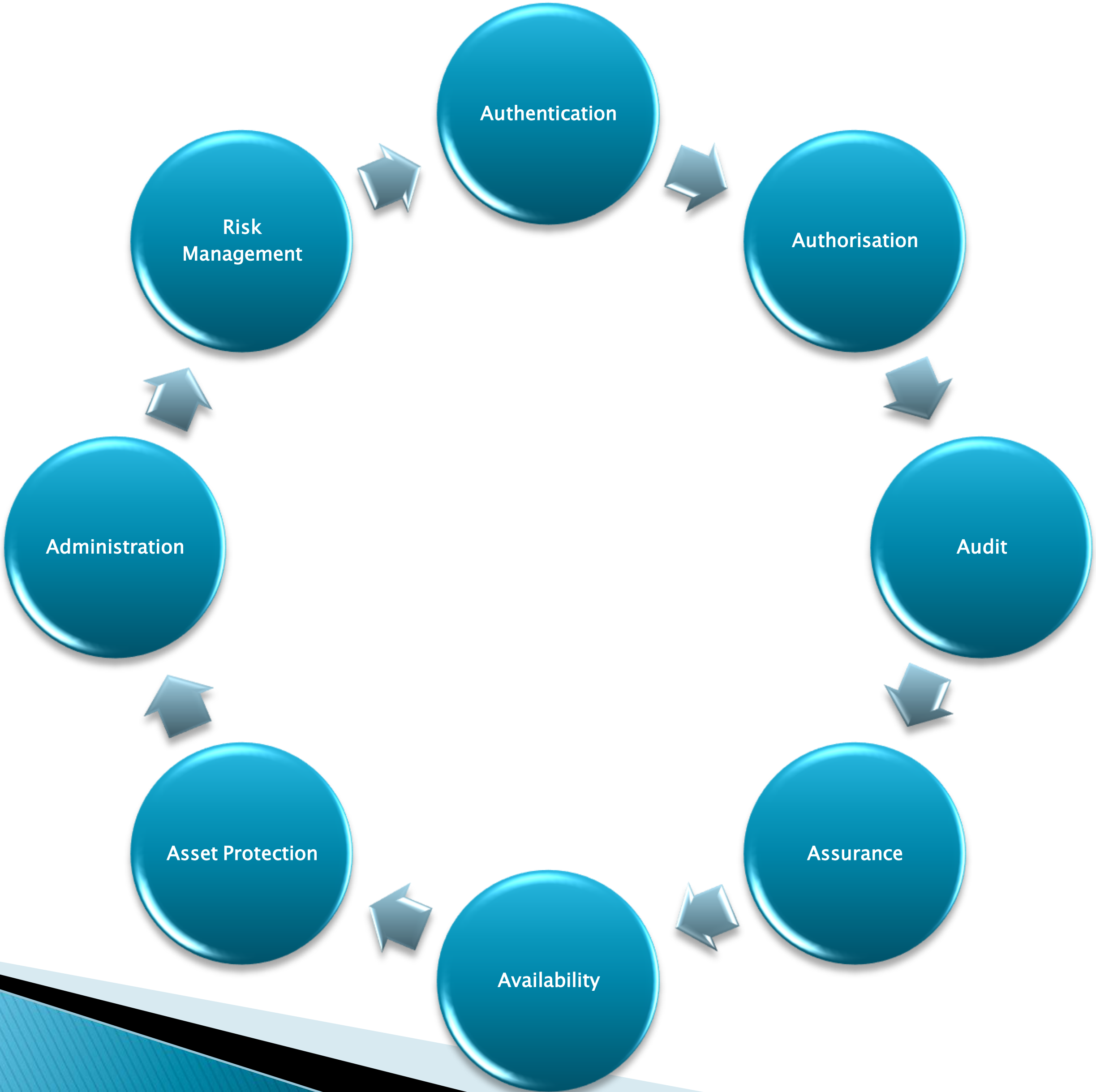
# TOGAF 9
# Security Architecture

Summarised - 2010

# Security Architecture Characteristics

- Security architecture has its own methods. These methods might be the basis for a discreet security methodology.
- Security architecture composes its own discrete view and viewpoints.
- Security architecture addresses non-normative flows through systems and among applications.
- Security architecture introduces its own normative flows through systems and among applications.
- Security architecture introduces unique, single-purpose components in the design.
- Security architecture calls for its own unique set of skill requirements in the IT architect.

