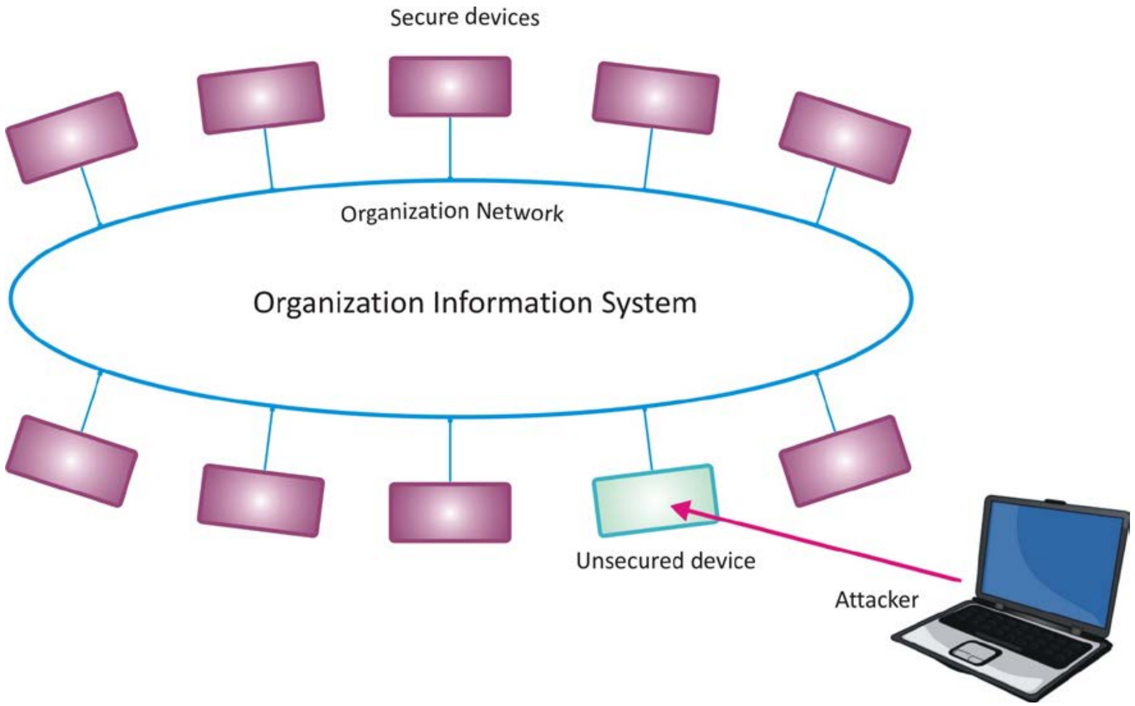
Management of Computer Security

Prof. Dr. Eşref ADALI

www. Adalı.net

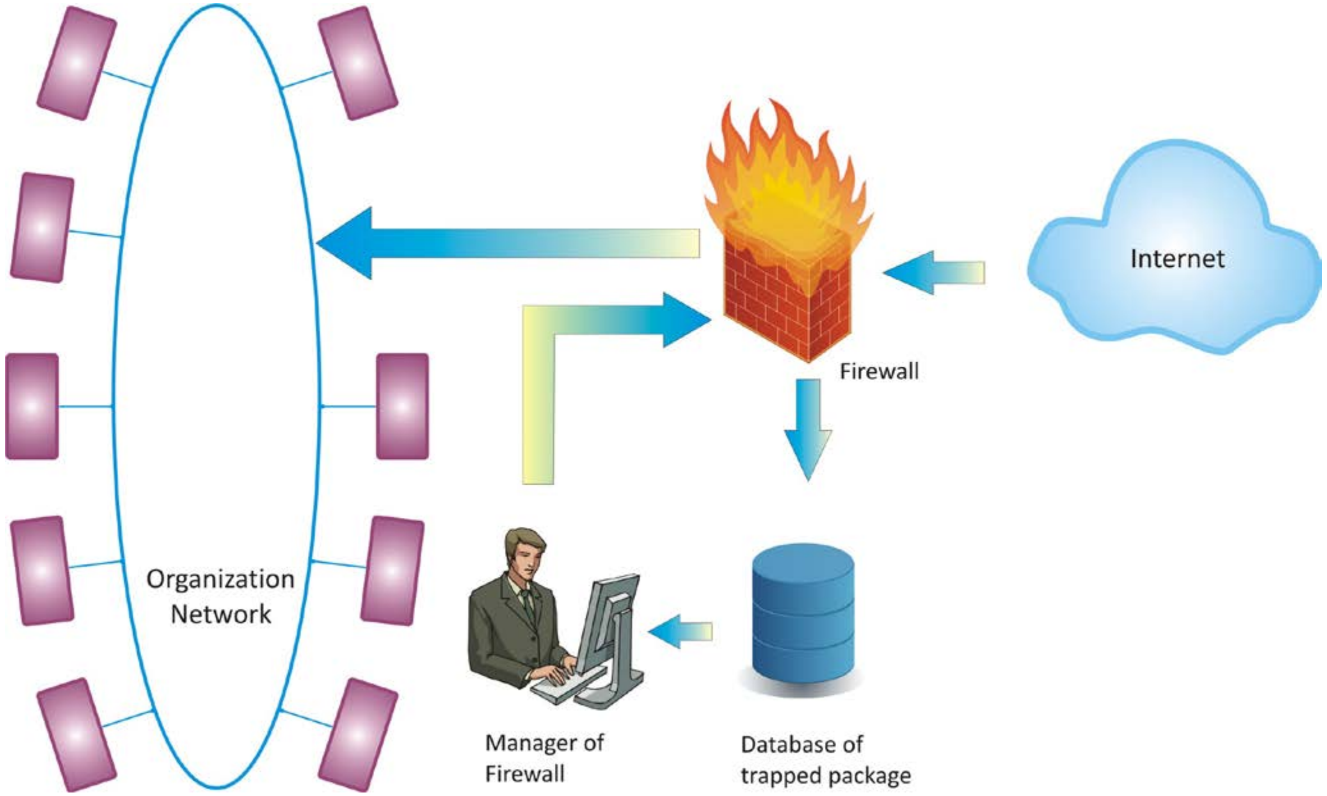
Vulnerability

- Security is a chain; and just as a chain is only as strong as the weakest link.
- Attacker will attack the weakest parts of the system because they are the parts most likely to be easily broken.
- The weakest part of the system will be administrators, users or technical support.
- Humans The weakest link in cyber security



Vulnerability Related Firewall

- A firewall is a network security system designed to prevent unauthorized access to or from a private network.
- All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
- Firewalls can be implemented in both hardware and software, or a combination of both.

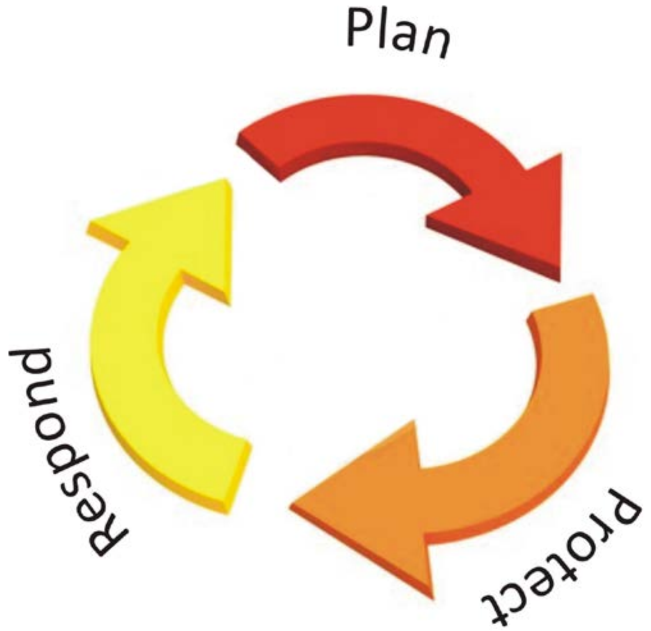


Phases of Security Management

Planning : Without an excellent plan, you will never have a comprehensive IT security

Protection : The plan based creation and operation of countermeasures.

