Introduction to Cyber Security

Information Security Governance and Risk Assessment

```
#include <iostream>
#include <cstdlib>
using namespace std;
int main()
{
  cout << "Hello, world!" << endl;
  return 0;
}
```

Learning Objectives

By the end of this lesson, you will be able to:

- Explain information security governance

- Describe risk management

- Summarize effective information security program

- Define supply chain

Information Security Governance

Information Security Governance

It is a set of responsibilities and practices exercised by the board and executive management to:

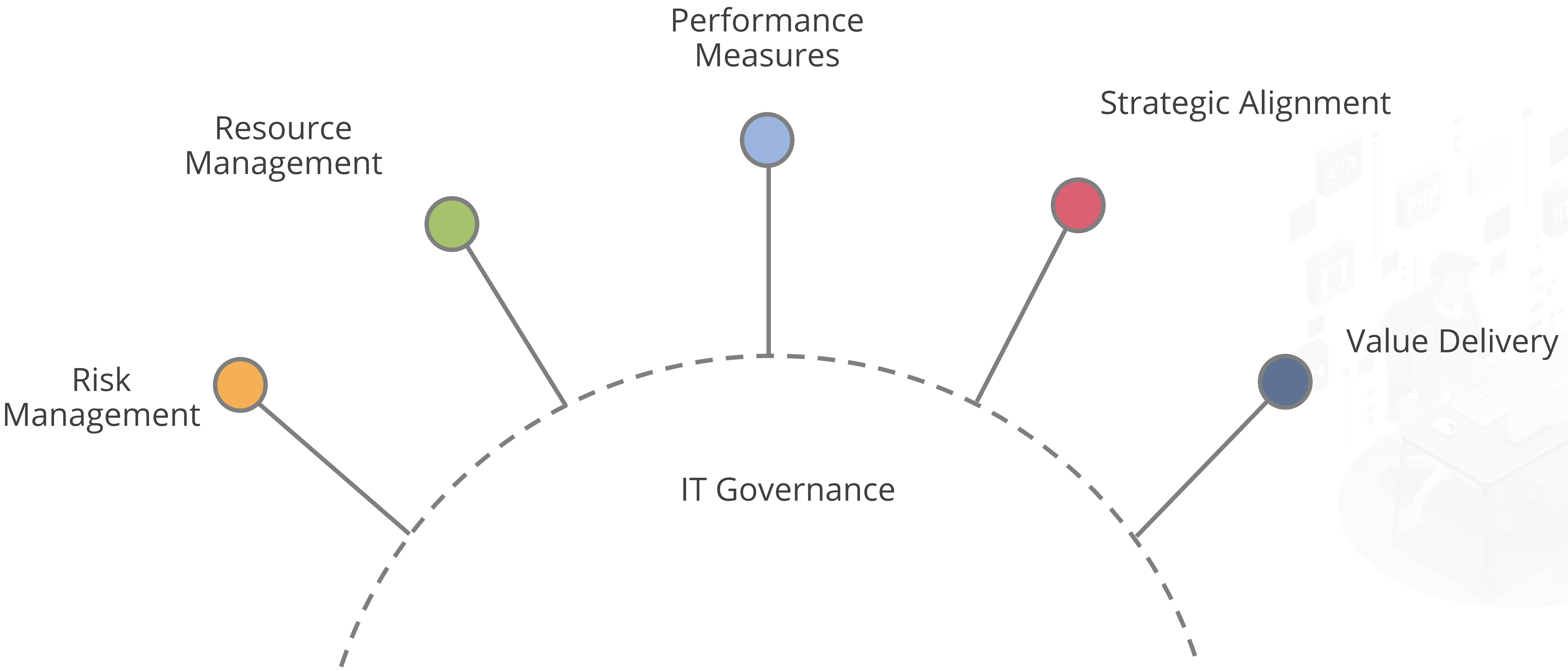
Achieve goals

Manage risks

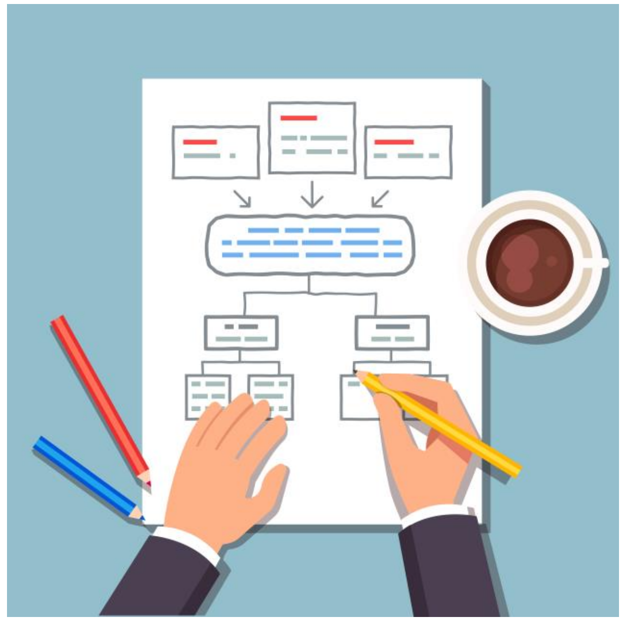
Meet objectives

Verify usage of resources

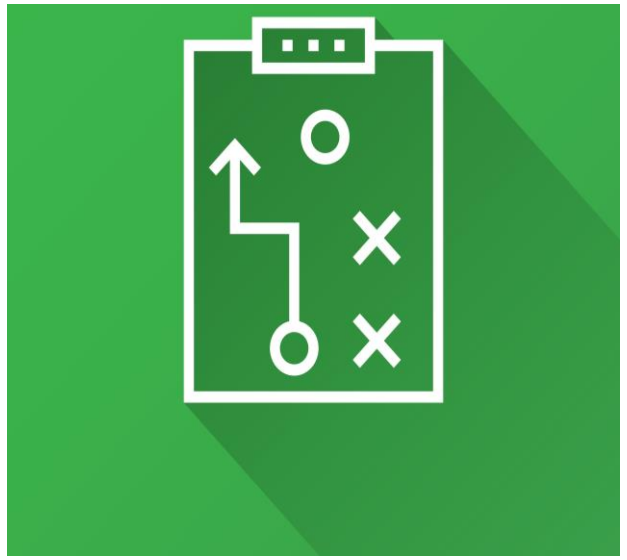
IT Governance Focus Areas



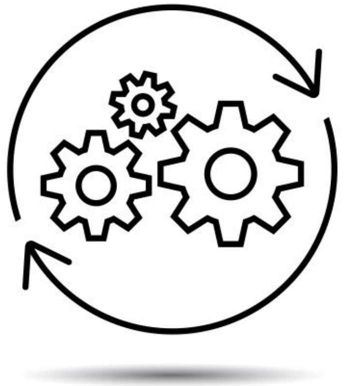
Business Goals and Objectives



Strategic Plan



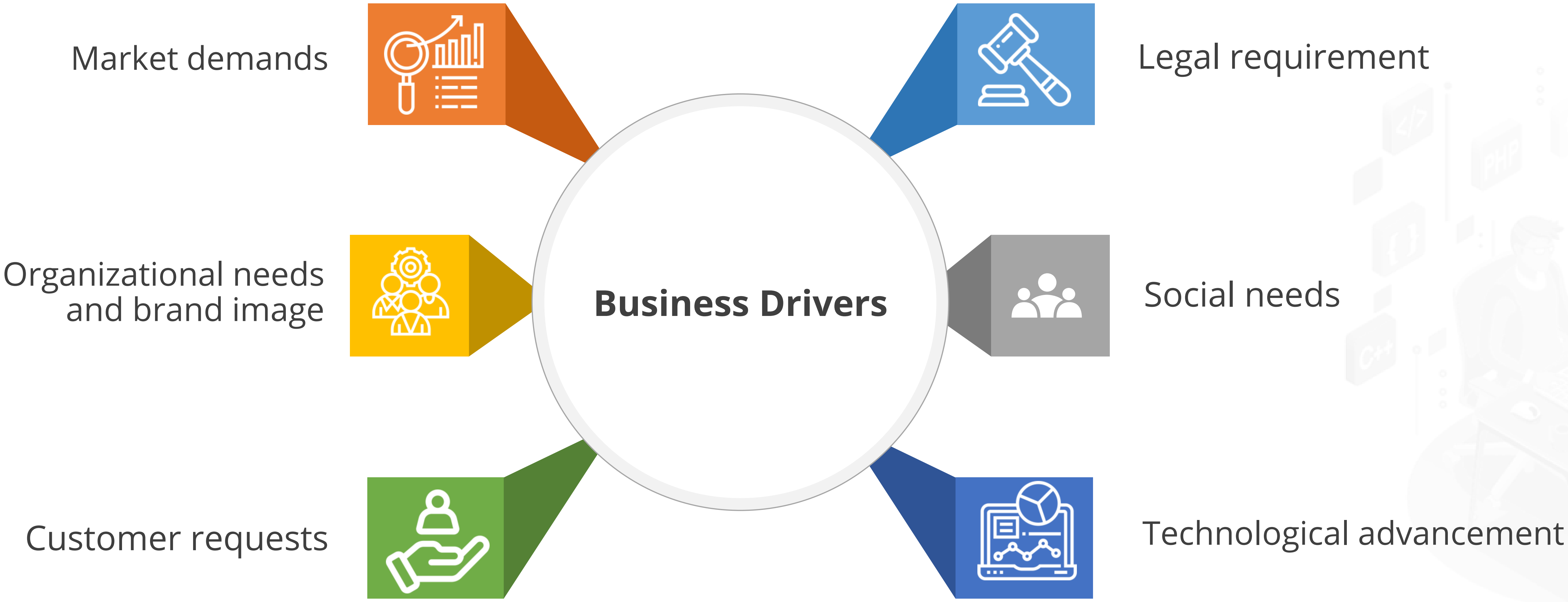
Tactical Plan



Operational Plan

To meet customer needs by ensuring that business processes and operations are in place

Business Drivers



Business Drivers

Market demands

Organizational needs and brand image

Customer requests

Legal requirement

Social needs

Technological advancement

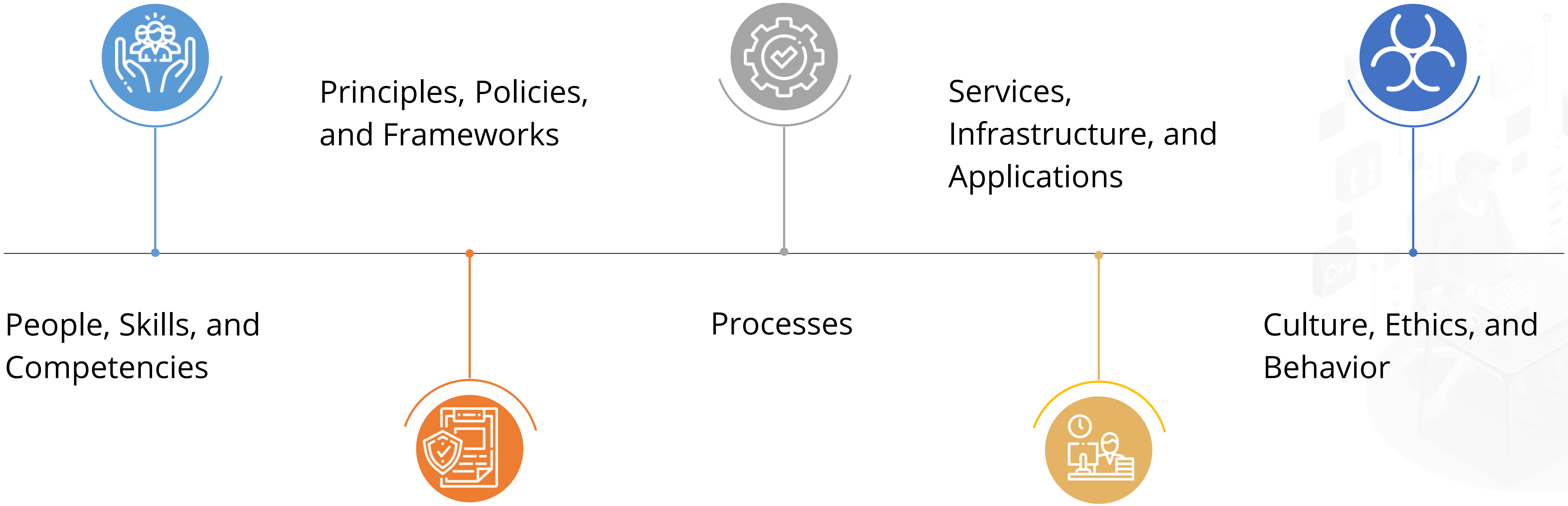
Enabling Technology

It is an invention or innovation that can be applied to drive radical change in the capabilities of a user or culture.

Enablers for Governance

Enablers are factors that individually and collectively influence whether something will work.