# Areas of Concern for Security Architecture



Authentication

Authorisation

Audit

Assurance

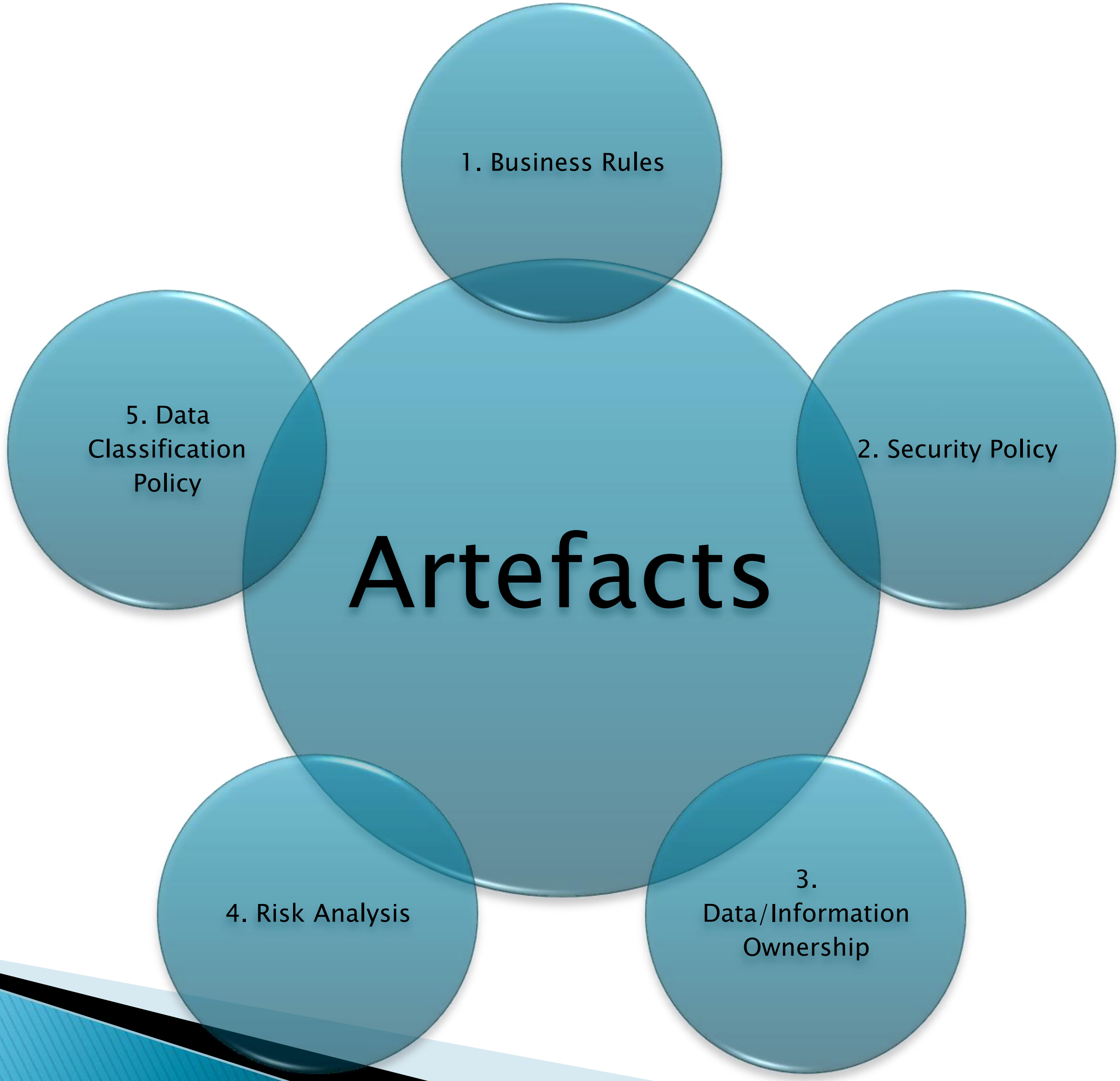
Availability

Asset Protection

Administration

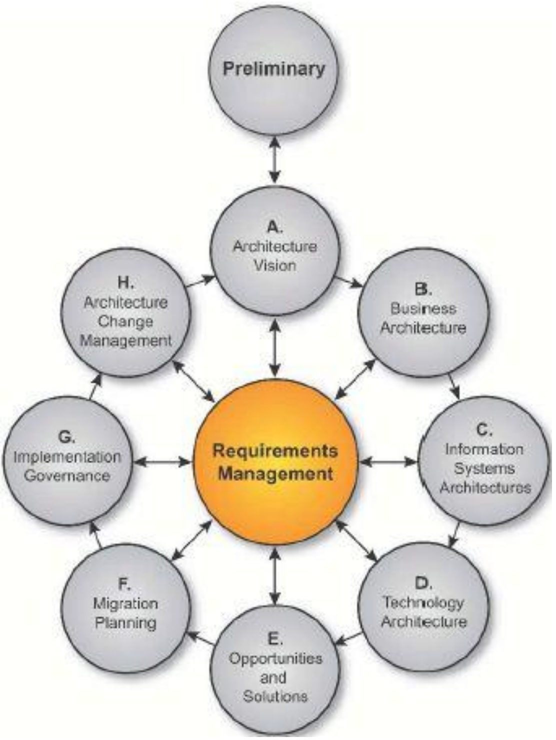
Risk Management

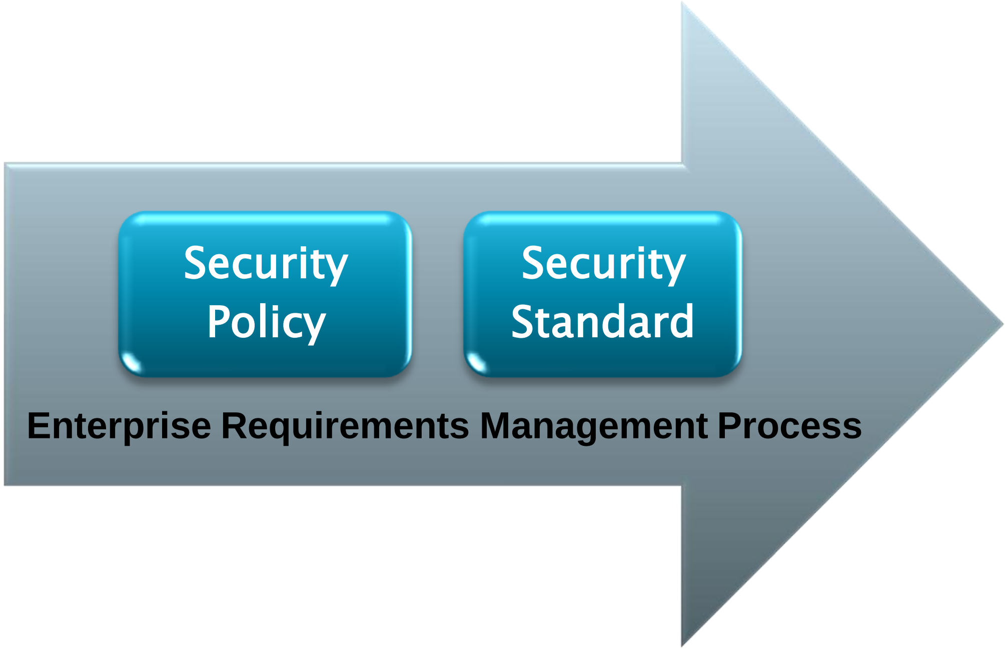
# Security Architecture Artefacts



# ADM – Security Architecture Requirements Management

# ADM Security Architecture Requirements Management


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management



Security Policy

Security Standard

Enterprise Requirements Management Process

**New Security Requirements arise from many sources:**

1

A new statutory or regulatory mandate

2

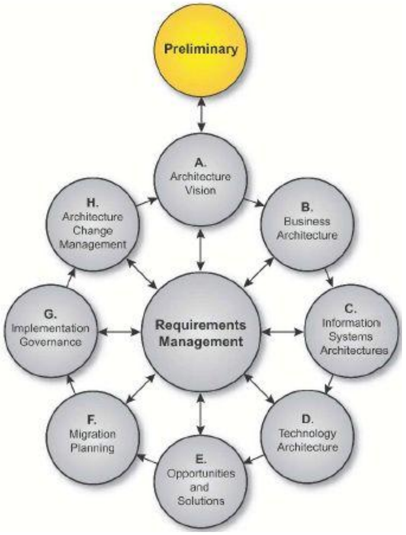
A new threat realized or experienced

3

A new IT architecture initiative discovers new stakeholders and/or new requirements