Response : Even with the best planning and good protection, some attacks will succeed



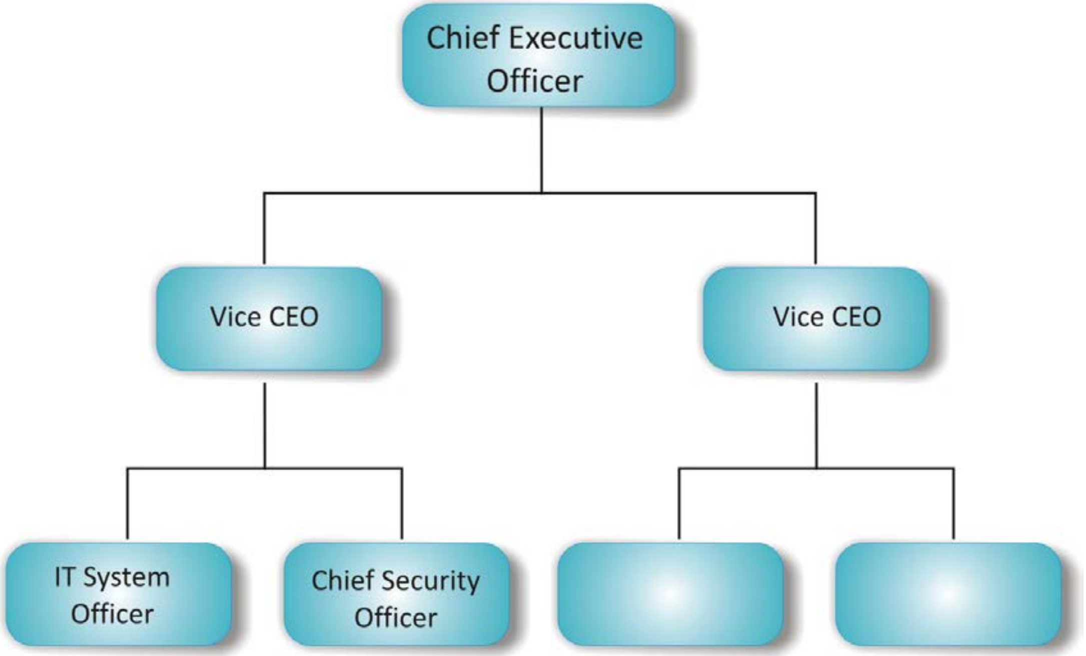
IT Security

CEO : The support of Chief Executive Officer is very important.

CSO : A Chief Security Officer is necessary. Depends on the size of organization, a security department will be required

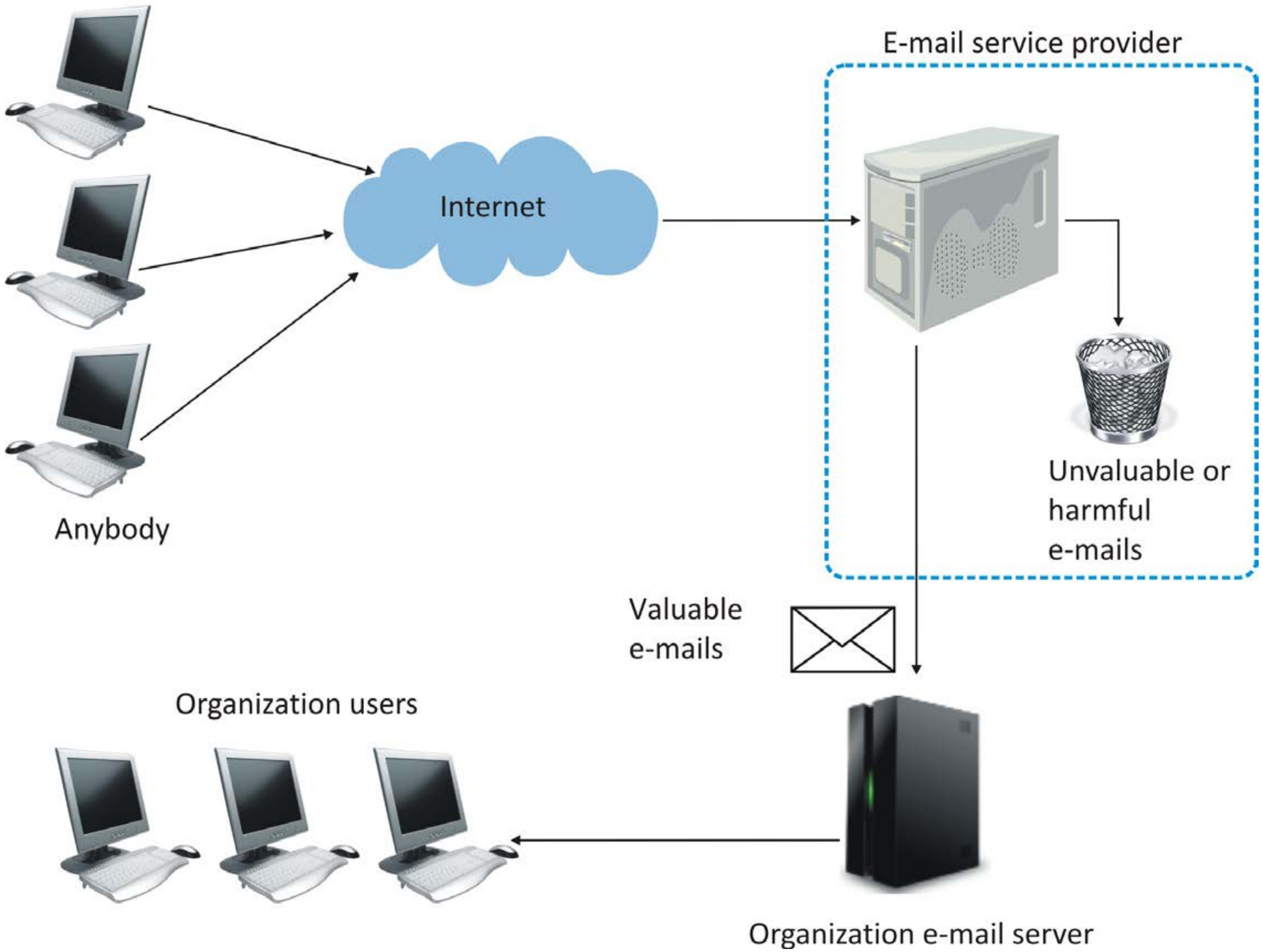
Related Department : A Chief Security Officer have to work with:

- IT Department
- Board of Ethic
- HR Department
- Legal adviser
- Inspection and control board
- Maintenance and Support
- Physical security