Enabler Categories



People, Skills, and Competencies

Principles, Policies, and Frameworks

Processes

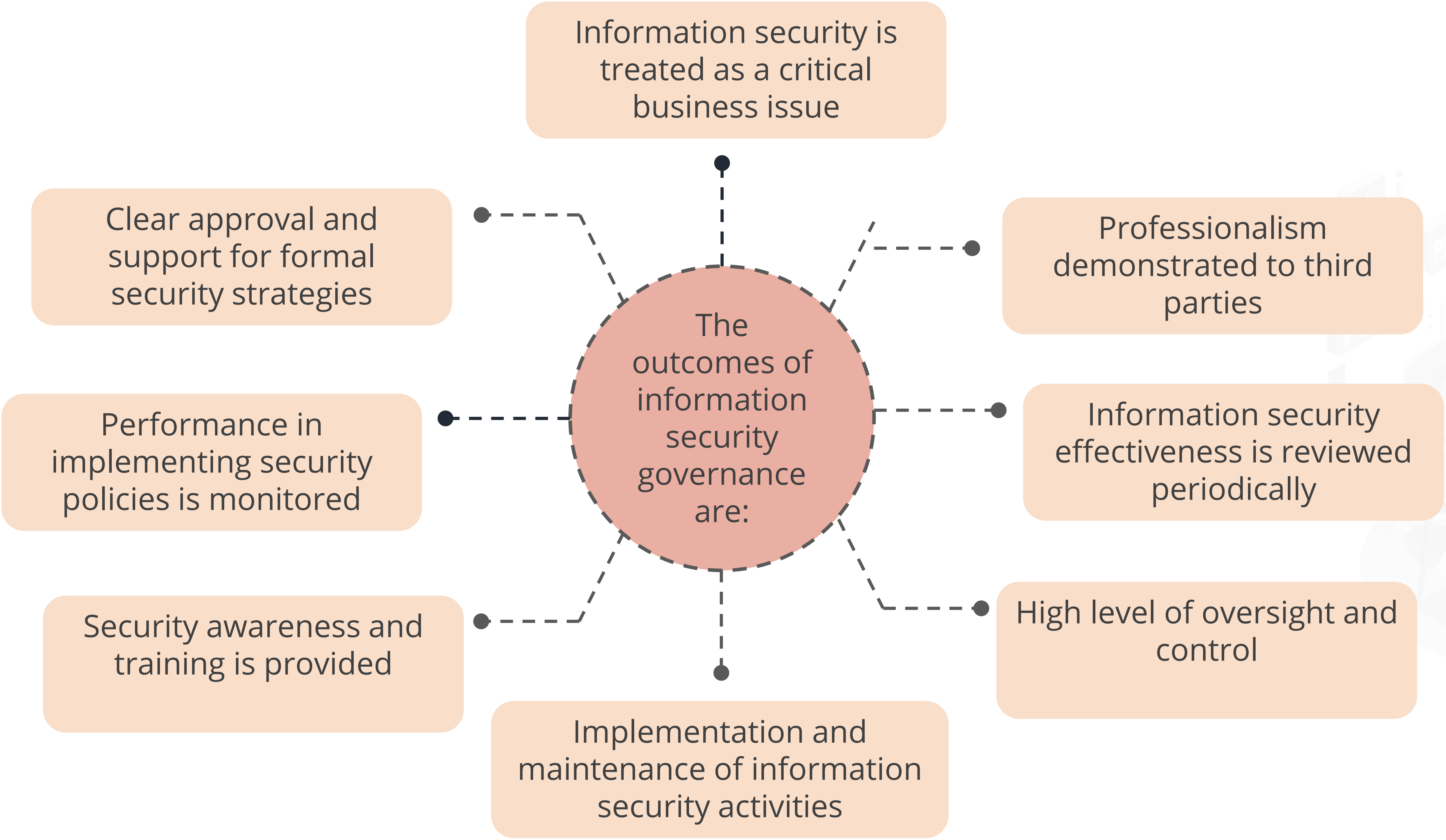
Services, Infrastructure, and Applications

Culture, Ethics, and Behavior

Information Security Governance

Is the responsibility of the board of directors and executive management and must have a clear organizational strategy for preservation

Information Security Governance: Outcomes



The outcomes of information security governance are:

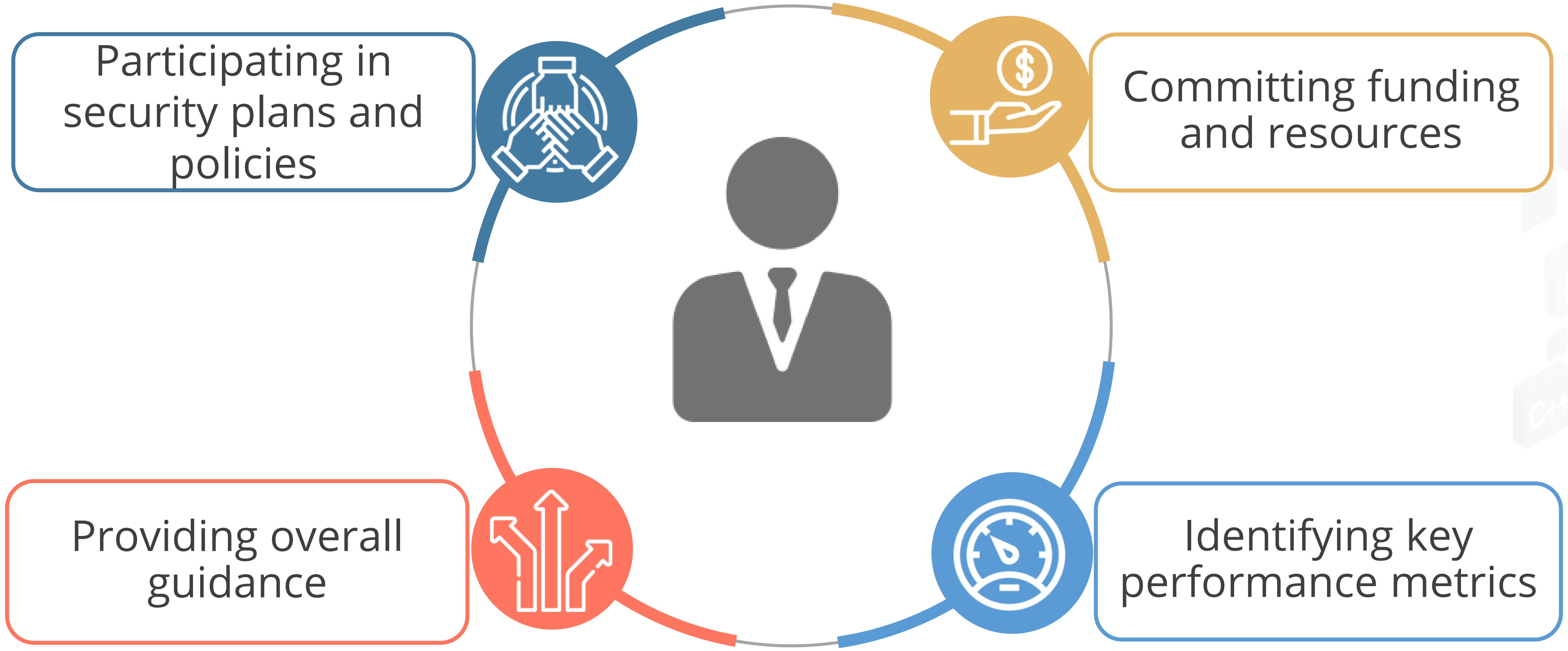
- Information security is treated as a critical business issue
- Professionalism demonstrated to third parties
- Information security effectiveness is reviewed periodically
- High level of oversight and control
- Implementation and maintenance of information security activities
- Security awareness and training is provided
- Performance in implementing security policies is monitored
- Clear approval and support for formal security strategies

Management Support

Management Support

It is the extent to which the senior management understands the importance of the security function and supports security goals and priorities.

Management Support



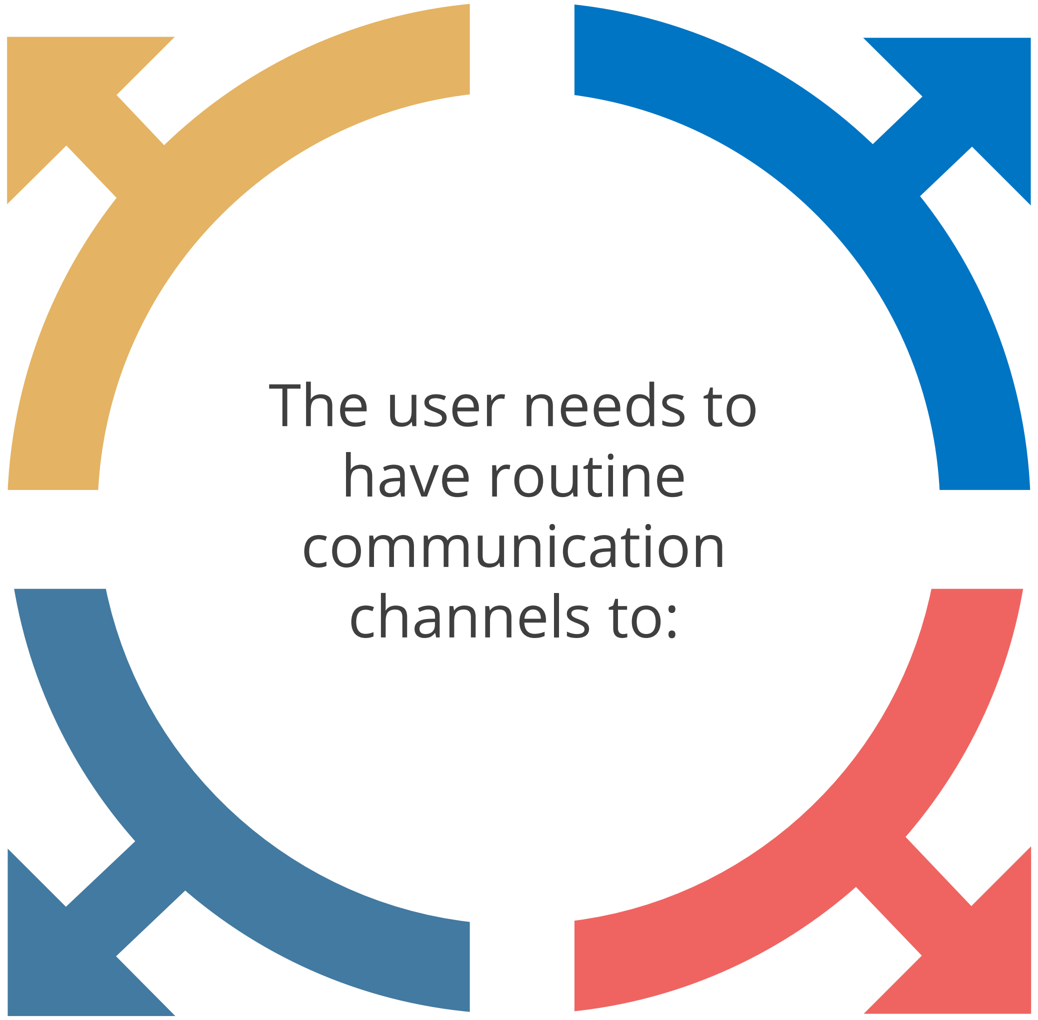
Participating in security plans and policies

Committing funding and resources

Providing overall guidance

Identifying key performance metrics

Establish Reporting and Communication Channels



The user needs to have routine communication channels to:

Senior management

Other management

Business process owners

Employees

Performance Management and Smart Metric

Performance Management

It is the systematic process by which the Department of Commerce involves its employees as individuals and members of a group.

IT balanced scorecard

Capability maturity model

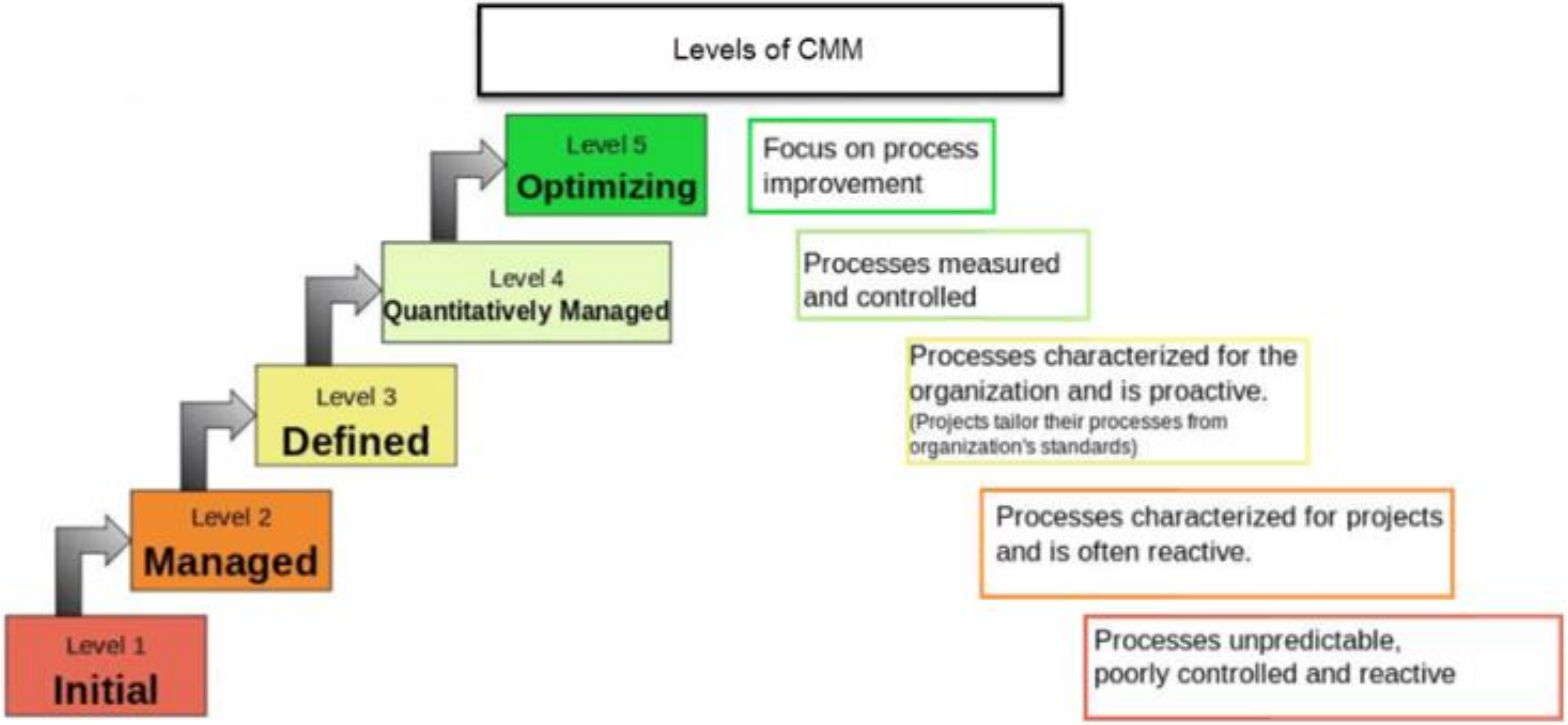
Types of Performance management

IT Balanced Scorecard

It is a performance metric used in strategic management to identify and improve various internal functions of a business.

