Information Security Program Development and Management

Chapter Eight

Topics

- IS Program Development and Resources
- IS Standards and Frameworks
- Defining an IS Program Road Map
- IS Program Metrics
- IS Program Management
- IS Awareness and Training
- Integrating the Security Program with IT Operations
- Program Communications, Reporting and Performance Management

IS Program Development and Resources

Essential Elements of an IS Program

Three elements are essential to ensure successful security program design, implementation and ongoing management. The program must:

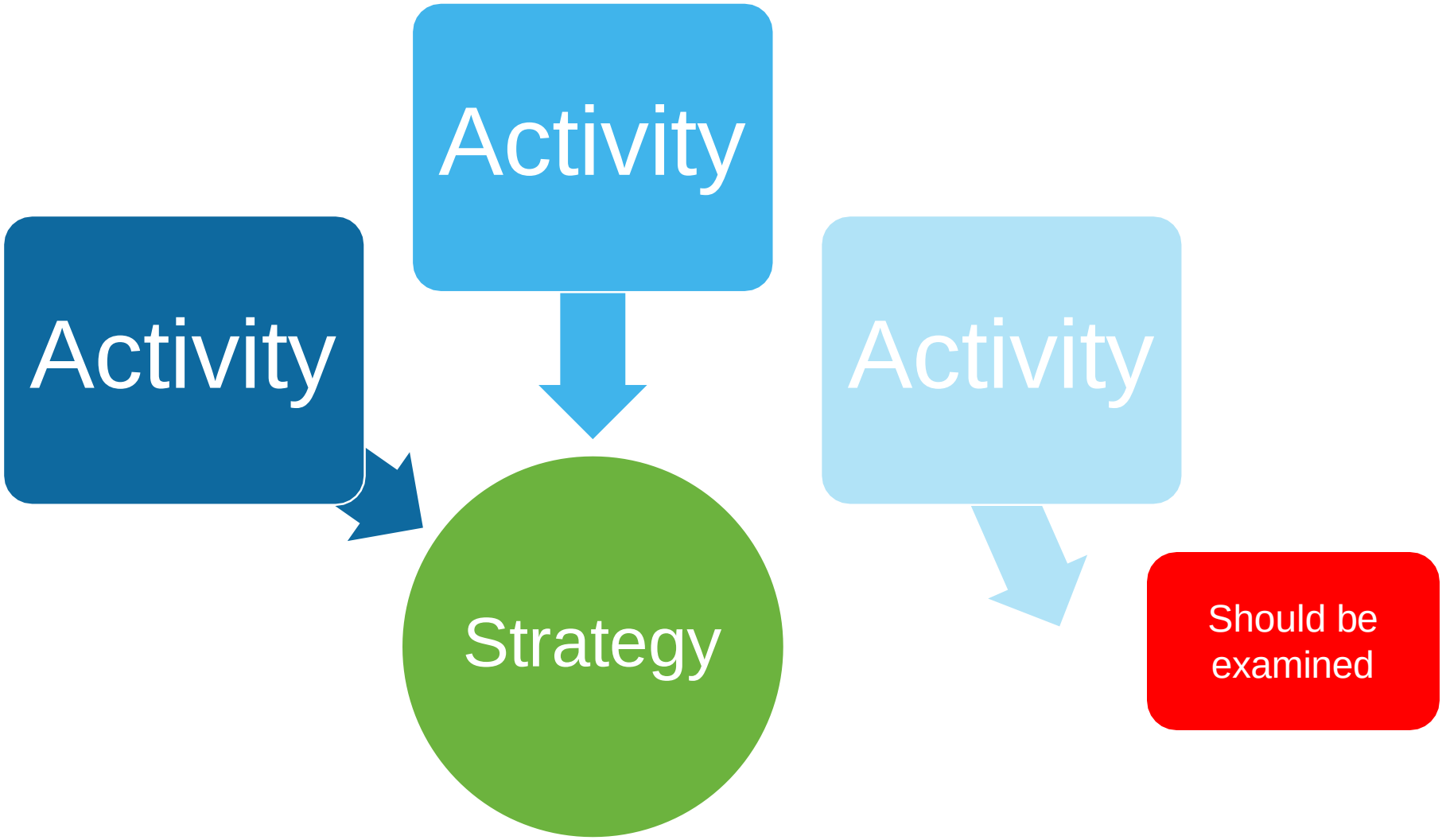
Demonstrate execution of a well-developed information security strategy that is closely aligned with and supports organizational objectives.

Be well designed with cooperation and support from management and stakeholders.

Provide feedback through metrics, to guide program execution to achieve the defined outcome.

ISACA

Strategic Alignment



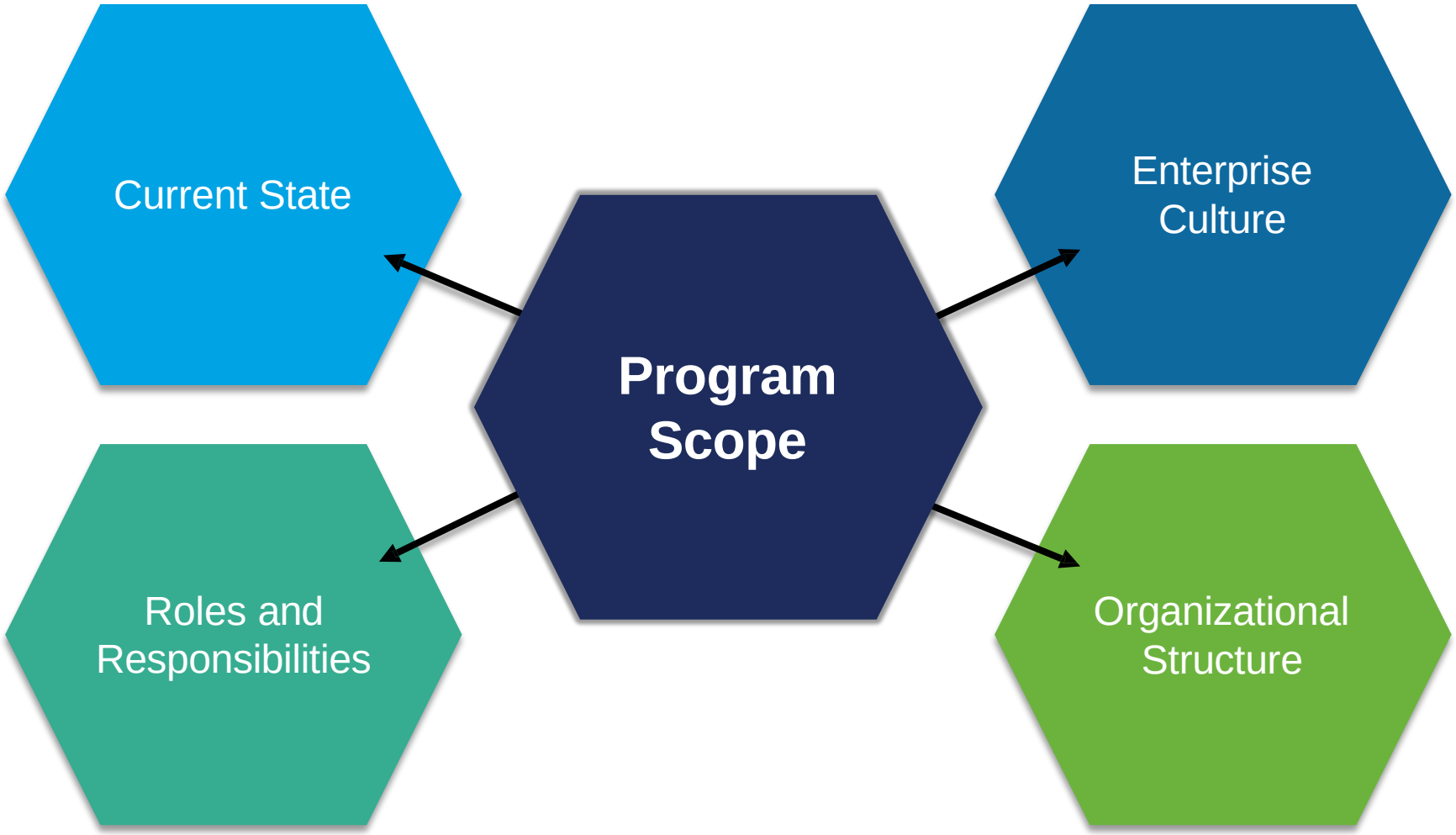
Applying the Security Program Business Case

The business case is the basis of major IS program projects and initiatives and outlines the needs of the enterprise, including:

IS Program Management Objectives

1. Strategic alignment
2. Risk management
3. Value delivery
4. Resource management
5. Performance measurement
6. Assurance process integration

Defining the Scope of the IS Program



Establishing the IS Program Scope and Charter

The information security manager determines the scope, responsibilities and charter of the program.

Scope

Established by developing a strategy in combination with risk management responsibilities

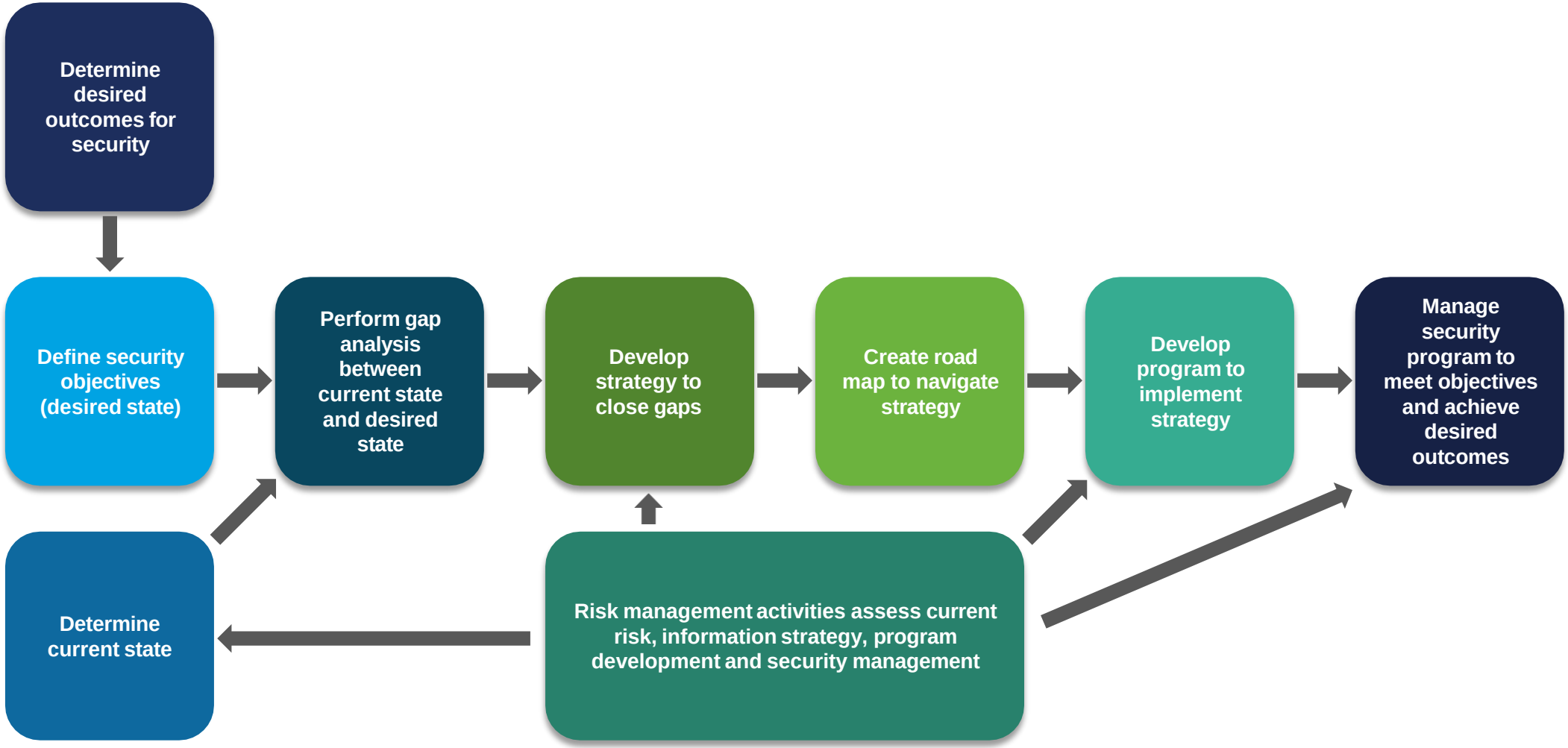
Charter

Determined by extent of management support of strategy implementation and risk management activities

Implementing a security program impacts established enterprise processes and procedures. The information security manager should:

- Integrate changes to policies and processes 
- Address resistance to change 

IS Program Development Steps



ISACA

Common Challenges and Constraints

Challenges

Management Support

- **Symptom**: Lack of program alignment with business goals and objectives
- **Solution**: Discuss changes and adaptations in ongoing dialogue

Funding

- **Symptom**: Low management support
- **Solution**: Leverage budgets or reprioritize resources

Staffing

- **Symptom**: Inadequate staffing levels to meet program requirements
- **Solution**: Demonstrate effort levels using workload management

Constraints

- Physical
- Ethics
- Culture
- Organizational Structure
- Costs
- Personnel
- Resources
- Capabilities
- Time
- Technology

Asset Identification and Valuation

Provide identification and classification of assets that need protection:

- Inventory information assets
- Determine relative business value
- Leverage classification and justification for protection
- Discover possible unidentified assets

Effective resource valuation is best based on loss scenarios.

Apply a consistent approach to prioritize efforts ahead of calculating exact valuation figures.