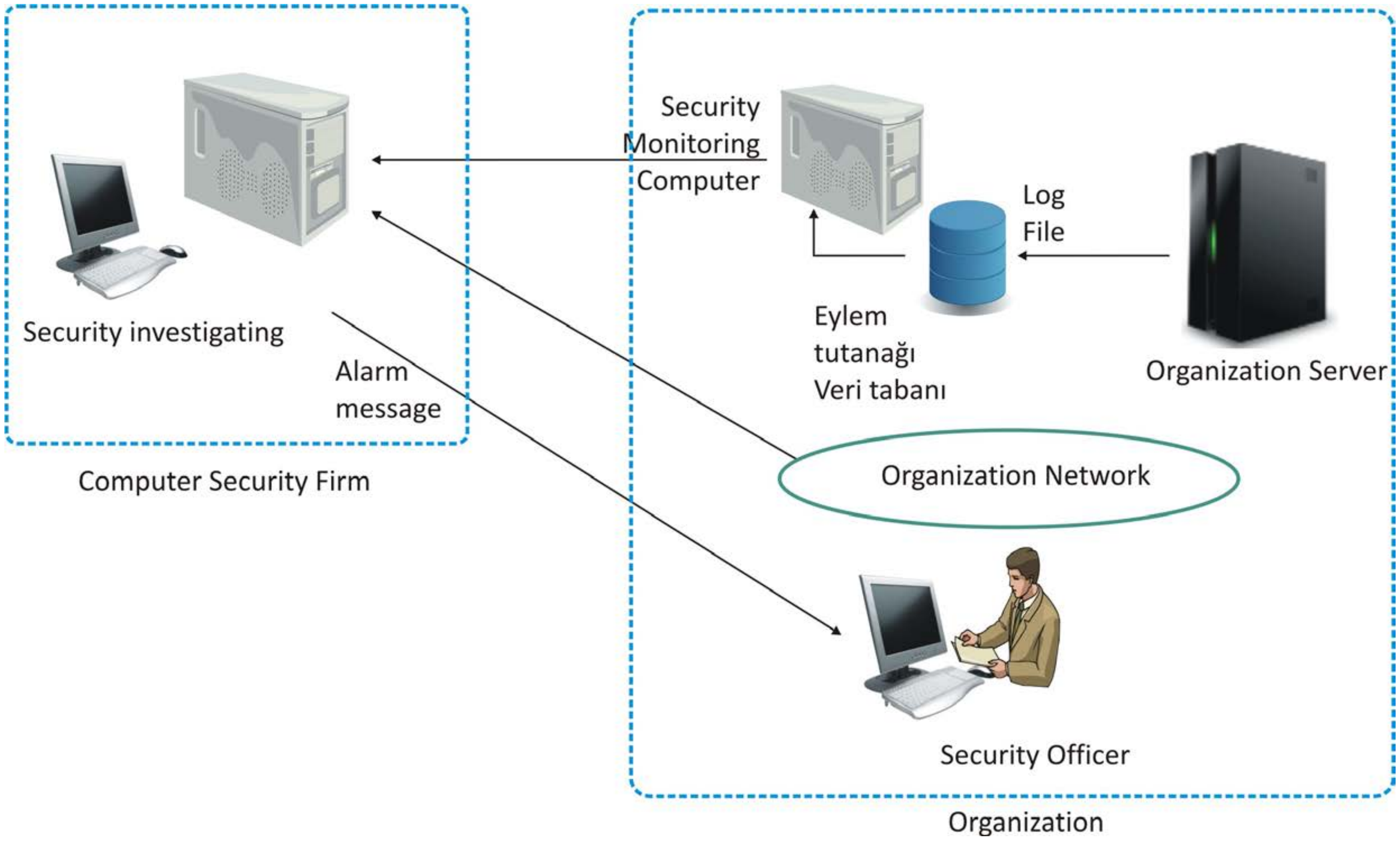
Outsourcing Security (e-mail Service)

- The outsourcer provide both inbound and outbound filtering service.
- Filtering includes:
  - Spam
  - Malware



Outsourcing Security (Security Service)

- Professional security service provider monitor over your organization.
- A logging server is placed in the organization. This server uploads the event log to the security service.
- At the security service, security expert look through the log file, classifying events by severity level and throwing out false positive.

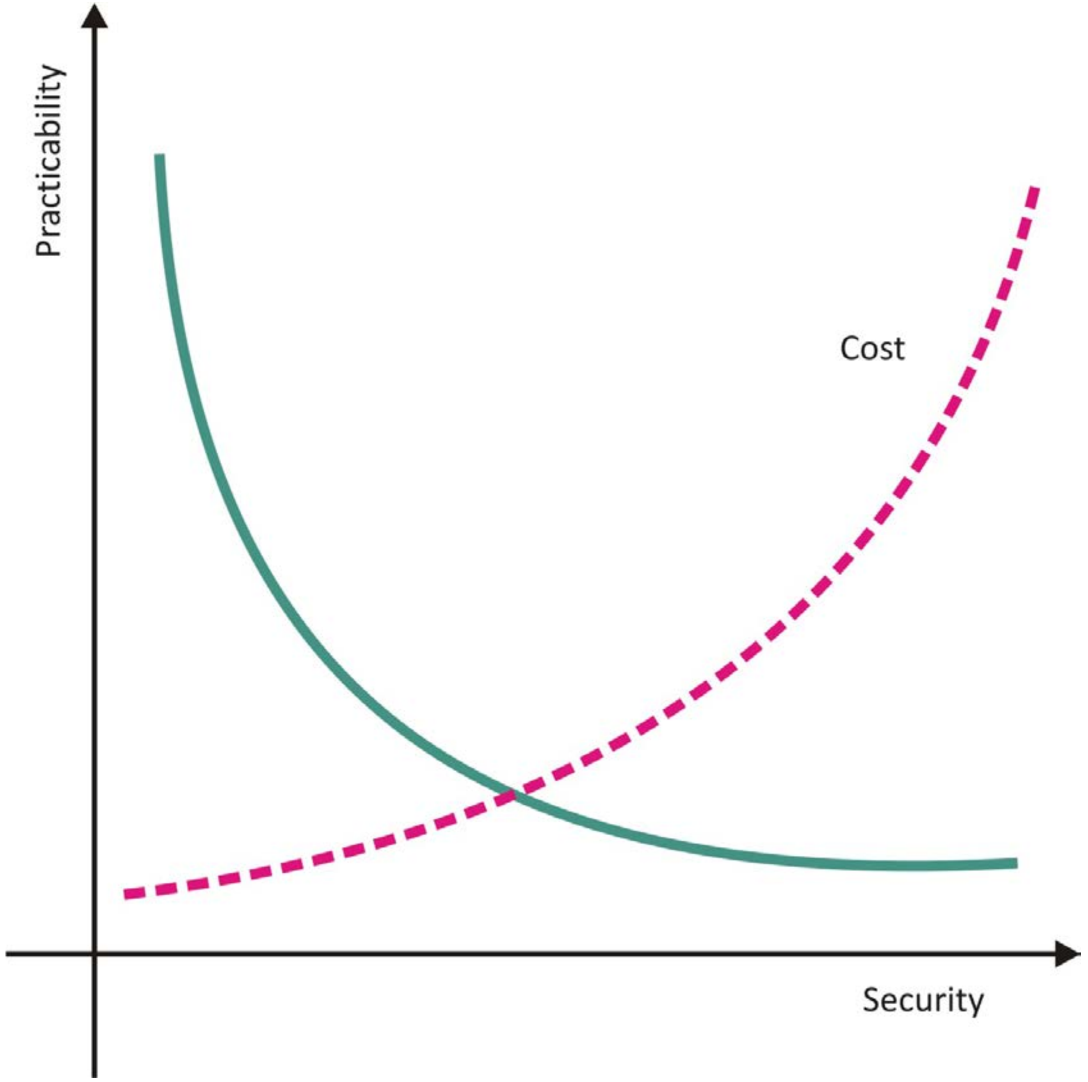


Risk Analysis

What is reasonable risk ?

How much security is needed?

Is it possible 100% security ?



Conventional Risk Analysis

		Countermeasure	
	Base Case	A	B
Asset Value (AV)	100.000	100.000	100.000
Exposure Factor (EF)	80%	20%	80%
Single Loss Expectancy (SLE) = AV*EF	80.000	20.000	80.000
Annualized Rate of Occurrence (ARO)	50%	50%	25%
Annualized Loss Expectancy (ALE) = SLE*ARO	40.000	10.000	20.000
ALE Reduction of Countermeasure Cost		30.000	20.000
Annualized Countermeasure Cost		17.000	4.000
Annualized Countermeasure Value		13.000	16.000

The result :
Countermeasure B is better.
Cost is 4.000
Net yield is 16.000

Difficulty of Risk Calculation of IT System

- Uneven Multiyear Cash Flows
- Total Cost of Incident
- Many to many relationships between countermeasures and resources
- Impossible of knowing the annualized rate of occurrence

Responding to Risk

Risk reduction

Risk acceptance

Risk Transference

Risk Avoidance

Security Architectures (Technical)

Definition

- All of the technical countermeasures of organization must be defined.
- How these countermeasures are organized must be defined.
- Complete system of protection must be defined.