Capability Maturity Model

It is a methodology used to develop and refine an organization's software development process.

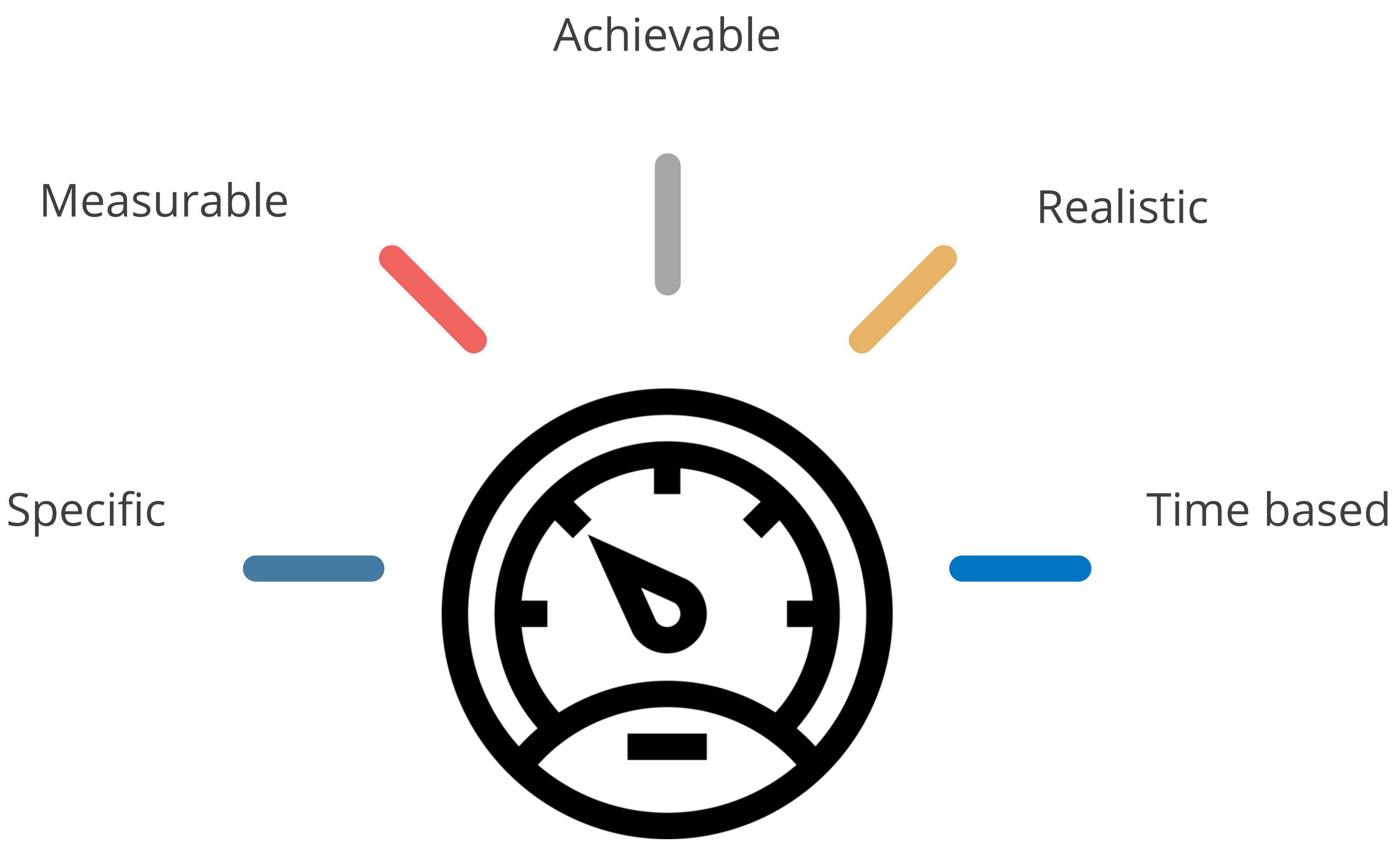


Levels of CMM

Level 5
Optimizing
Focus on process improvement
Level 4
Quantitatively Managed
Processes measured and controlled
Level 3
Defined
Processes characterized for the organization and is proactive. (Projects tailor their processes from organization's standards)
Level 2
Managed
Processes characterized for projects and is often reactive.
Level 1
Initial
Processes unpredictable, poorly controlled and reactive

SMART Metric

A smart metric stands for specific, measurable, achievable or acceptable, realistic, and time specific or trackable.



Achievable

Measurable

Realistic

Specific

Time based

Risk Management

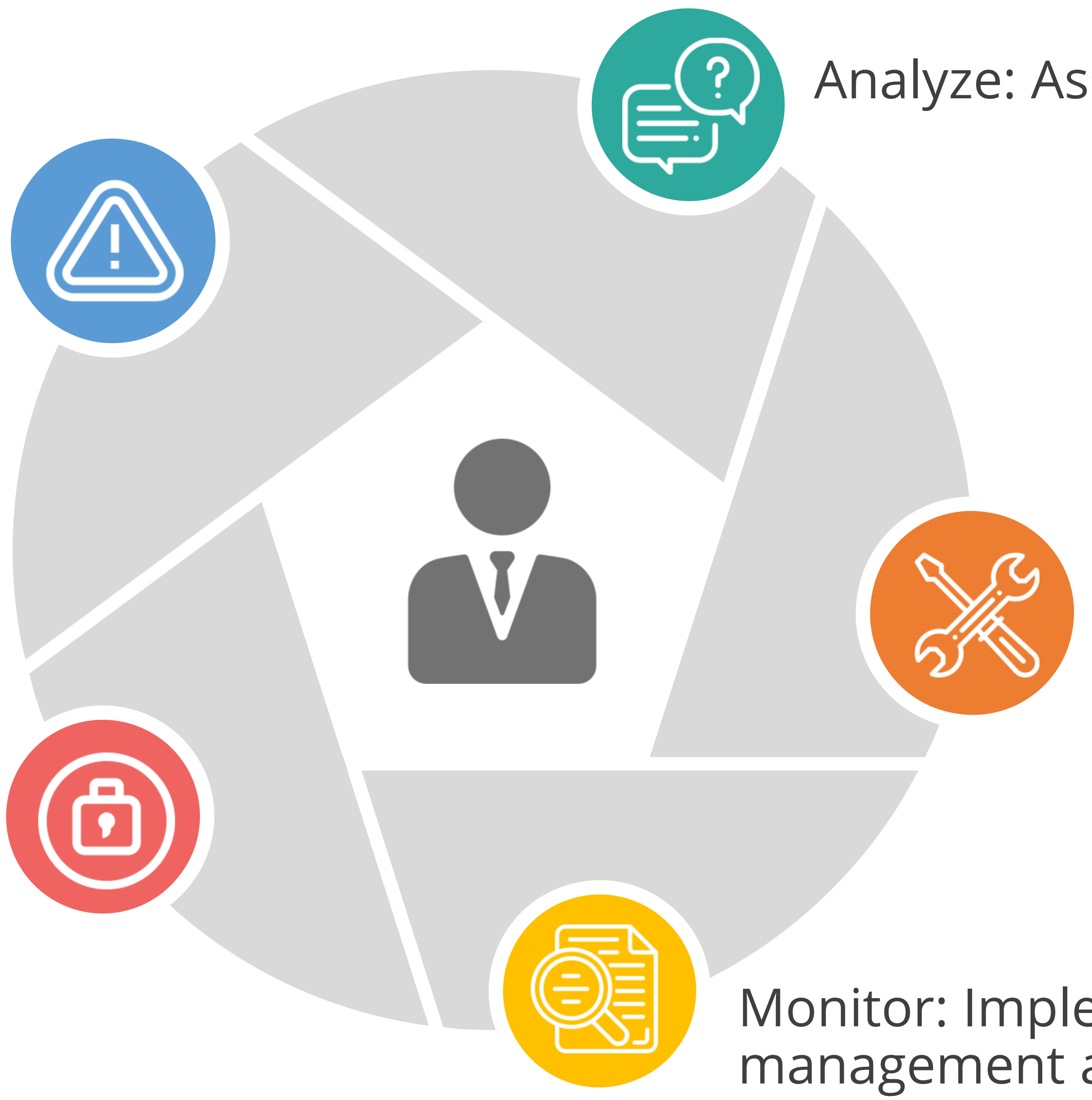
Risk Management

It is the process of identifying, assessing, monitoring, and controlling events arising from risks.

Risk Management

Risk cannot be removed but it can be minimized to an acceptable level.

Risk Management Process



Identify: Identify the risk

Analyze: Assess the risk

Action: Develop a risk management plan

Monitor: Implement risk management actions

Control: Reevaluate the risk

Quantitative Risk Analysis

It is a technique used to assess the effect of risk exposure events on overall organizational objectives.

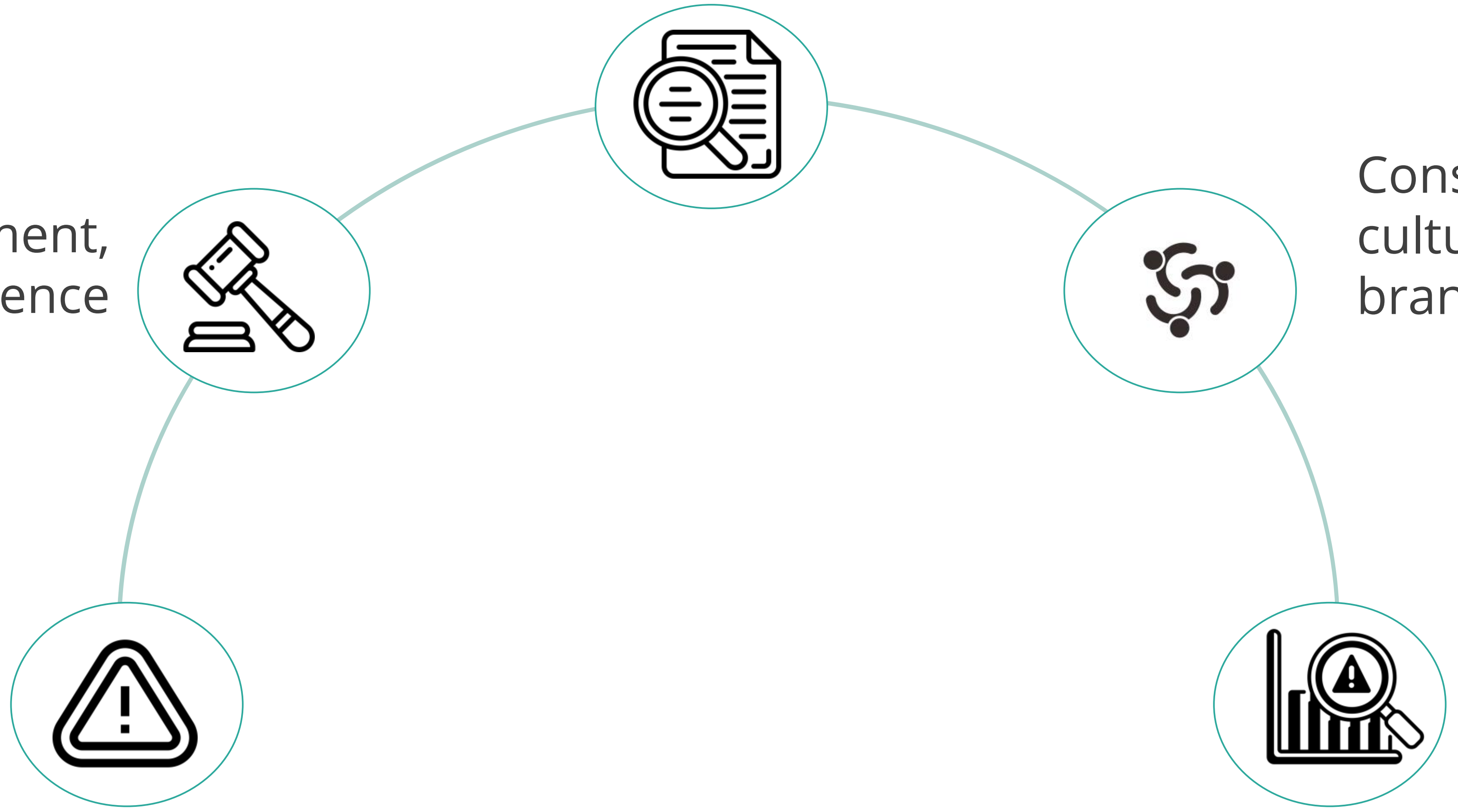
Quantitative Risk Analysis

Enables business to prioritize risks

Assists in measuring the magnitude of impact

Calculates absolute financial values

Quantitative Risk Analysis



Provides initial assessment to identify risks

Is based on expert judgment, intuition, and experience

Considers organization culture, reputation, and brand image

Uses different risk scenarios and ranks threats

Ranks risks based on severity

Risk Management Methods

Risk Management methods are:

Risk Mitigation: Implement measures to eliminate vulnerabilities

Risk Transfer: Transfer the risks to another entity

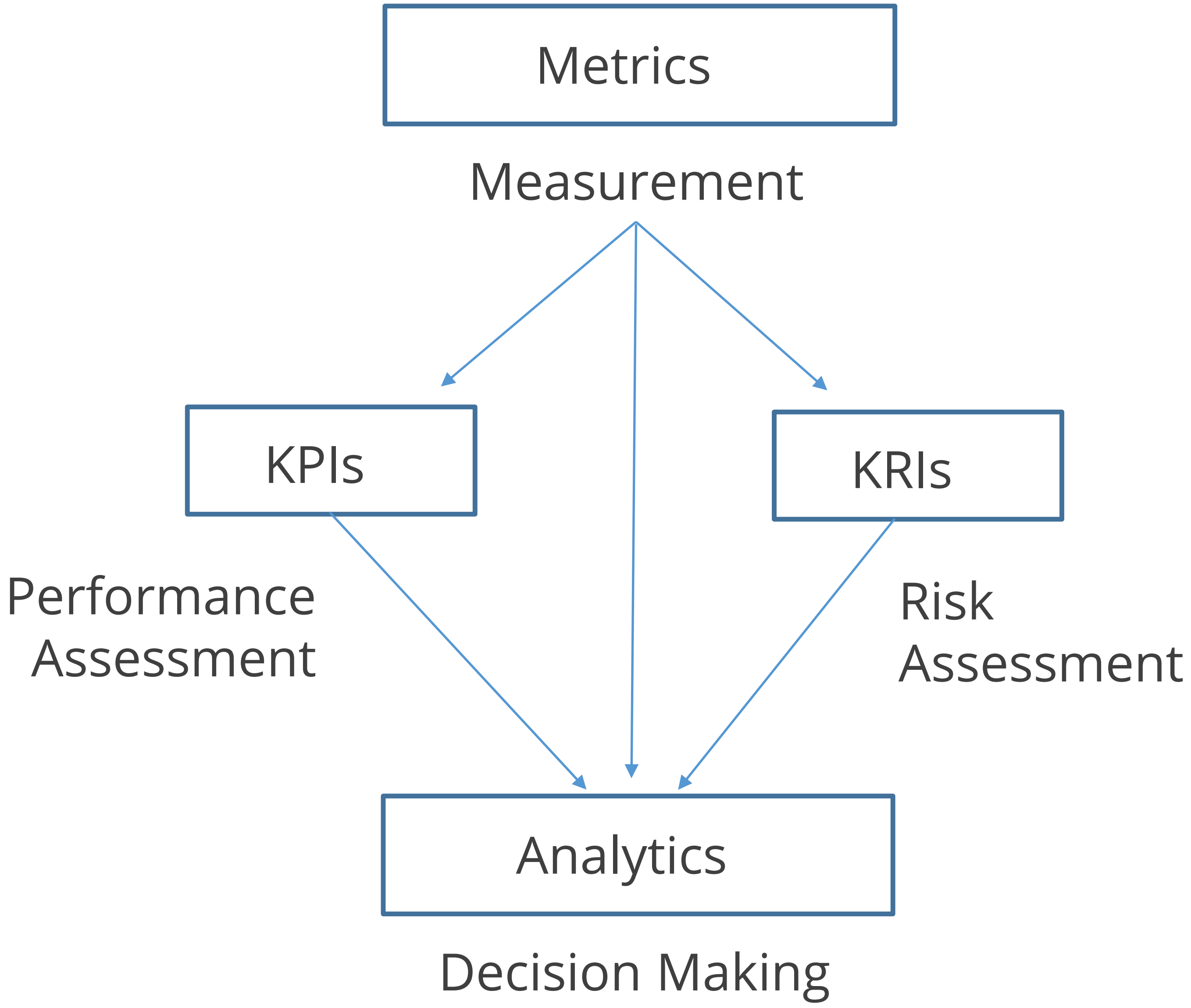
Risk avoidance: Eliminate activities that involve risks

Risk acceptance: Make decisions to live with the risks

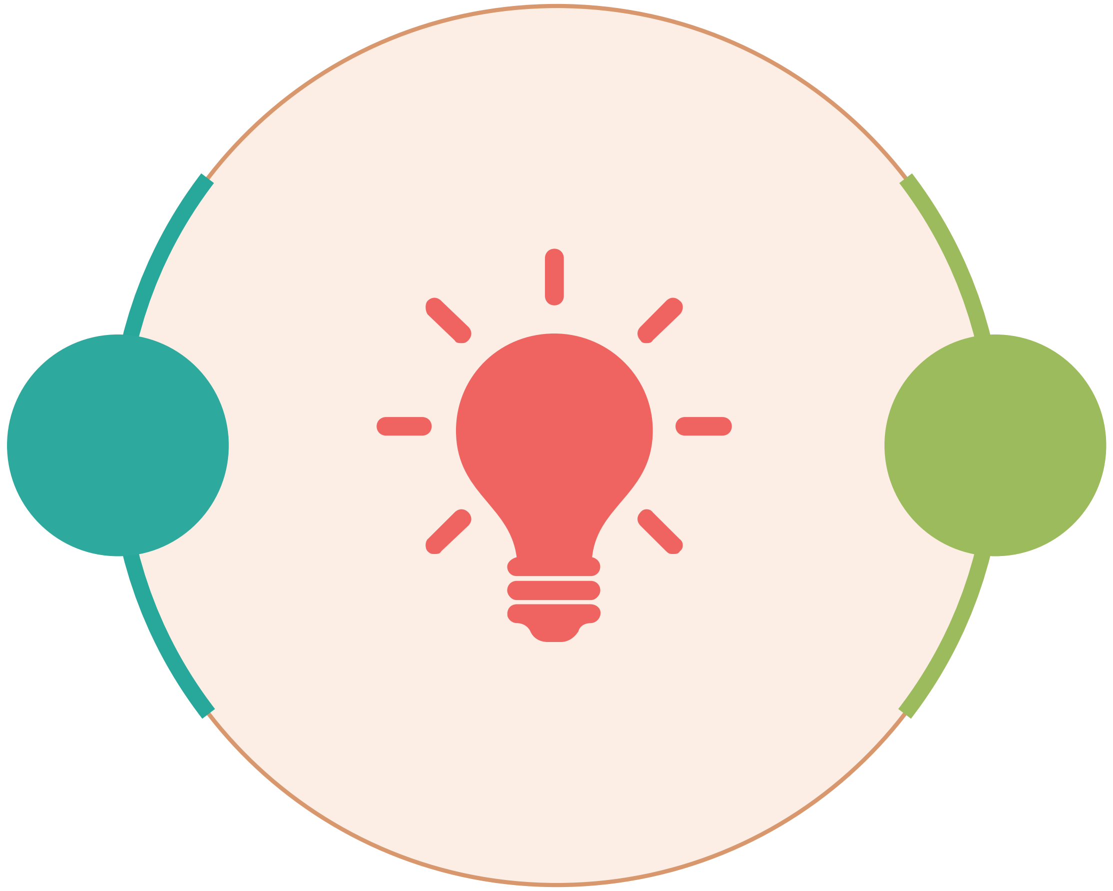
Key Risk Indicator and Key Performance Indicator

Key Performance Indicator is a quantifiable metric that reflects how well an organization is achieving its stated goals and objectives.

Key Risk Indicators are metrics used by organizations to provide an early signal of increasing risk exposure in various areas of the enterprise.



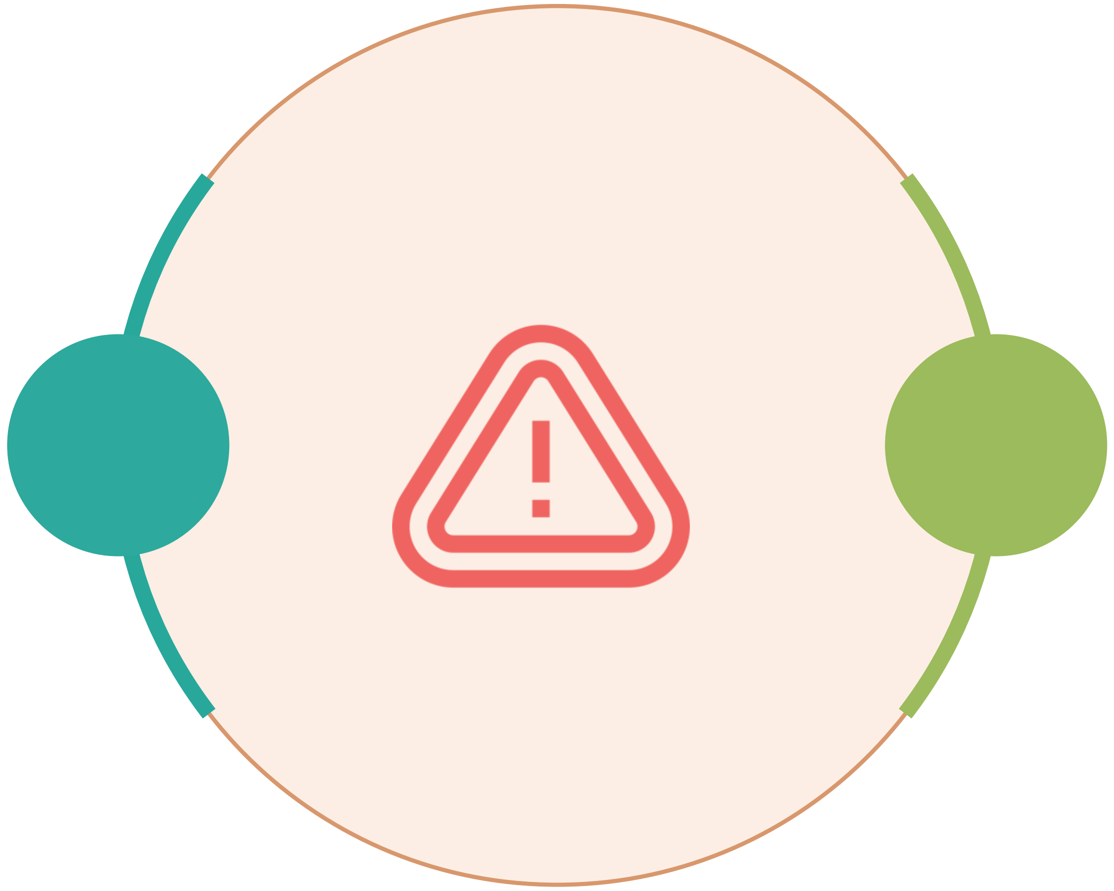
Key Performance Indicator



Provides a high-level overview of the past performance

Measures the performance of security controls

Key Risk Indicator



Serves as an early warning indicator

Is selected for its impact on the senior leaders’ decisions

Risk IT Framework

It is a framework based on a set of guiding principles featuring business processes and management guidelines.