Consider the range of potential loss and impacts:

- Contribution to revenue
- Legal or regulatory sanctions
- Loss of trade secrets

ISACA

Asset Classification

- Necessary to determine the relative sensitivity and criticality of information assets
- Criticality is determined by the impact arising from loss of that asset
- Sensitivity is based on the potential damage to the enterprise from unauthorized disclosure
- Consider business dependency assessment to allocate proportional protective activities

- Ensure the information asset inventory is complete (data location, owners, users, custodians)
- Determine the appropriate classification based on business value of information assets
- Coordinate use with end-user managers in processes and to determine user access levels
- Identify security measures that can consistently be applied at various levels

Methods to Determine Criticality and Impact

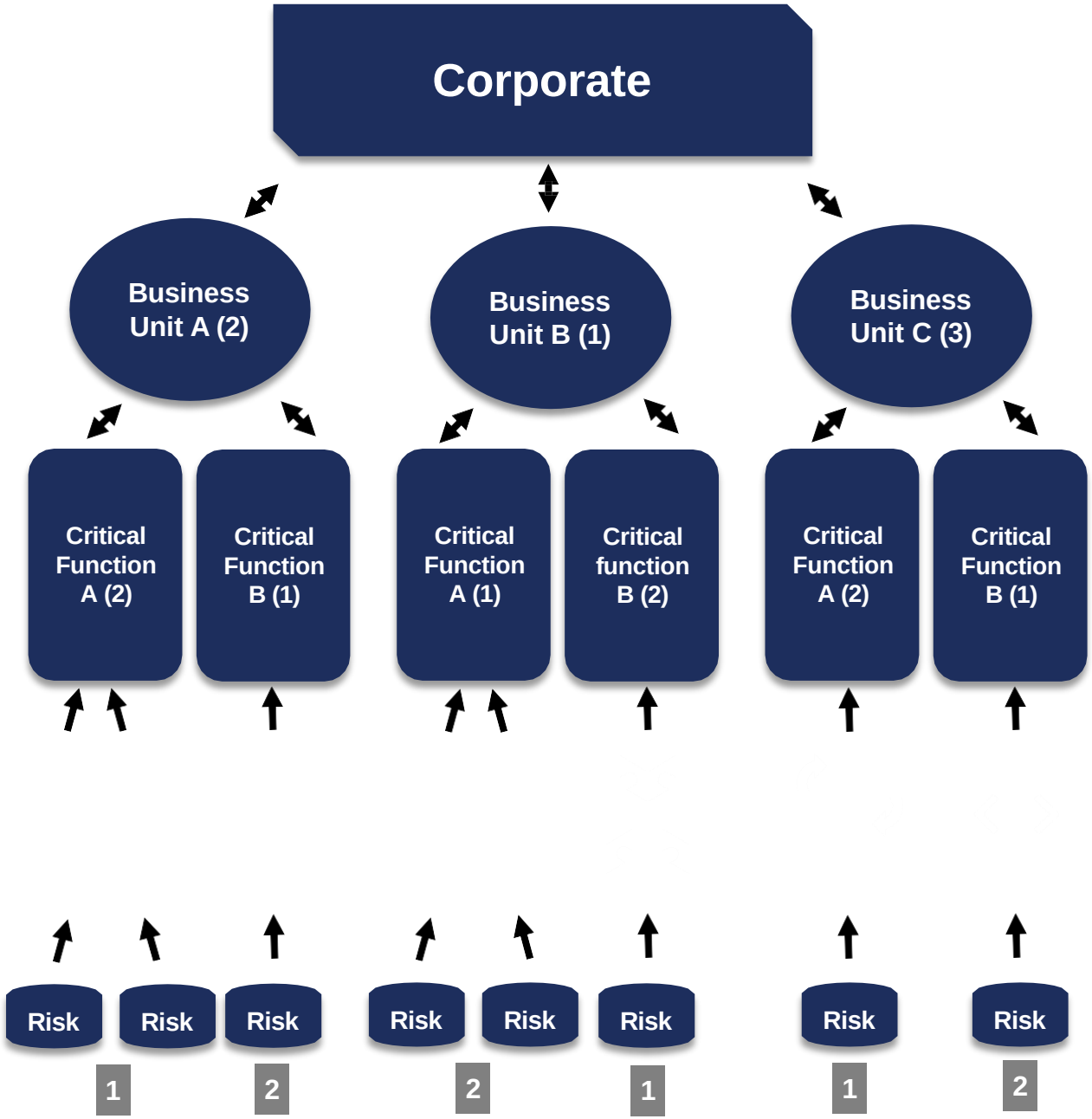
Performing a BIA is a typical approach.

Focus on the enterprise impact of a loss of information assets.

Ensure considerations include direct and downstream impacts.

Determine information asset importance:

1. Break the organizational structure into business units or departments.
2. Identify critical organizational functions.
3. Demonstrate how identified risk can impact business operations.

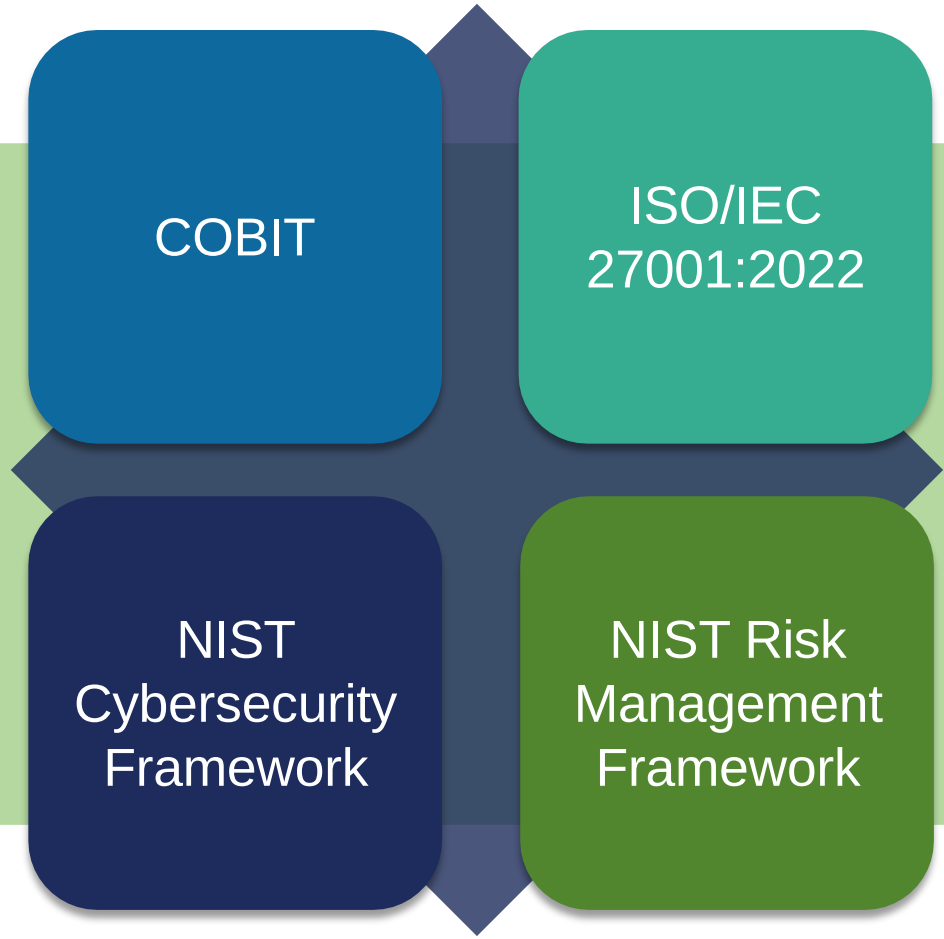


IS Standards and Frameworks

IS Frameworks and the Security Program

Frameworks should serve enterprise business needs, which often means adapting them to the specific requirements of a particular organization.

Incremental adoption may help when tailoring a framework to a particular business context.



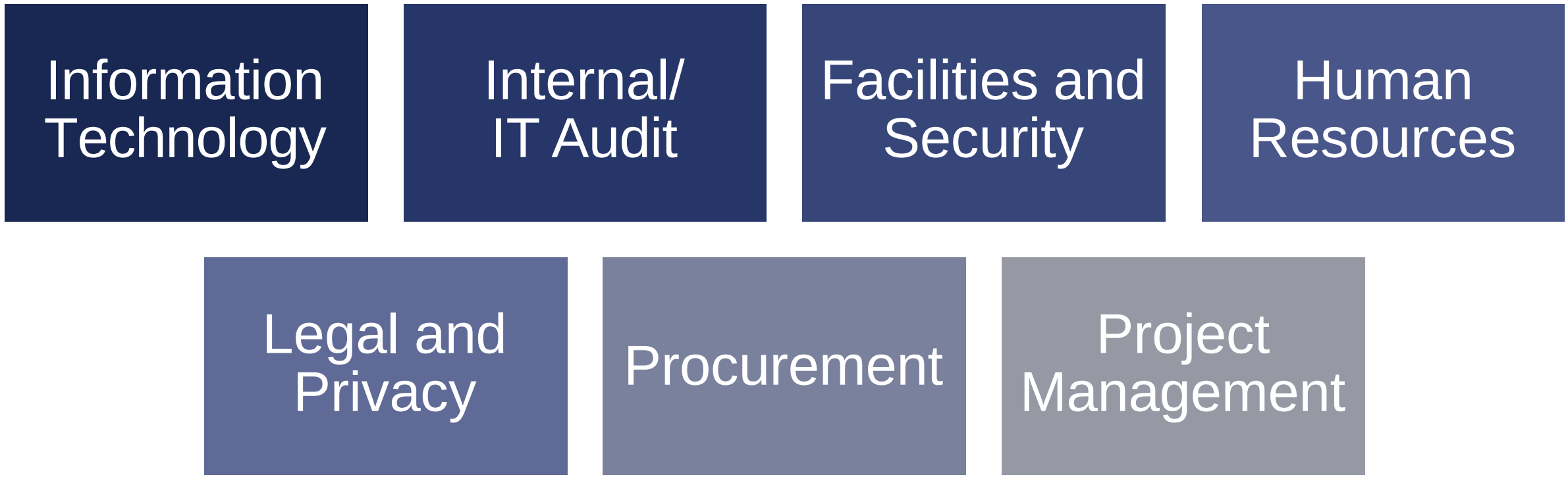
Engaging the Business

A **steering committee** reaffirms the business's commitment to information security.

- **Day-to-day engagement** helps to create a sense of shared responsibility
- **Cultural alignment** is important.

Regular reports to executives can promote awareness.

Key Relationships



Information Technology

Information Security

- Wants to secure things
- Wants to implement controls, which can slow down processes and are costly
- Designs

Information Technology

- Wants to get things done
- Wants to be fast and cost effective
- Maintains and monitors controls and directs controls

Internal/IT Audit

Audits can produce positive outcomes.

- Findings can draw attention from senior management, leading to greater support

If policies and standards are not available, auditors assess a program against industry practices.

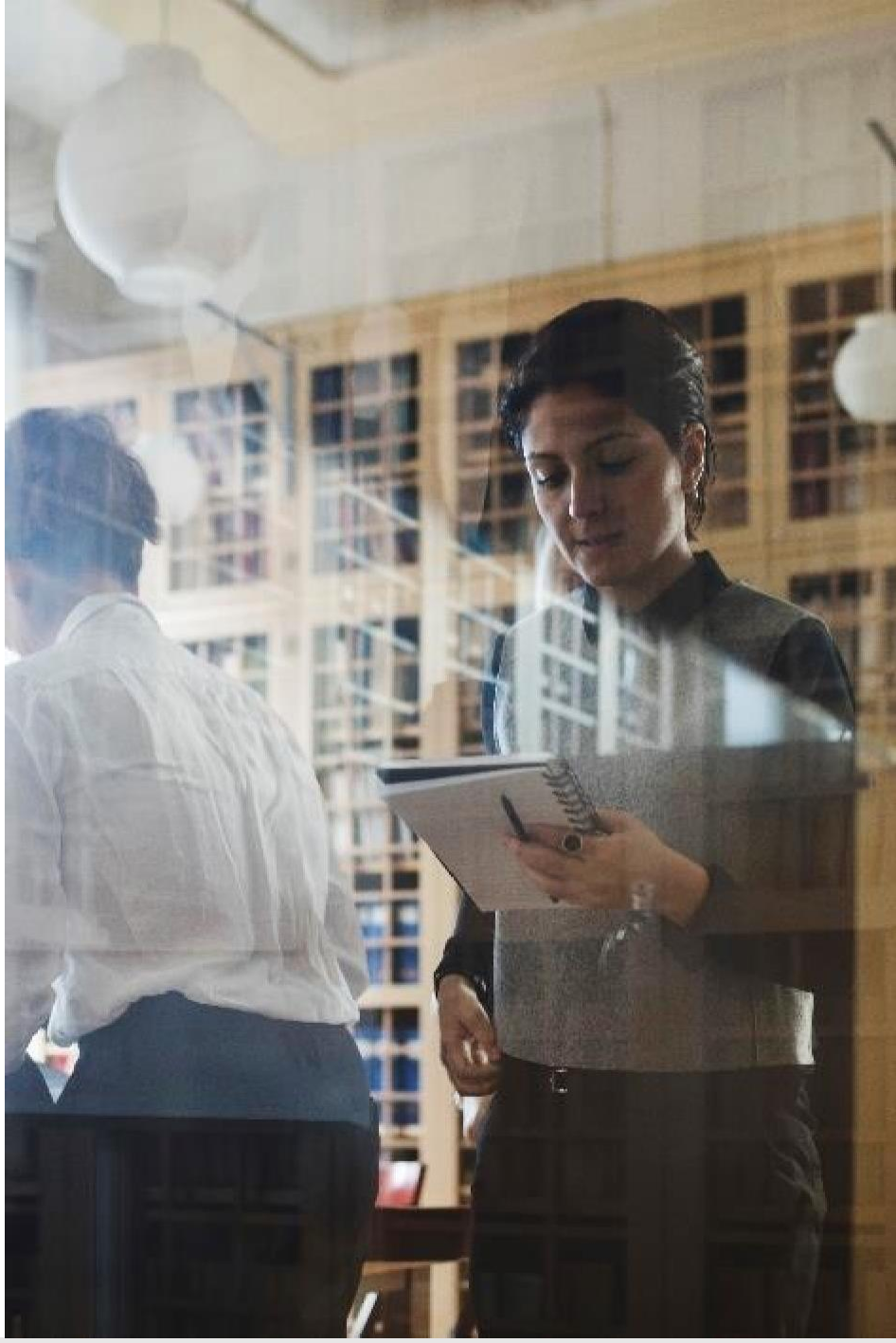
Proper documentation can lead to an audit that provides relevant, useful insight.

Facilities and Security

Physical access has huge implications for information security.

Information also includes that on hard/paper copies.

Collaboration can enhance the effectiveness of the information risk management.



Human Resources

- Background checks
- Pre-employment screening
- Security awareness in orientation
- Disciplinary actions

Skills inventory

Compilation of the skills, education and experiences of the team.

Organizations use these inventories to assess whether current staff can meet company goals.

Understanding the company's pool of current skills/talents and future skill requirements aids in strategic planning efforts.

Legal and Privacy

Laws and regulations regarding privacy vary across jurisdictions.

Legal considerations apply to investigations of computer crimes.

Opinions of legal and privacy professionals will help to design effective controls.

Procurement

If information security is not connected with **purchasing technology, business units** may deploy IT tools that compromise security.

Mature integrated processes include lists of approved devices and software.

At a minimum, technical purchases should be coordinated with information security for risk assessment.

Project Management

Identifying all projects that affect information systems/data is key.

Early involvement can:

- **Improve project design**
- **Make controls more cost-effective**

A distinct PMO can help to facilitate integration.

Policies, Standards, Procedures, and Guidelines

Policies

- Capture intent, expectation and direction
- Support and align with enterprise strategic security objectives

Standards

- Determine whether procedures, processes or systems meet policy requirements
- Multiple standards may exist for each policy

Procedures

- Include all necessary steps to accomplish specific tasks
- Define expected and unexpected outcomes

Guidelines

- Contains information helpful in executing procedures
- Includes clarifications of policies and standards or relevant background information

Policies, procedures, standards and guidelines should reference each other and reflect mutual commitment to the same enterprise goals.