Architectural Decisions

- Must be well planned to provide strong security with few weaknesses

Dealing with legacy Technologies

- Technologies put in place previously
- Too expensive to upgrade all legacy Technologies immediately
- Must upgrade if serious impairs security
- Upgrades must justify their cost

Security Architectures (Principles)

Defense in Detail

- Resource is guarded by several countermeasures in series
- Attackers must breach them all
- If one countermeasure fail, the resource remains safe

Defense in Detail versus Weakest Links

- Multiple independent countermeasures must be defeated.
- A single countermeasure with multiple independent components must all succeed for the countermeasure to succeed

Avoiding Single Points of vulnerability

- Failure at the single point can have drastic consequences. Eg: DNS server, central security management server, etc

Minimizing Security Burdens

Realistic Goals

- Cannot change the protection level of organization overnight
- Measure as quickly as possible

Security Architectures (Elements)

- Border management
- Internal site management
- Management of remote connections
- Inter organizational system
- Centralized security management

Security Management

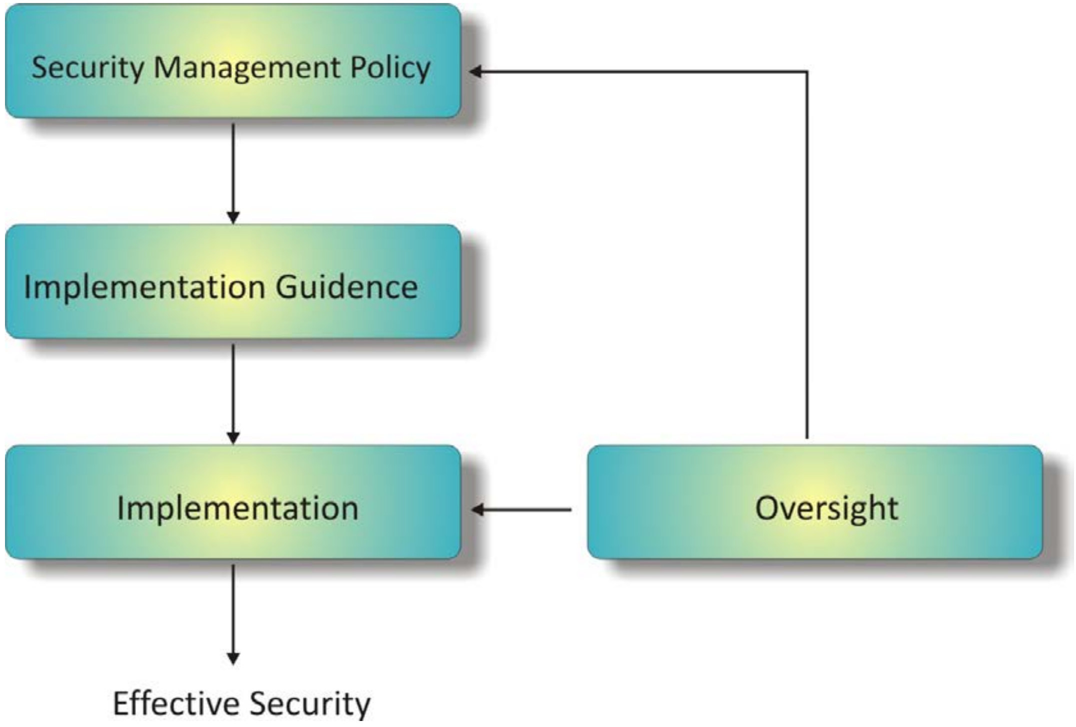
Policy : Policies are statement of what should be done under specific circumstances

Guidance : Implementation guidance limits the discretion of implementation

Implementation : Standards and guidance should be used for implementation, such as;

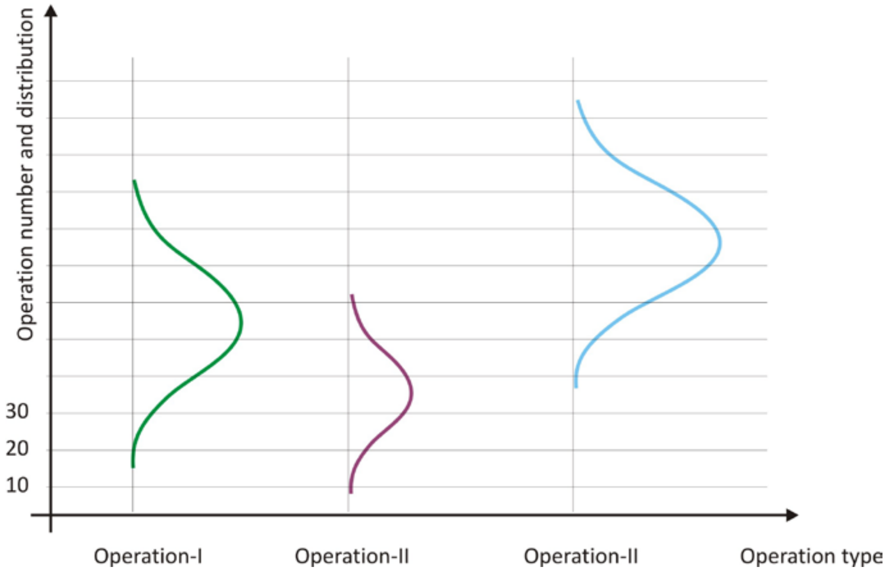
- Procedures
- Processes
- Basic standard
- Best practices and recommendation
- Accountability
- Ethics

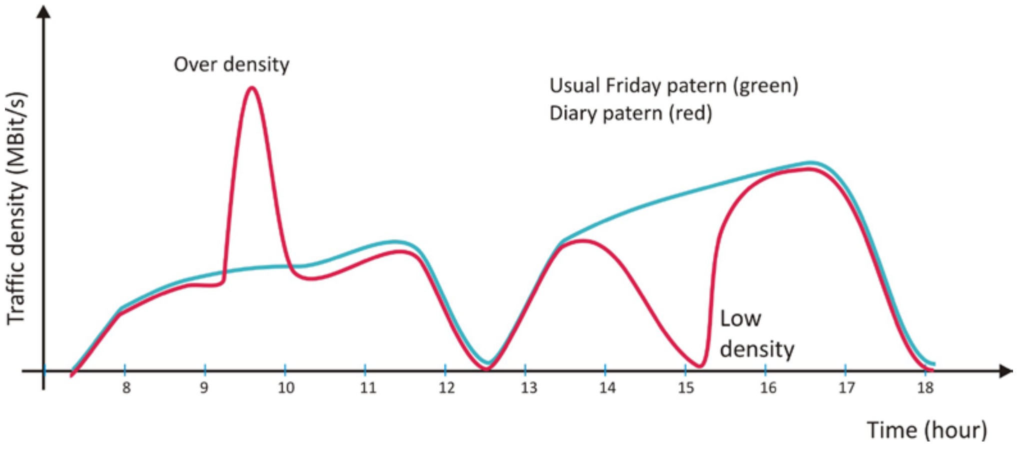
Oversight : An oversight is necessary for comparing policies and implementation



Monitoring

- Behaviors of external users
- Behaviors of internal users
- Monitoring of network traffic
- Attacks to sensitive values
- Discovering of vulnerability
- Control



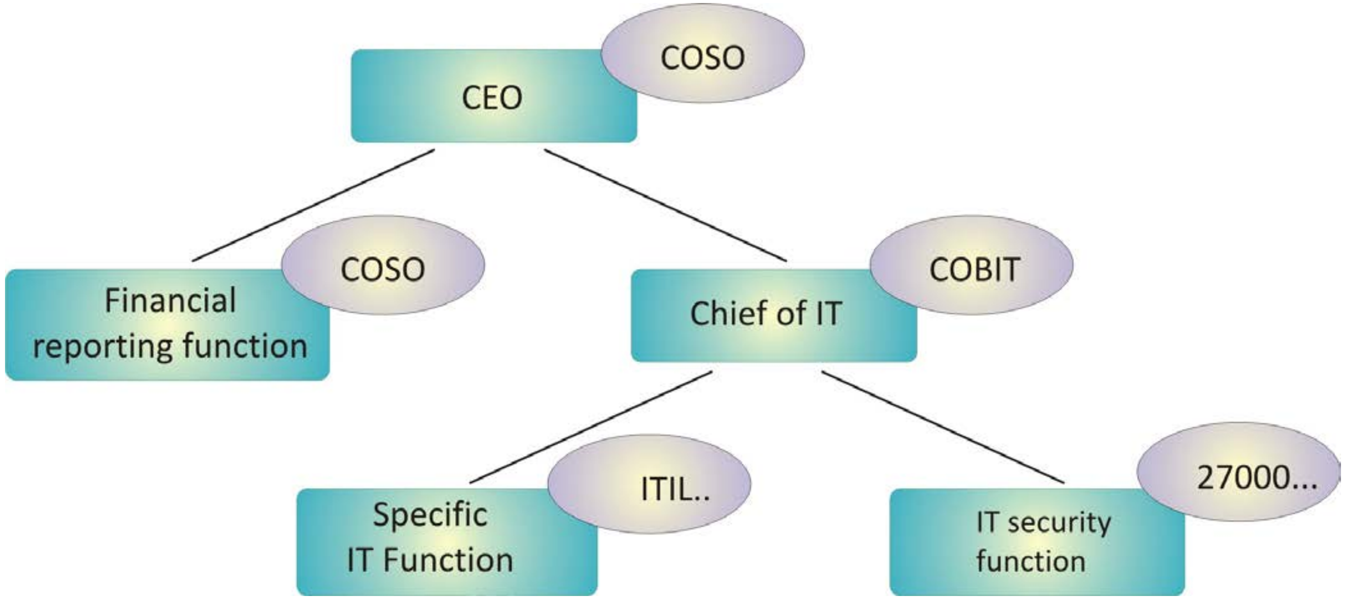


COSO

- COSO is a framework and developed by Committee of Sponsoring Organizations of the Treadway Commission (COSO), in 1994.