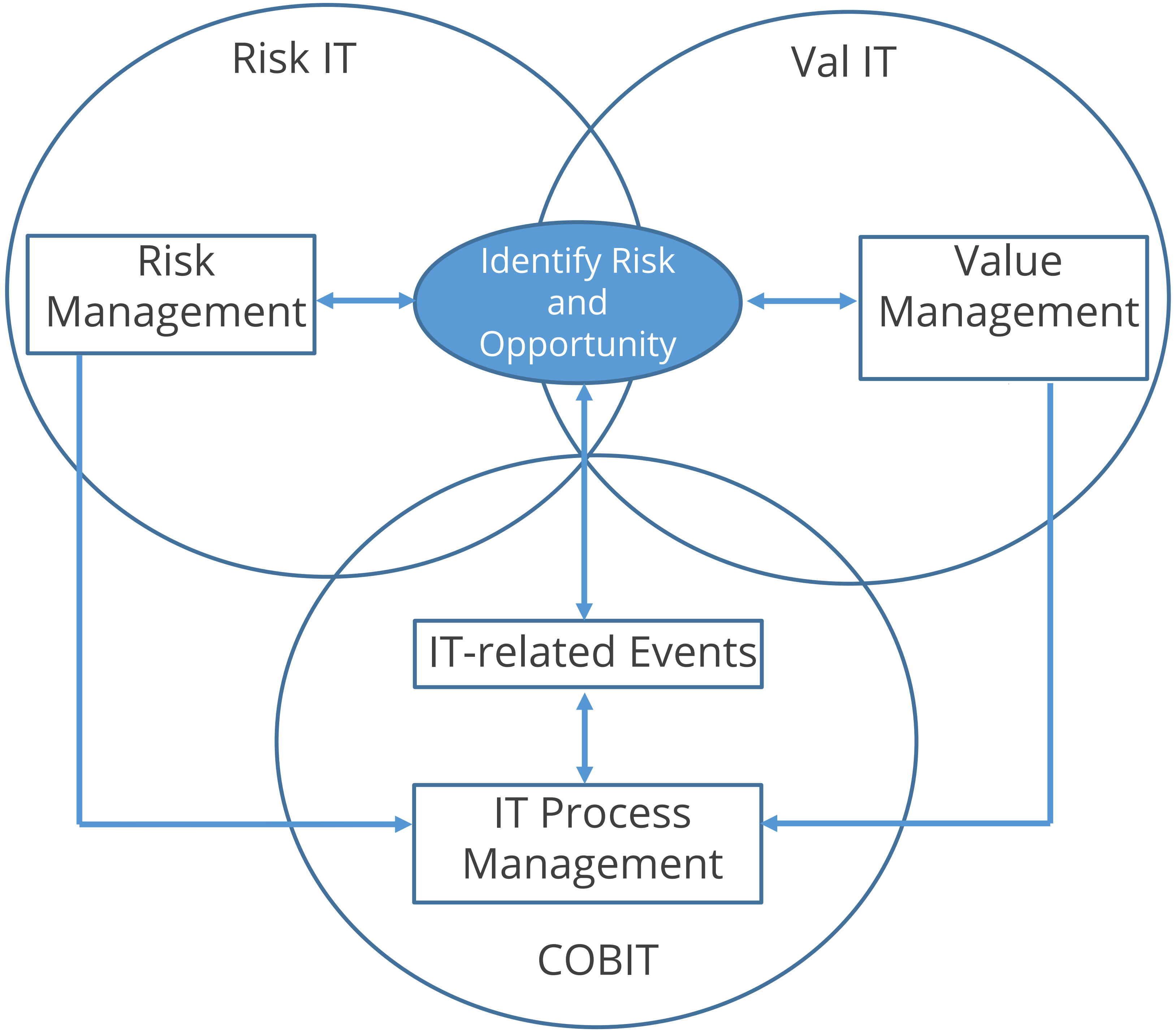
A structured process to identify potential organization threats

A strategy for minimizing the impact of risks

A mechanism to effectively evaluate strategies

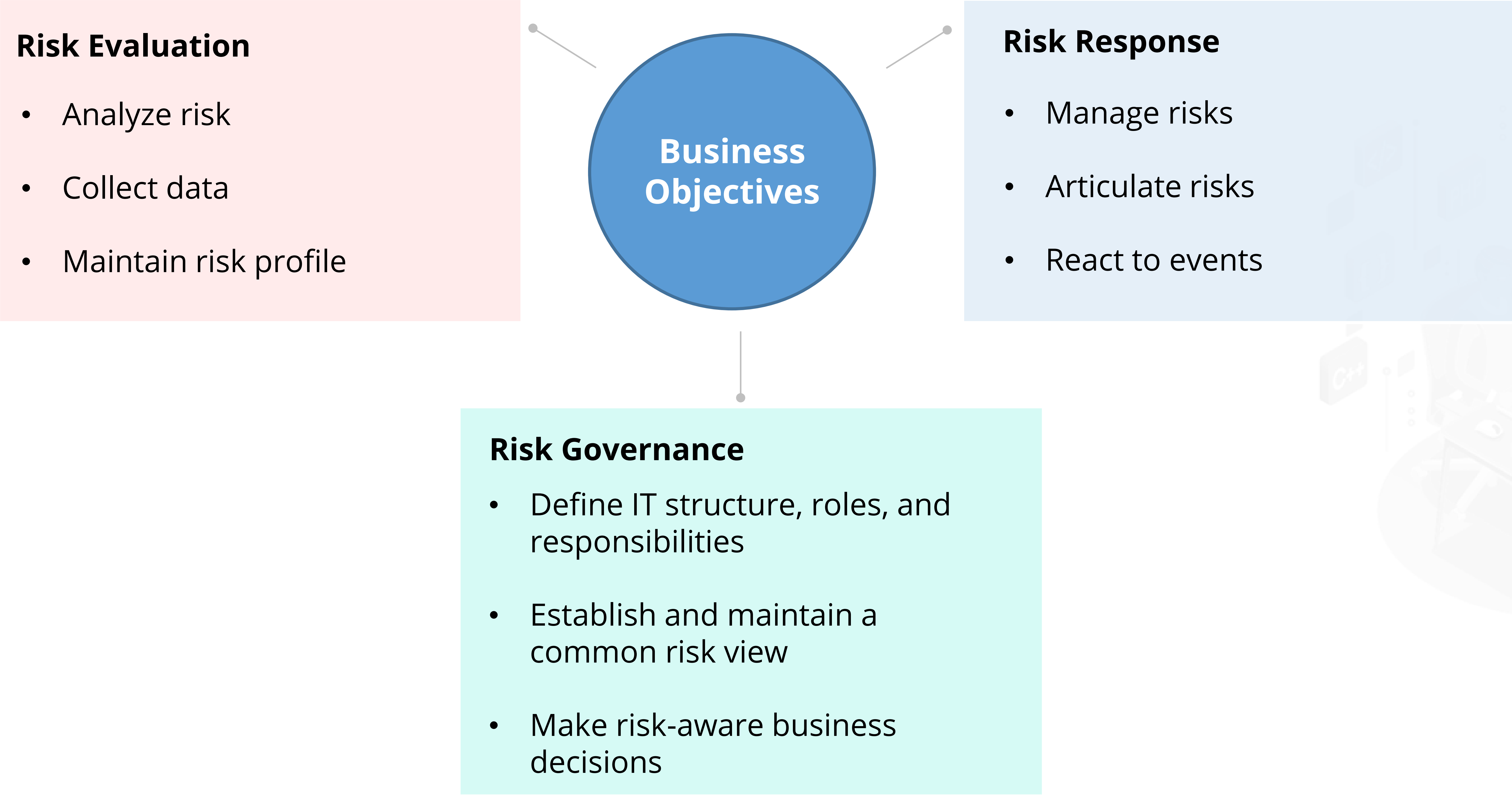
Risk IT Framework

Complements COBIT



Helps implement IT governance

Risk IT Framework



Business Objectives

Risk Evaluation

- Analyze risk
- Collect data
- Maintain risk profile

Risk Response

- Manage risks
- Articulate risks
- React to events

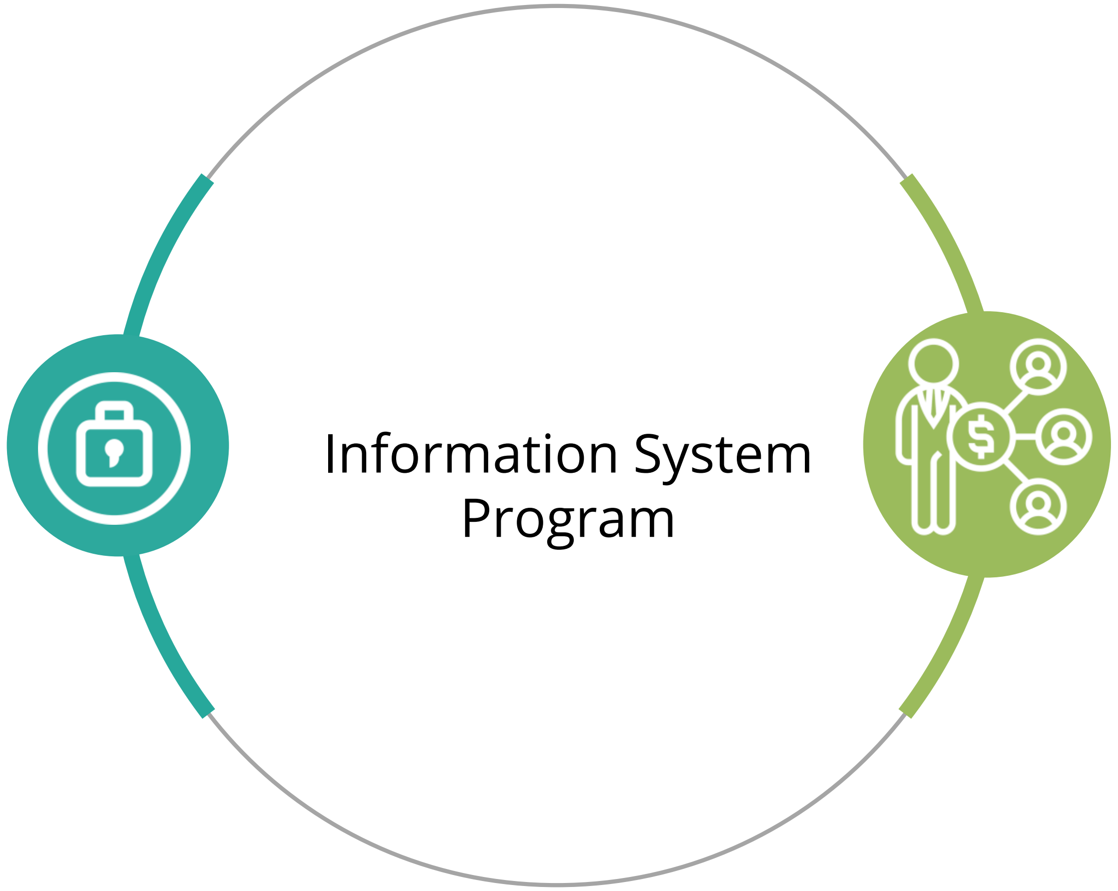
Risk Governance

- Define IT structure, roles, and responsibilities
- Establish and maintain a common risk view
- Make risk-aware business decisions

Information Security Programs

Information System (IS) Programs

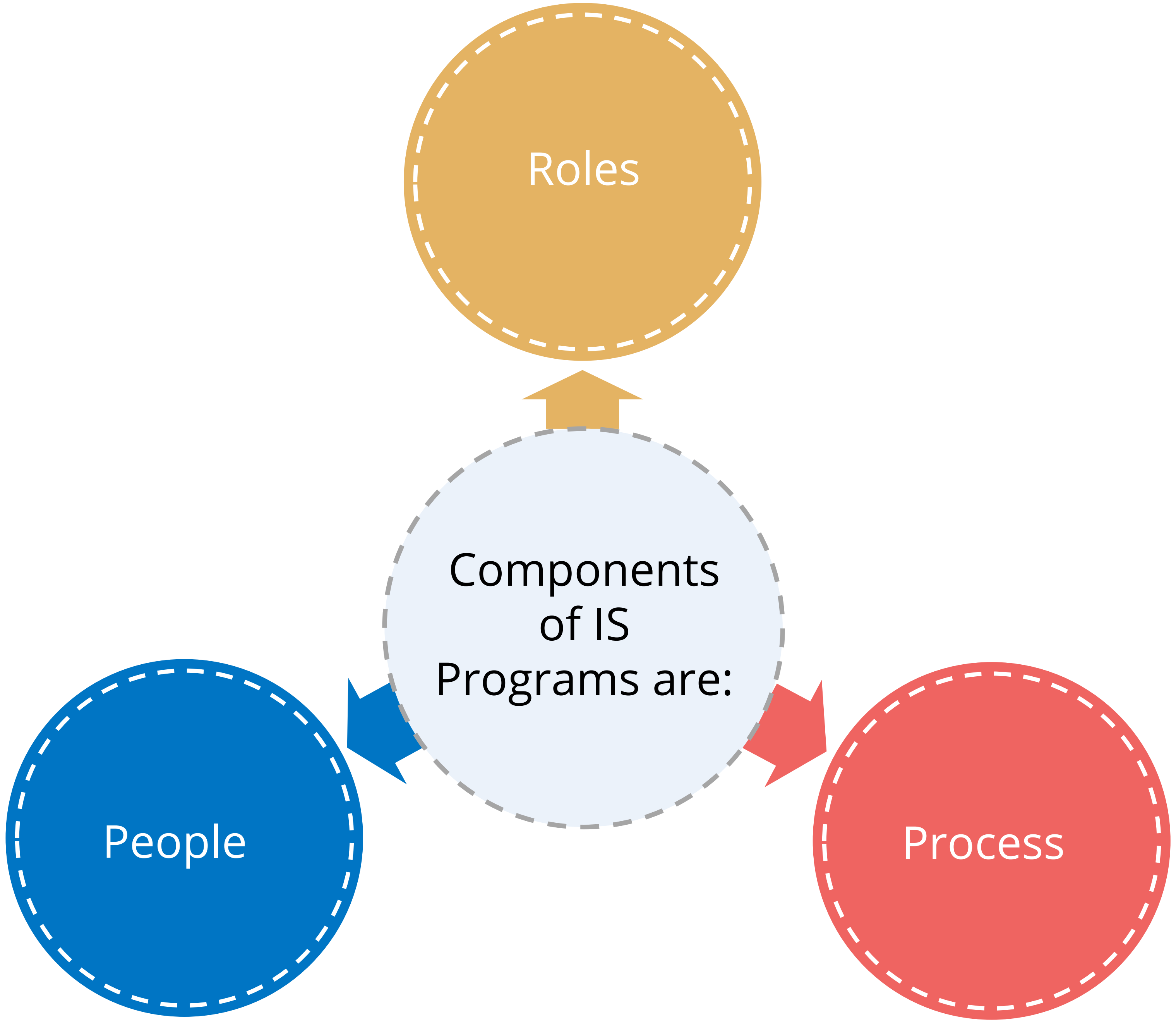
Ensures that an organization’s information assets are protected



