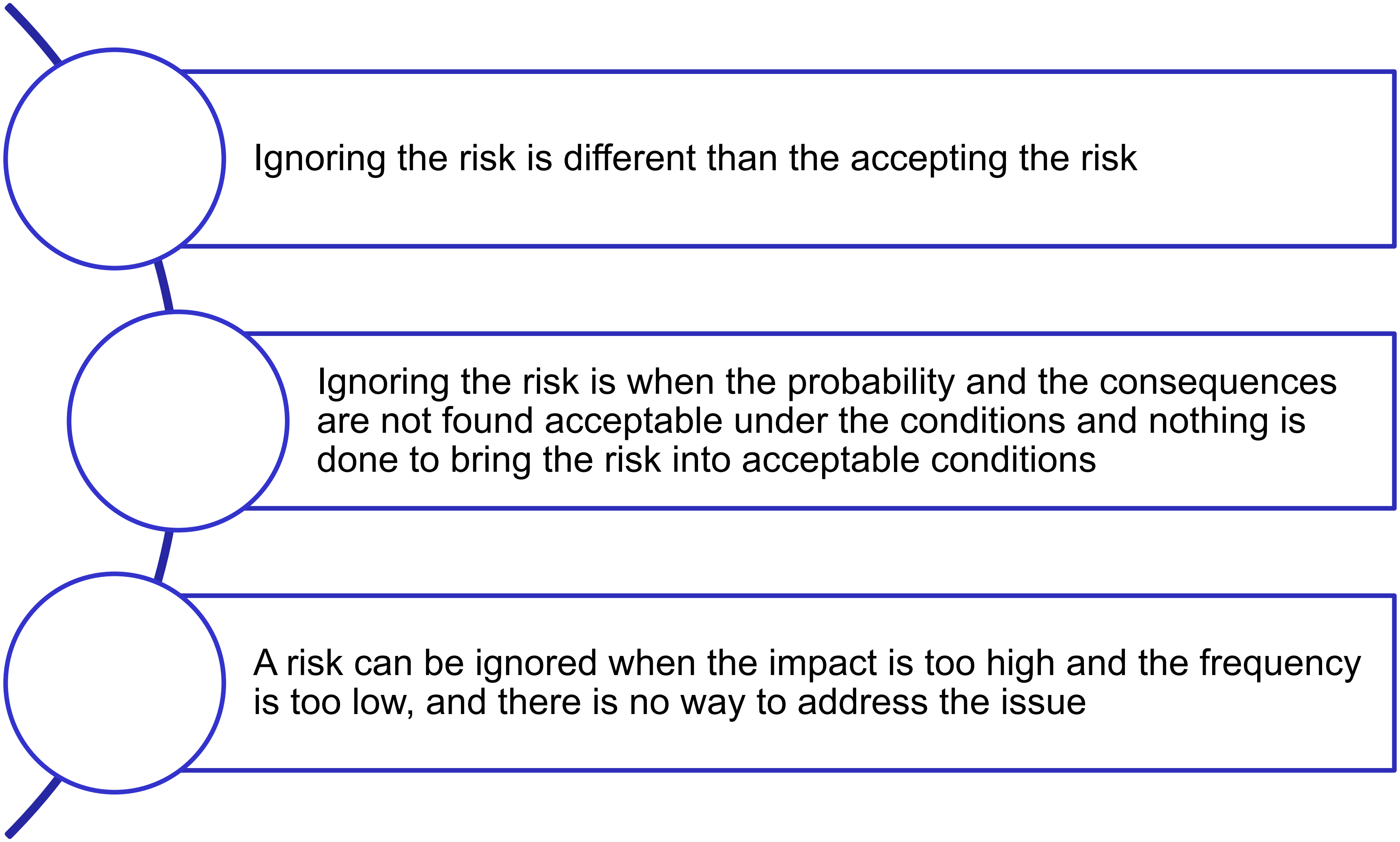
- Avoid the risk by eliminating the source of the risk

Risk

Ignore

- Ignore the risk, which could have severe consequences

Ignore The Risk

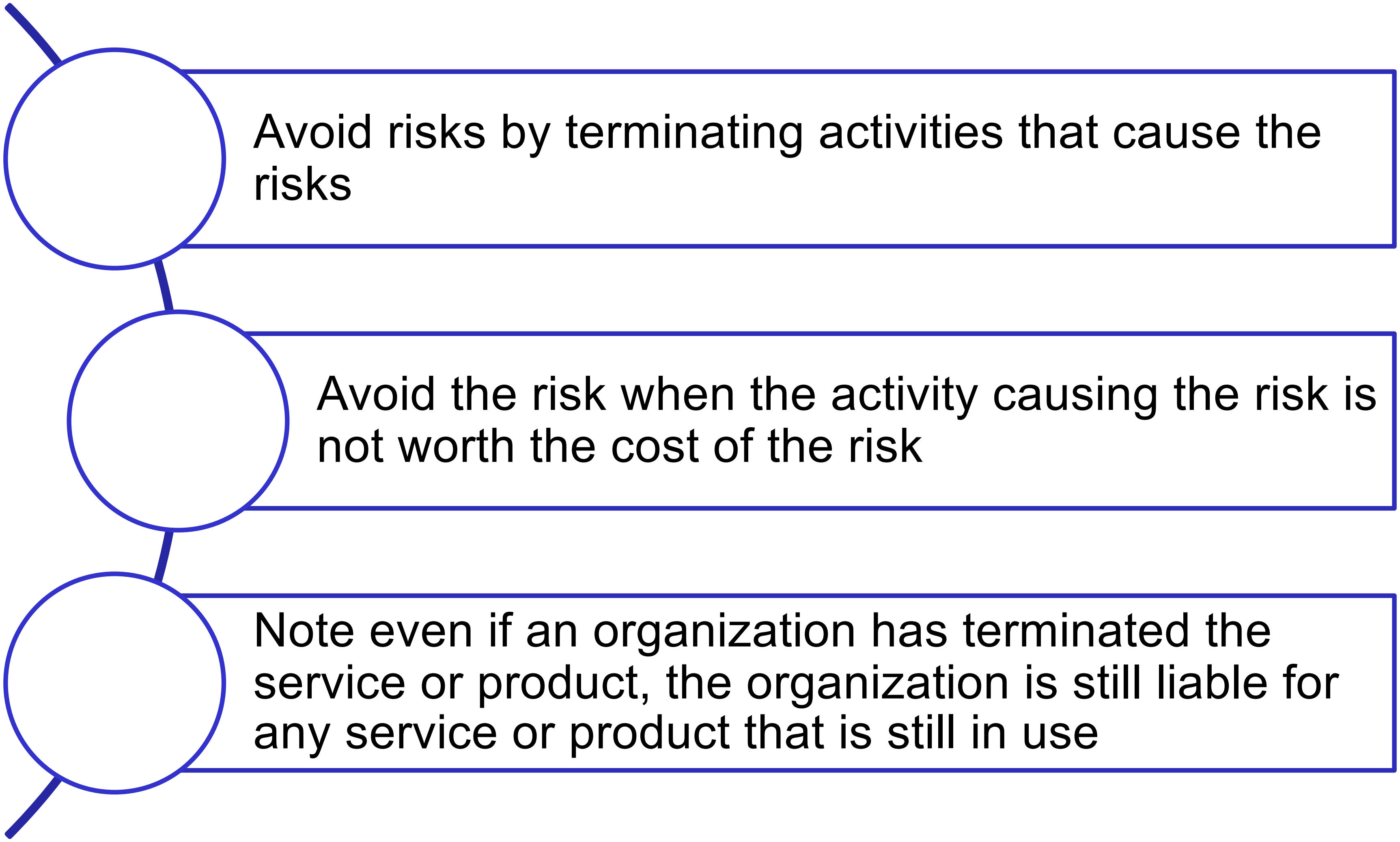


Ignoring the risk is different than the accepting the risk

Ignoring the risk is when the probability and the consequences are not found acceptable under the conditions and nothing is done to bring the risk into acceptable conditions

A risk can be ignored when the impact is too high and the frequency is too low, and there is no way to address the issue

Avoid The Risk



Avoid risks by terminating activities that cause the risks

Avoid the risk when the activity causing the risk is not worth the cost of the risk

Note even if an organization has terminated the service or product, the organization is still liable for any service or product that is still in use

Transfer The Risk

- Risk transfer is sharing the risk with another party to reduce the impact
- For example insurance can be purchased to reduces areas of risk and cover some or all the cost associated with the impact
- Insurance companies get premium payments that accounts for the degree of risk it obtains
- When transferring risk to third-party contracts it is important to discourse the liability and responsibility of both parties

Mitigate The Risk

Ways to mitigate risk

Improve security controls

Establish countermeasures

Change or terminate risky processes

Accept The Risk

Risk may be accepted in a variety of conditions

- If the cost of mitigating is too high in comparison to the value of the asset
- If effectively reducing or eliminating the risk is not achievable
- If the impact of the risk is low

Any risk that is accepted must be

- Documented appropriately and accurately
- Regularly reviewed to ensure the acceptance of the risk is still valid

Risk Acceptance Framework

Low

- Local management can accept risk

Medium

- Chief information officer (CIO) can accept risk

High

- CIO, director, or chief information security officer (CISO), accept risk depending on the possible impact