# ADM – Security Architecture Preliminary

# ADM – Security Architecture Preliminary


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

**Objective**

- A written Security Policy for the organisation must be in place

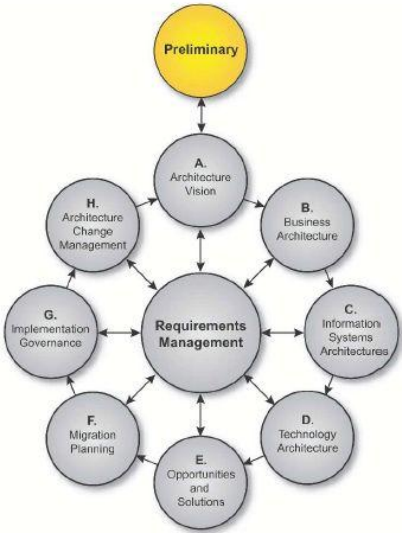
**Security Assessment**

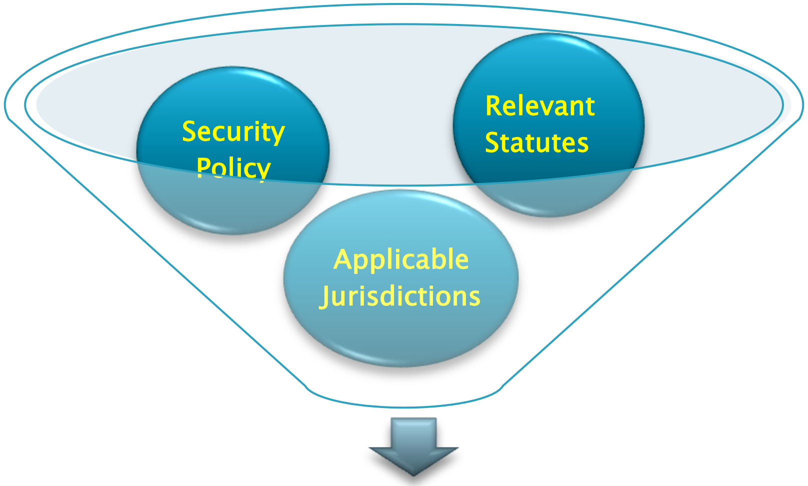
- ISO/IEC 17799:2005 a basis for the security policy
- Architecture constraints established in the security policy must be communicated

**Regulatory Requirements**

- Dependent upon the functionality of the system and the data collected or maintained.
- The jurisdiction where the system or service is deployed

# ADM – Security Architecture Preliminary


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

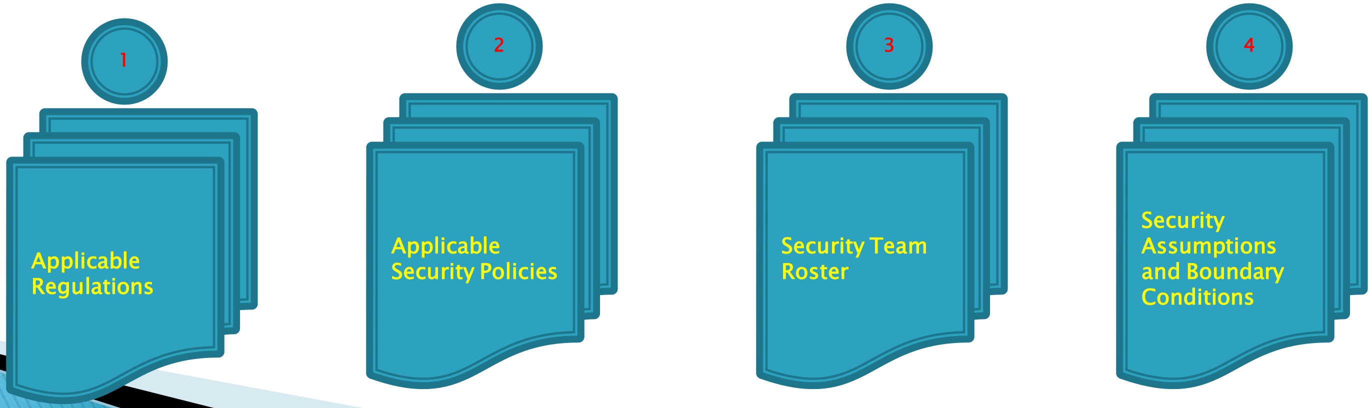


Security Policy

Relevant Statutes

Applicable Jurisdictions

Input



1 Applicable Regulations

2 Applicable Security Policies

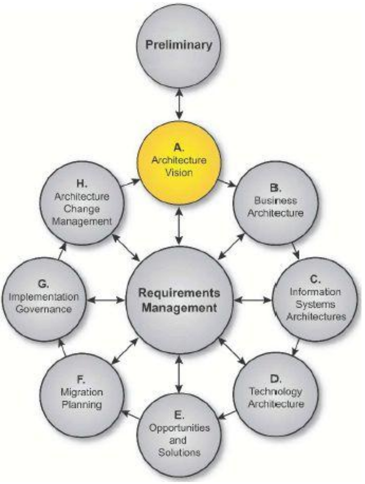
3 Security Team Roster

4 Security Assumptions and Boundary Conditions

Output

# Phase A – Security Architecture Vision

# Phase A – Security Architecture Vision



Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

Management Support

- Obtain management support for security measures

Milestones

- Define necessary security-related management sign-off milestones of this architecture development cycle

DR and BCM

- Determine and document applicable disaster recovery or business continuity plans/requirements

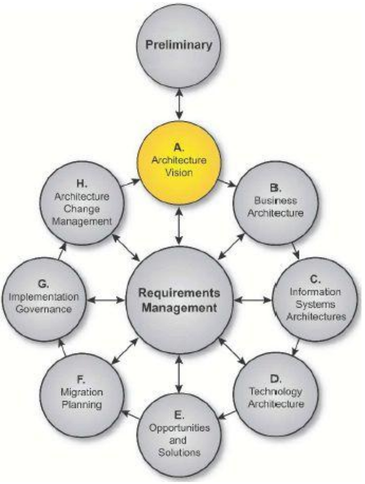
Environment

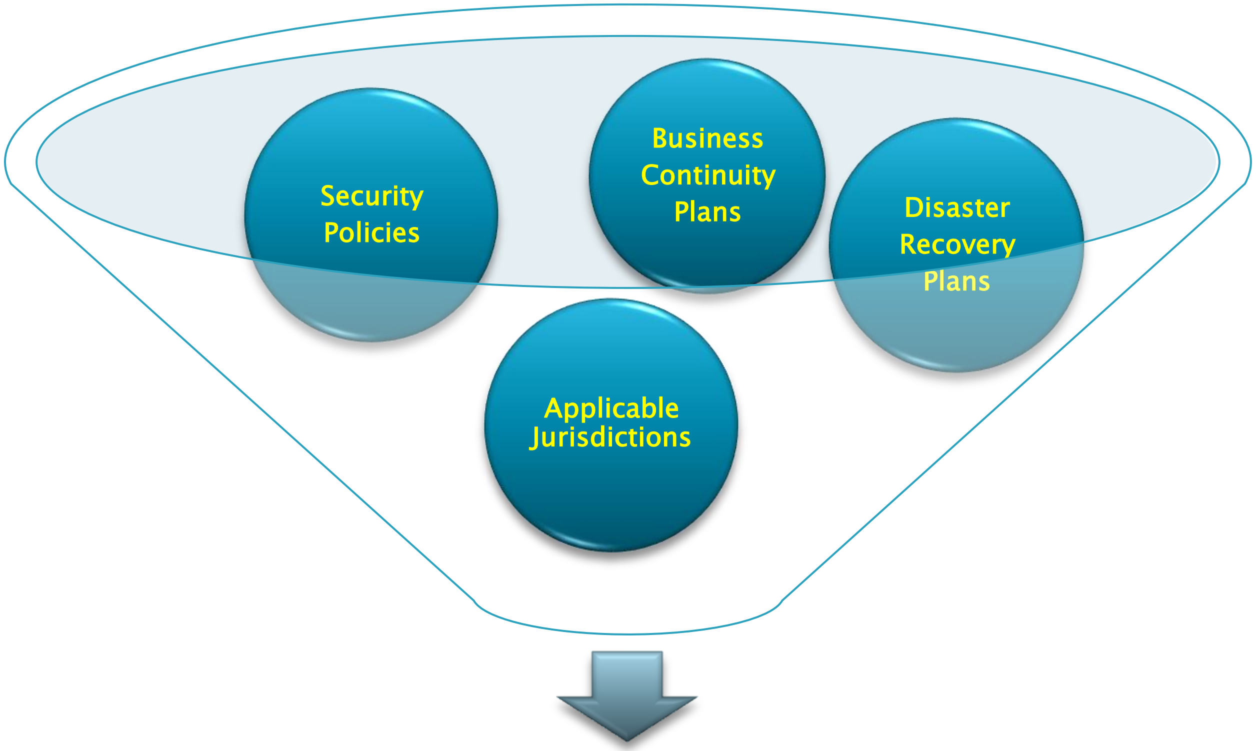
- Identify and document the anticipated physical/business/regulatory environment(s) in which the system(s) will be deployed