- There are three objectives:
  - Operations
  - Financial Reporting
  - Compliance

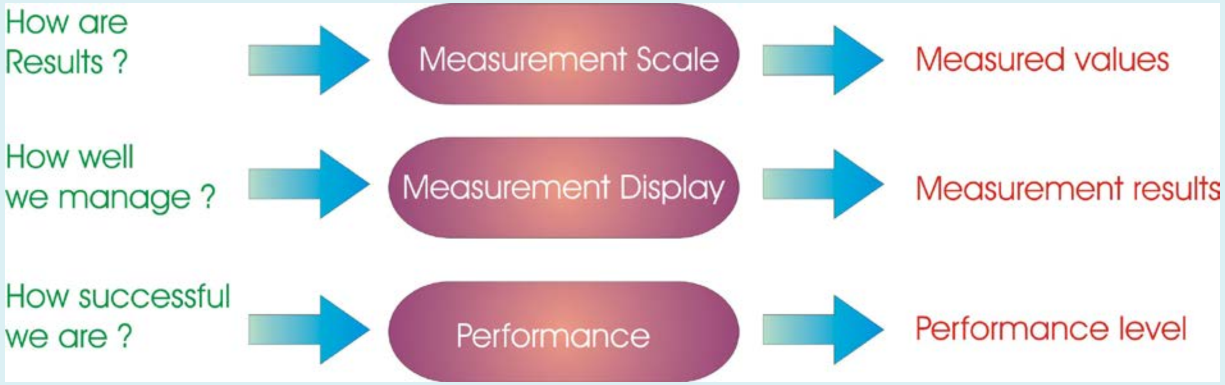
- COSO is a general control planning and assessment tool for organization.



COBIT - I

- COBIT is a framework and developed by IT Governance Institute.

- There are four objectives:
    - Planning and Organization
    - Acquisition and Implementation
    - Delivery and Support
    - Monitoring



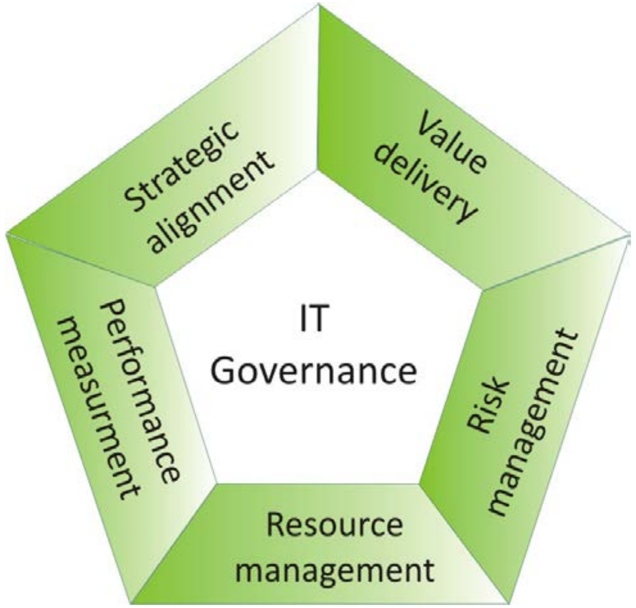
How are Results ? → Measurement Scale → Measured values

How well we manage ? → Measurement Display → Measurement results

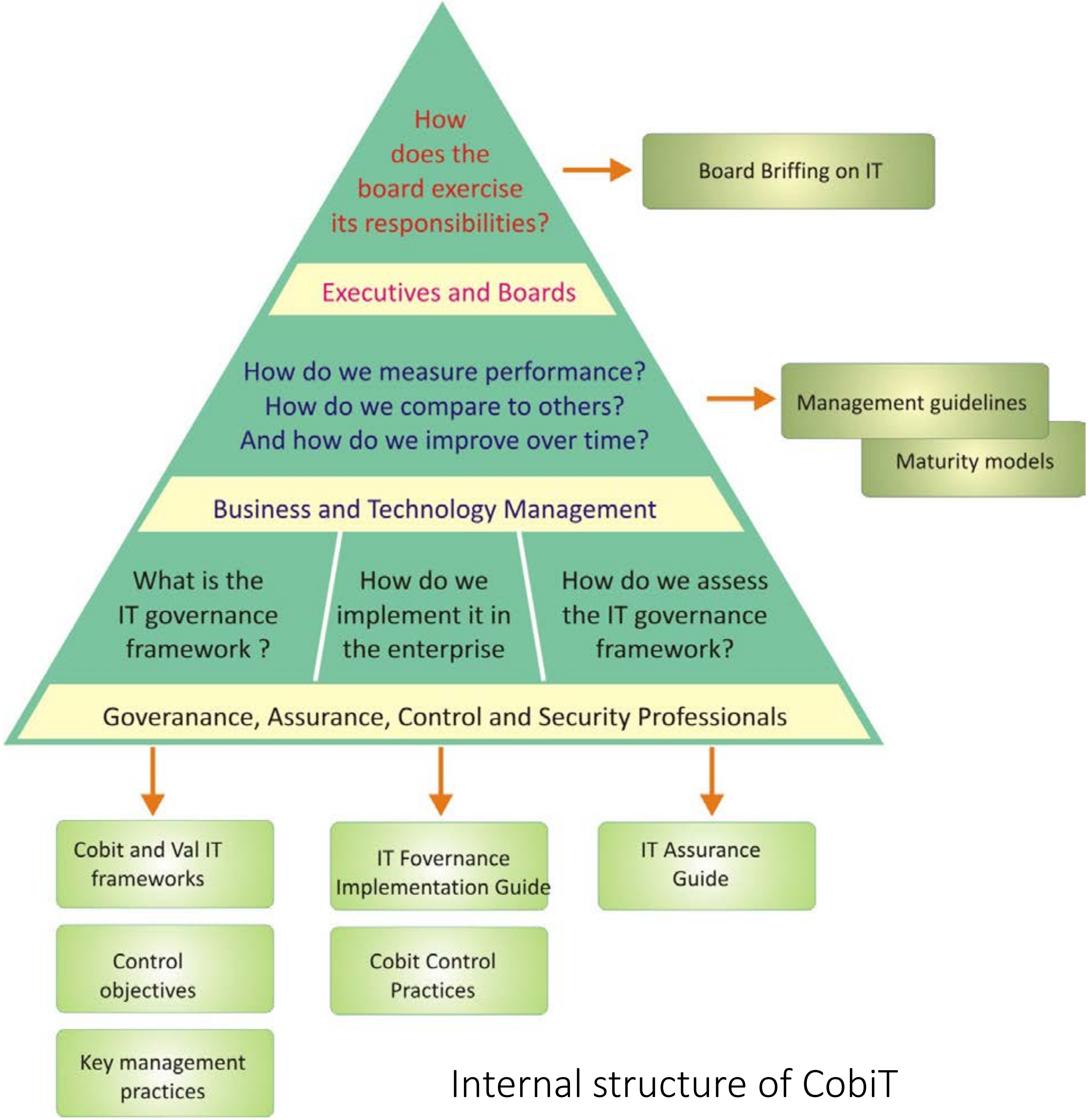
How successful we are ? → Performance → Performance level