Exceptions to Policies and Standards

Policy Exceptions

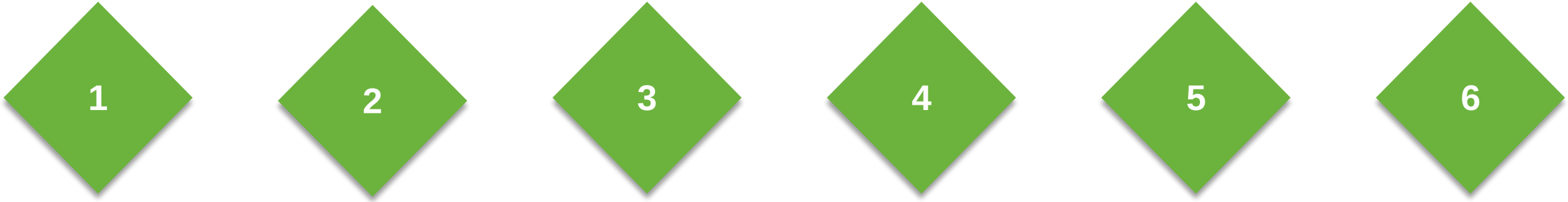
- Created for situations when policy compliance cannot be obtained
- Includes formal documented governance oversight acknowledging risk acceptance
- May be addressed by sub-policies specific to organizational units
- Should be time-bound, not open-ended

Standards Exceptions

- Commonly arise in cases where objectives are not readily attainable for technological or other reasons
- Frequently addressed by application of compensating controls
- Should be approved at a level equal to or higher than the owner of the standard

Defining an IS Program Road Map

Defining an IS Program Road Map



Strategic alignment

Risk management

Value delivery

Resource management

Assurance process integration

Performance measurement

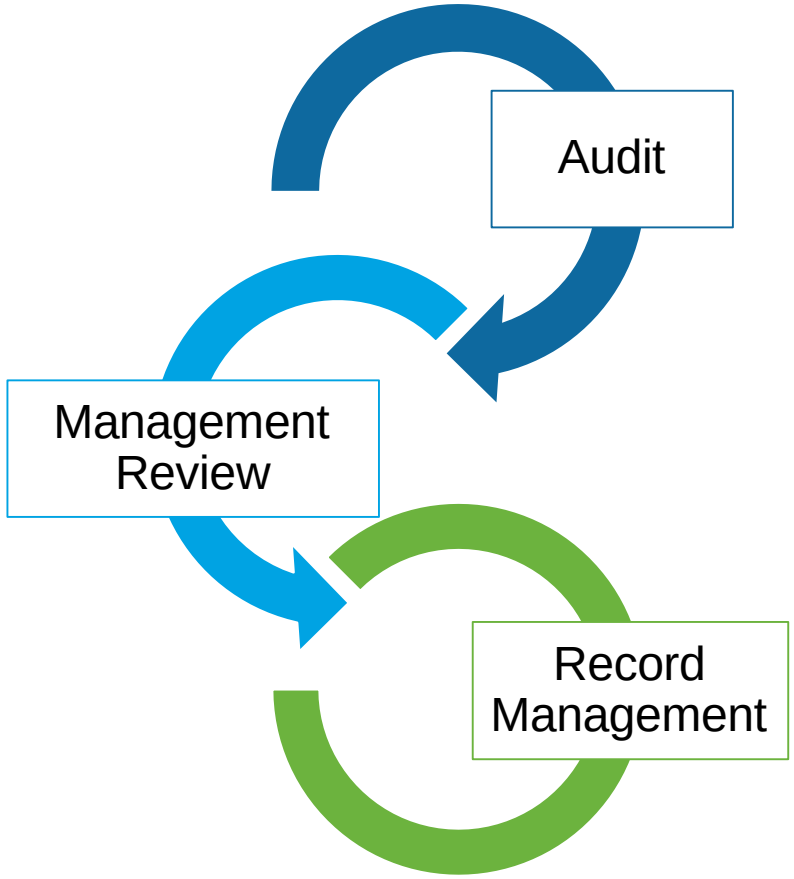
Define key goals during the development of a security strategy**:**

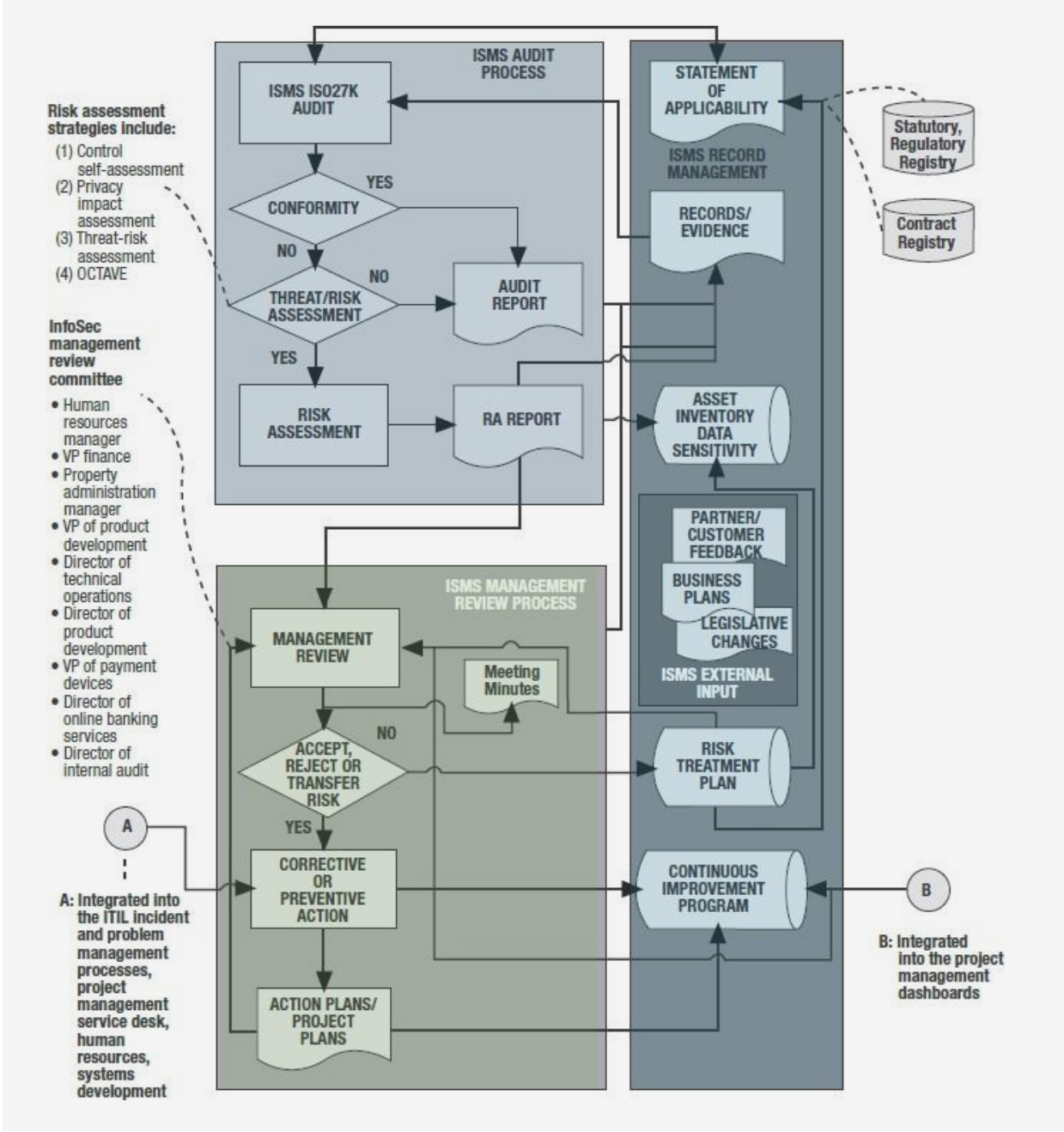
- Consider each key goal in detail
- Clarify as road map evolves
- Develop the program in stages

ISACA

IS Management System Controls Process

Demonstrates a process flow between:





ISACA

Applying Frameworks and Architectures

Architectures and Frameworks

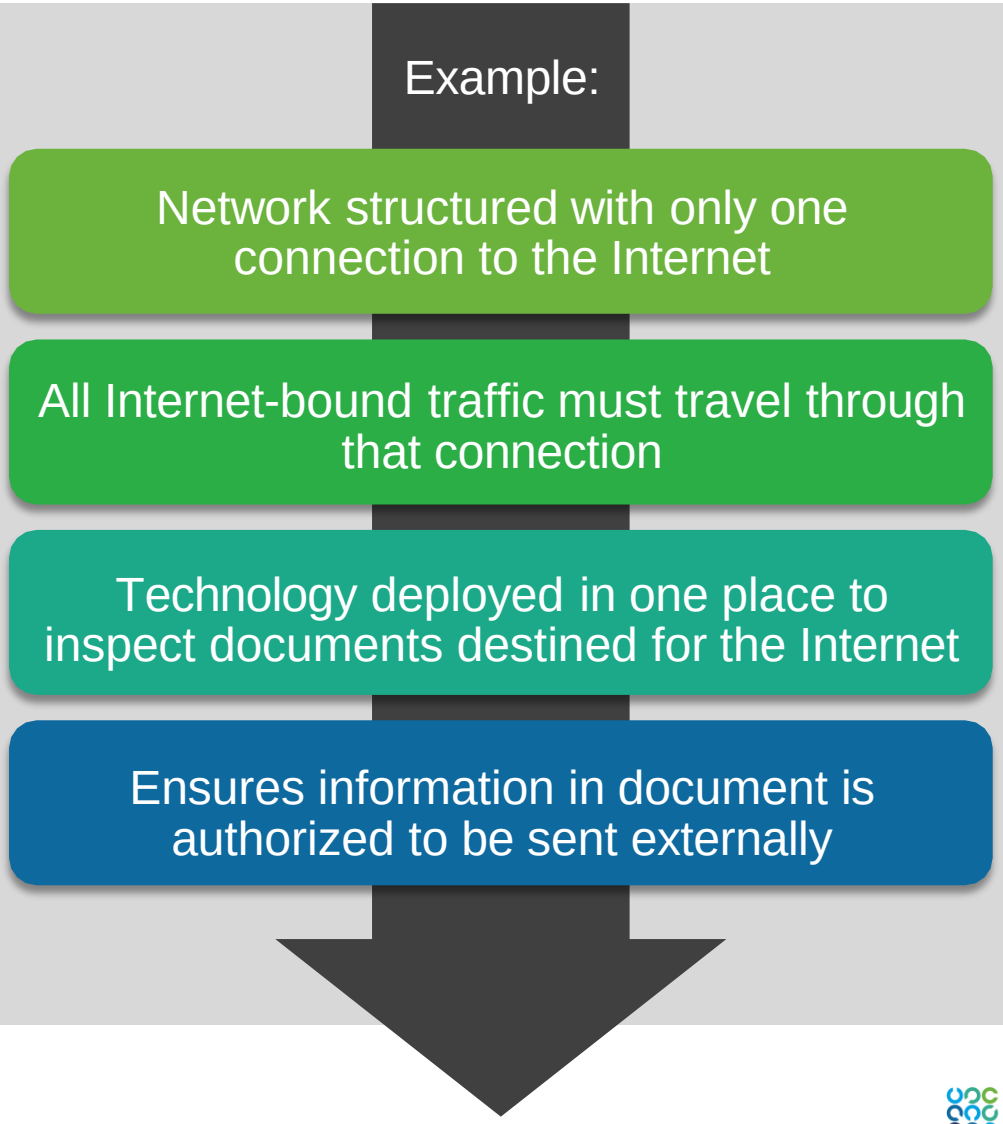
- Act as roadmaps for projects and services to be integrated
- Facilitate teamwork across business functions
- May align with existing standards
- Can be adapted to extract relevant elements best suited to the enterprise

Layering and Modularization

- Architectures address issues for design and construction of technology required for delivery of business services
- Successful architectures consider:
  - Goals
  - Environment
  - Technical capabilities

Architecture and Control Objectives

- A systems architect can combine technologies to provide control points in system infrastructure
- Control points combine with control activities and associated procedures
- Control points ensure that policy compliance is preserved as new systems are deployed within the infrastructure
- Technology may not be specified by architecture, leaving a wide range of choices for control points



Gap Analysis

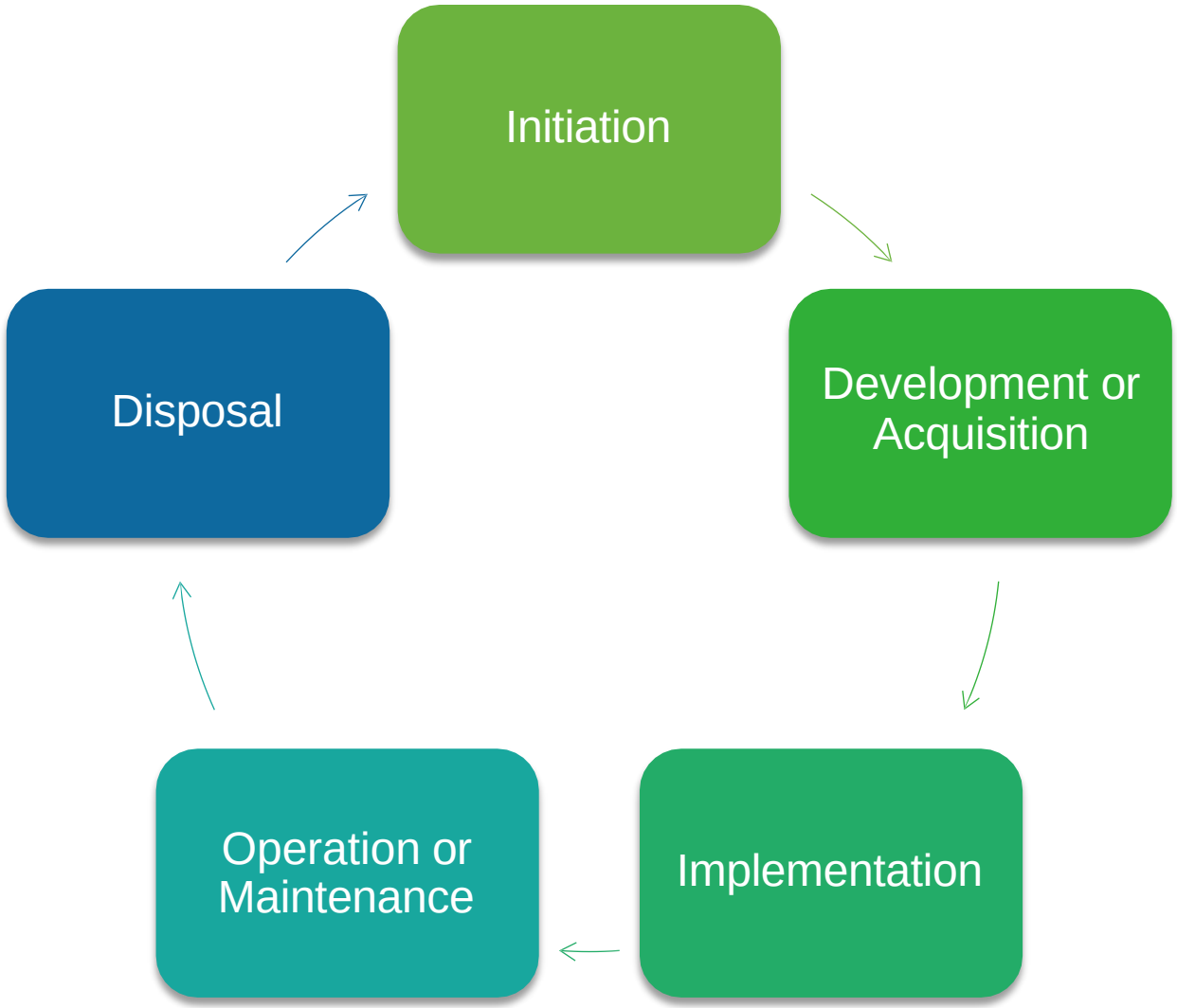
Establishing a procedure to monitor achievement of control objectives provides a basis for the security program to evolve and mature.

- Identify where control objectives are not adequately supported by controls
- Identify control points and assist in monitoring development processes
- Concentrate on KGIs and KPIs when executing new processes
- Validate that control objectives are met
- Confirm that progress toward control objectives achieves program goals

Life Cycle Principles and the Road Map

The IS manager should view the security program as a life cycle. Using this approach:

- Contributes to resource optimization
- Enables incremental updates to program and risk management processes



ISACA

IS Program Metrics

Security Program Metrics and Monitoring

Security metrics should inform about the state or degree of safety relative to a reference point.