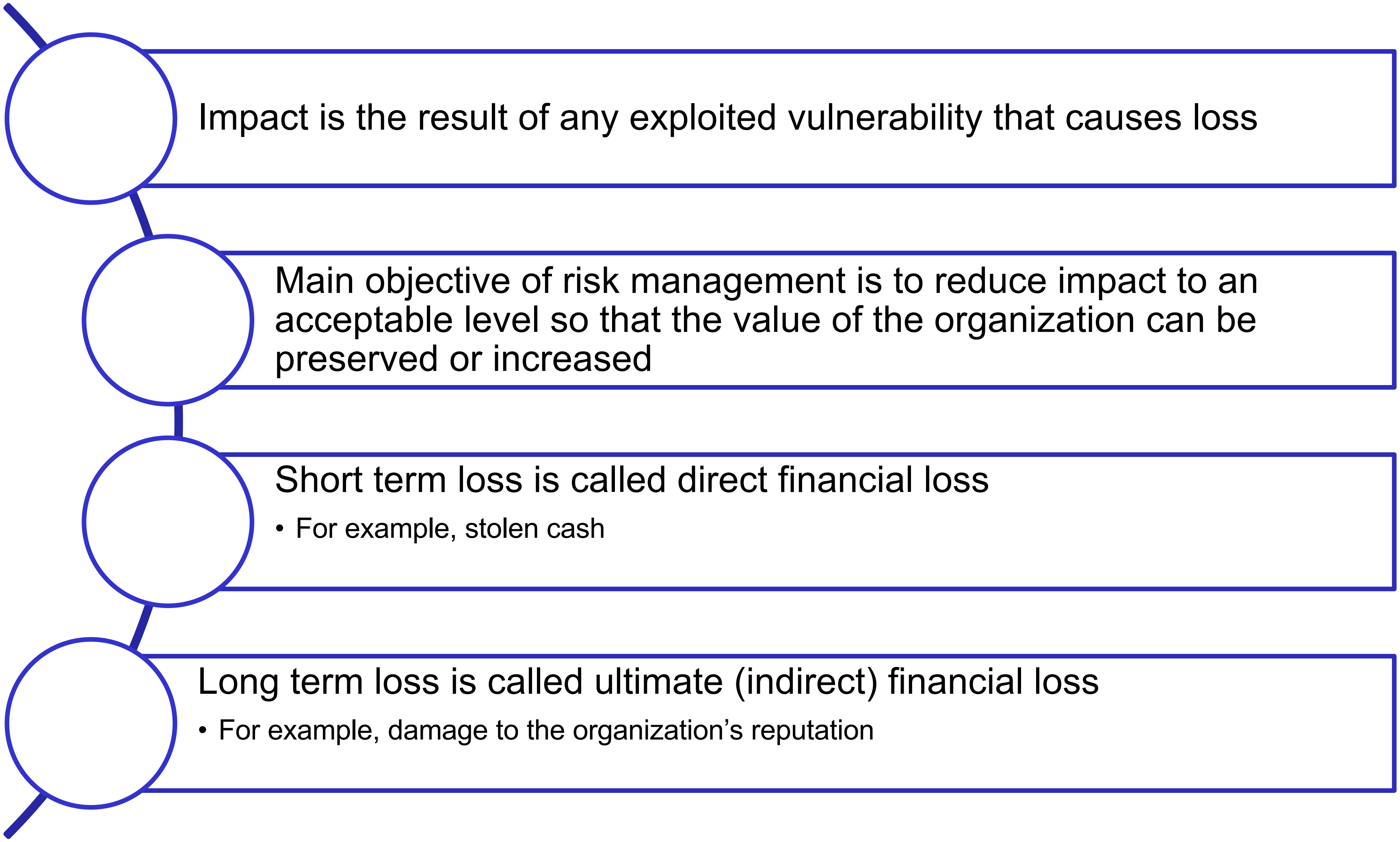
Severe

- Only at a board level can risk be accepted, it depends on the possible impact
- It is mandatory to reduce risk through rigorous controls or monitoring
- The process of notifying management is required

Residual Risk

- Risk before mitigation is inherent risk
- Residual risk is risk that remains after the implementations of countermeasures and controls
- There is always residual risk, reducing one risk inevitably presents another risk
- Ensure all residual risk is within the organization’s criteria of acceptable risk
- Risk tolerance is the permitted deviation from acceptable risk and is presented as a range or a percentage

Impact



Impact is the result of any exploited vulnerability that causes loss

Main objective of risk management is to reduce impact to an acceptable level so that the value of the organization can be preserved or increased

Short term loss is called direct financial loss

- For example, stolen cash

Long term loss is called ultimate (indirect) financial loss

- For example, damage to the organization’s reputation

Impact

Impact calculations

- Quantitative calculations are usually used for ranging possible financial impact
- Qualitative calculations are usually used for loss of reputation or market shares

Perform a business impact analysis (BIA) and subsequent analysis to determine the impacts

Generally a Semiquantitative analysis approach is used to determine the criticality and sensitivity of information assets

- This provides the basis for setting access control authorization
- This also provides the basis for business continuity planning (BCP)

Controls

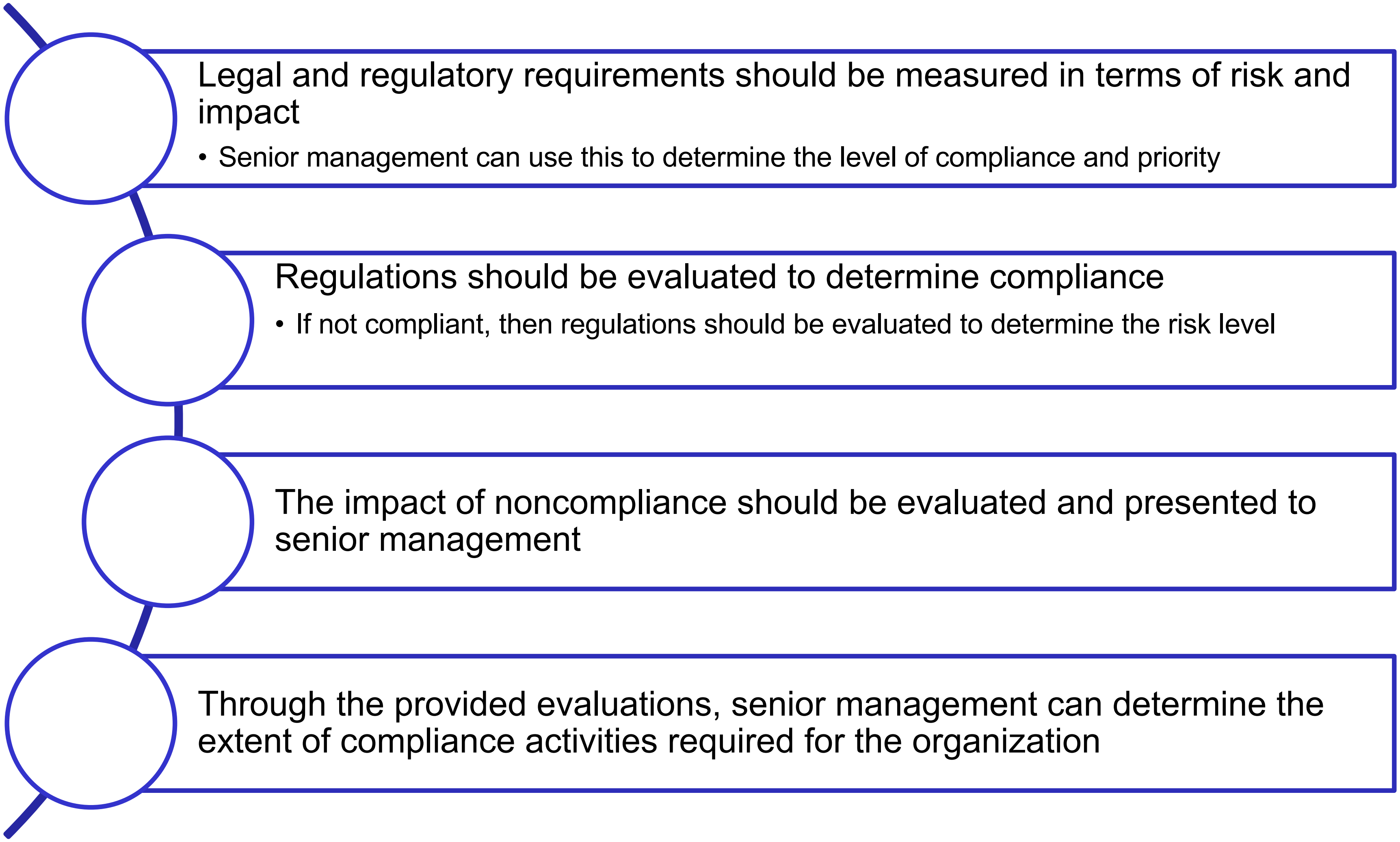
Controls are anything that helps to regulate an activity or mitigate risk

- Technology
- Process
- Practice
- Policy
- Standard
- Procedure

Controls can be

- Administrative in nature
- Technical in nature
- Management in nature
- Legal in nature

Legal And Regulatory Requirements



Legal and regulatory requirements should be measured in terms of risk and impact

- Senior management can use this to determine the level of compliance and priority

Regulations should be evaluated to determine compliance

- If not compliant, then regulations should be evaluated to determine the risk level

The impact of noncompliance should be evaluated and presented to senior management

Through the provided evaluations, senior management can determine the extent of compliance activities required for the organization

Cost And Benefits

The cost and benefits should be considered when developing controls and countermeasures

Generally accepted information security principles (GAISP) describes the following