Criticality

- Determine and document the criticality of the system: safety-critical/mission-critical/noncritical

# Phase A – Security Architecture Vision


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management



Security Policies

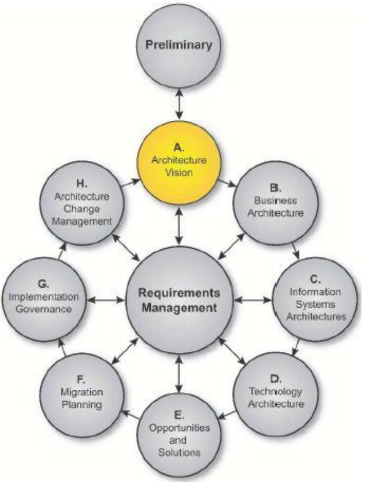
Business Continuity Plans

Disaster Recovery Plans

Applicable Jurisdictions

INPUT

# Phase A – Security Architecture Vision


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

Output

1 Physical Security Environment Statement

2 Business Security Environment Statement

3 Regulatory Environment Statement

4 Security Policy Cover Letter Signed

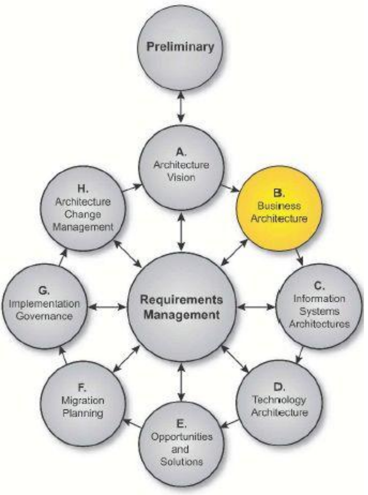
5 List of Architecture Development Checkpoints for Sign-off

6 Disaster Recovery and Business Continuity Plans

7 System Critical Statement

# Phase B – Business Architecture

# Phase B – Business Architecture


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

Legitimate Actors

- Determine who are the legitimate actors who will interact with the product/ser vice/process

Baseline

- Assess and baseline current security-specific business processes (enhancement of existing objective)

Security Measures

- Determine whom/how much it is acceptable to inconvenience in utilizing security measures

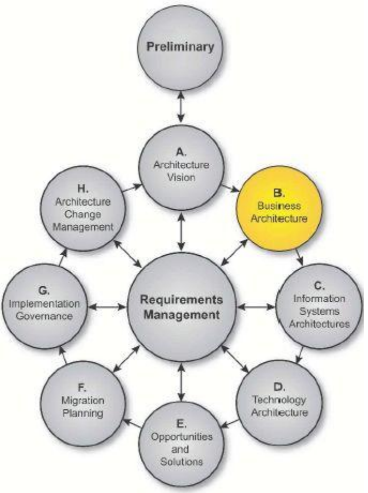
Interconnecting Systems

- Identify and document interconnecting systems beyond project control

Assets at Risk

- Determine the assets at risk if something goes wrong — ‘‘What are we trying to protect?’’

# Phase B – Business Architecture


Preliminary
A. Architecture Vision
H. Architecture Change Management
B. Business Architecture
G. Implementation Governance
Requirements Management
C. Information Systems Architectures
F. Migration Planning
D. Technology Architecture
E. Opportunities and Solutions

**Cost**

- Determine the cost (both qualitative and quantitative) of asset loss/impact in failure cases