1. Are metrics necessary to track and guide program development at multiple levels?
2. Will metric development be needed for ongoing management of program results?

An IS program requires technical and broader metrics to report program effectiveness and resource optimization.

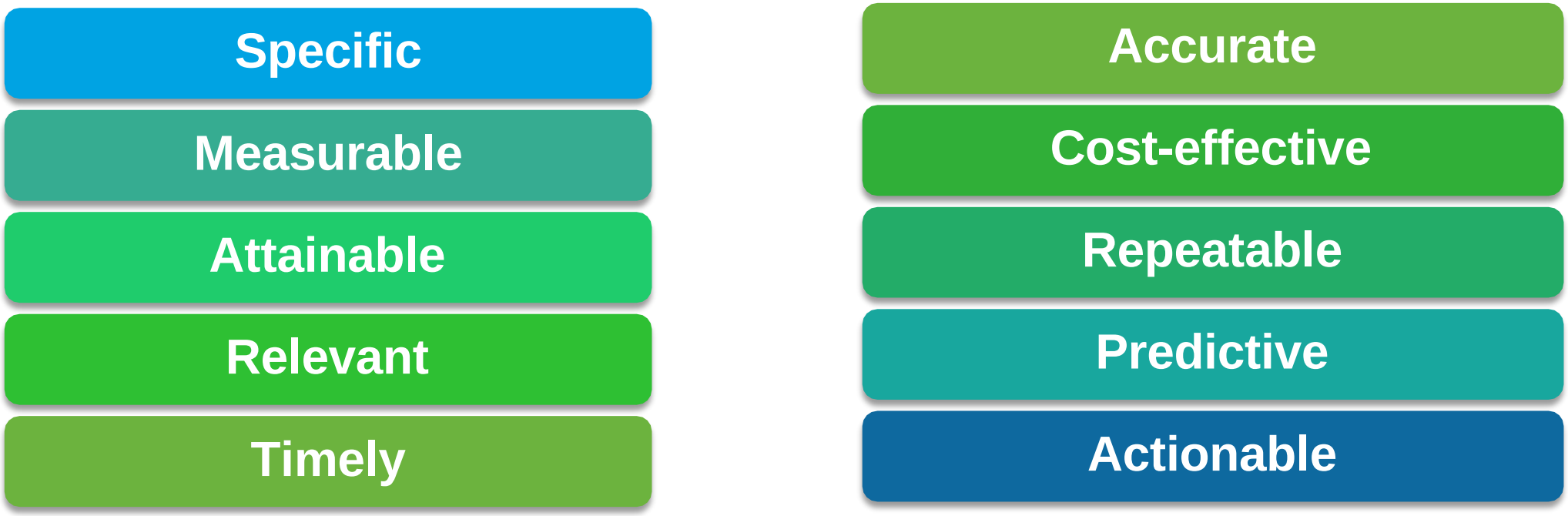
Select controls based on their ability to be monitored and measured effectively.

Key controls that cannot be monitored pose an unacceptable risk and should be avoided.

Developing Relevant Measures

Effective Security Metrics

- Measure achievement toward a process goal using a quantifiable entity
- Provide decision support with information relevant to roles and responsibilities
- Use a set of criteria to determine the most suitable metrics



Standard Security Metrics

- Typically include information relating to aspects of security useful to IT operations
- May not accurately reflect the security status of the enterprise
- May not satisfy criteria for effective security metrics

Examples

- ISO/IEC 27004:2009
- COBIT
- The Center for Internet Security (CIS)
- NIST Special Publication 800-55

A lack of useful security metrics hinder effective management.

Security Management Metric Levels

Determine the ongoing effectiveness of security to meet the defined objectives at various levels.

Strategic

- Compilations indicating the security program is on track and achieving outcomes
- Navigational information to provide oversight to senior management and IS manager

Management

- Metrics needed to manage the security program
- Information used to make decisions required for effective management

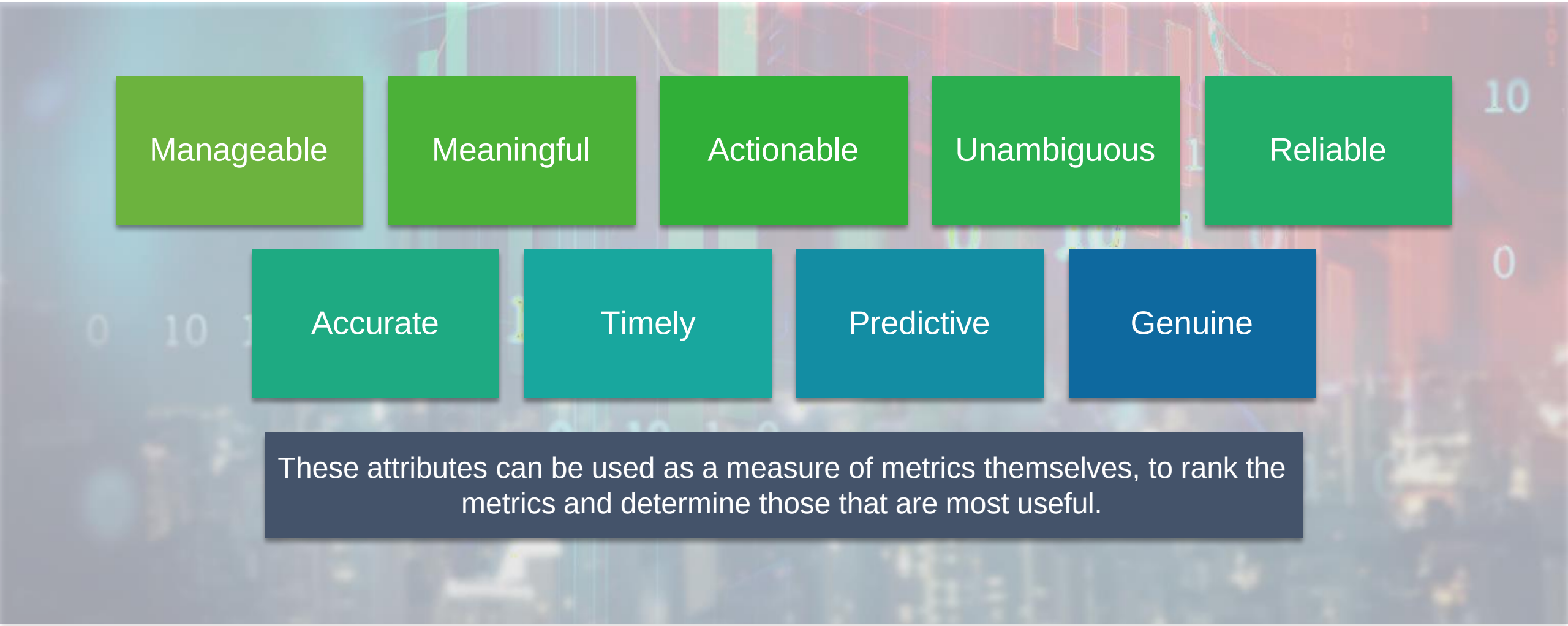
Operational

- Common technical and procedural metrics
- Primarily useful for IT security managers and system administrators

Technical

- Metrics to ensure machinery is operating properly
- Not indicative of direction but can indicate the outcome cannot be reached

Considerations for Developing Metrics



IS Program Management

ISACA

Managing Risk Through Controls

Controls are the means of managing risk.

Controls

- Provide reasonable assurance that business objectives are achieved, and undesirable events are prevented, detected or corrected
- Are any process necessary to achieve objectives
- Achieve specific objectives and enable stakeholder goals through the strategic program plan

Control Objectives

- Support the alignment between security and privacy goals and their achievement
- Are the desired result or purpose to be achieved by implementing the control
- When aligned with organizational objectives, help to ensure alignment with the IS program
- When aligned with IS program, support a cost-effective approach to balance IT value with resource and risk optimization

Control Categories

Controls should be implemented using categories to create a defense-in-depth strategy.

Preventative

- Directly addresses risk
- Inhibits attempts to violate security policy

Detective

- Warns of attempted or actual violations of security policy

Corrective

- Addresses and remediates impact
- Can provide recourse from extensive harm

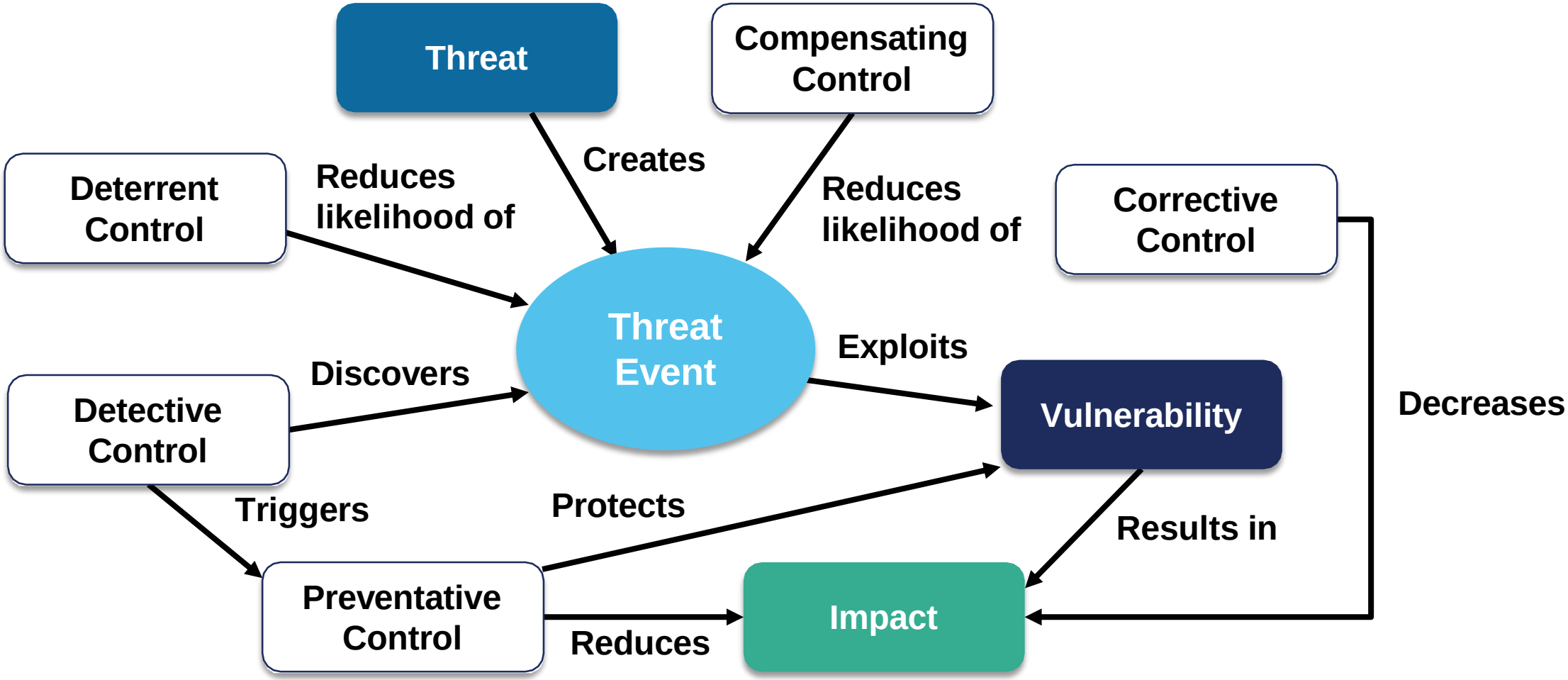
Compensating

- Internal controls that reduce risk of control weaknesses

Deterrent

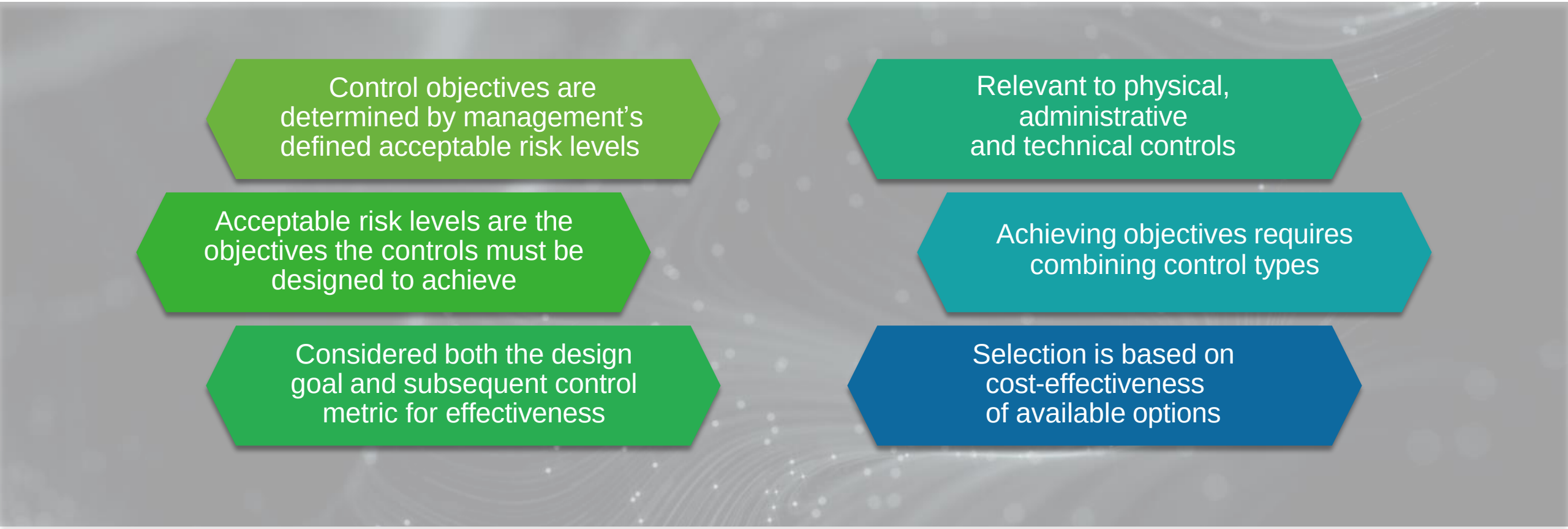
- Addresses threat
- Provides warnings to deter potential compromise

Control Categories and Effect



Defining Control Objectives

Controls are most efficiently approached using a top-down, risk-based approach.



Control Design Considerations

- Productivity impacts
- Cost
- User acceptance
- Cultural and ethical acceptability
- Legal and regulatory requirements and restrictions
- Adaptability to changing risk
- Scalability
- Ability to monitor
- Provide notification
- Robustness
- Resilience
- Reliability
- Testing
- Acceptable failure mode
- Tamper resistance

Implementation Methods

Managerial (administrative)	Technical (logical)	Physical
• Apply to processes and behaviors	• Apply to information systems, software and networks	• Apply to facilities and areas within them

Note: Controls of any effect category can be implemented using any of the three implementation methods.

Physical and Environmental Controls

All efforts to protect information need a strong physical barrier protecting the physical media where information resides.