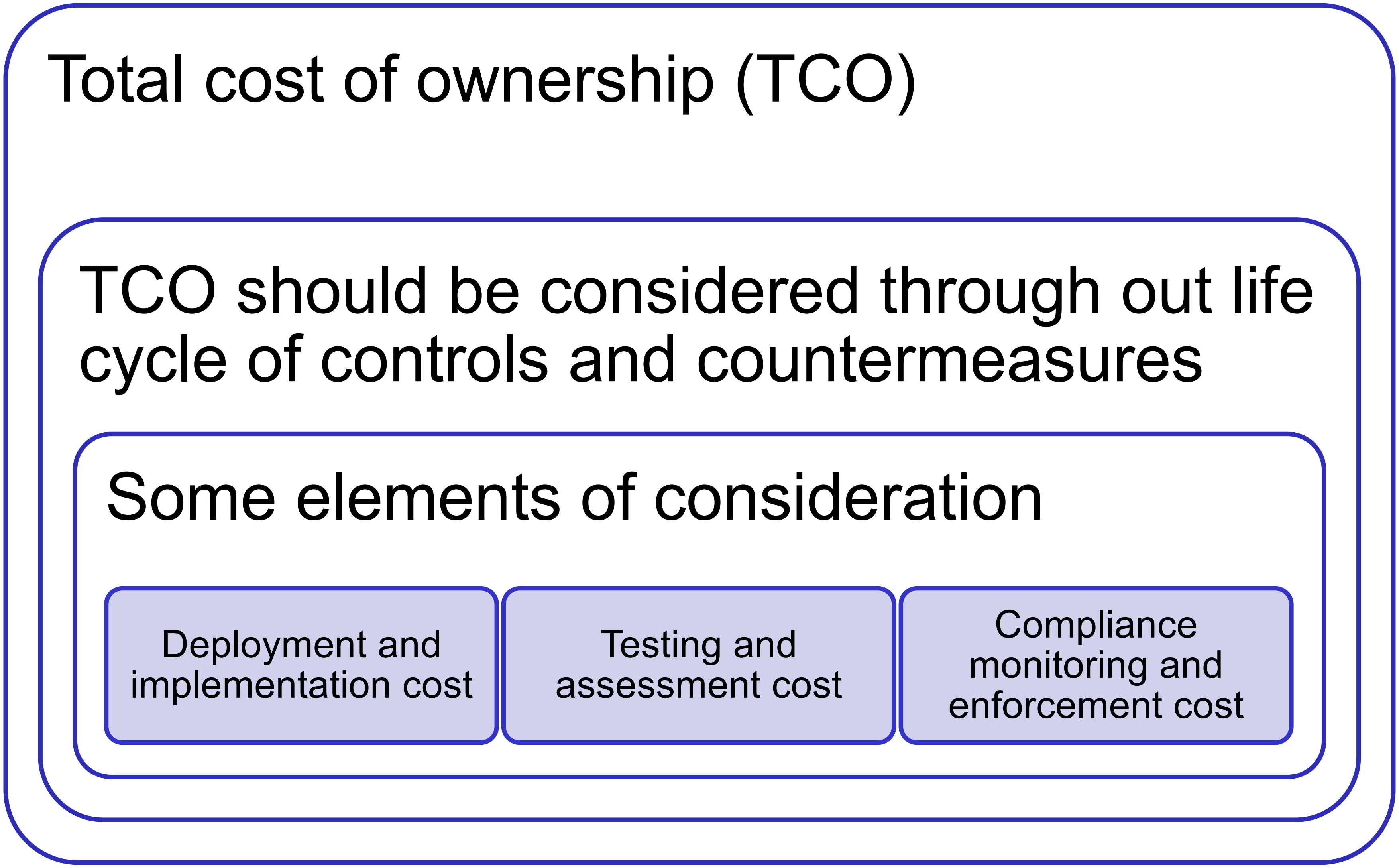
- The cost of a control or countermeasure should never exceed the expected benefits

Cost-benefit analysis helps derive a financial impact view of risk and helps determine the cost of protecting assets

Common measurements of potential loss

- Impacts on staff productivity
- Losses in revenue
- Events that have direct cost

Cost And Benefits



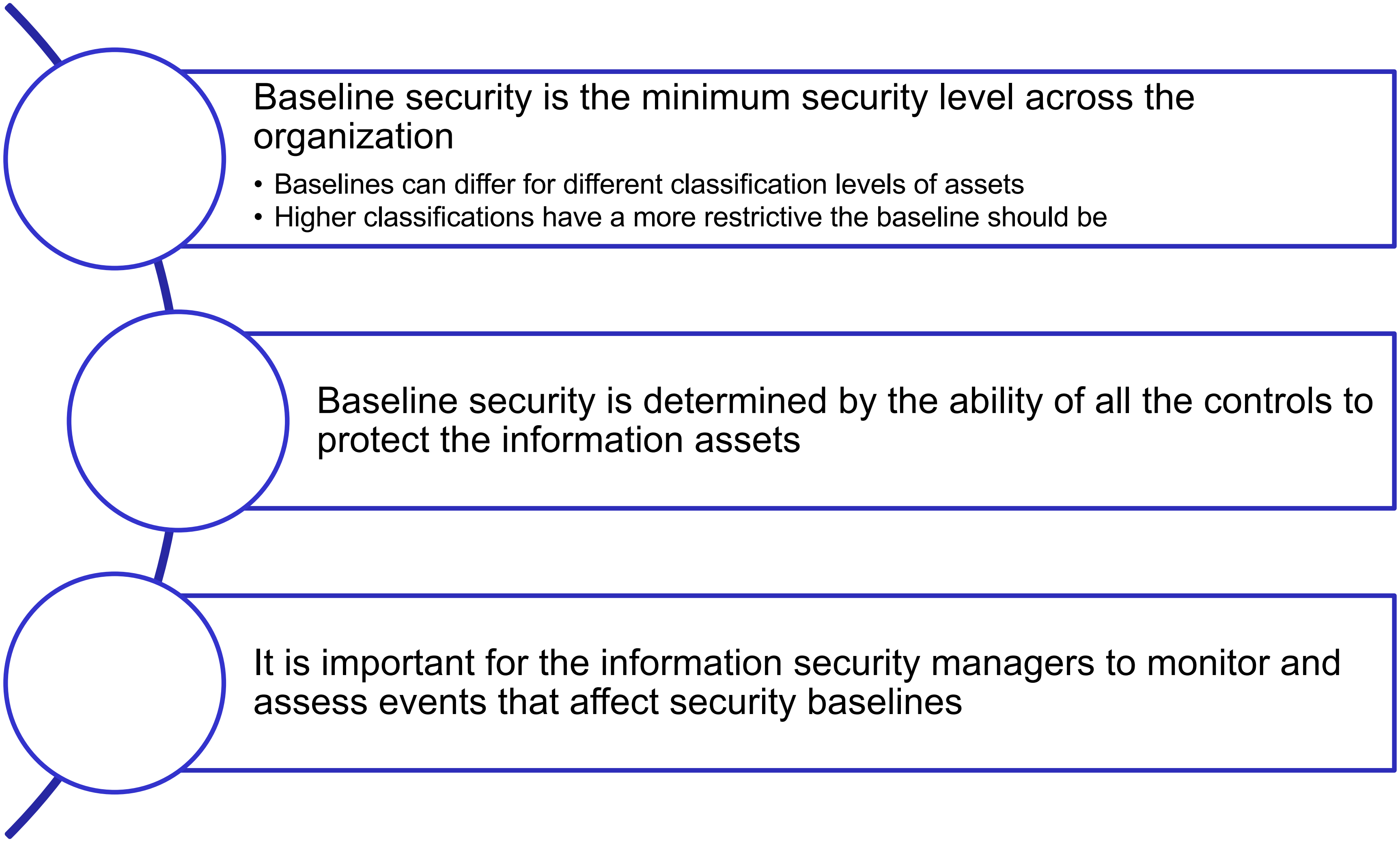
Total cost of ownership (TCO)

TCO should be considered through out life cycle of controls and countermeasures

Some elements of consideration

- Deployment and implementation cost
- Testing and assessment cost
- Compliance monitoring and enforcement cost

Events Affecting Security Baselines



Baseline security is the minimum security level across the organization

- Baselines can differ for different classification levels of assets
- Higher classifications have a more restrictive the baseline should be

Baseline security is determined by the ability of all the controls to protect the information assets

It is important for the information security managers to monitor and assess events that affect security baselines

Events Affecting Security Baselines

Events that affect baseline security

Baselines for physical security may need to be extended for a time if there is civil unrest in proximity of the organization

New regulations or laws would affects the security baseline

Finding unacceptable levels of risk due to new threats would require the security baseline to be modified or increased

Information Asset Classification

Domain 2
Information Risk Management

Information Asset Classification

Information asset classification defines the sensitivity and criticality of the information asset

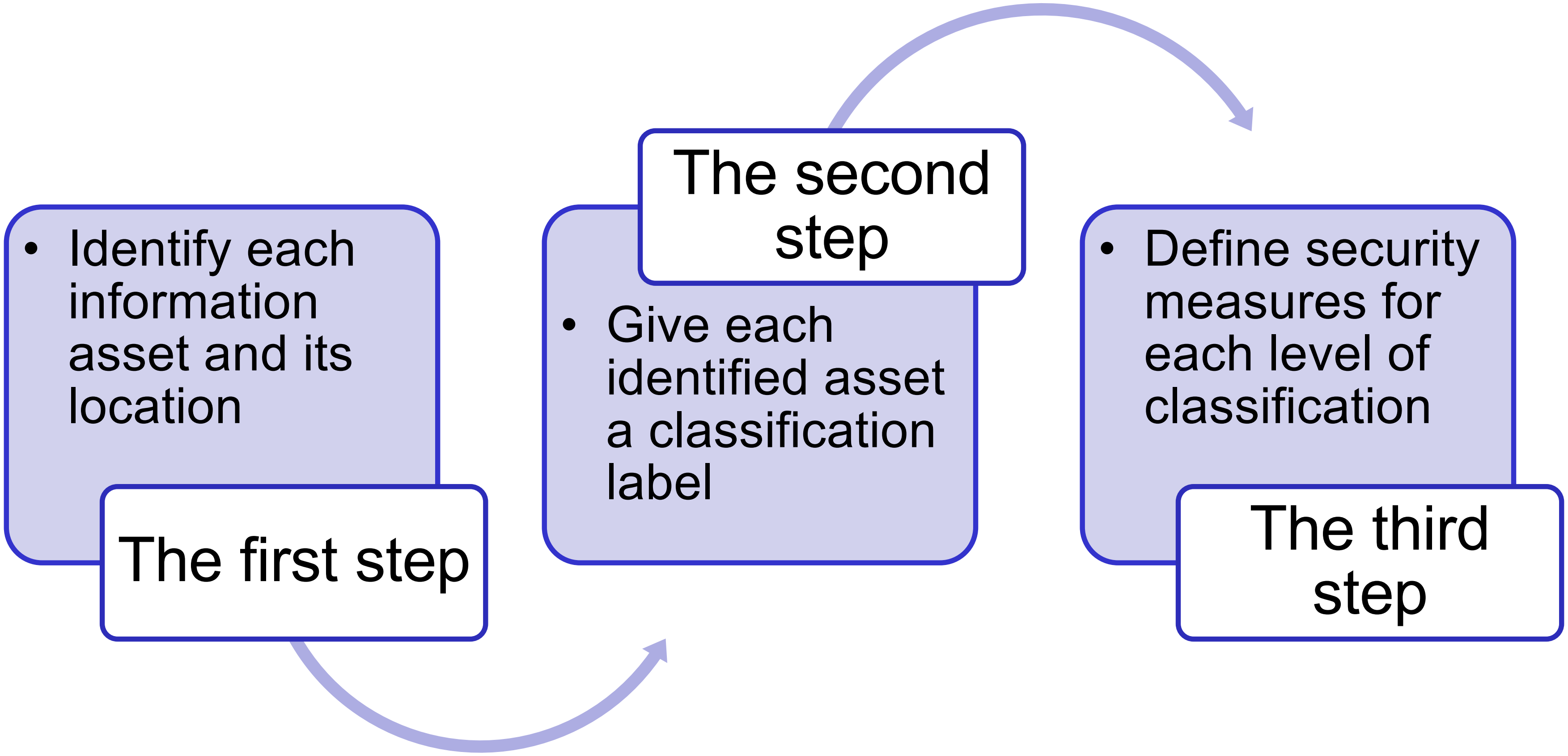
Criticality is determine by the impact on the organization due to loss of an asset