Conventional management system

COBIT - II



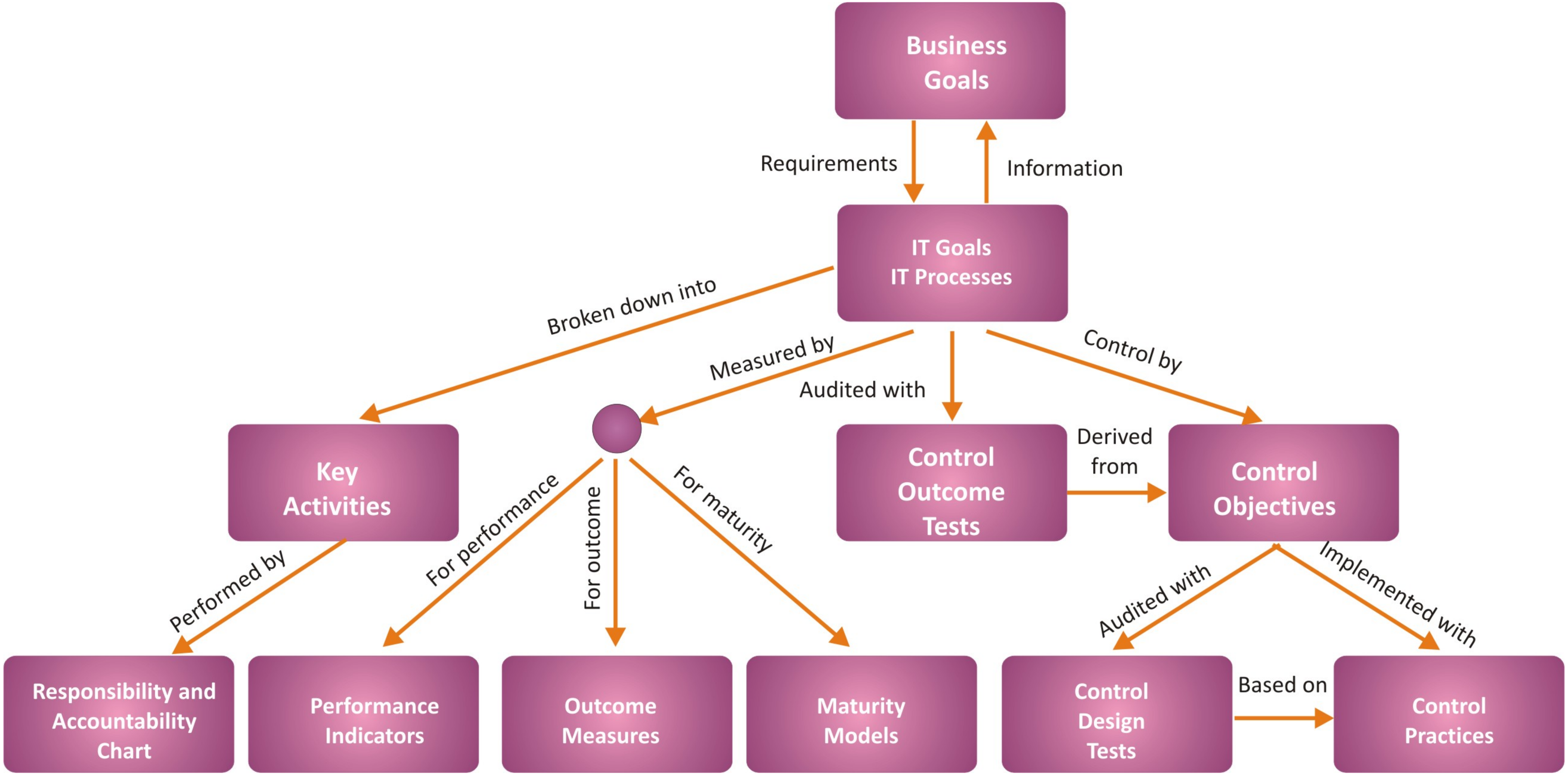
Focus areas of IT systems



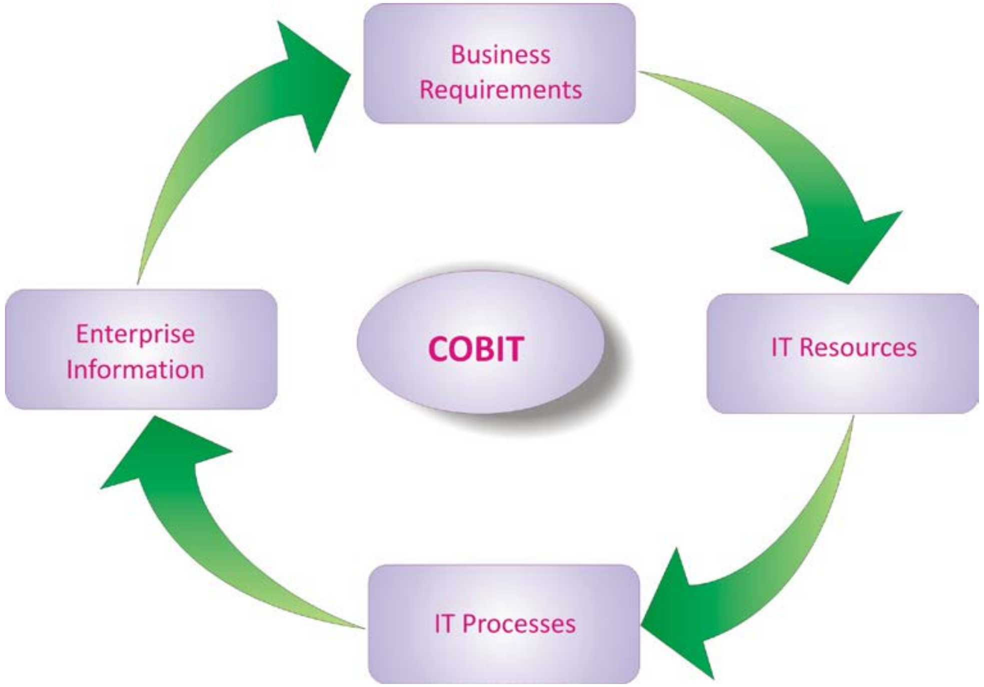
How does the board exercise its responsibilities?
Board Briffing on IT
Executives and Boards
How do we measure performance?
How do we compare to others?
And how do we improve over time?
Management guidelines
Maturity models
Business and Technology Management
What is the IT governance framework ?
How do we implement it in the enterprise
How do we assess the IT governance framework?
Goveranance, Assurance, Control and Security Professionals
Cobit and Val IT frameworks
Control objectives
Key management practices
IT Fovernance Implementation Guide
Cobit Control Practices
IT Assurance Guide