**Asset Ownership**

- Identify and document the ownership of assets

**Forensic Process**

- Determine and document appropriate security forensic processes

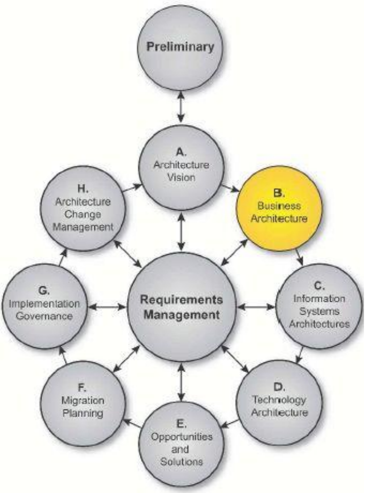
**Criticality**

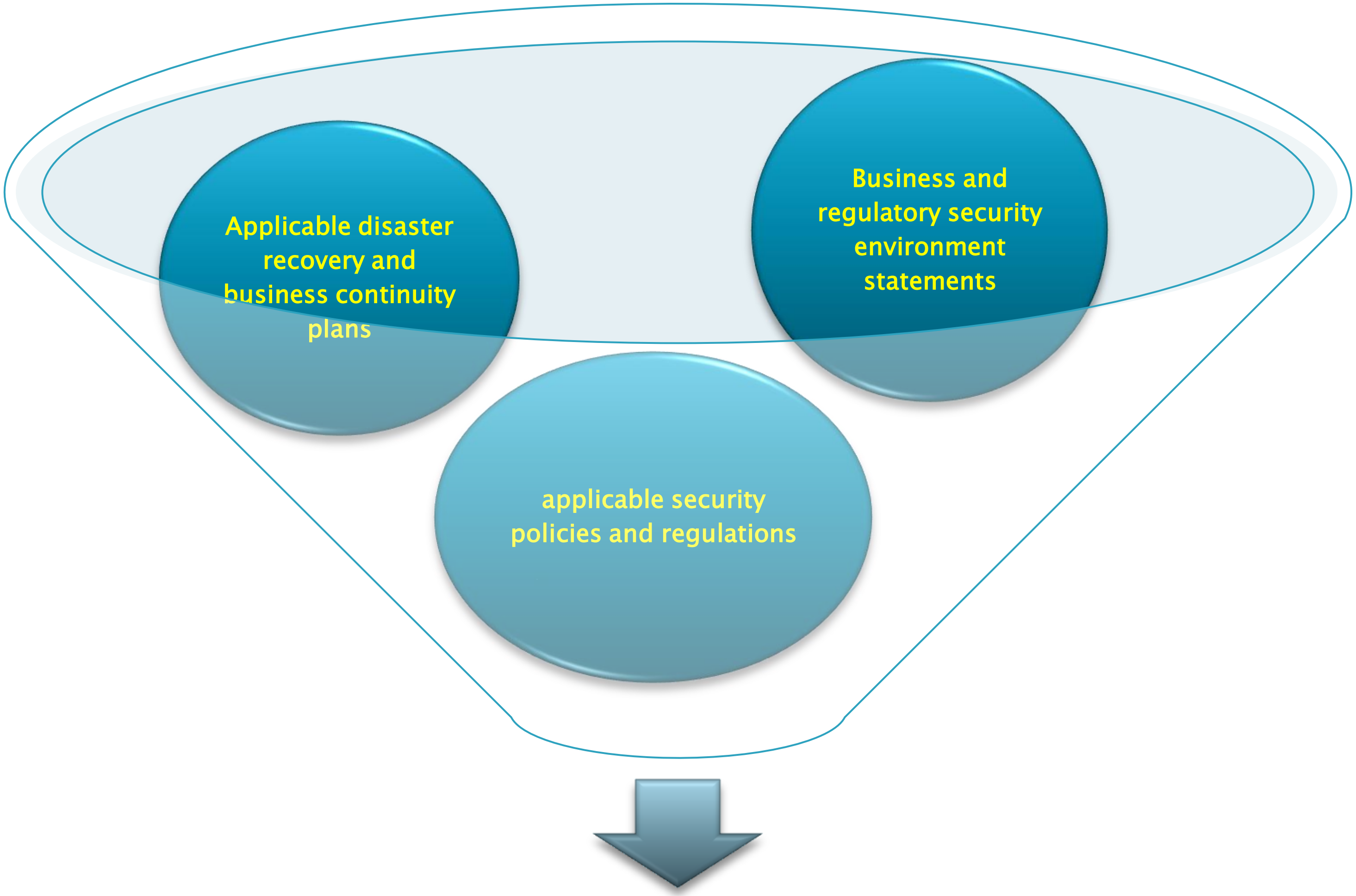
- Identify the criticality of the availability and correct operation of the overall service

**Re-assess**

- Reassess and confirm Architecture Vision decisions

# Phase B – Business Architecture


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management



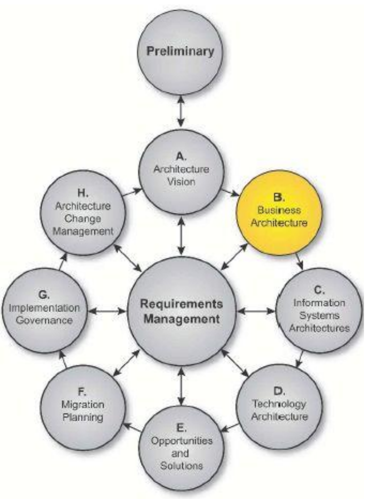
Applicable disaster recovery and business continuity plans

Business and regulatory security environment statements

applicable security policies and regulations

Input

# Phase B – Business Architecture


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

## Output

1 Forensic Processes

2 New disaster recovery and business continuity requirements

3 Validated business and regulatory environment statements

4 Validated security policies and regulations

5 Target security processes

6 Baseline security processes

7 security actors

8 Interconnecting Systems

9 security tolerance for each class of security actor

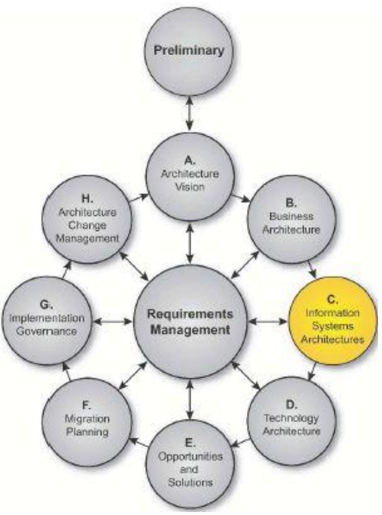
10 Asset list with values and owners

11 List of trust paths and Availability impact statement(s)

12 Threat analysis matrix

# Phase C – Information Systems Architecture

# Phase C – Information Systems Architecture



Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

**Baseline Architecture Elements**

- Assess and baseline current security-specific architecture elements (enhancement of existing objective)

**Default Actions and Failure States**

- Identify safe default actions and failure states
- Safe default actions and failure modes must be defined for the system informed by the current state, business environment, applicable policies, and regulatory obligations.

**Guidelines and Standards**

- Identify and evaluate applicable recognized guidelines and standards

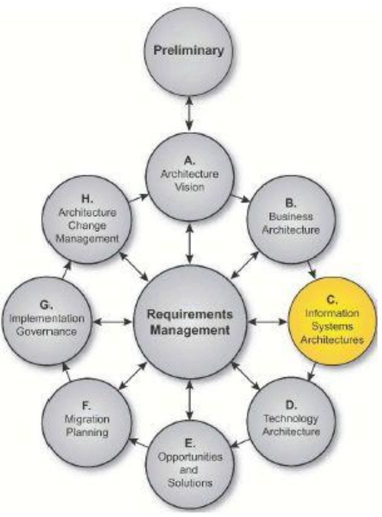
**Revisit Interconnecting Systems**

- Revisit assumptions regarding interconnecting systems beyond project control
- In light of the risk assessments performed, assumptions regarding interconnecting systems may
- require modification

**Classification Level**

- Determine and document the sensitivity or classification level of information stored/created/used
- Identify and document custody of assets
- Identify the criticality of the availability and correct operation of each function

# Phase C – Information Systems Architecture


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

**DR and BCM**

- Determine the relationship of the system under design with existing business disaster/continuity plans
- Identify what aspects of the system must be configurable to reflect changes in policy/business environment/access control

**Lifespan**

- Identify lifespan of information used as defined by business needs and regulatory requirements
- Determine approaches to address identified risks