Sensitivity is potential damage to the organization due to unauthorized disclosure of information

Comprehensive classification is not possible in some cases such as constraints on resources

One option would be a business dependency assessment but it is less effective

Classification Process



- Identify each information asset and its location

The first step

- Give each identified asset a classification label

The second step

- Define security measures for each level of classification

The third step

Information Asset Classification

Implementing a classification system

- Classification is based on business value or levels of sensitivity and criticality of assets
- Keep the number of classification levels to a minimum
- Classification should be simple such as labeling assets by differing degree of sensitivity and criticality

Benefits of implanting a classification system

- Reduces the risk of underproduction
- Reduces the cost of overprotection

Methods To Determine Criticality Of Assets And Impact Of Adverse Events

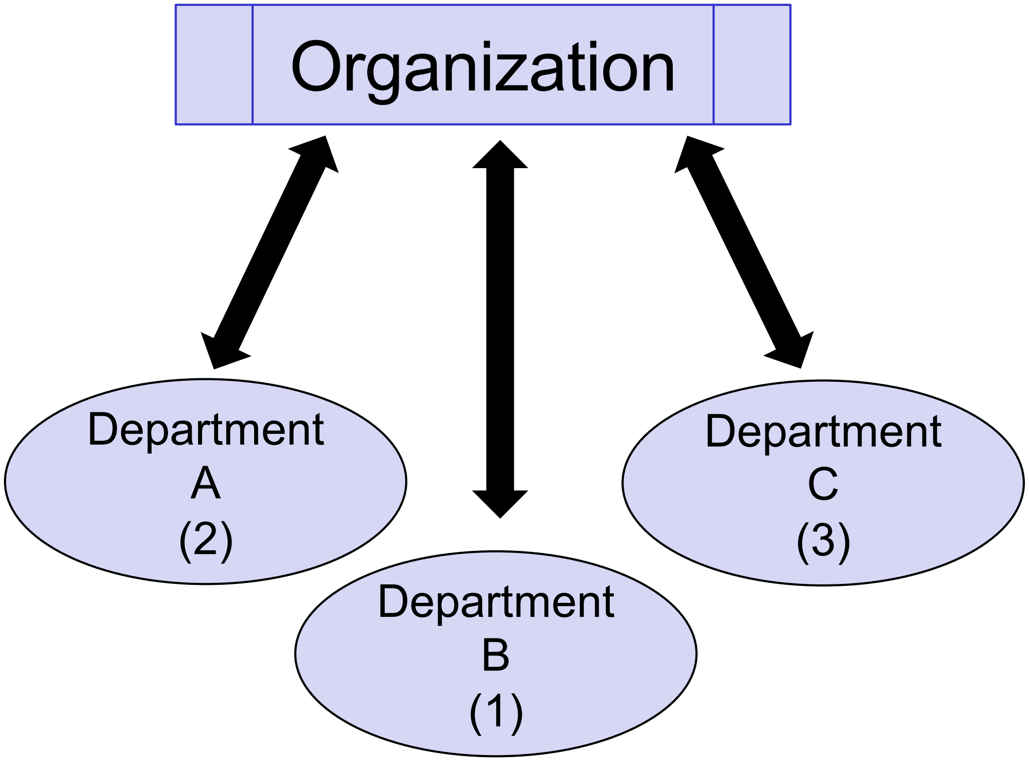
Determining the importance of information assets

First step

- Break up the organizational structure into departments and rate each department by value or importance

Each is rated from most important (1) to least important (3)

Numerically rating each against the other will help prioritize risk remediation efforts



Methods To Determine Criticality Of Assets And Impact Of Adverse Events

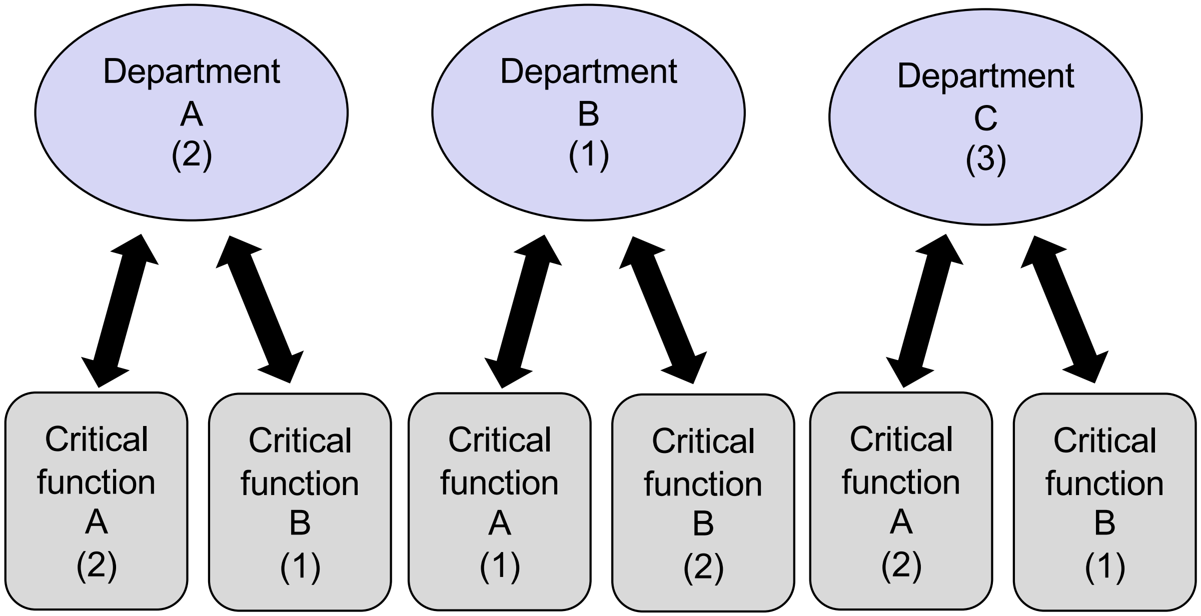
Determining the importance of information assets

Second step

- Identify critical departmental functions and rate each function by value or importance

The critical function layer has a two-level structure to represents complex operations

Operational elements are the focus in this step



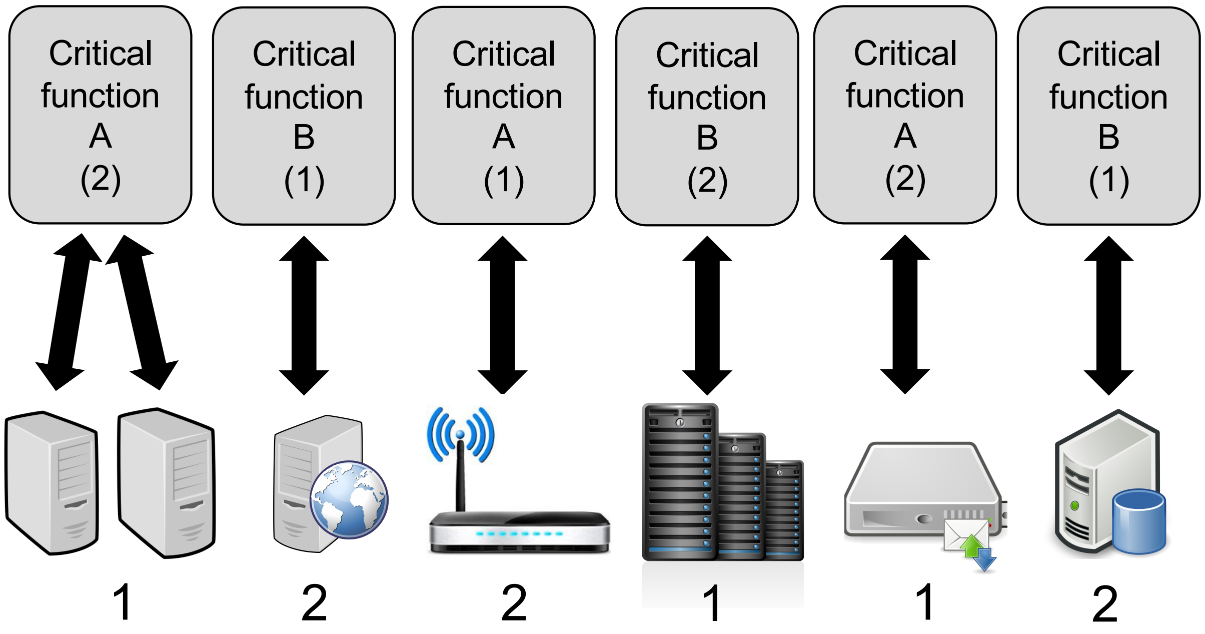
Methods To Determine Criticality Of Assets And Impact Of Adverse Events

Determining the importance of information assets

Third step

- Identify critical function assets and resources and rate each by value or importance

Since assets and resources can be exploited by threats, there is risk



Critical function A (2)

Critical function B (1)

Critical function A (1)

Critical function B (2)

Critical function A (2)

Critical function B (1)