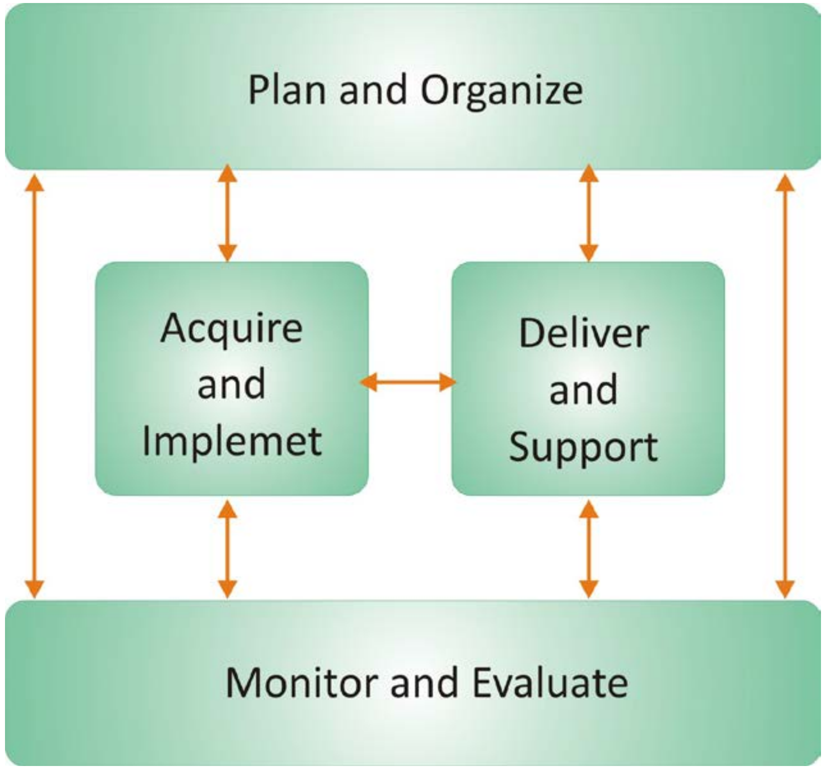
Internal structure of CobiT

Relationship Between CobiT Elements - I

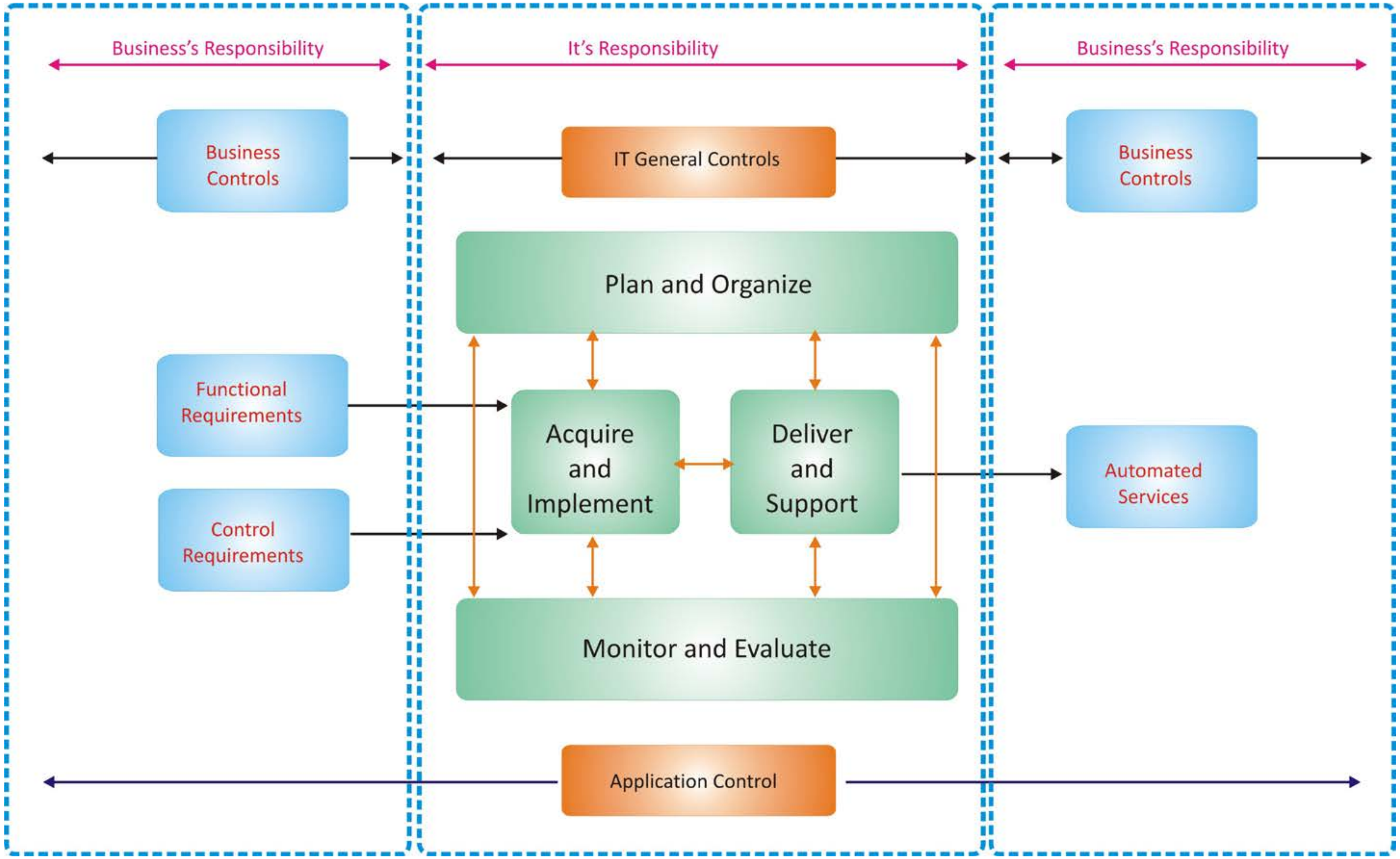


Relationship Between CobiT Elements-II





Relationship Between CobiT Elements-III



Business's Responsibility

It's Responsibility

Business's Responsibility

Business Controls

IT General Controls

Business Controls

Plan and Organize

Functional Requirements

Acquire and Implement

Deliver and Support

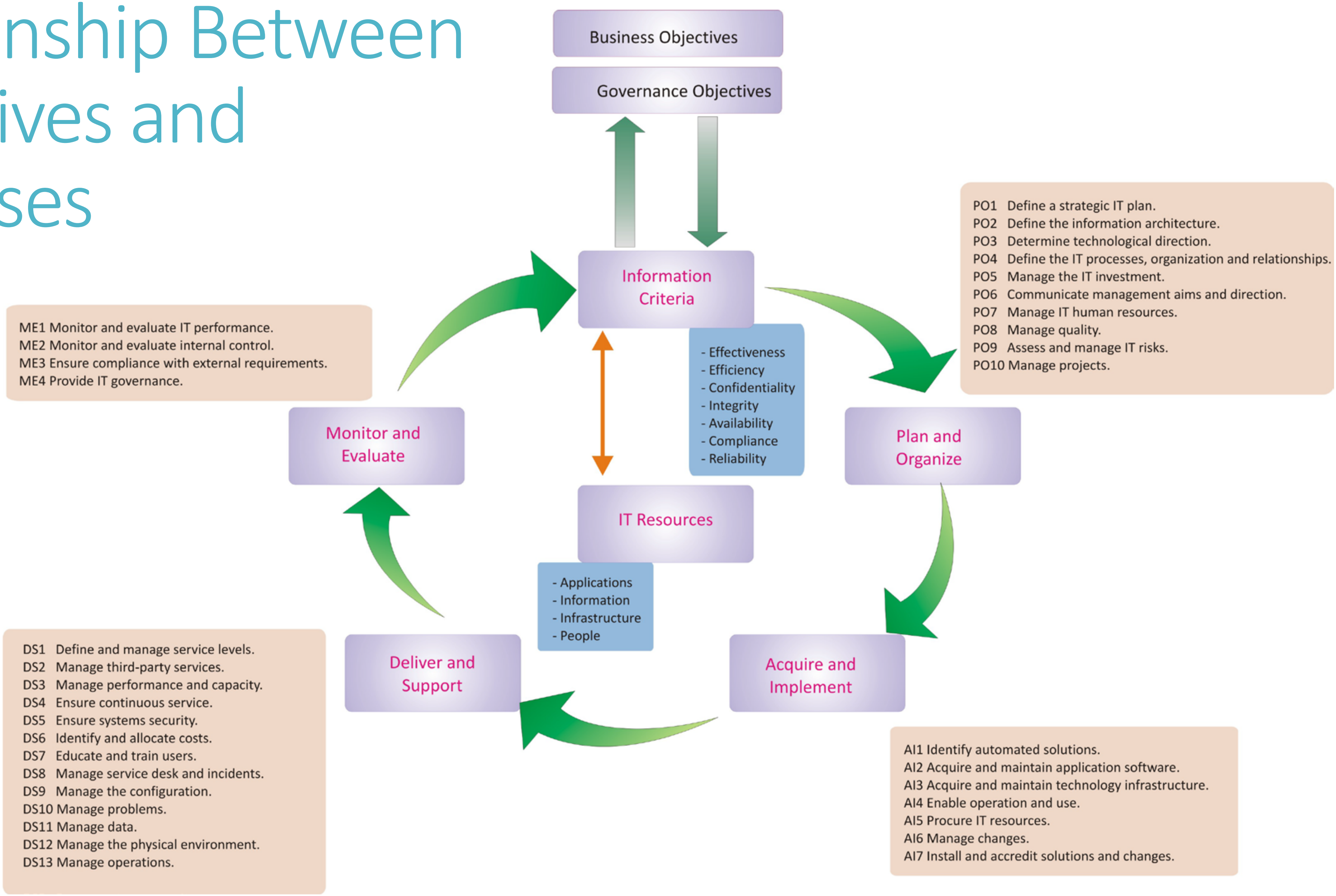
Automated Services

Control Requirements

Monitor and Evaluate

Application Control

Relationship Between Objectives and Processes



- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

- Applications
- Information
- Infrastructure
- People

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organization and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