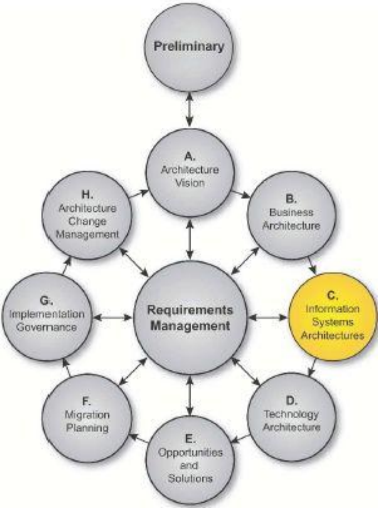
**Logs**

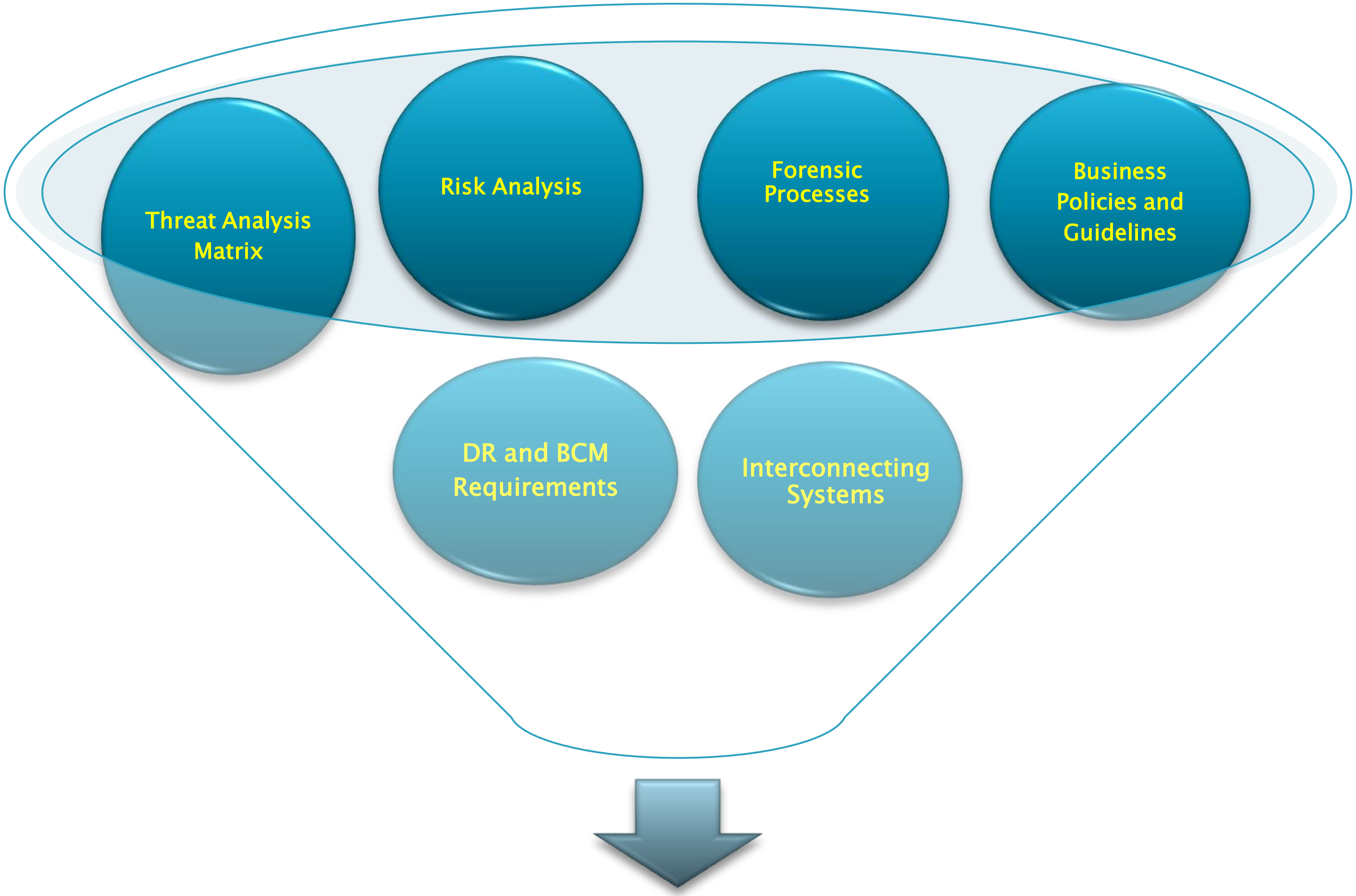
- Identify actions/events that warrant logging for later review or triggering forensic processes
- Identify and document requirements for rigor in proving accuracy of logged events (non-repudiation)

**Attacks**

- Identify potential/likely avenues of attack
- Thinking like an adversar y will prepare the architect for creation of a robust system that resists malicious tampering and, providentially, malfunction arising from random error

# Phase C – Information Systems Architecture


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management



Threat Analysis Matrix

Risk Analysis

Forensic Processes

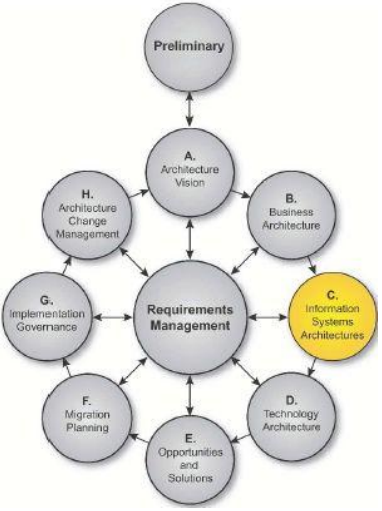
Business Policies and Guidelines

DR and BCM Requirements

Interconnecting Systems

Security Input

# Phase C – Information Systems Architecture


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

## Security Output

1 Event log-level matrix and requirements

2 Risk Management Strategy

3 Data Life Cycle Definitions

4 List of configurable system elements

5 Baseline list of security-related elements of the system

6 New or augmented security-related elements of the system

7 Security use-case models, List of applicable security standards

8 Validated interconnected system list

9 Information classification report, List of asset custodians

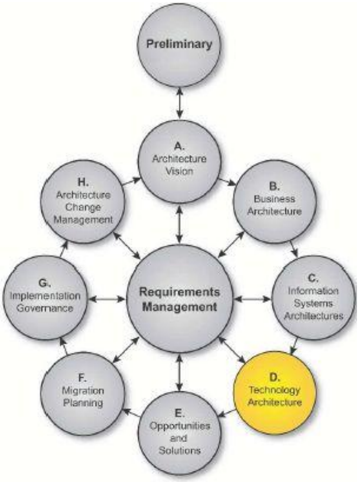
10 Function criticality statement

11 Revised disaster recovery and business continuity plans

12 Refined threat analysis matrix

# Phase D – Technology Architecture

# Phase D – Technology Architecture



Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

**Baseline Technologies**

- Assess and baseline current security-specific technologies (enhancement of existing objective)
- Revisit assumptions regarding interconnecting systems beyond project control
- Identify and evaluate applicable recognized guidelines and standards

**Measures**

- Identify methods to regulate consumption of resources
- Engineer a method by which the efficacy of security measures will be measured and communicated on an ongoing basis
- Identify minimal privileges required for any entity to achieve a technical or business objective