1

2

2

1

1

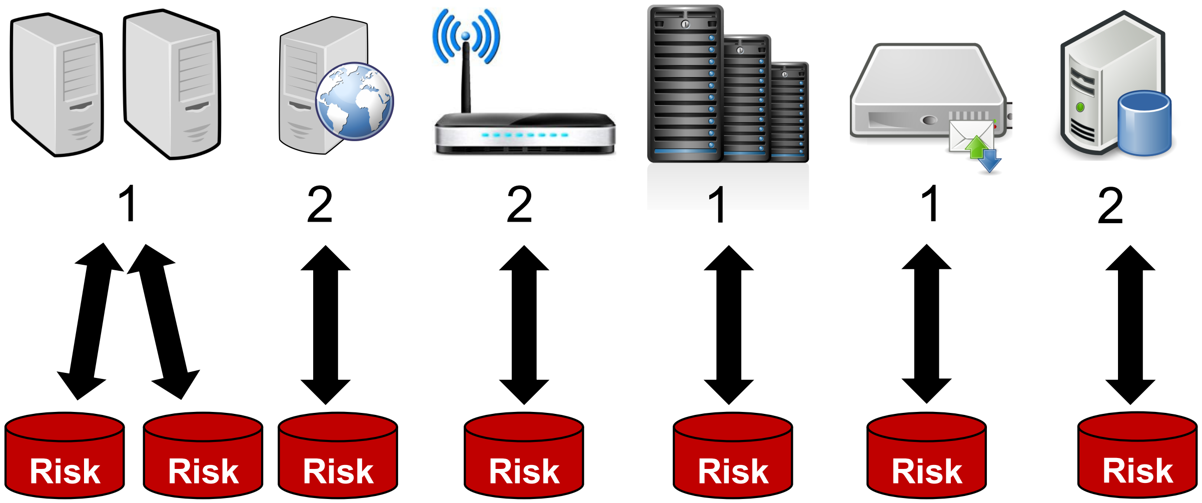
2

Methods To Determine Criticality Of Assets And Impact Of Adverse Events

Determining the importance of information assets

Fourth step

- Identify risks associated with the critical assets and resources

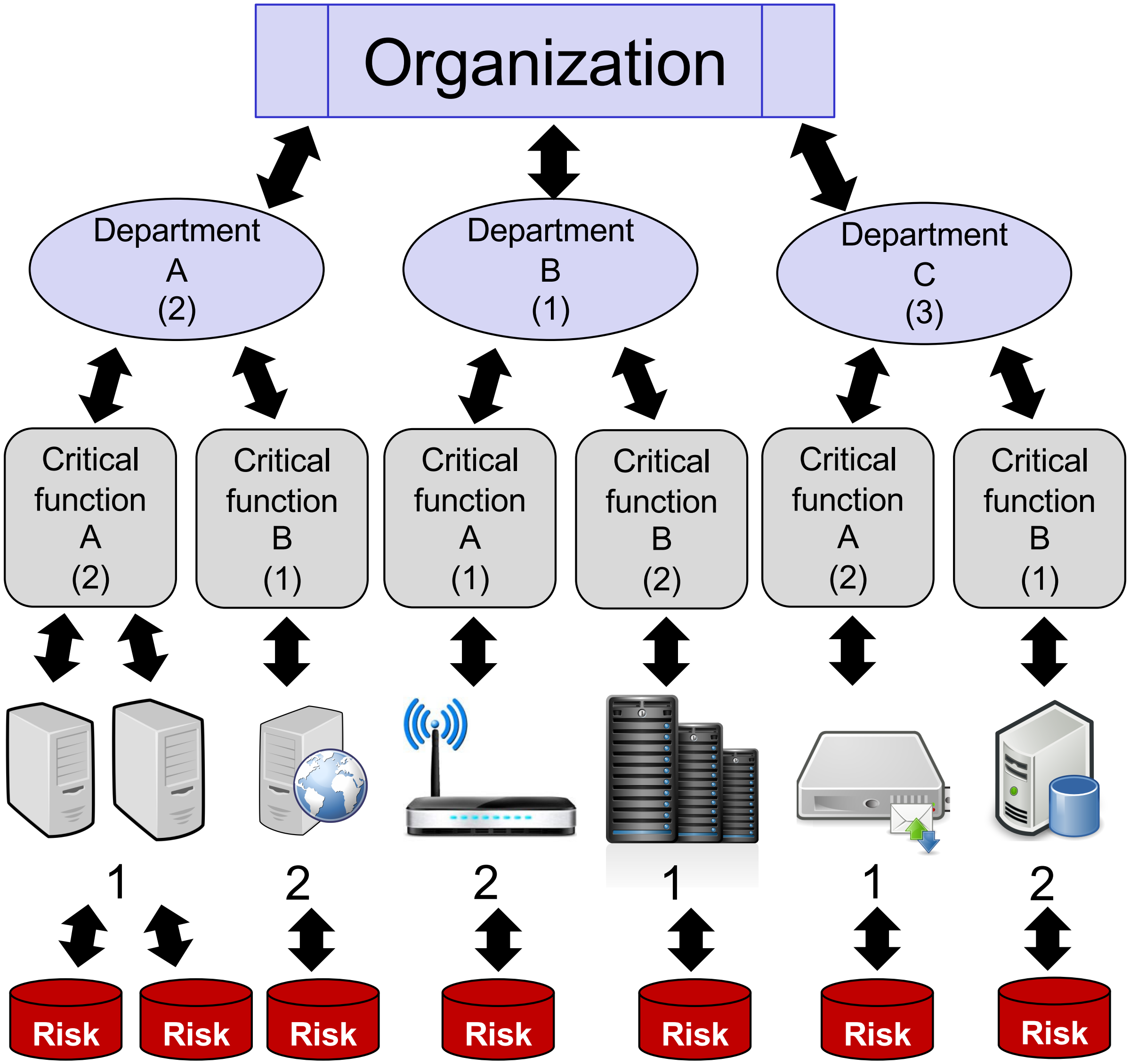


Methods To Determine Criticality Of Assets And Impact Of Adverse Events

This diagram combines all the steps of determining the importance of information assets

With this diagram management can easily see critical functions' risk-level and prioritize protection efforts

Displays the organization's most valuable assets and how risk exposer may impact these assets



Impact Assessment And Analysis

Business Impact Analysis (BIA)

Determines the possible impact of losing the availability of organizational resources

Calculates the escalation of loss over time

Identifies the minimum resources for recovery

Prioritizes the recovery of processes and supporting systems

Impact Assessment And Analysis

These type of assessments determine the worst-case scenario, which represents only a few of the events

- Can result in impact inflation
- Management tends to devalue these assessments as unrealistic

A more effective approach to determine a range of potential outcomes

- Preform a small set of scenario analysis with key stakeholders
- Range of outcomes can be used to define a quantitative distribution scale of impact
- This will give management more realistic assessments of potential impact

Impact Assessment And Analysis

Information necessary to begin the impact analysis on a set of assets

System mission: IT systems or personnel process objectives

System and data criticality: the system's value or importance level

System, personnel, and data criticality: unintended discloser impact

If this information does not exist or has not been gathered the system and data sensitivity can be determined by the level of protection needed to maintain the availability, integrity, and confidentiality of the system and data

Impact Assessment And Analysis

Loss of Integrity

- System and data integrity requires that information is accurate, consistent, not improperly modified
- The impact from not meeting these requirements is the loss of integrity

Impact Assessment And Analysis

Loss of Availability

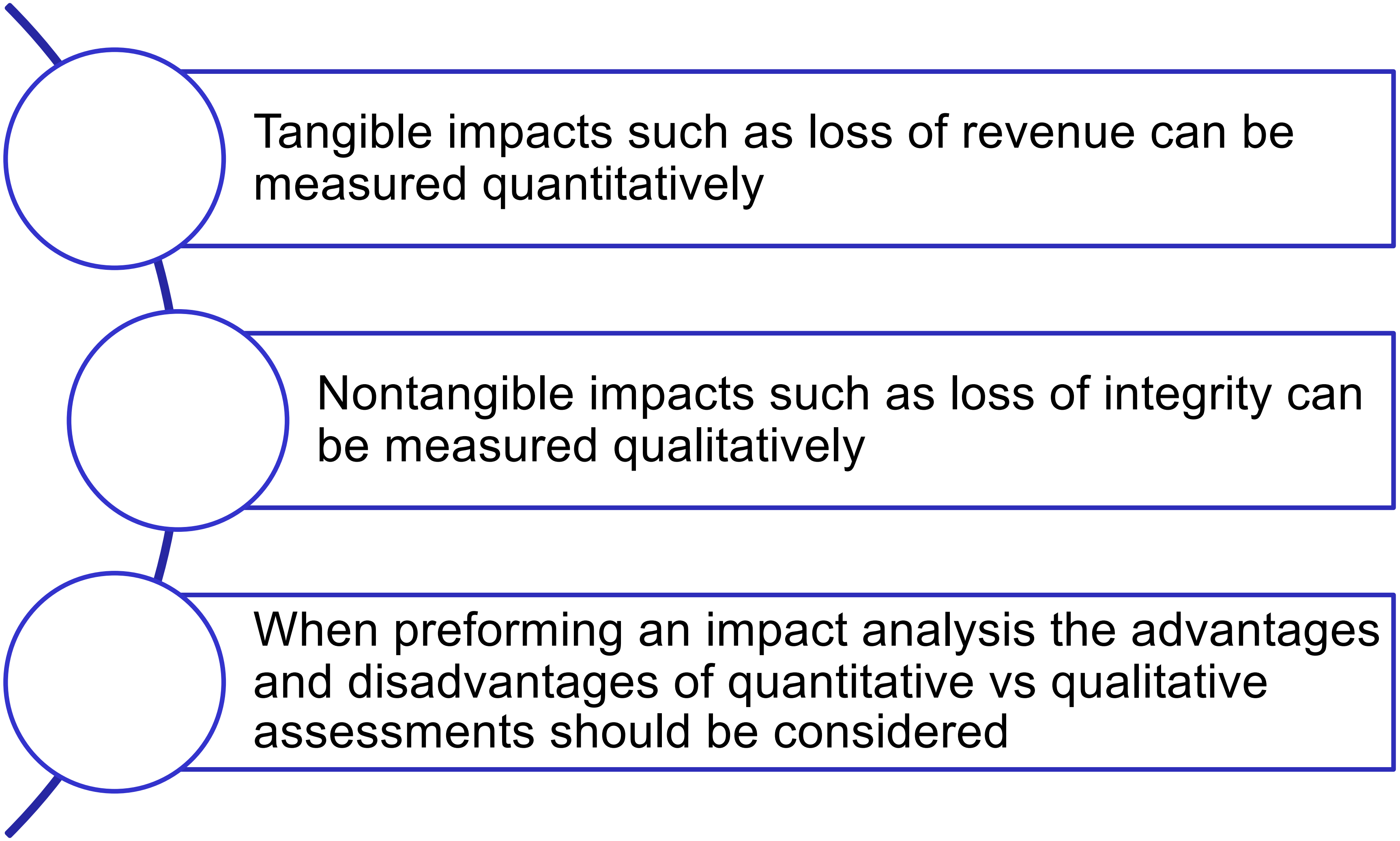
- Availability refers to the requirement that systems and process are available to the end-user
- If mission-critical takes required system availability, the loss of availability would impact the productivity
- If end users are unable to preform their functions due to loss of availability this may be costly to the organization