Information System Program

Describes a complete organizational structure

IS Programs Components



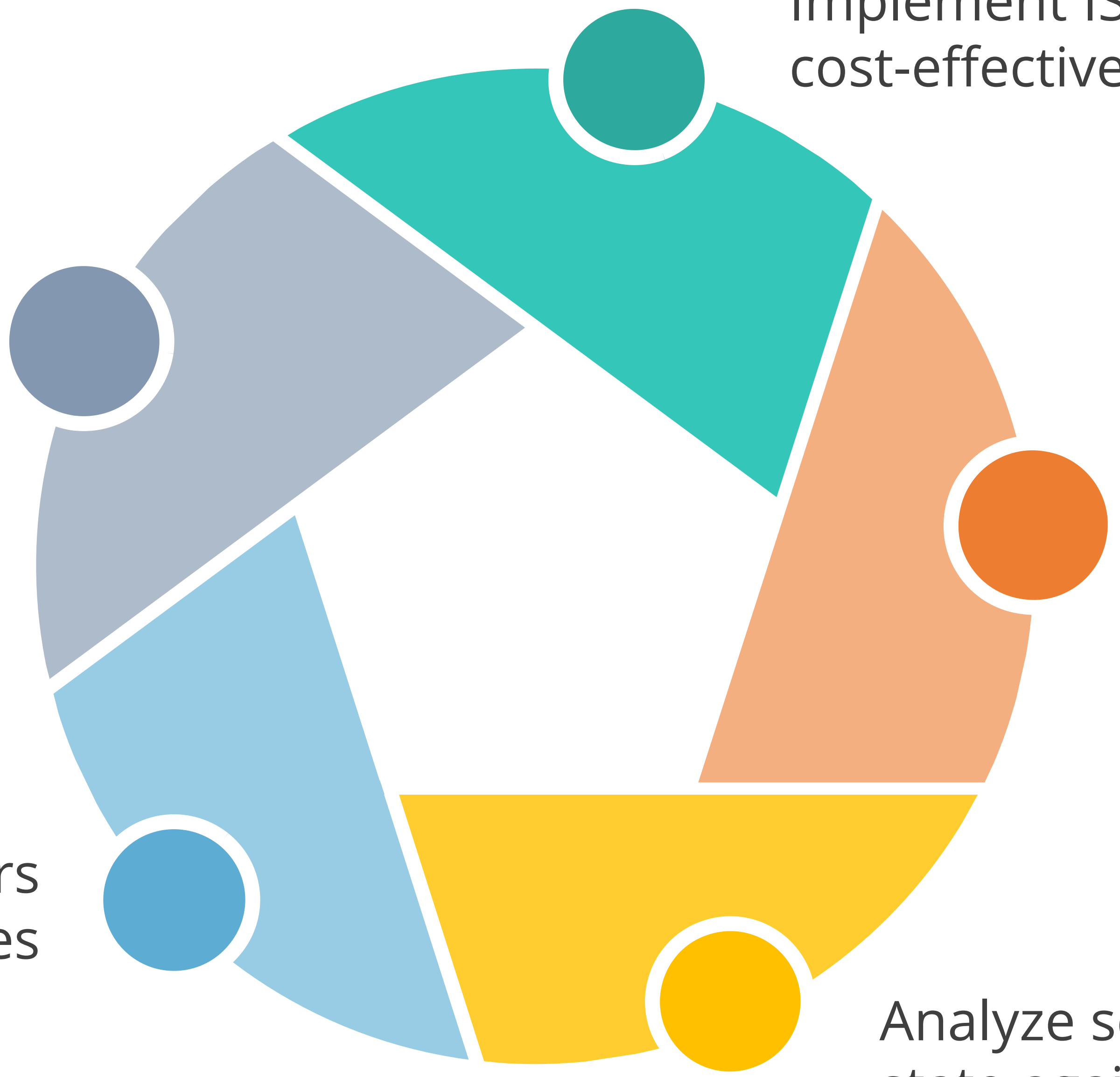
Roles

Components of IS Programs are:

People

Process

IS Programs Objectives



Implement IS strategy in a cost-effective manner

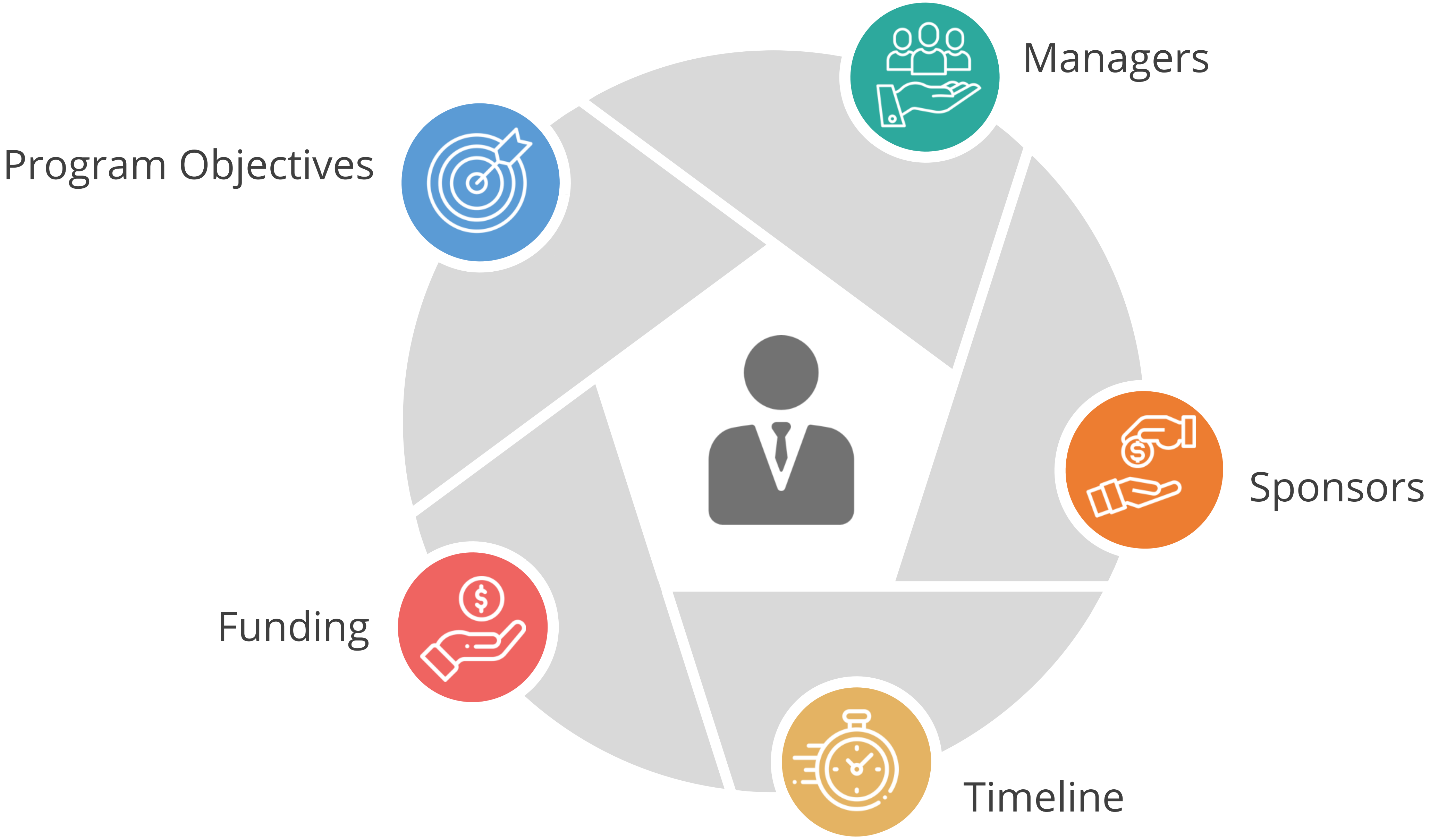
Tackle issues during the execution

Analyze security of current state against the desired state

Develop key goal indicators to reflect objectives

Develop methods to measure progress

IS Program Charter

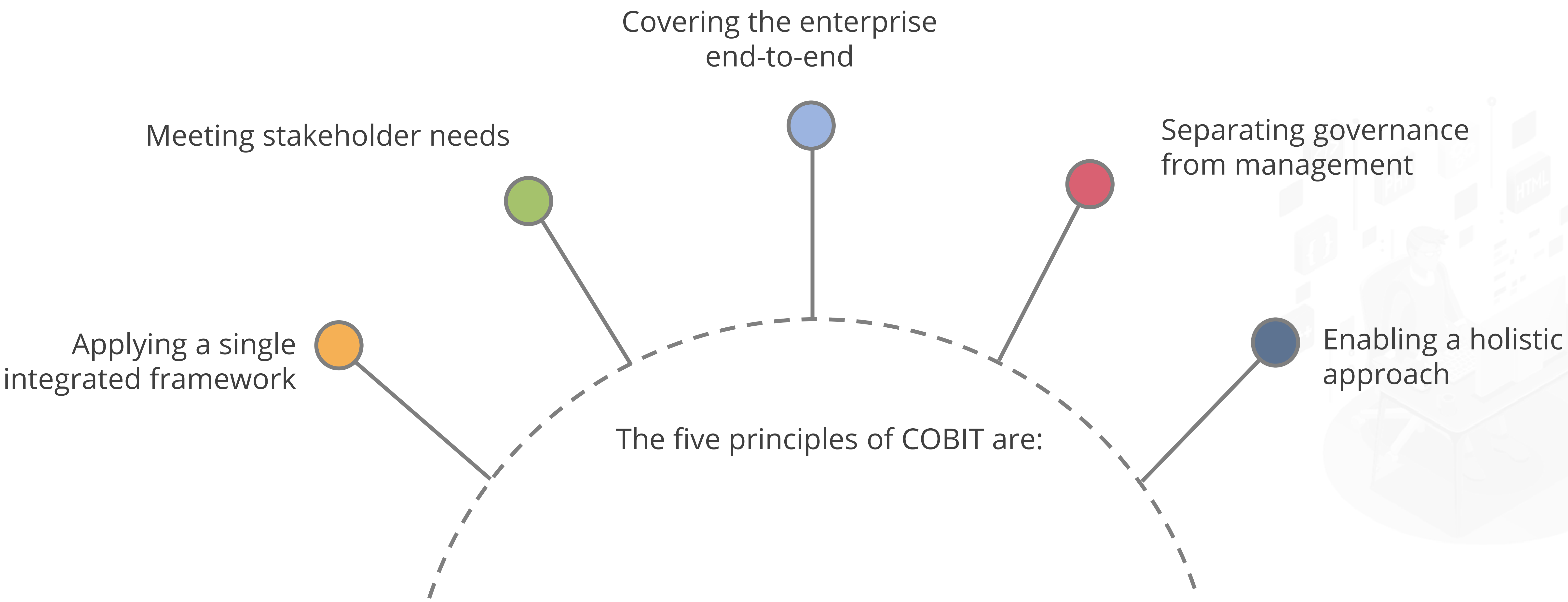


IS Management Framework: COBIT®

It helps the companies map their IT processes to ISACA’s best practices standard.

Control Objectives for Information and Related Technologies

Five Principles of COBIT



The five principles of COBIT are:

Applying a single integrated framework

Meeting stakeholder needs

Covering the enterprise end-to-end

Separating governance from management

Enabling a holistic approach

IS Management Framework: ISO/IEC 27001:2013

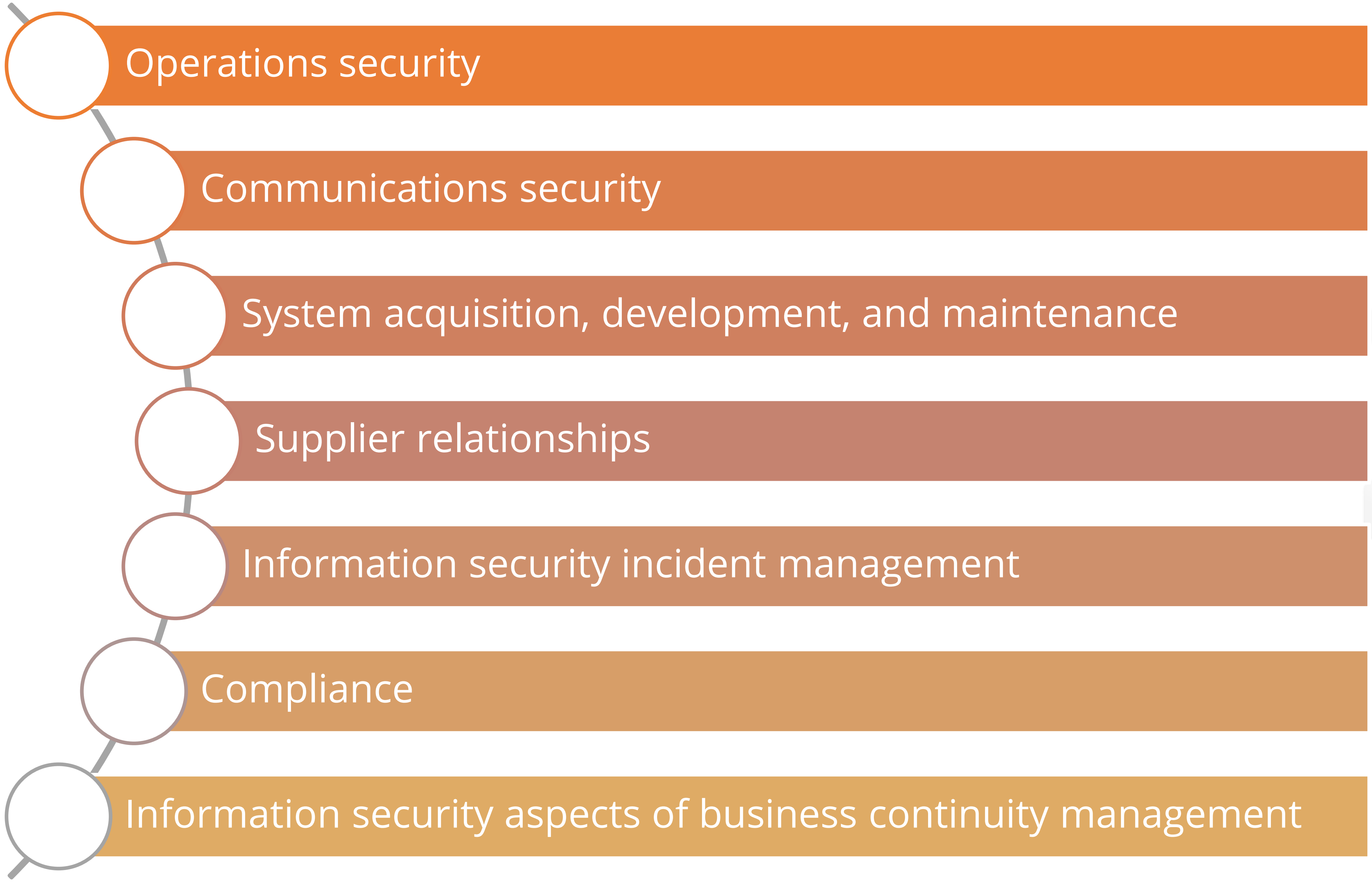
This is an internationally recognized structure methodology dedicated to information security.