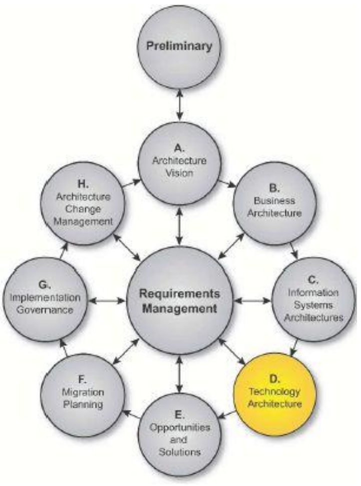
**Privileges**

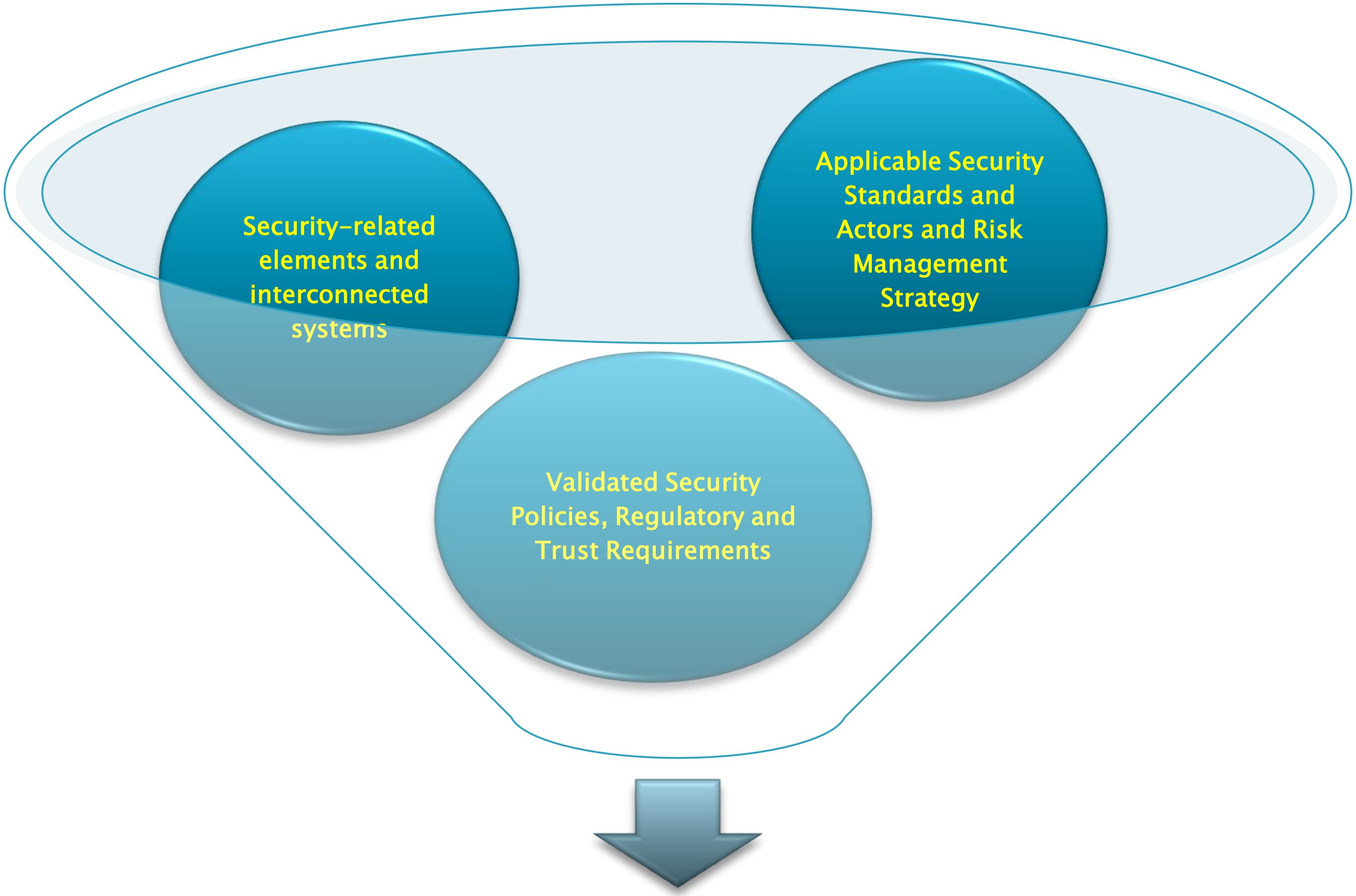
- Identify minimal privileges required for any entity to achieve a technical or business objective

**Trust**

- Identify the trust (clearance) level of:
  - All users of the system
  - All administrators of the system
  - All interconnecting systems beyond project control

# Phase D – Technology Architecture


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management



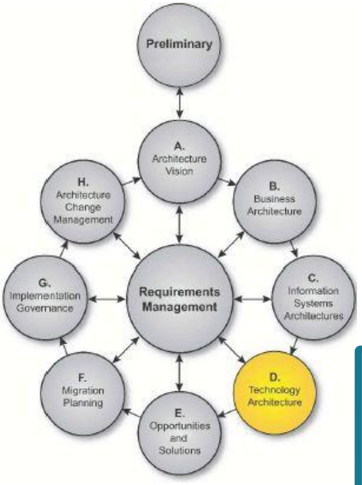
Security-related elements and interconnected systems

Applicable Security Standards and Actors and Risk Management Strategy

Validated Security Policies, Regulatory and Trust Requirements

Security Input

# Phase D – Technology Architecture


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

## Security Output

1 Baseline list of security technologies

2 Validated interconnected systems list

3 Selected security standards list

4 Resource conservation plan

5 Security metrics and monitoring plan

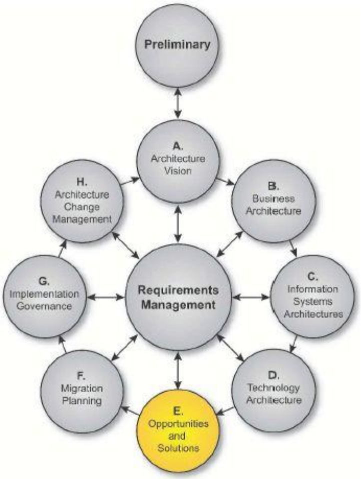
6 User authorization policies

7 Risk management plan

8 User trust (clearance) requirements

# Phase E – Opportunities and Solutions

# Phase E – Opportunities and Solutions


Preliminary
A. Architecture Vision
H. Architecture Change Management
B. Business Architecture
G. Implementation Governance
Requirements Management
C. Information Systems Architectures
F. Migration Planning
E. Opportunities and Solutions
D. Technology Architecture

**Security Services**

- Identify existing security services available for re-use
- Statutory or regulator y requirements may call for physical separation of domains which may eliminate the ability to re-use existing infrastructure

**Mitigation**

- Engineer mitigation measures addressing identified risks
- Mitigation measures must be designed, implemented, deployed, and/or operated.