Impact Assessment And Analysis

Loss of Confidentiality

- Confidentiality in this context is protecting information form unauthorized discloser
- Unintentionally disclosing private data is loss of confidentiality and can result in loss of integrity

Impact Assessment And Analysis



Tangible impacts such as loss of revenue can be measured quantitatively

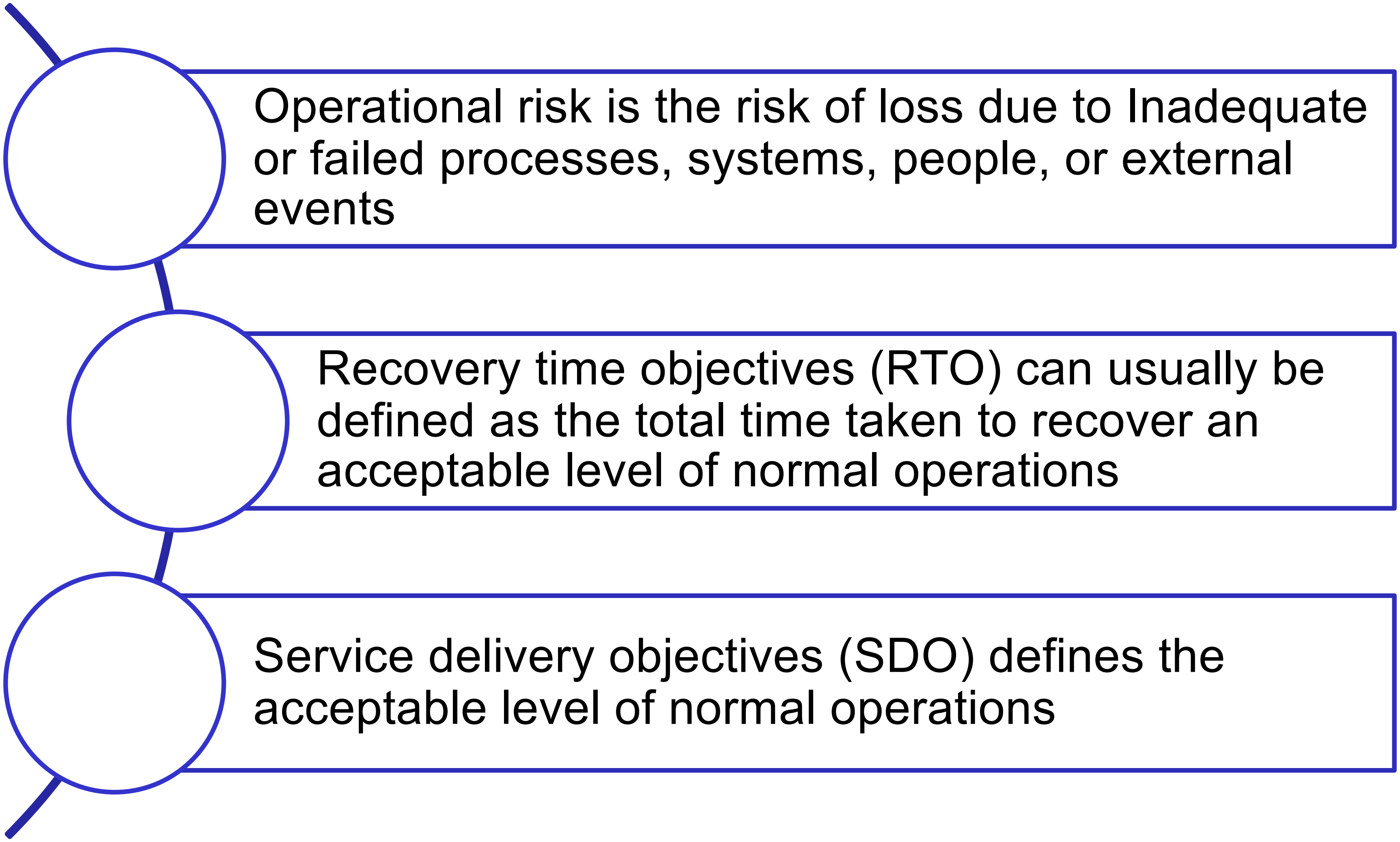
Nontangible impacts such as loss of integrity can be measured qualitatively

When preforming an impact analysis the advantages and disadvantages of quantitative vs qualitative assessments should be considered

Operational Risk Management

Domain 2
Information Risk Management

Recovery Time Objectives



- Operational risk is the risk of loss due to Inadequate or failed processes, systems, people, or external events
- Recovery time objectives (RTO) can usually be defined as the total time taken to recover an acceptable level of normal operations
- Service delivery objectives (SDO) defines the acceptable level of normal operations

Recovery Time Objectives

RTO determination factors

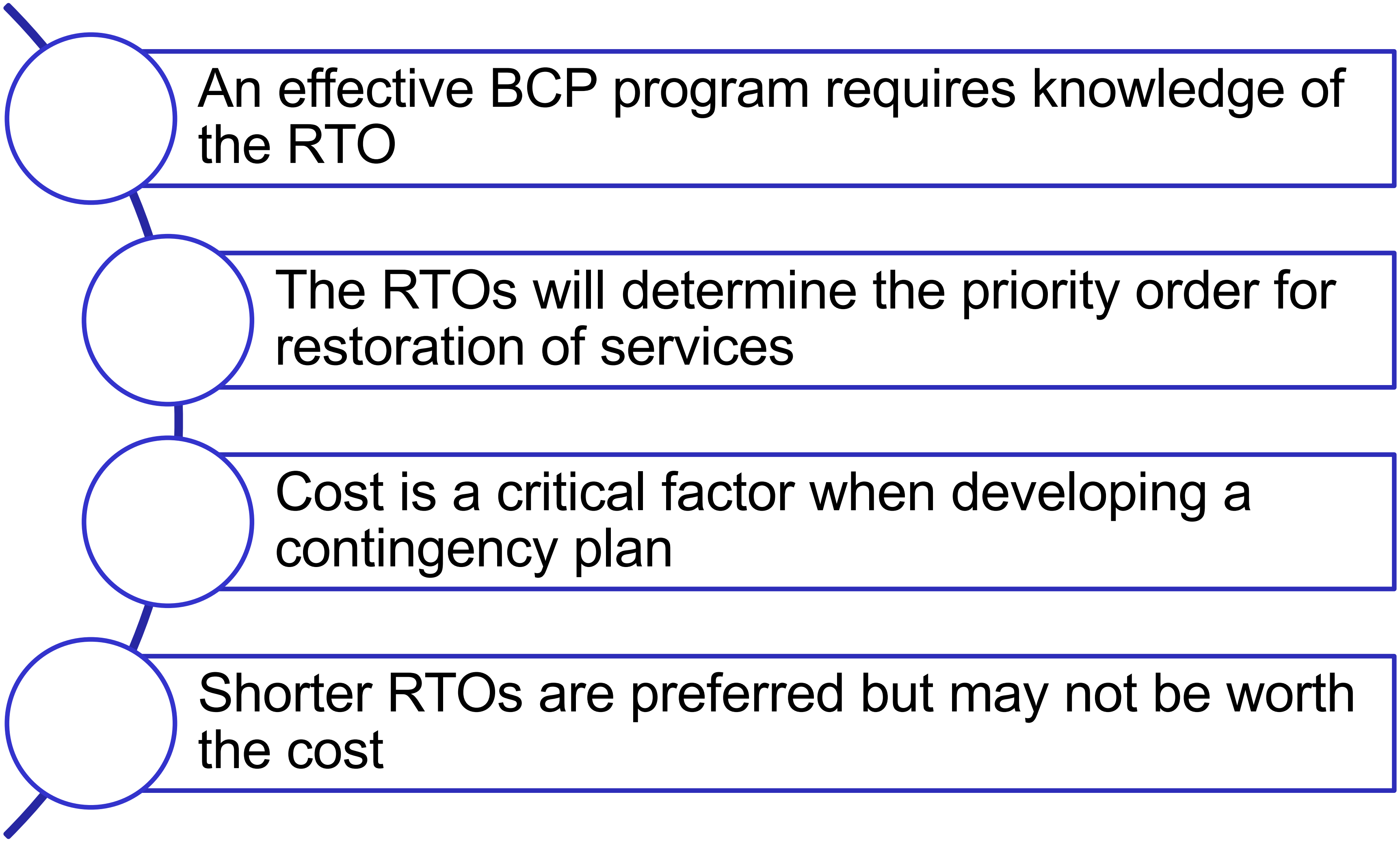
- Cyclical need of the information and the organization
- Interdependencies between information and organizational requirements
- Cost of available options

The timing of the month or year may affect the RTO

- Information dependencies change at different points in a business cycle
  - The beginning of the month may not be as critical for financial information
  - At the end of the month, the same information may have a high level of criticality

RTOs are determined by conducting a BIA in coordination with developing a business continuity plan (BCP)