Physical

- Prevent or mitigate damage to facilities or tangible resources caused by natural or technological events
- Protect equipment from theft
- Features that allow physical mechanisms to override logical controls
- Enable an escalation path to ensure that requirements are met
- Validate technology choices supporting physical security

Environmental

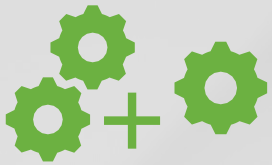
- Measures designed to ensure facilities meet physical limitation of system operation requirements
- Aid to prevent, detect and recover from physical damage to systems
- General and application control activities are ineffective or useless if damage occurs

Control Technology Categories

When determining controls, consider operational authority and the types of control technology available to maintain security.

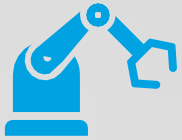
Native

- Often directly impact operations
- Use is governed by IS
- Configured and operated by IT
- Maintains SoD and reduces change and ownership risk



Supplemental

- More appropriate to implement outside the primary system
- More specialized
- Shared responsibility



Support

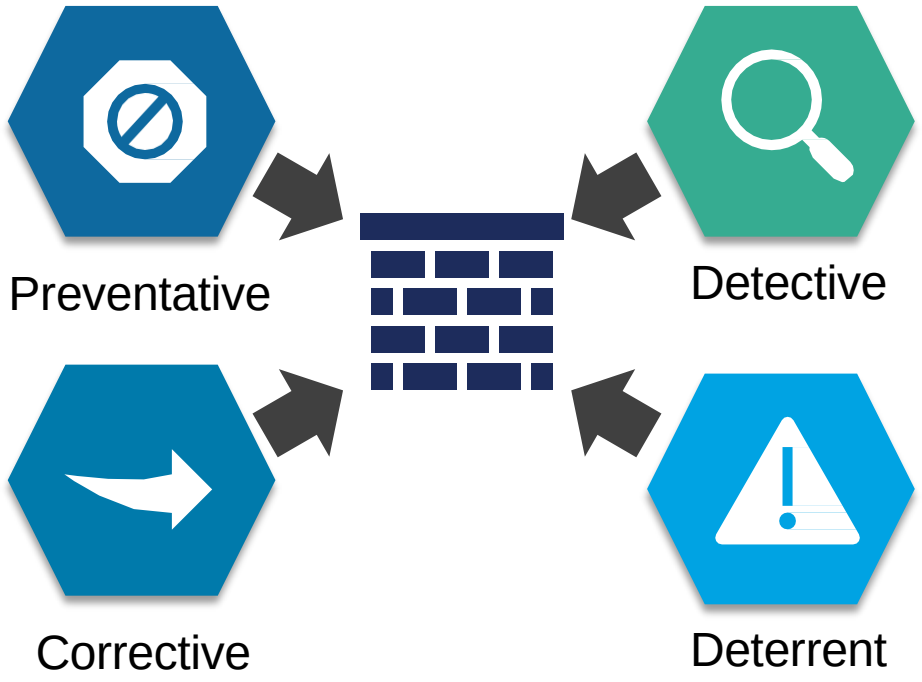
- Used by the security organization
- Enforce SoD to commonly implement and support security operations
- Automated to increase effectiveness of program and capabilities

IS Control Implementation and Integration

Effective information security requires controls that affect all aspects of an enterprise.

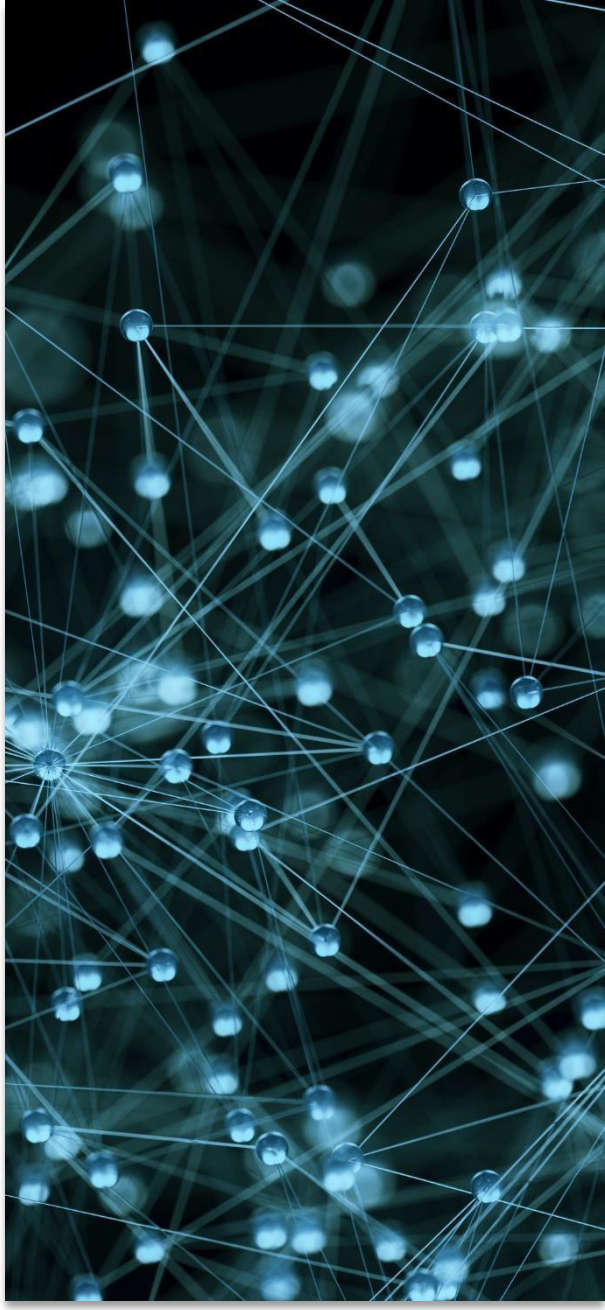
- Provide a core component of strategy implementation
- Combining controls can achieve control objectives
- Control options can be unlimited
- Firewalls are a typical example

Firewall: Filters network traffic to limit protocols



IS Control Testing and Evaluation

- Evaluate the extent to which controls achieve their intended purpose
- Ensure layers of control achieve acceptable level of risk
- Testing and evaluation of control types continue throughout operation
- Includes system-specific controls continually assessed during the life cycle
- Evaluation must continually evolve to ensure continued achievement of control objectives



ISACA

Control Testing and Modification

Changes to the technical or operational environment can modify the protective effect of controls or create new weaknesses that existing controls are not designed to mitigate.

Control Changes

- Use change control procedures and gain stakeholder approval
- Analyze proposed control environment
- Determine if new or recurring vulnerabilities exist
- Ensure proper control design
- Conduct acceptance testing to ensure enforcement

Procedure Changes

- Use review and approval through the change management process
- Consider changes made and coordinate modifications to related processes and technology
- Consider workload and impact on operational quality
- Coordinate training required to implement
- Perform walkthrough to ensure proper implementation

Manual vs. Automated Controls

Automated controls are generally preferred to manual controls.

- Analysis is needed to confirm if this is the case.

High volume of data may require automation.

SIEM software can help to create useful reports out of automation.

Fail States

Controls should be designed in ways that result in clearly established states of failure:

- Fail safe: Allow all activity when they fail
- Fail secure: Prevent all activity when they fail

Biometric systems often experience the following:

- False acceptance rate (FAR)
- False rejection rate (FRR)

IS Awareness and Training

Information Security Awareness Overview

Many security incidents are caused by human error.

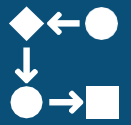
A comprehensive information security awareness and training protocol is an effective control to manage human error by:

- Building program awareness and its importance to the enterprise
- Connecting policies and standards to daily tasks
- Tailoring relevant security program information to each audience
- Educating staff involved in strategy implementation

Understand:

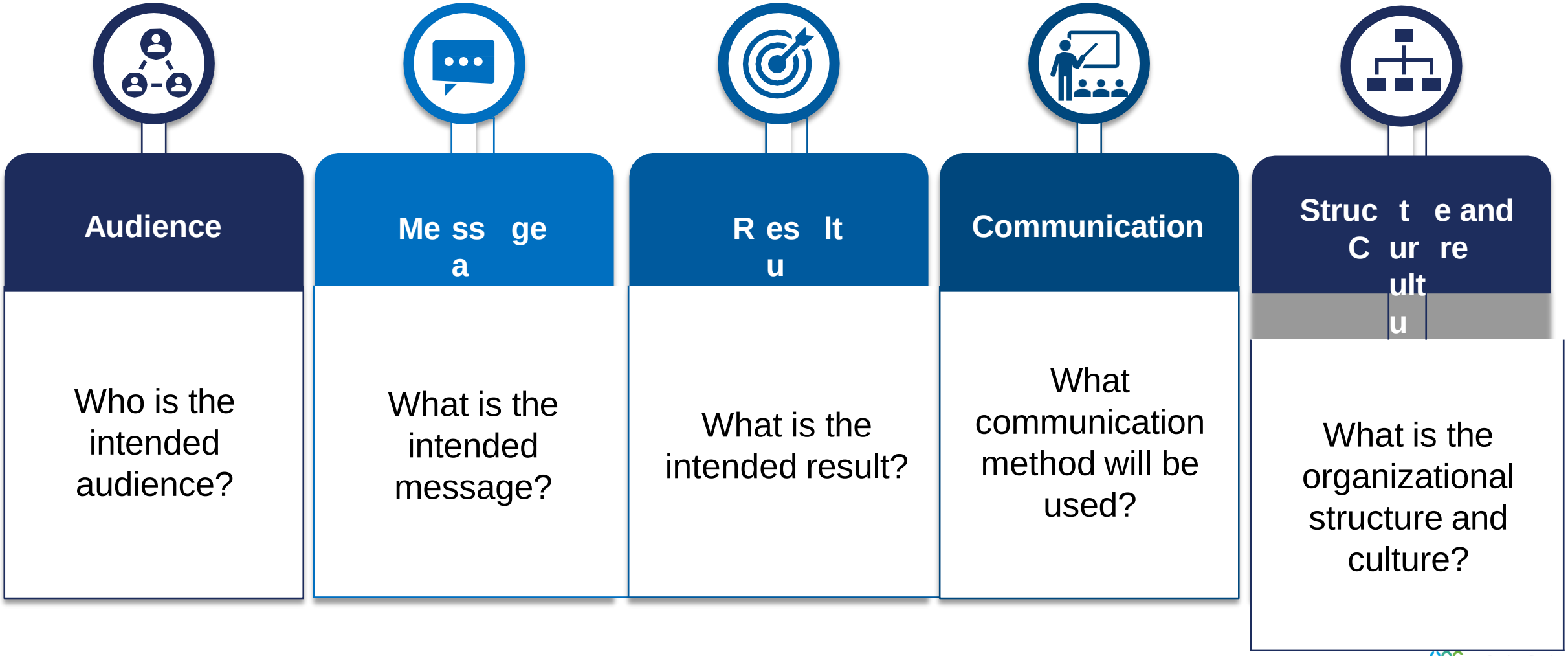
Strategy objectives (KGIs)

Activity process and performance metrics (KPIs)



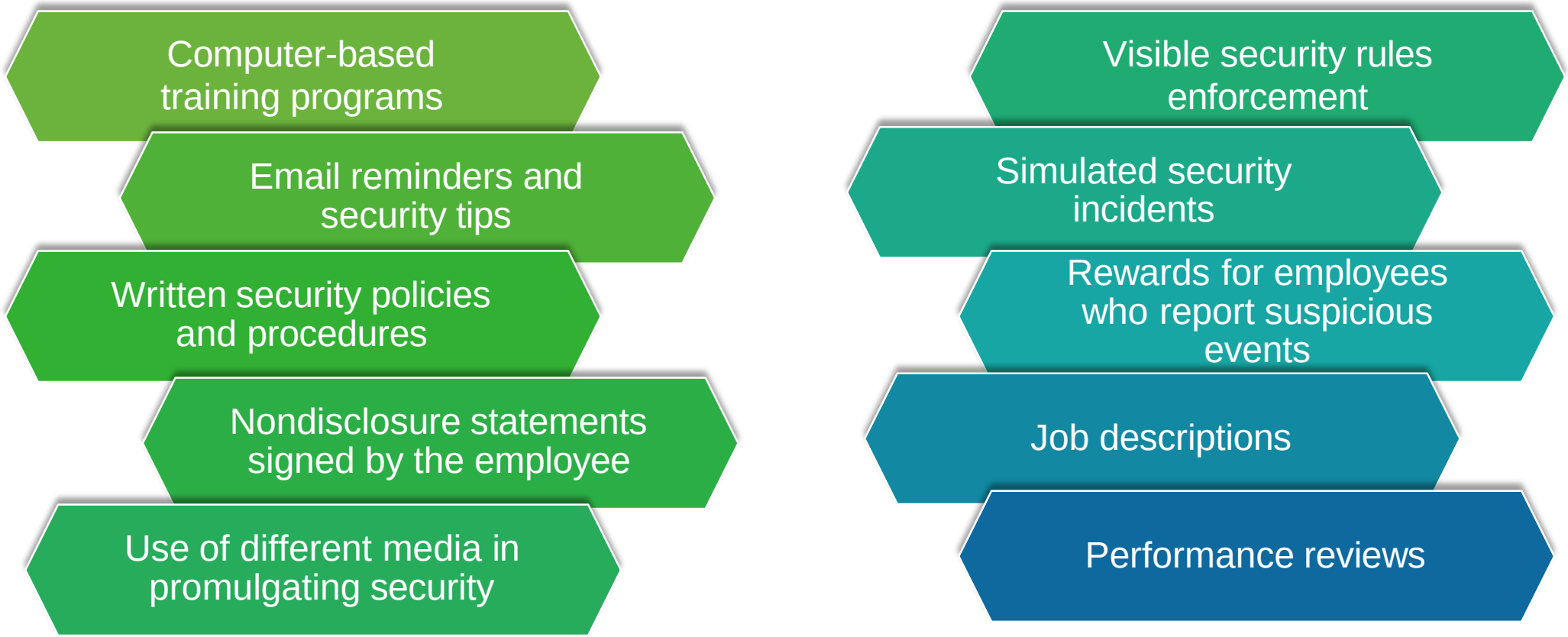
Elements or events that must occur (CSFs)

Developing an IS Awareness Program



Mechanism to Raise Awareness

Various methods exist to inform and reinforce security training to fulfill expectations and minimize the likelihood of a security incident:



Training and Education Metrics

Use a systematic approach to measure and track training delivery and results.