- A management process to evaluate, implement, and maintain an ISMS
- A comprehensive set of controls
- Applicable to all industry sectors
- Emphasis on prevention
- 114 controls mapped to 14 security domains

ISO 27001:2013 Domains

- Security policies
- Organization of information security
- Human resources security
- Access control
- Cryptography
- Asset management
- Physical and environmental security

ISO 27001:2013 Domains



Operations security

Communications security

System acquisition, development, and maintenance

Supplier relationships

Information security incident management

Compliance

Information security aspects of business continuity management

IS Program Roadmap

Review current security levels

Security level of data, applications, systems, facilities, and processes

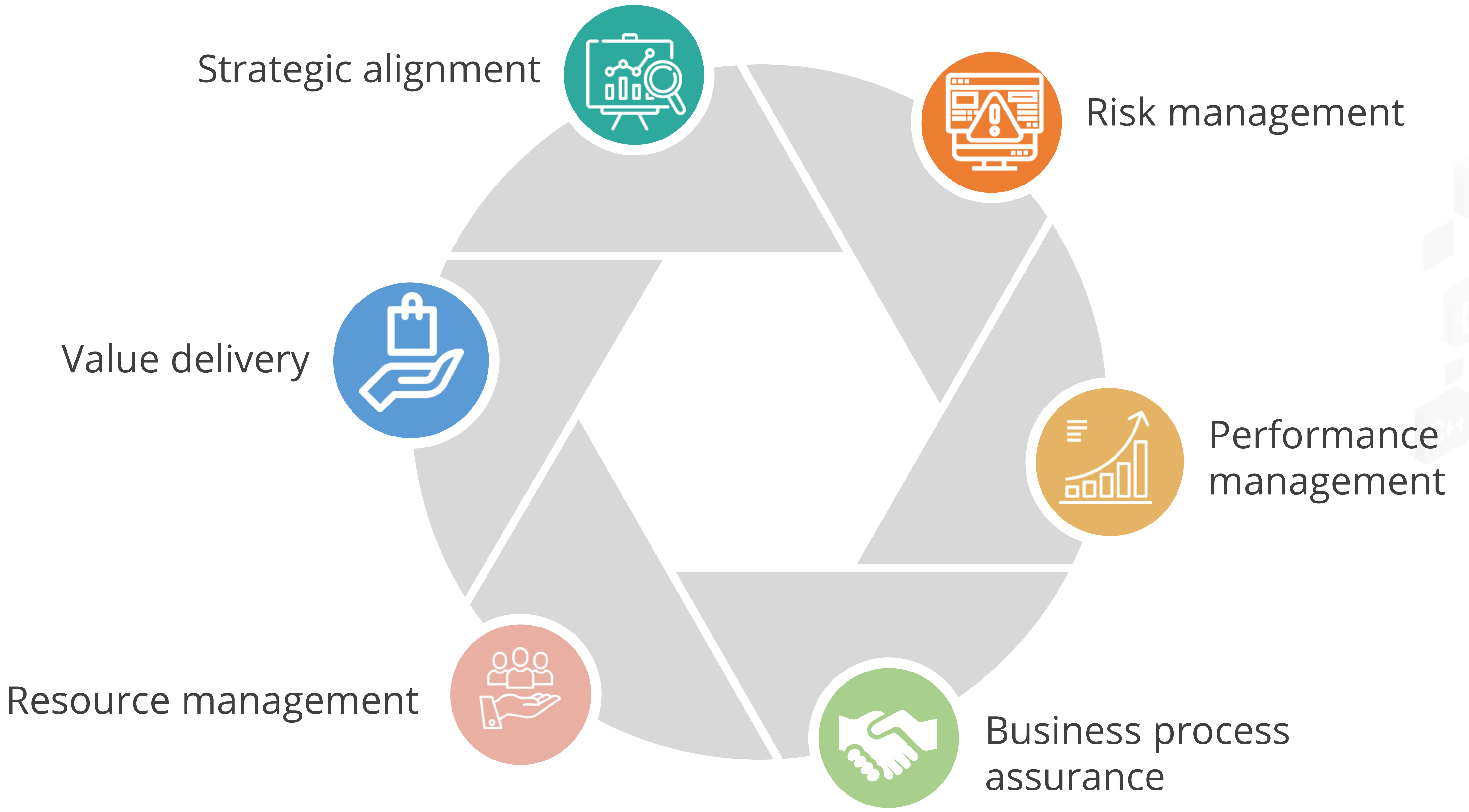
Develop IS program roadmap

- High-level plan
- Architectural design
- Milestones to achieve KGI, CSF, and KPI

Perform gap analysis

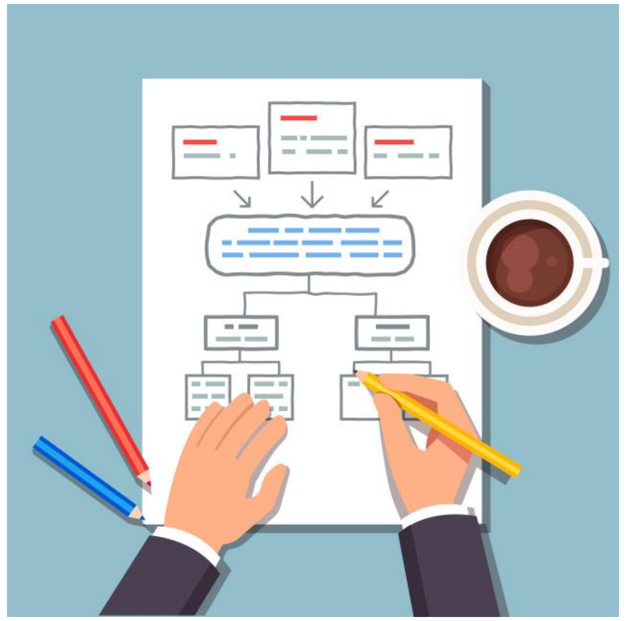
- Analyze gaps
- Identify areas with inadequate control objectives
- Establish control points
- Monitor controls

Outcomes of IS Program



Outcomes of IS Program

- Strategic alignment
- Risk Management
- Value Delivery
- Resource Management
- Performance Management
- Business Process Assurance



- It determines the competitiveness of an organization.
- It explains how organizations can increase growth and profitability.

Outcomes of IS Program

- Strategic alignment
- **Risk Management**
- Value Delivery
- Resource Management
- Performance Management
- Business Process Assurance

- Information security manager is responsible for information assets.
- IS manager must understand threats to the organization, its vulnerabilities, and the risk profile.

Outcomes of IS Program

- Strategic alignment
- Risk Management
- **Value Delivery**
- Resource Management
- Performance Management
- Business Process Assurance

IS program must deliver the required level of security effectively and efficiently.

Outcomes of IS Program

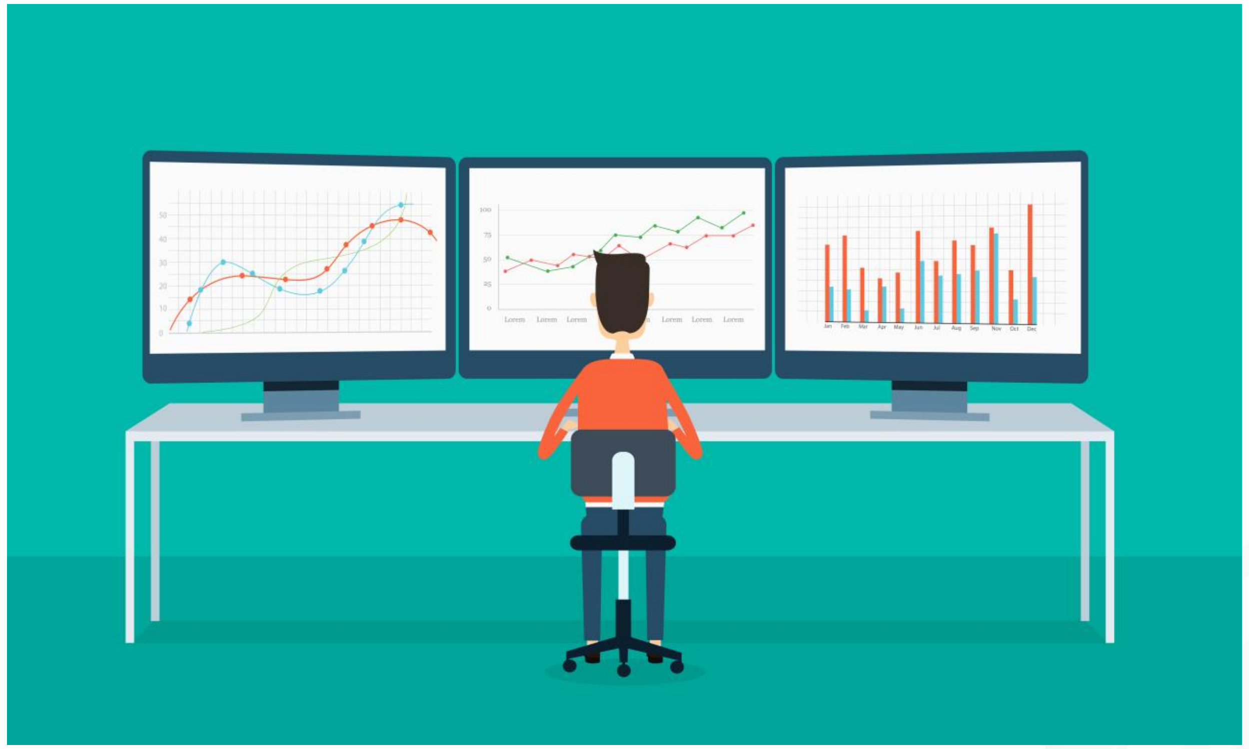
- Strategic alignment
- Risk Management
- Value Delivery
- **Resource Management**
- Performance Management
- Business Process Assurance

RECRUITMENT
SERVICES
Lorem ipsum dolor sit amet, coectetur adi sed do eiusmod tempor incididunt Lorem ipsum dolor sit amet.
Learn more

- IS manager must use human technical knowledge and financial resources effectively.
- Security practices and processes must be documented and consistent.
- Security architecture is developed to define and utilize infrastructures.

Outcomes of IS Program

- Strategic alignment
- Risk Management
- Value Delivery
- Resource Management
- **Performance Management**
- Business Process Assurance



- It must develop monitoring process and metrics.
- IS managers must seek independent assurance.

Outcomes of IS Program

- Strategic alignment
- Risk Management
- Value Delivery
- Resource Management
- Performance Management
- **Business Process Assurance**

IS manager must understand that IS is only a part of effective security.

Supply Chain

Supply Chain

It is a system of organizations, people, activities, information, and resources involved in moving product to customer.

Supply Chain Management (SCM)

It is an expansive and complex undertaking that relies on each partner; from suppliers to manufacturers.

Supply Chain Risk Management (SCRM)

It is the implementation of strategies to manage both everyday and exceptional risks.