RTO And ITS To Business Continuity Planning



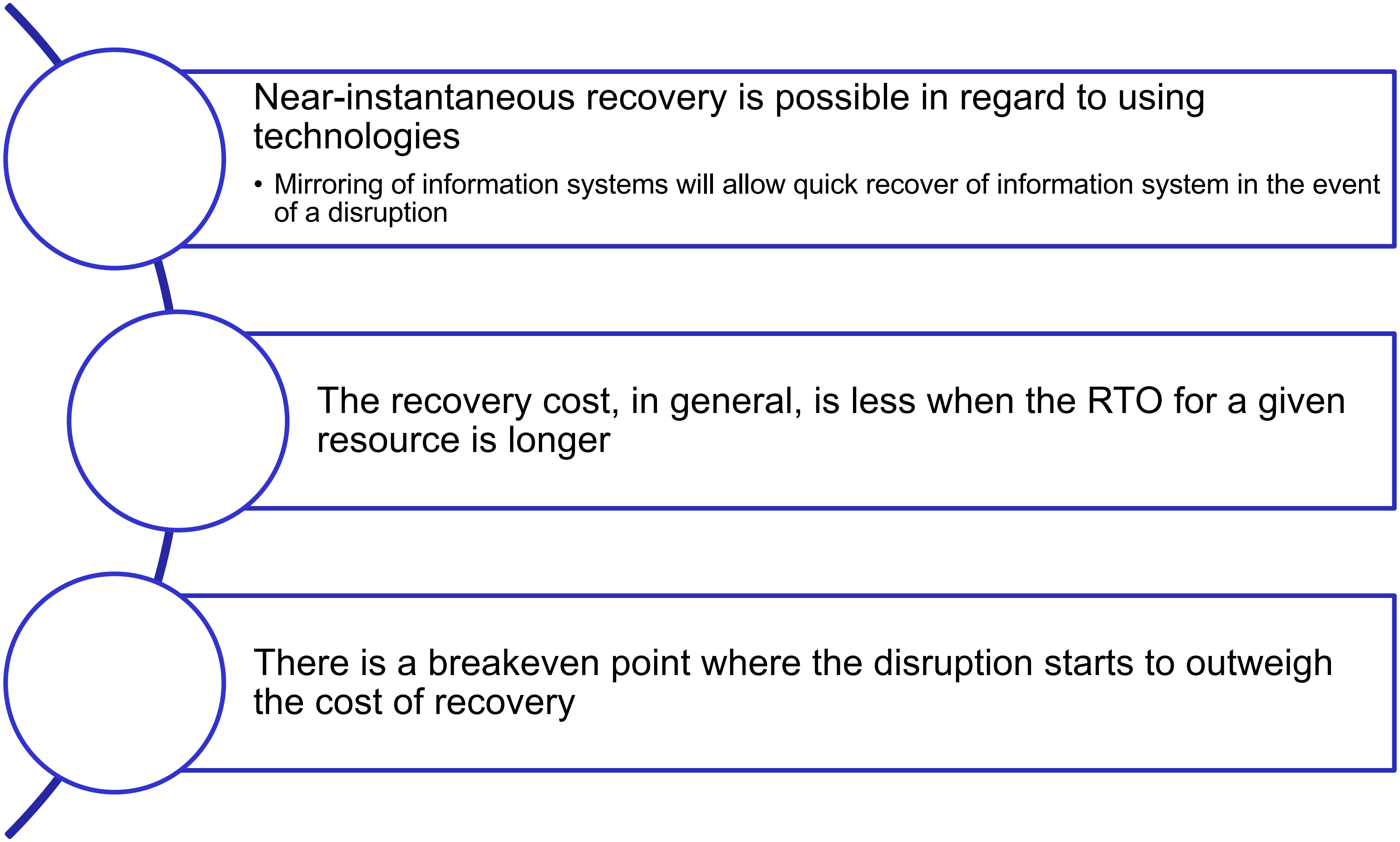
An effective BCP program requires knowledge of the RTO

The RTOs will determine the priority order for restoration of services

Cost is a critical factor when developing a contingency plan

Shorter RTOs are preferred but may not be worth the cost

RTO And ITS To Business Continuity Planning



Near-instantaneous recovery is possible in regard to using technologies

- Mirroring of information systems will allow quick recover of information system in the event of a disruption

The recovery cost, in general, is less when the RTO for a given resource is longer

There is a breakeven point where the disruption starts to outweigh the cost of recovery

Recovery Point Objectives

Recovery point objective (RPO)

Determined by the identified acceptable loss of data in the case of disruption of operations

RPO indicates the most recent point in time that is acceptable to recover the data, which is typically the latest backup

Depending on the volume of data it might be best to reduce the time between backups

- Recovery of the data may be impossible if the volume of data is too large
- If recovery of data takes too much time the RTO may be impossible to achieve

Service Delivery Objectives

Service delivery objectives (SDO)

Defines the minimum level of services that are required to be restored after an event to meet business requirements until normal operations are resumed

RTOs and RPOs effect SDOs

Typically higher levels of service will need more resources and more current RPOs

Maximum Tolerable Outage

Maximum tolerable outage (MTO)

Defines the maximum amount of time an organization can operate in recovery mood

Factors that may affect MTO

- The fuel need to operate emergency generators
- The accessibility of a remote recovery site

MTO affects RTO, which inevitably affect the RPO

Allowable Interruption Window

Allowable interruption window (AIW)

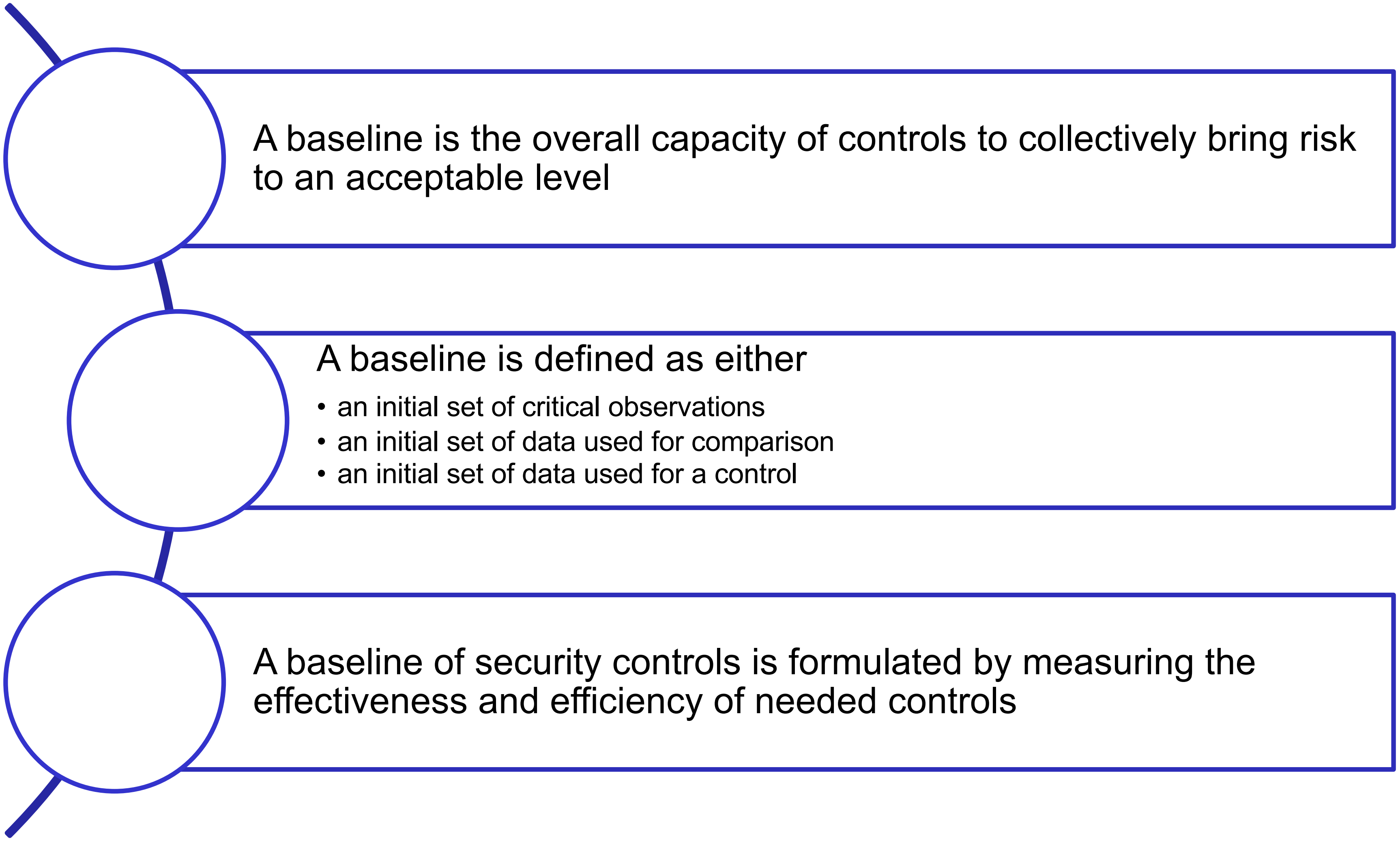
The amount of time normal options can be down before the organization is effected by financial complications

The MTO should be as long as AIW to minimize risk to the organization in the case of a disaster

Security Control Baselines

Domain 2
Information Risk Management

Security Control Baselines



A baseline is the overall capacity of controls to collectively bring risk to an acceptable level

A baseline is defined as either

- an initial set of critical observations
- an initial set of data used for comparison
- an initial set of data used for a control

A baseline of security controls is formulated by measuring the effectiveness and efficiency of needed controls

Security Control Baselines

A Security Control Baseline

Is the overall capacity of controls to collectively bring risk to an acceptable level

Is defined as either

- an initial set of critical observations
- an initial set of data used for comparison
- an initial set of data used for a control

A baseline of security controls is formulated by measuring the effectiveness and efficiency of needed controls