Coverage

Grading

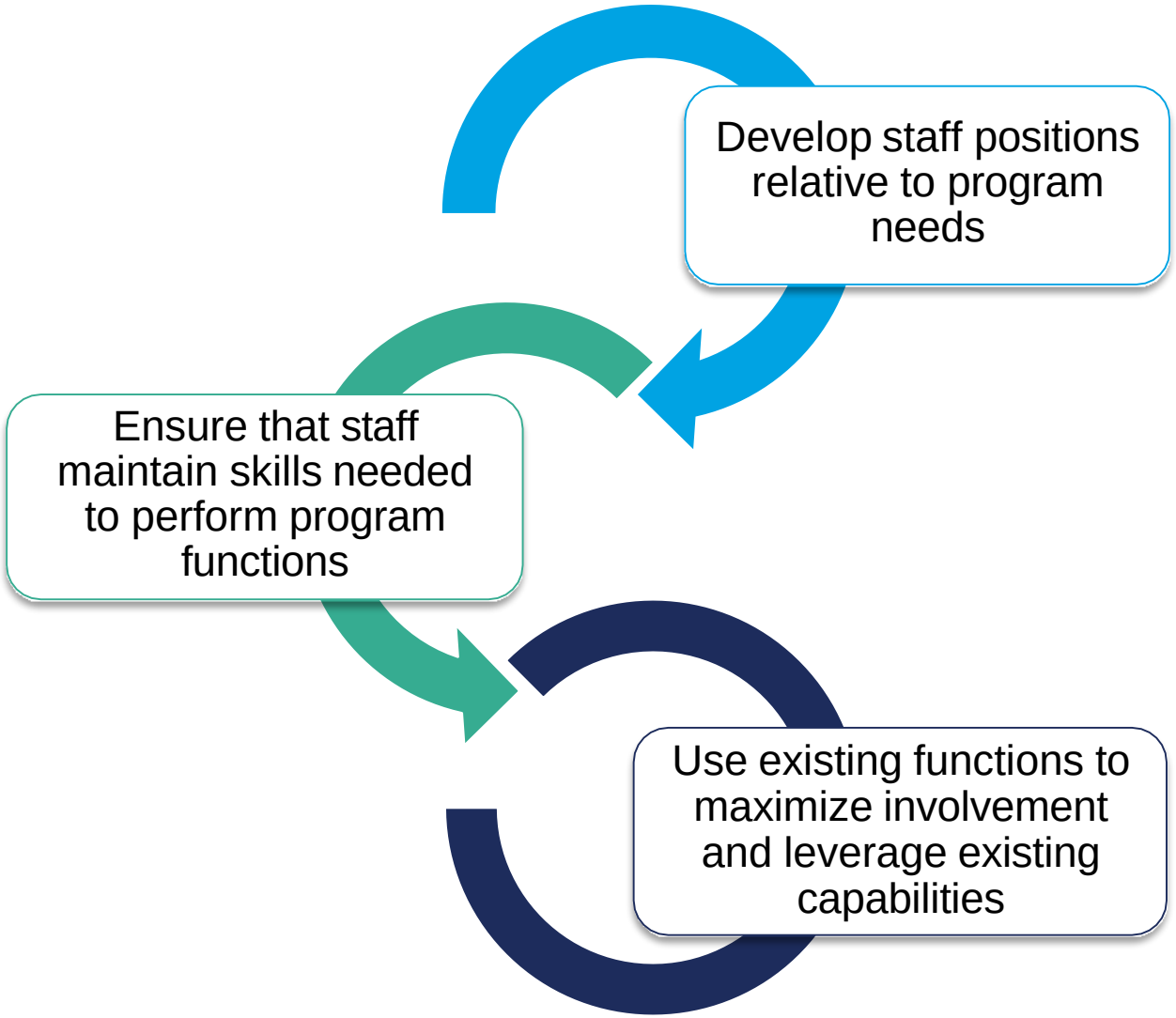
Automation and Deployment

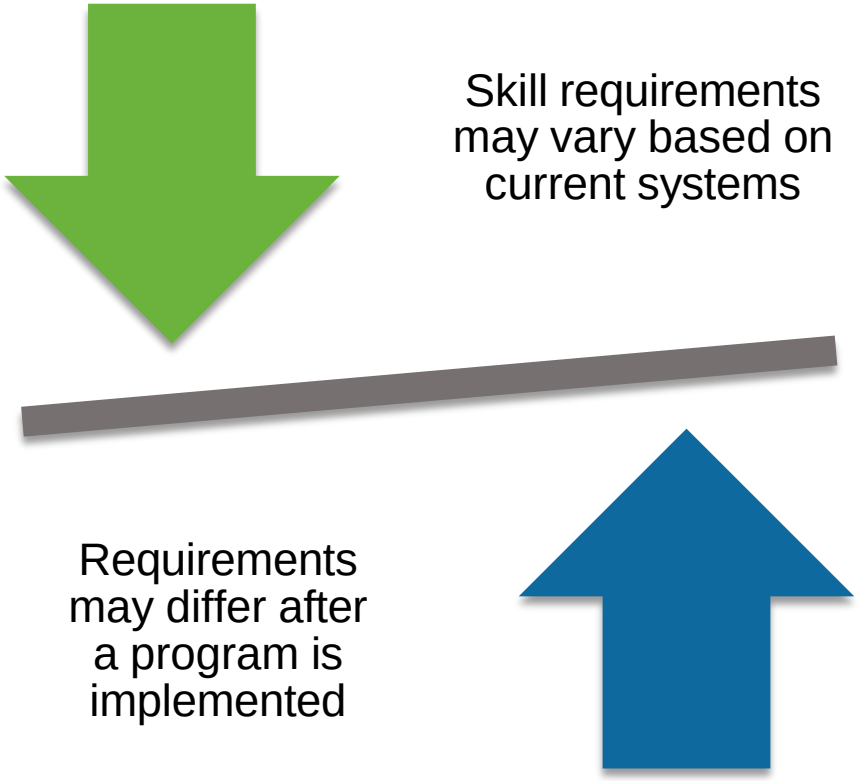
ISACA

Integrating the Security Program with the Operations

ISACA

Personnel and Culture





ISACA

Role Assignment

- Allows assignment of responsibilities or access rights based on functions performed
- Assigning roles during onboarding can streamline the process
- Reduces administrative cost because roles change less often
- Clearly designated roles ensure effective implementation and management
- RACI charts can define roles associated with aspects of developing the IS program
- Confidential information may require a background check performed by HR

Skills

Training, expertise and experience of personnel

- Ensure proficiencies of available personnel map to competencies required to implement the program
- Acquire specific skills needed for program implementation through training or using external resources

Balance the cost of hiring vs training for specialized skills:

- Consider skilled external resources who are more cost-effective in the short term
- Acquire rarely needed skills through service providers (integrators or consulting firms)
- Establish formal employment agreements for personnel with specific information security responsibilities

Security-Related Documentation

Create and maintain documentation required to manage the information security program:

- Ensure governance system components address documentation processes
- Provided as a part of enterprise document management
- Protect documentation using controls and practices at the same level as other sensitive information assets
- Remain consistent with organizational requirements, classification and labeling standards
- Update standards and procedures to address changes while remaining consistent with policies

Examples:

Program objectives

Road maps

Business cases

Required resources

Controls

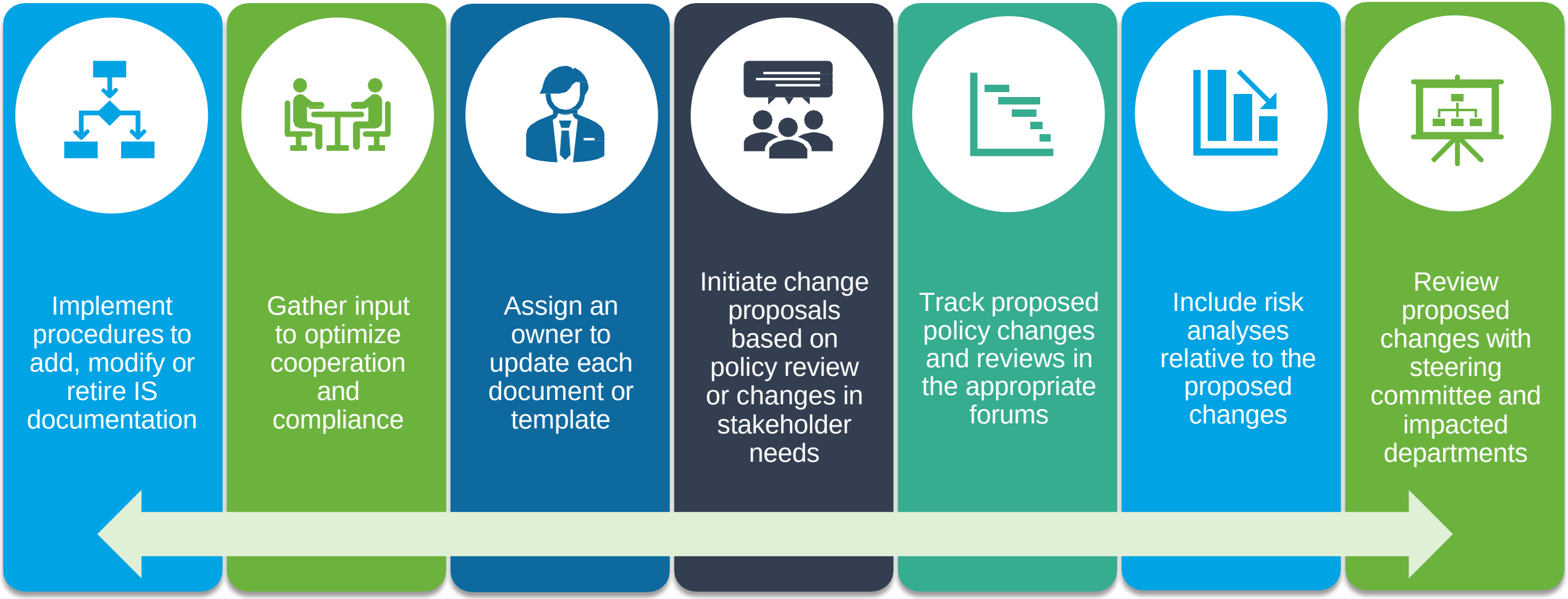
Budgets

Systems designs/architectures

Policies, standards, procedures, guidelines

Metrics

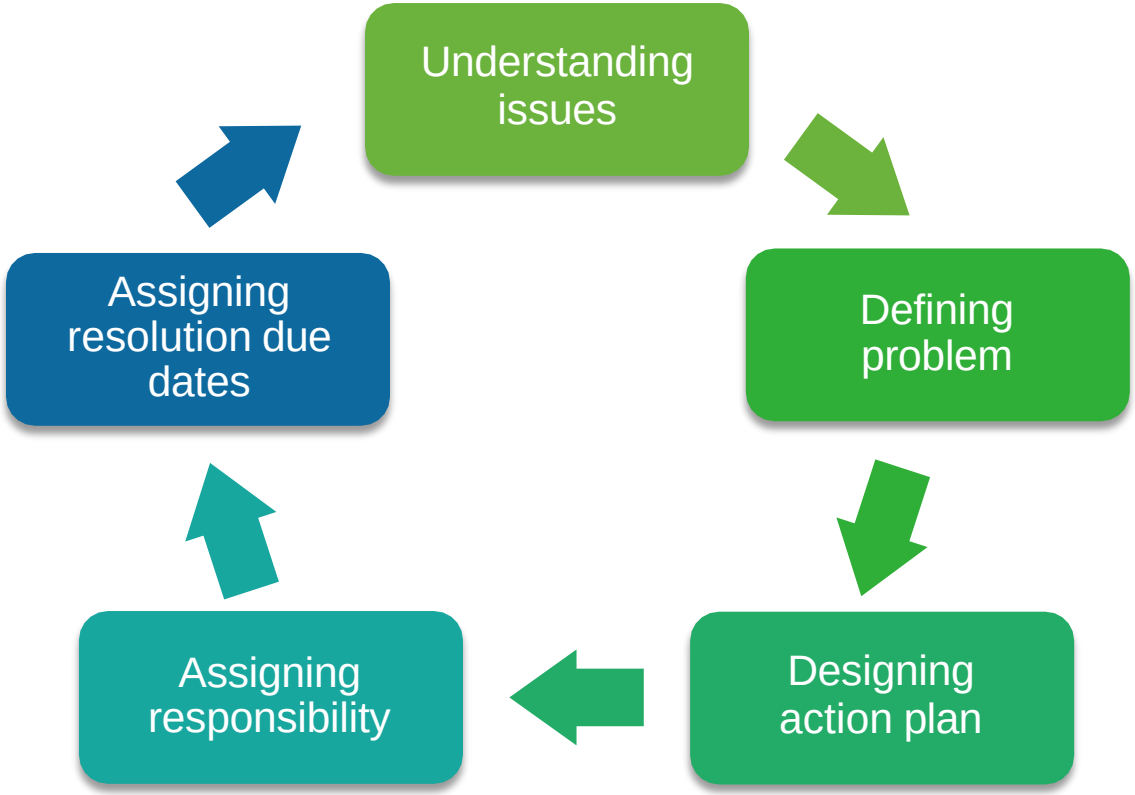
Documenting Changes



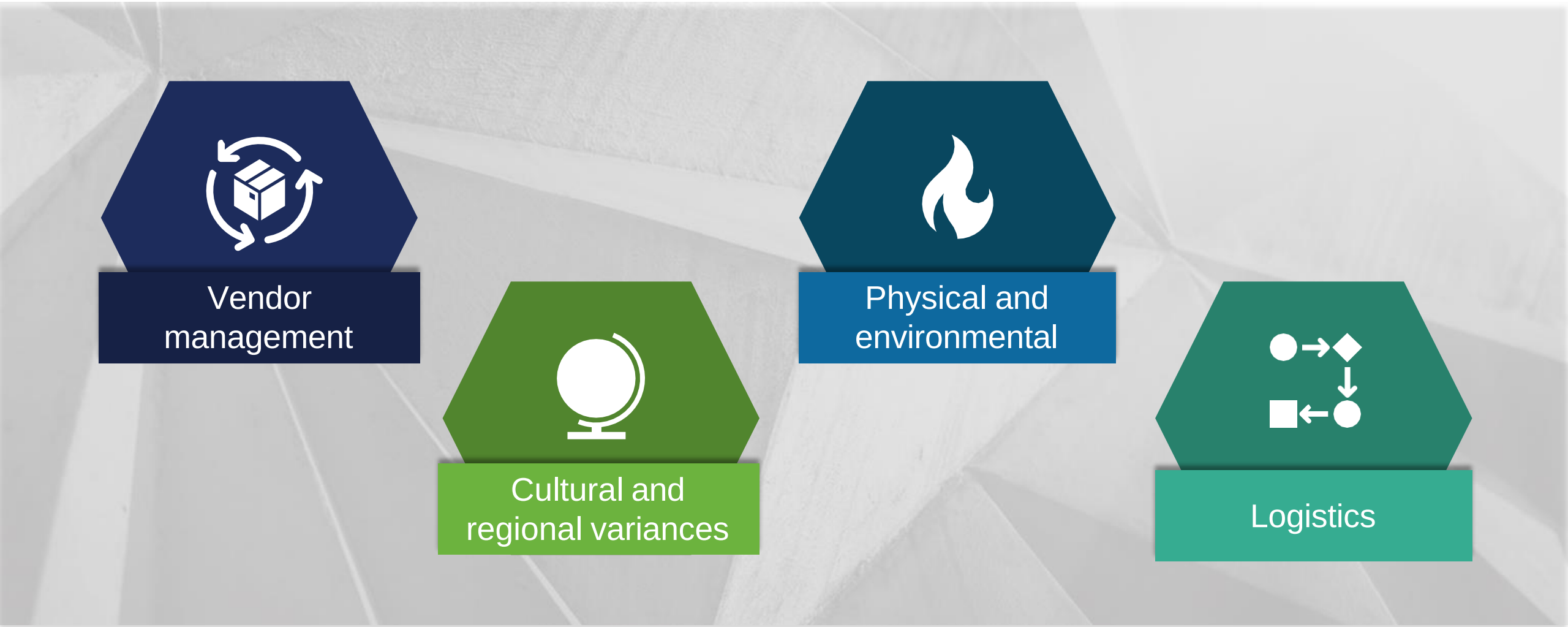
Issue Resolution through the IS Program

Security controls may develop a problem as information systems change and adapt:

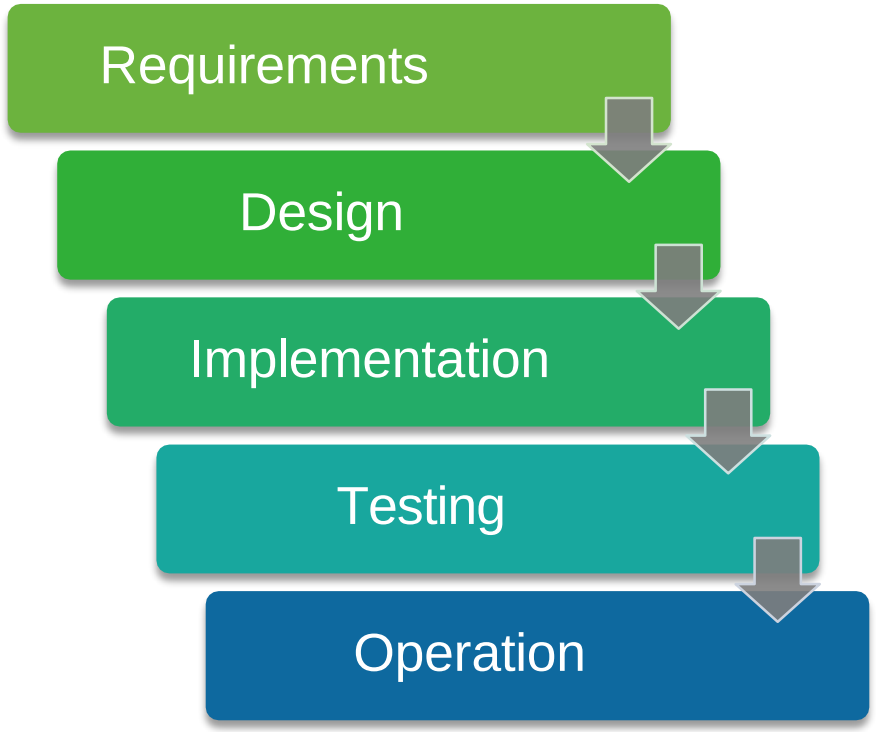
- Use problem management techniques to ascertain the root cause of issues
- Implement a reporting process to track results and ensure problems are solved
- Employ mitigating controls if the primary security control fails
- Take alternative actions to protect information resources until resolution



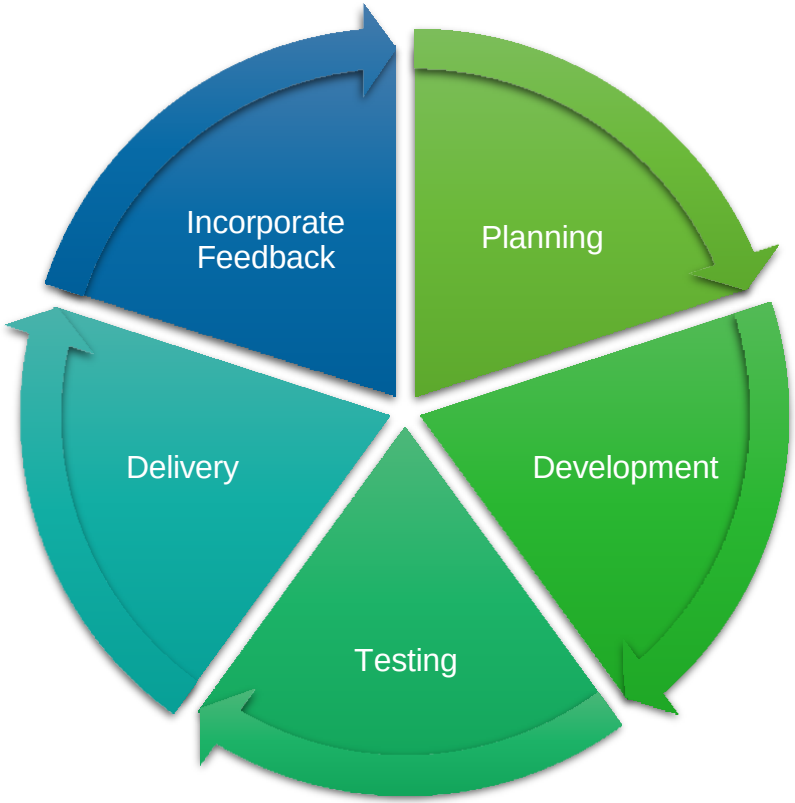
Types of Security Issues



Models to Apply the SDLC



Waterfall



Agile

ISACA

DevOps and DevSecOps

DevOps

- Integrated development and operations
- Combines concepts of agile development, infrastructure and flexible operations
- Enables rapid, continuous releases and ongoing improvement in IT value creation
- Breaks large projects into smaller deliverables
- Improves efficiency for a continuous integration/continuous development (CI/CD) pipeline
- Enables enterprises to deploy software daily

DevSecOps

- Integrated development and security operations
- Applies the same principles to cybersecurity as DevOps to IT processes
- Improves efficiency and removes manual intervention
- Shifts security by incorporating security assurance at every stage of the CI/CD pipeline
- Ensure effective integration of processes
- Review policies, procedures and SLAs for adaptability

Cloud Computing

Cloud computing represents a significant portion of enterprise IT.

NIST defines cloud computing as:

A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

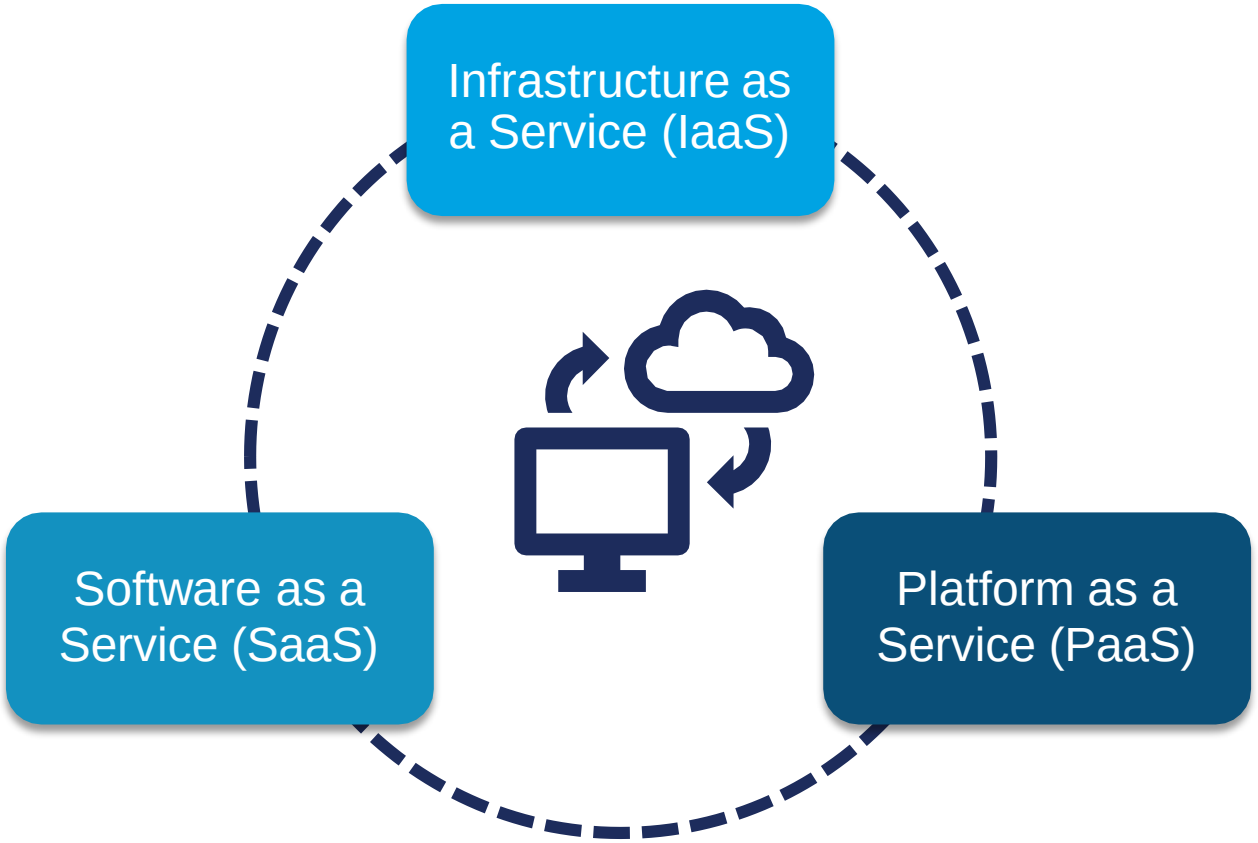
Processing and data are somewhere in the cloud as opposed to being in a specific known location.

Public hosting for multiple unrelated entities.

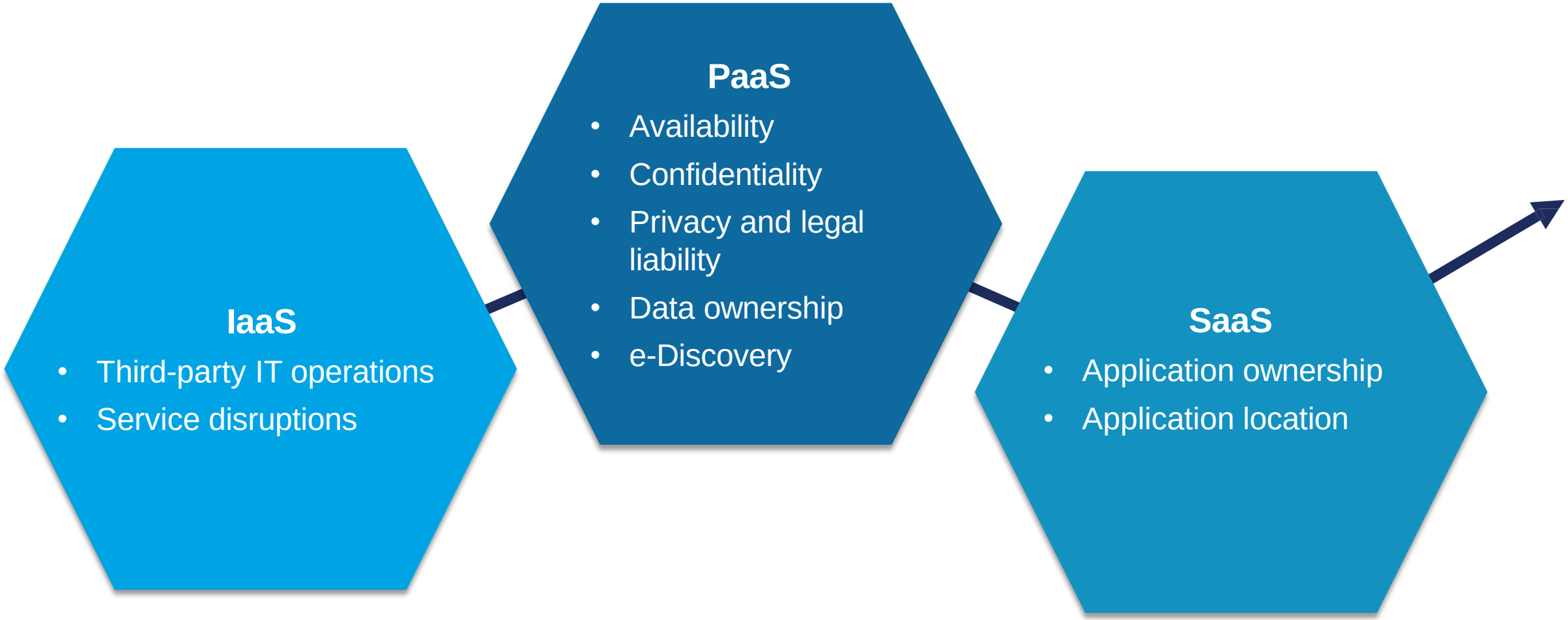
Private hosting for enterprises that want greater control over the environment.

Essential Characteristics of the Cloud

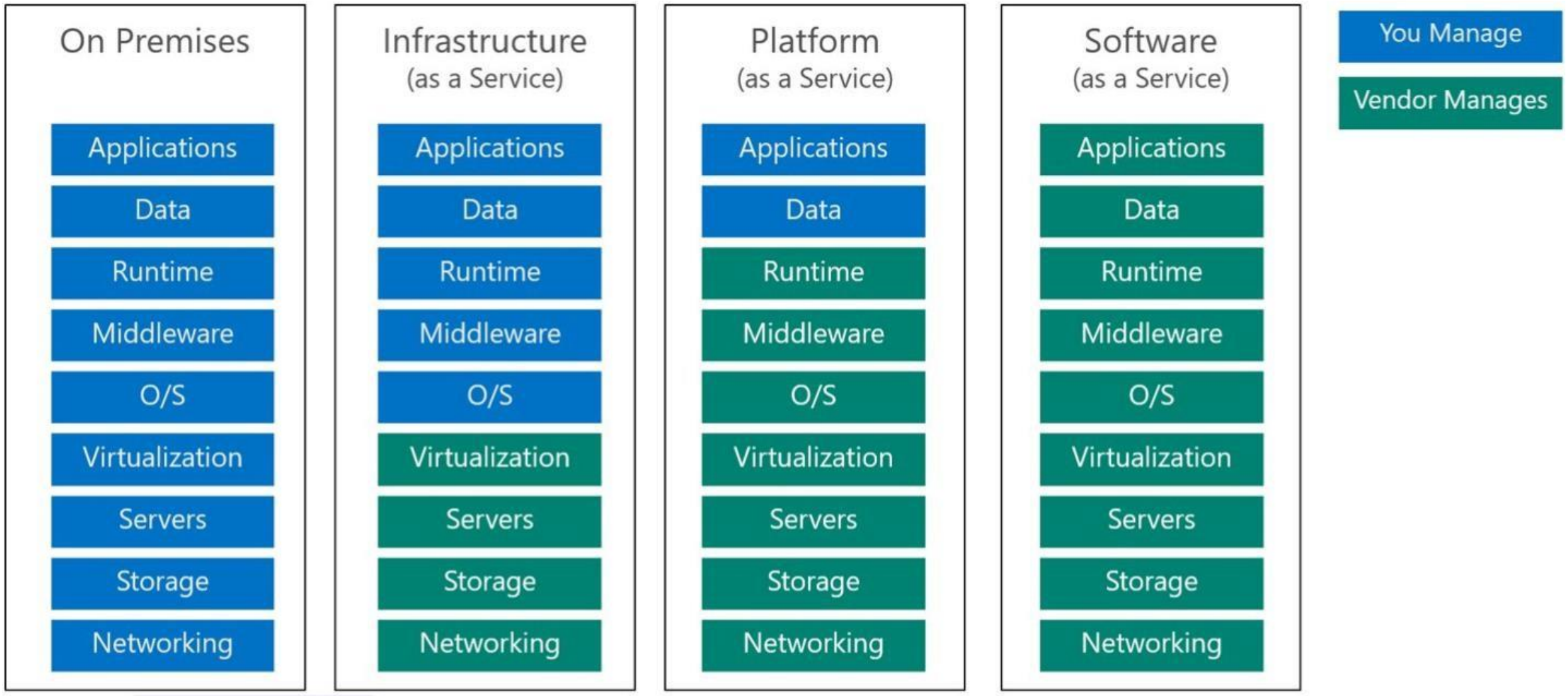
- On-demand self-service
- Broad network access
- Resource pooling
- Elasticity
- Measured service



Cloud Service Model Considerations



Cloud Service Model Responsibilities



Cloud Computing Drivers

Cloud computing is a significant change to the platform where business services are translated, used and managed.