**Evaluate**

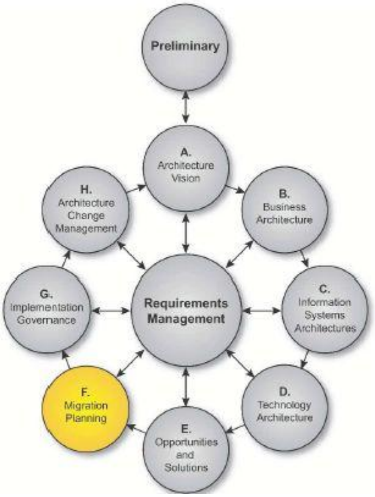
- Evaluate tested and re-usable security software and security system resources

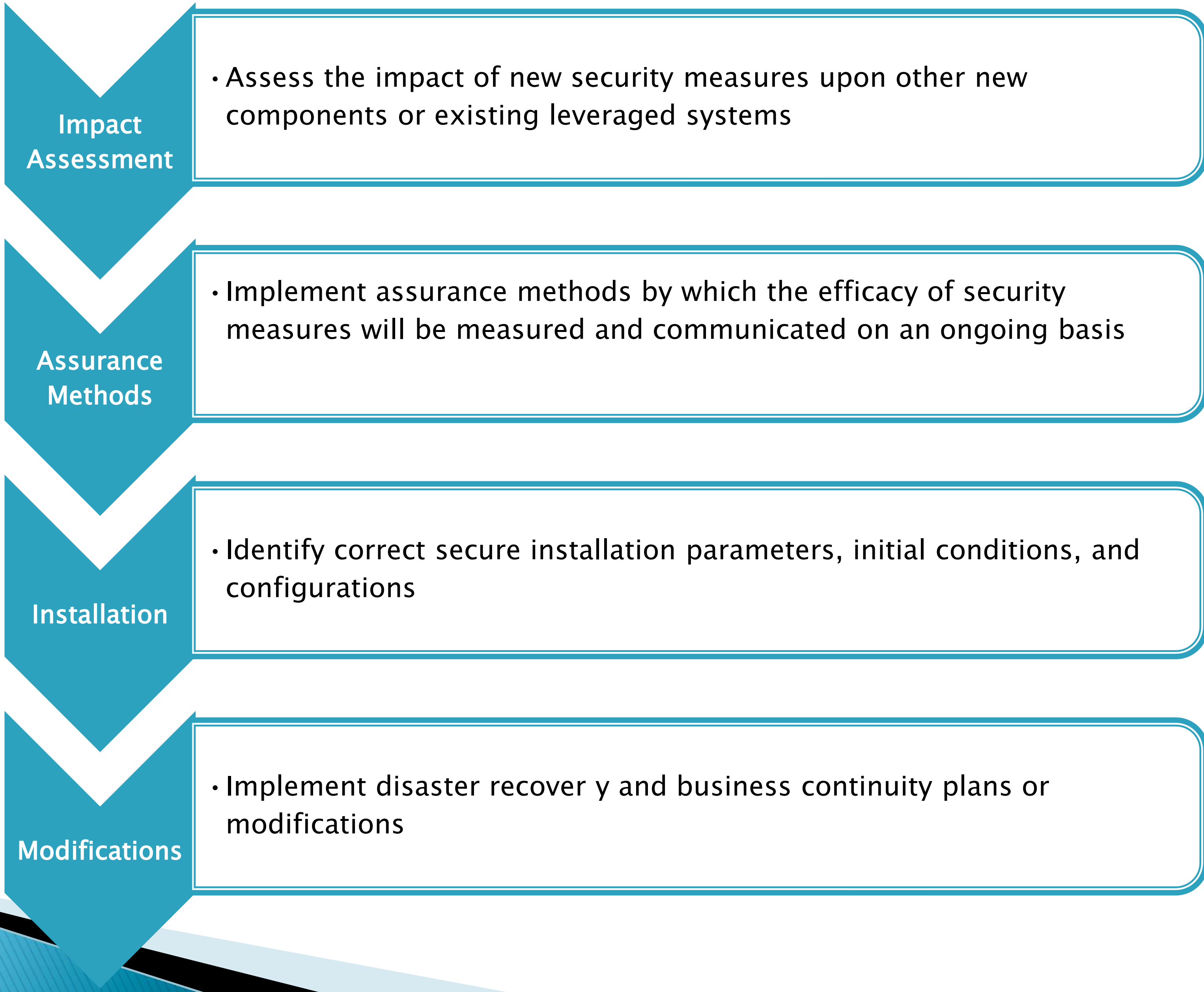
**Re-Use**

- Identify new code/resources/assets that are appropriate for re-use
- It is appropriate to evaluate those new solutions for inclusion into any existing libraries, archives, or other repositories for future re-use.

# Phase F – Migration Planning

# Phase F– Migration Planning


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management



**Impact Assessment**

- Assess the impact of new security measures upon other new components or existing leveraged systems

**Assurance Methods**

- Implement assurance methods by which the efficacy of security measures will be measured and communicated on an ongoing basis

**Installation**

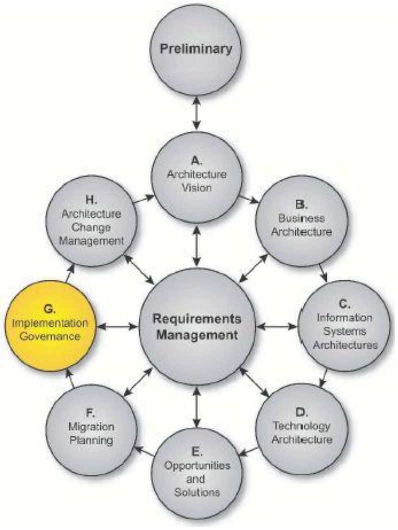
- Identify correct secure installation parameters, initial conditions, and configurations

**Modifications**

- Implement disaster recover y and business continuity plans or modifications

# Phase G – Implementation Governance

# Phase G – Implementation Governance


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

**Review**

- Establish architecture artifact, design, and code reviews and define acceptance criteria for the successful implementation of the findings

**Evidence**

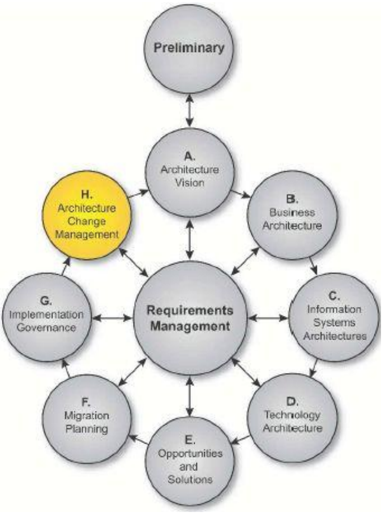
- Implement methods and procedures to review evidence produced by the system that reflects operational stability and adherence to security policies

**Training**

- Implement necessary training to ensure correct deployment, configuration, and operations of security-relevant subsystems and components; ensure awareness training of all users and non-privileged operators of the system and/or its components

# Phase H – Architecture Change

# Phase H– Architecture Change


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

**Requirements**

- Change is driven by new requirements. Changes in security requirements are often more disruptive than a simplification or incremental change.

**Statutes and Regulations**

- Changes in security policy can be driven by statute, regulation, or something that has gone wrong

**Standards**

- Changes in security standards are usually less disruptive since the trade-off for their adoption is based on the value of the change. However, standards changes can also be mandated

# Reference

- TOGAF Version 9, The Open Group Architecture Framework (TOGAF), 2009

If you have one last breath use it to say…