Security Control Baselines

Implementing baselines for security process

Sets the minimum security requirements across the organization

Which makes them consistent with acceptable risk levels

Different baselines should be set for different security classification levels

Benefits of setting security baselines

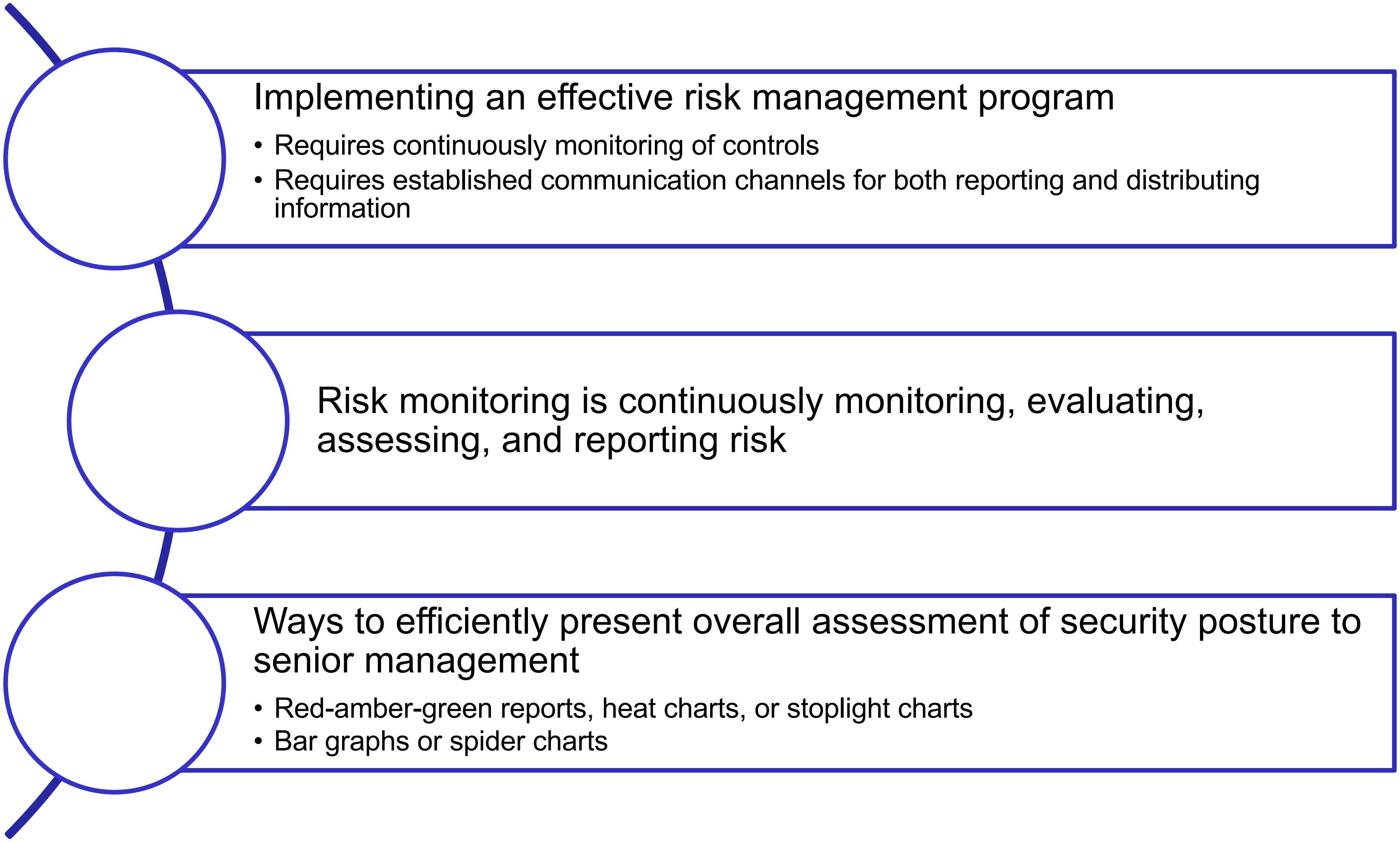
Standardizes the minimum amount of security measures that are required

Provides a point of reference to measure changes to security and identify equivalent effects on risk

Risk Monitoring and Communication

Domain 2
Information Risk Management

Risk Monitoring



Implementing an effective risk management program

- Requires continuously monitoring of controls
- Requires established communication channels for both reporting and distributing information

Risk monitoring is continuously monitoring, evaluating, assessing, and reporting risk

Ways to efficiently present overall assessment of security posture to senior management

- Red-amber-green reports, heat charts, or stoplight charts
- Bar graphs or spider charts

Key Risk Indicators

Key Risk Indicators (KRI)

Is used as a way of reporting and monitoring risk

Can be defined as measures that indicate when an organization is outside the acceptable level of risk

Can provide early warning sign of possible problems or shed light on particular risk areas

Key Risk Indicators

Measures that will serve as effective KRIs are

- Highly relevant
- Have high probability of predicting/indicating major changes in risk

KRIs are selected based on sources such as

- Industry benchmarks
- External threat reporting services
- Any factor that can be monitored and indicates alterations in risk

Key Risk Indicators

Selection of KRIs is based on

Impact

- Indicators for risk with high impact probability

Effort to implement, measure, and report

- The indicators that are easily measured are preferred for indicators of equal sensitivity to changing risk

Reliability

- The indicator must have a high connection with risk
- Must be a good predictor or outcome measure

Sensitivity

- Must be capable indicating variance in the level of risk

Key Risk Indicators

- An organization external and internal environments are constantly changing
- This constant change also effects the risk environment, which is highly dynamic
- Naturally the set of KRIs will also change over time
- Define trigger levels by evaluating the risk appetite and tolerance level that each KRI is associated with
- Trigger levels will enable stakeholders to take action more effectively

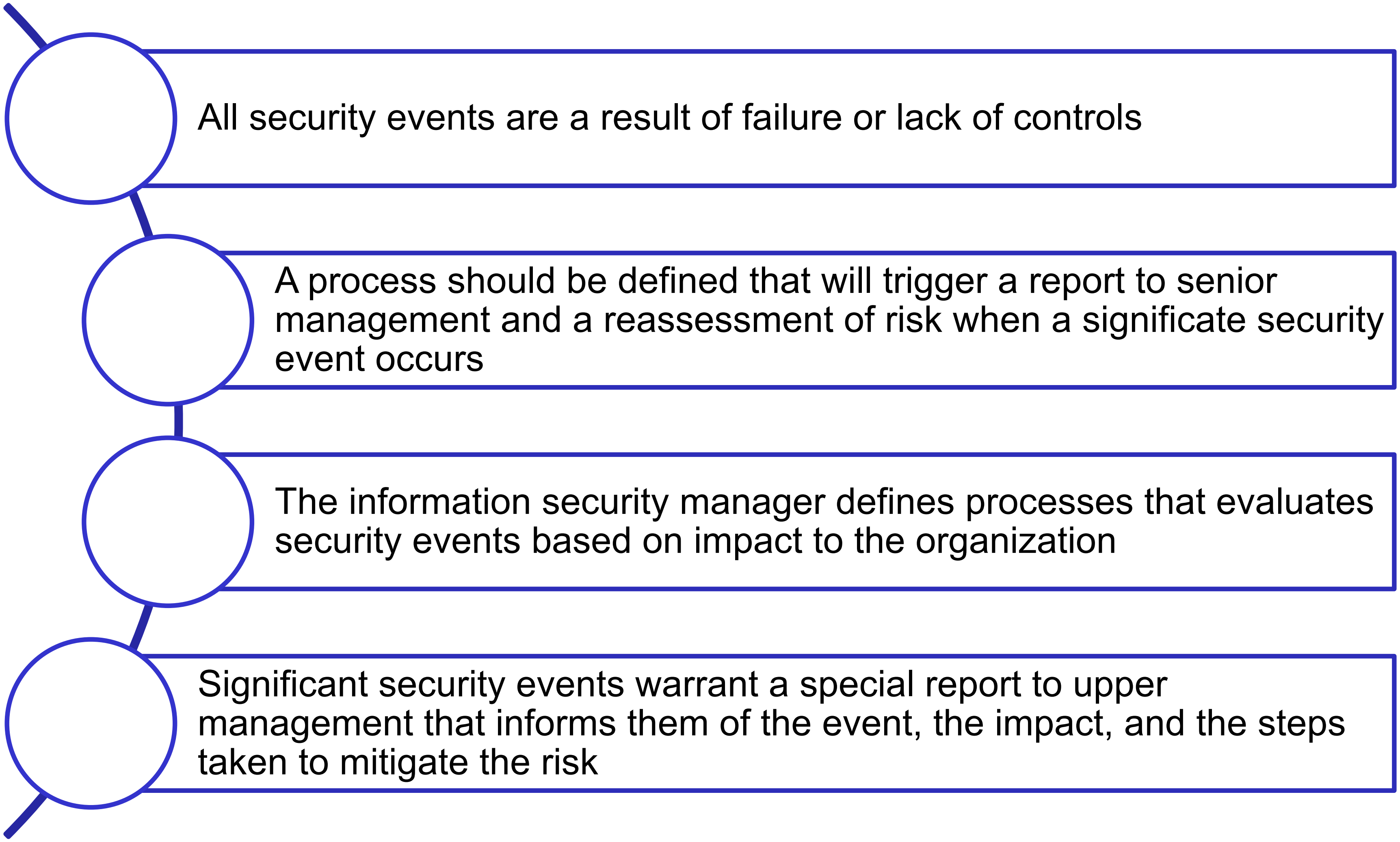
Reporting Significant Changes In Risk

The risk assessment must be kept up-to-date to ensure its continued accuracy as changes to the organization occur

These changes must be reported to the appropriate levels of management at the appropriate times

It is important for the information security manager to have periodic meetings with senior management to present the changes in risk level

Reporting Significant Changes In Risk



All security events are a result of failure or lack of controls

A process should be defined that will trigger a report to senior management and a reassessment of risk when a significate security event occurs

The information security manager defines processes that evaluates security events based on impact to the organization

Significant security events warrant a special report to upper management that informs them of the event, the impact, and the steps taken to mitigate the risk

Summery and Review

Domain 2
Information Risk Management

Summary

- The management of risk
- Strategies to manage risk
- Effective methods of managing information risk
- The implementation of risk management
- The assessment of risk
- Applying security classification to information assets
- Operational risk management
- Security control baselines
- Risk monitoring and communication