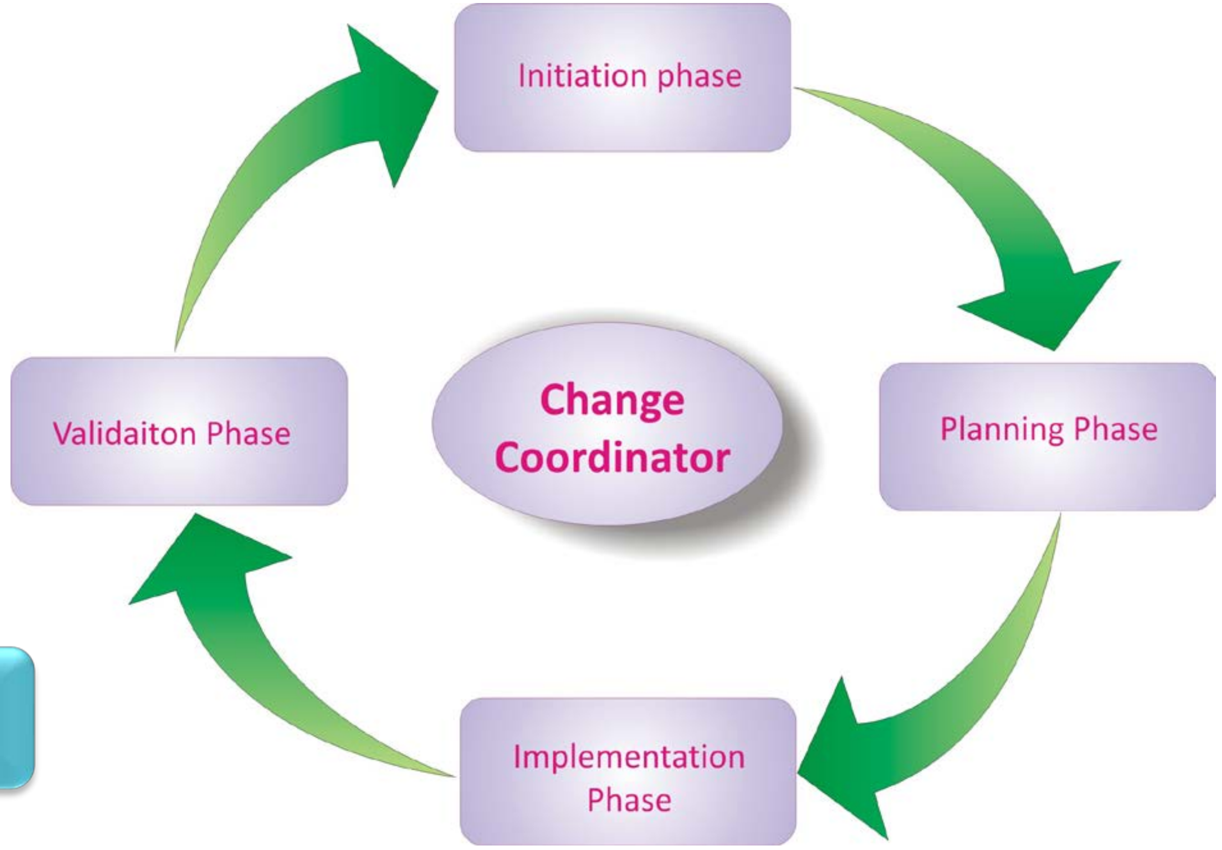
AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

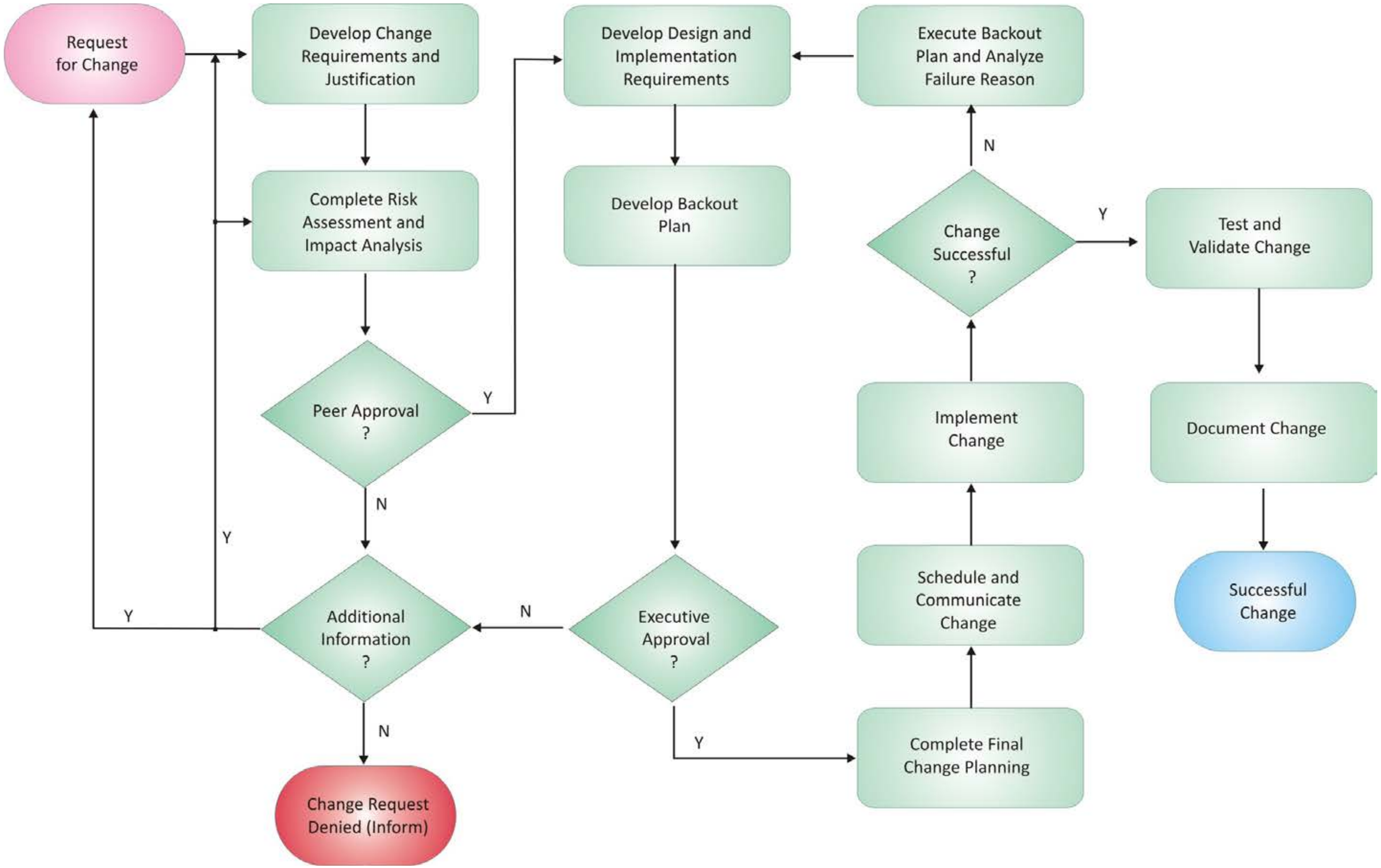
ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.

Change Management

- Request for Change
- Classification and priority of change
- Analysis and justification
- Approval and timing
- Verification of change



Phases of Change Management


Request for Change
Develop Change Requirements and Justification
Complete Risk Assessment and Impact Analysis
Peer Approval ?
Y
N
Additional Information ?
Y
Y
N
Change Request Denied (Inform)
Develop Design and Implementation Requirements
Develop Backout Plan
Executive Approval ?
N
Y
Complete Final Change Planning
Schedule and Communicate Change
Implement Change
Change Successful ?
N
Execute Backout Plan and Analyze Failure Reason
Y
Test and Validate Change
Document Change
Successful Change