Supply Chain Risks

The supply chain risks are:

Compromised software or hardware purchased from suppliers

Vulnerabilities in supply chain management or supplier systems

Poor Information Security practices by lower-tier suppliers

Counterfeit hardware or hardware with embedded malware

Third-party data storage or data aggregators

Third-party service providers or vendors

Supply Chain Countermeasures

Compliance and governance

Presence of robust IT security solutions internally

Certification of international standards

Supplier Management Controls

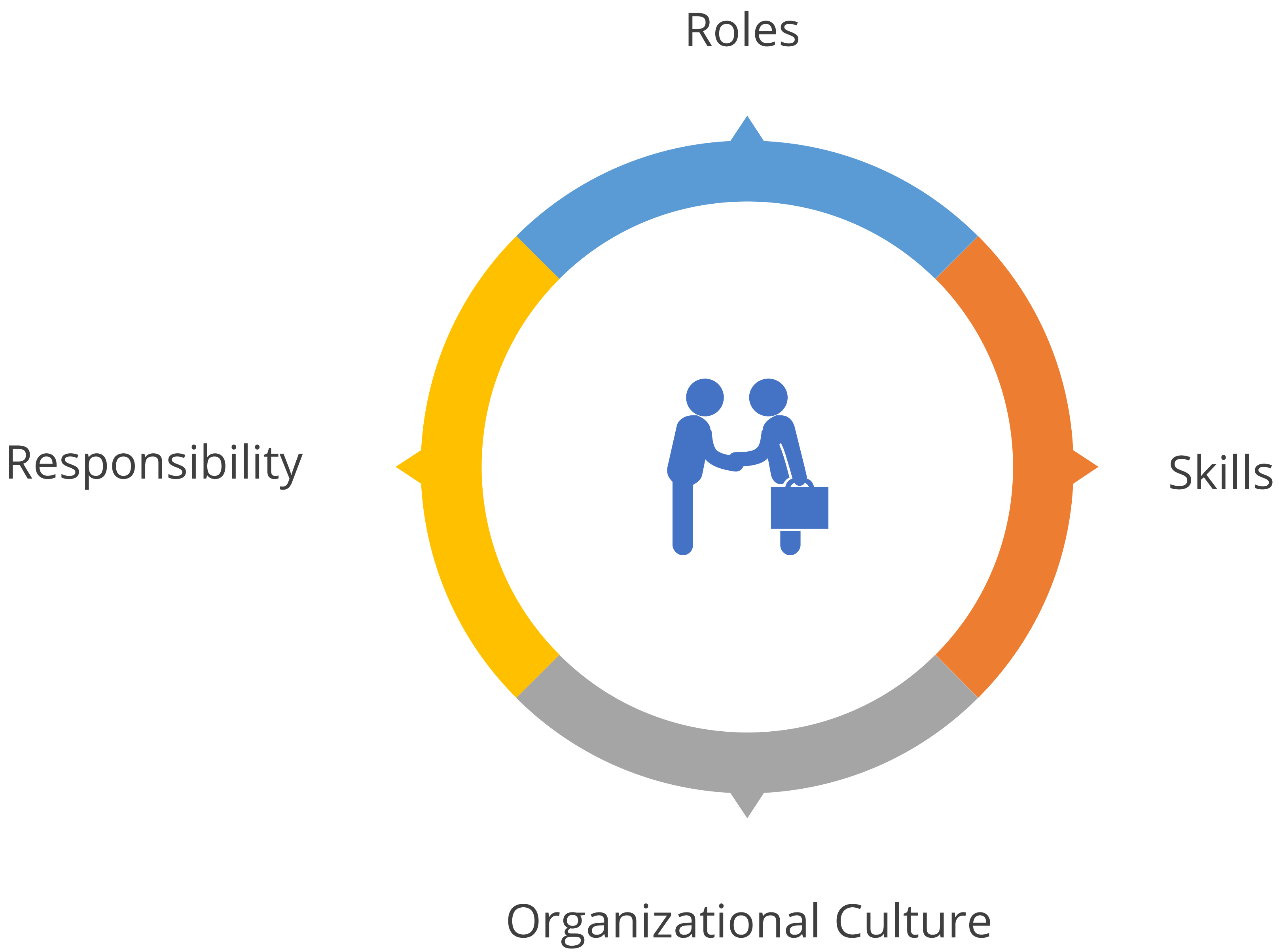
It is the process whereby companies monitor and manage interactions with all external parties with which they have a relationship.

Personnel Management

Personnel Management

It refers to planning, organizing, compensation, integration, and maintenance of people for the purpose of contributing to organizational, individual, and societal goals.

Personnel Management

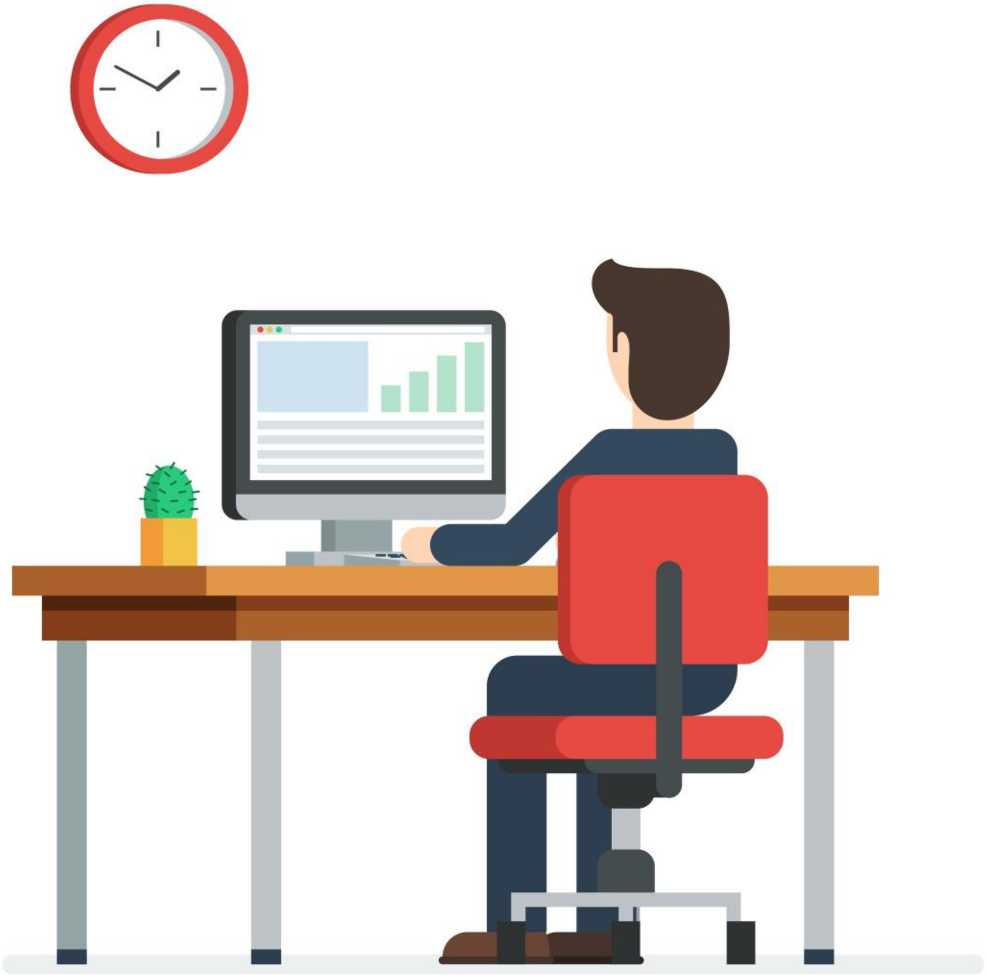


Case Study: AWS Outage

Problem Statement: In May 2017, Amazon faced a big A.W.S. outage that took down a bunch of large internet sites for several hours on a Tuesday afternoon.

Case Study: AWS Outage

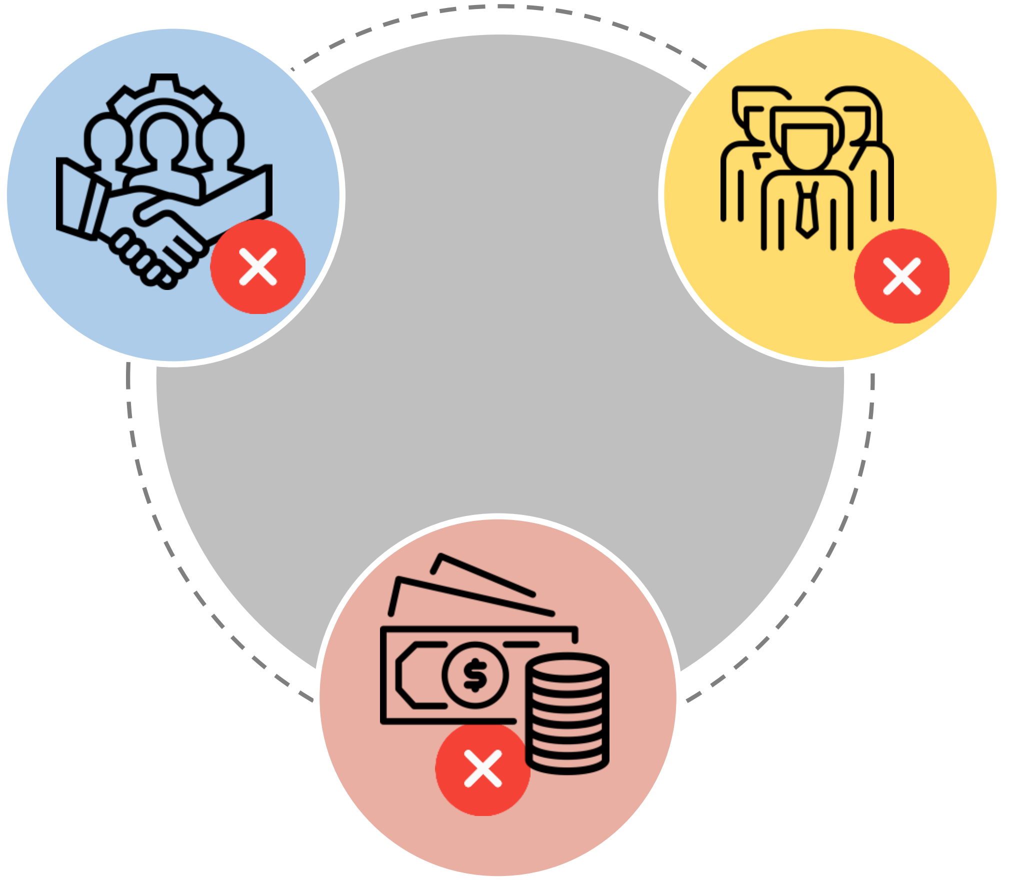
Cause of the problem: In a blog post, the company said that one of its employees was debugging an issue with the billing system and accidentally took more servers offline than intended. That error started a domino effect that took down two other server subsystems and so on.



Case Study: AWS Outage

This case illustrates the importance of change management and internal governance in organizations.

Common IS Program Challenges



Inadequate management support

Inadequate staffing

Inadequate funding

Key Takeaways

- Information security governance is the set of responsibilities and practices exercised by the board and executive management.

- Risk management is the process of identifying, assessing, monitoring, and controlling events arising from risks.

- The information security program consists of controls, processes, and practices to increase the resilience of the computing environment.

- Supply chain is a system of organizations, people, activities, information, and resources involved in moving a product to customer.

Knowledge Check

Knowledge Check

1

Which of the following model describes a five-level evolutionary path of increasingly organized and systematically more mature processes?

a. Measureable

b. Initial

c. Achievable

d. Reliable

Knowledge Check

1

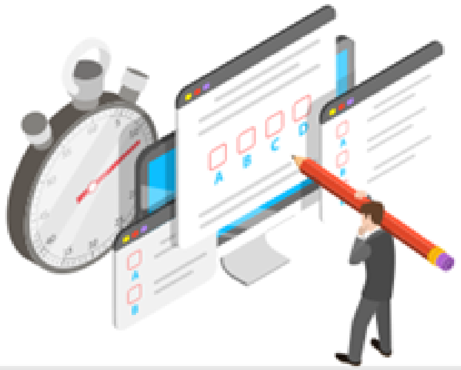
Which of the following model describes a five-level evolutionary path of increasingly organized and systematically more mature processes?

a. Measureable

b. Initial

c. Achievable

d. Reliable



The correct answer is **b**

The model which describes a five-level evolutionary path of increasingly organized and systematically more mature processes is initial.

Knowledge Check

2

Which of the following is a system of organizations, people, activities, information, and resources involved in moving a product to customer?

a. Supply chain management

b. Supply chain risk management

c. Supply chain

d. Supplier management controls

Knowledge Check

2

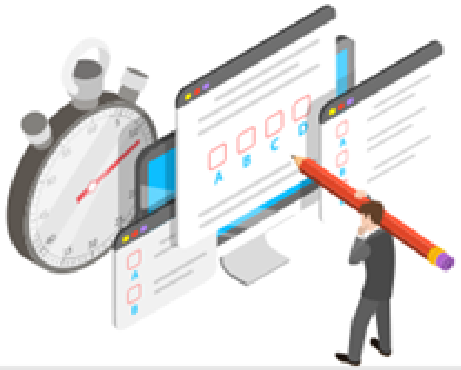
Which of the following is a system of organizations, people, activities, information, and resources involved in moving a product to customer?

a. Supply chain management

b. Supply chain risk management

c. Supply chain

d. Supplier management controls



The correct answer is **c**

Supply chain is a system of organizations, people, activities, information, and resources involved in moving a product to customer.

Knowledge Check

3

Which of the following are the components of IS Programs?

a. Roles

b. Skills

c. Responsibility

d. Process

Knowledge Check

3

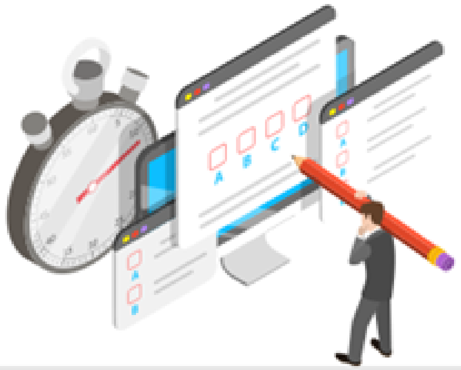
Which of the following are the components of IS Programs?

a. Roles

b. Skills

c. Responsibility

d. Process



The correct answer is **a and d**

The components of IS Programs are: Roles and Process.