Optimized resource utilization

Cost savings

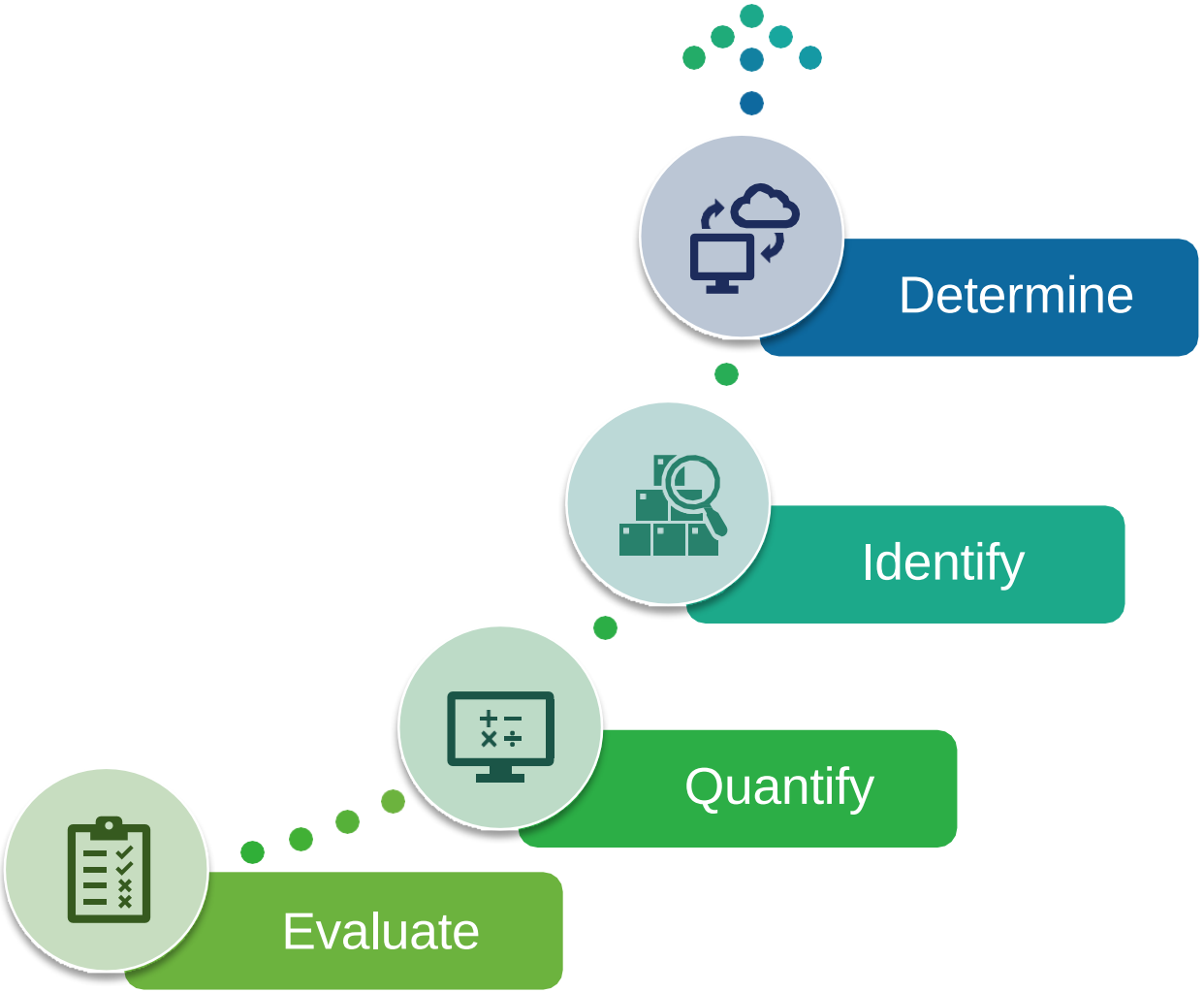
Better responsiveness

Faster innovation cycle

Reduced implementation time

Resilience

Evaluating Cloud Service Providers (CSPs)



Consider:

- Abstraction created between physical infrastructure and the data owner
- Services provided are controlled by multiple enterprises
- Provider failures could result in loss of critical operations

Governance of Third-Party Relationships

Managing Security

- Address the potential risk and possible impacts of relationships
- Assess impacts of possible security failures to ensure protection
- Recognize and manage potential failures to limit their potential impact
- Establish a formalized engagement model between IS and groups engaging third parties

Controls and Implementation Disconnection

Define and implement

1. Controls among different outsourced functions in the enterprise

2 Measures protecting information residing on third-party platforms

Outsourcing Challenges

Outsourced information service providers may be reluctant to share technical details on the nature and extent of their information protection mechanisms.

Security

- Specify levels of protection in SLA and contracts
- Perform specific audits or certification
- Analyze third-party auditor comments
- Review periodic compliance assessments

Risk Management

- Include response and recovery activities and testing
- Implement an incident response plan with the outsourcing entities
- Support regulatory notification with set time frames

Third-Party Access

Review frequency factors:

- **Criticality of information to which access rights are given**
- **Criticality of privileges given**
- **Period of contract**

ISACA

Outsourcing Contracts

Purpose and Use

- Address complex security questions depending on enterprise processes and needs
- Ensure awareness of each party's responsibilities and address disagreements
- Be familiar with provisions and address issues with the legal department

Provisions

- Confidentiality and nondisclosure
- Maintain appropriate security controls
- Responsibility for connection security
- Expected network connectivity security

Economics of Outsourcing

Early engagement of the IS manager can ensure decision makers do not compromise security for cost.

- Understand the TCO of outsourcing for the duration of the contract
- Negotiating service levels can be lengthy causing adverse effects to changing needs
- Consider costs of repatriating outsourced services after the contract ends

Right to Audit and Inspect

Contracts with providers determined beyond a predetermined risk threshold should always contain right-to-audit and right-to-inspect provisions.

Right-to-Audit:

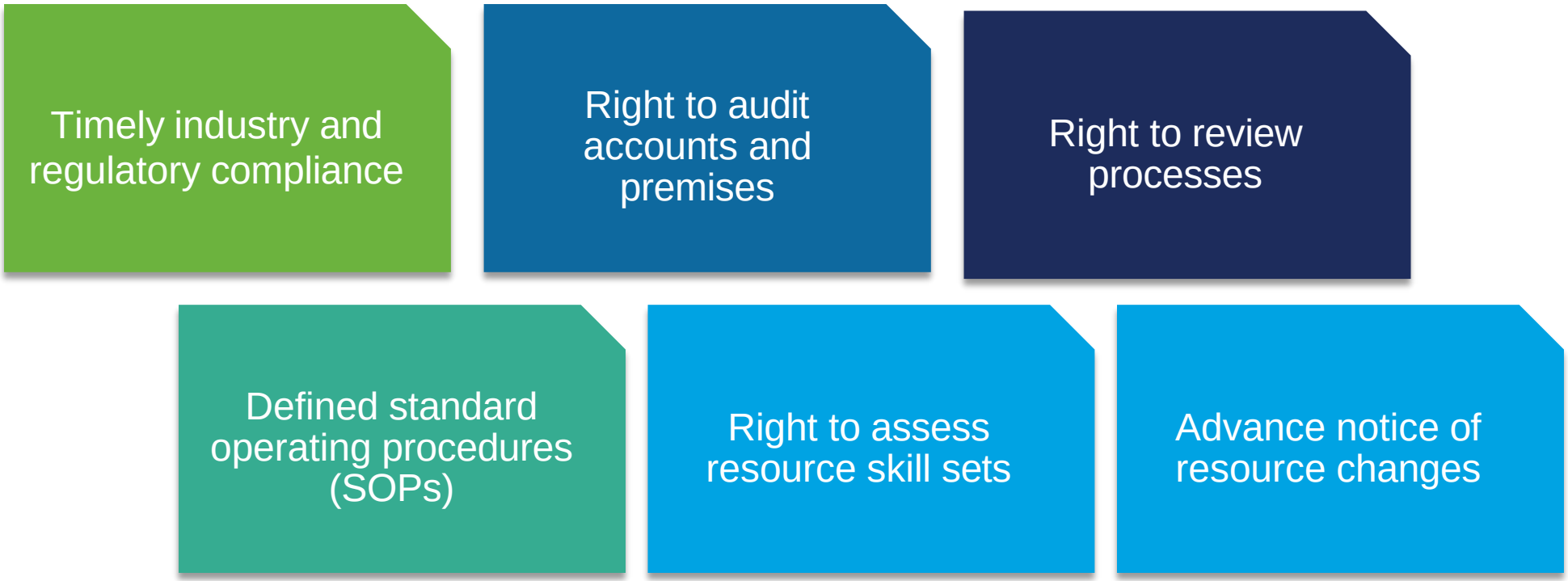
- Requires notice
- Allows in-depth audit of the third-party program and processes
- Verify control effectiveness
- Include explicit parameters of audit

Right-to-Inspect:

- Without notice
- Provides incentive to adhere to contractual obligations
- Few constraints

Service Level Agreements (SLAs)

Some portion of risk associated with outsourced information services can be transferred by incorporating indemnity clauses in SLAs.



Program Communications, Reporting and Performance Management

ISACA

Program Management Evaluation

Effective communications and reporting are among the most important outcomes of the IS program.

Senior Leaders

Responsible for remaining aware of risk factors.
Failure to do so can cause legal issues.

IS Manager

Uses assessment, monitoring and reporting techniques to:

- Fulfill commitments made in the business case
- Demonstrate successful implementation of the security strategy
- Ensure relevant stakeholders are informed of monitoring results

Security Reviews

During program development and management, it is essential the IS manager:

- Applies a consistent approach to assessing and evaluating the state of program aspects
- Track trend information to serve as improvement metrics
- Gather policy, process and control weakness information across the enterprise
- Use data to prioritize efforts

Security reviews contain:

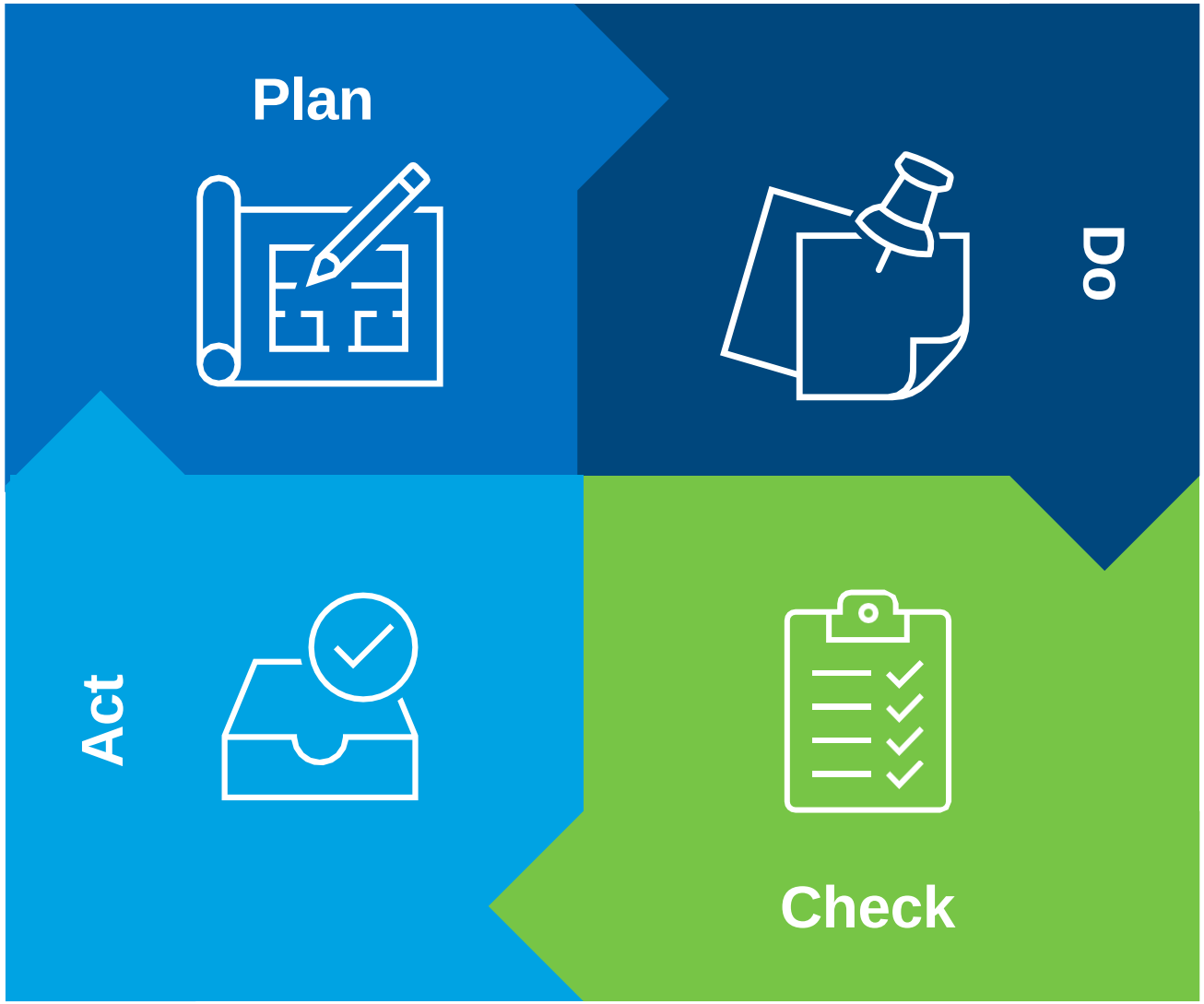
- Objective
- Scope
- Constraints
- Approach
- Result

Assessing the Current State

An IS manager may need to assess the current state of the IS program at various points, sharing results with the steering committee and key stakeholders.

Plan-Do-Check-Act

An iterative four-step management method used in business for the control and continuous improvement of processes and products.



Audits

Auditors identify, evaluate, test and assess the effectiveness of controls using a consistent approach

Documentation maps controls to control objectives, testing procedures and links results to final assessment

With unfinalized policies and procedures, select externally published standards to determine compliance

Judge control effectiveness based on meeting control objective criteria

With finalized policies and procedures audits are useful to determine full implementation

Ensure external standards used closely reflect the intended standards to be implemented

Auditors

Implement security standards by providing feedback to senior management

Influence the tone at the top and create high-level support for security activities

Provide strong, independent feedback for the steering committee or management to assess IS program effectiveness

Integrating with audit activities

- Audits can be compulsory or voluntary
- Coordinate with audit to allocate time and resources
- Establish procedures in advance

Addressing deficiencies

- Work with auditors to determine risk, mitigating factors and control objectives
- Craft potential solutions to fit enterprise environment
- Combine mitigating or compensating controls that enforce control objectives

Resolution of Noncompliance Issues

Noncompliance issues may result in risk to the enterprise.

Develop specific processes to deal with noncompliance timely and effectively:

- Provide quick resolutions for serious risk issues
- Determine criticality and use a risk-based response
- Develop a timetable to document each item
- Record and assign responsibility to address items
- Perform regular follow-up to ensure items are addressed

Identified through:

- **Normal monitoring**
- **Audit reports**
- **Security reviews**
- **Vulnerability scans**
- **Due diligence work**

Continuous Monitoring

Implementing continuous monitoring of security activities is necessary and may be a regulatory requirement.

- Performed by IT personnel
- Define monitoring requirements in operating standards with severity criteria and escalation processes
- Monitor IDSs and firewalls continuously to provide real-time information on attempts to breach perimeter defenses
- Train help desk personnel to escalate suspicious reports signaling a breach or attack
- Use information to take timely corrective action