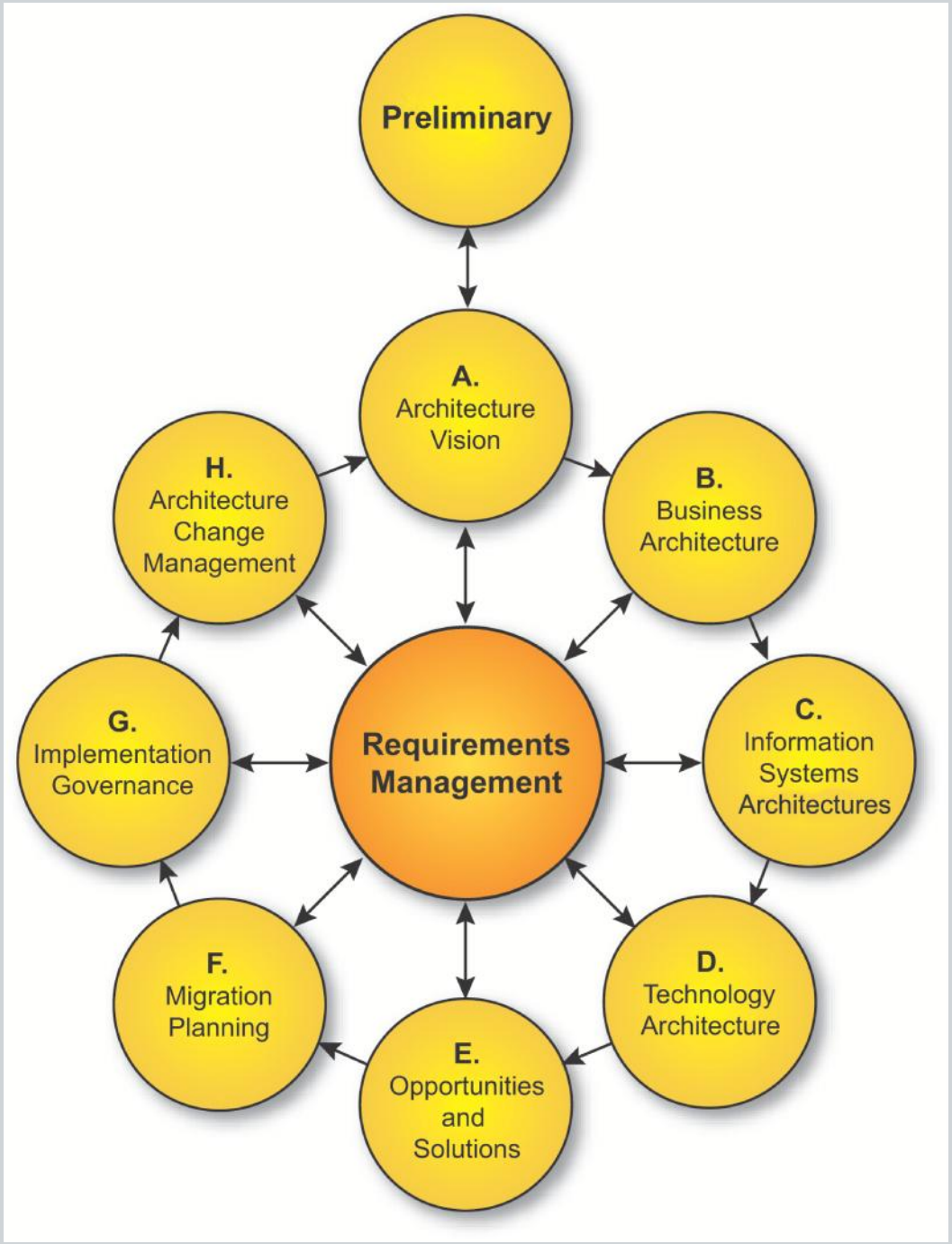
TOGAF®

Version 9.1 Enterprise Edition

Module 31
Adapting the ADM: Security

Published by The Open Group, January 2009



Adapting the ADM: Security

TOGAF®

Roadmap

Part I - Introduction
Preface, Executive Overview, Core Concepts, Definitions and Release Notes
Part II – Architecture Development Method
Introduction to ADM
ADM Phase Narratives
Part III – ADM Guidelines and Techniques
Guidelines for Adapting the ADM Process
Techniques for Architecture Development
Part IV – Architecture Content Framework
Content Metamodel
Architectural Artifacts
Architecture Deliverables
Building Blocks
Part V – Enterprise Continuum and Tools
Enterprise Continuum
Architecture Partitioning
Architecture Repository
Tools for Architecture Development
Part VI – Reference Models
Foundation Architecture: Technical Reference Model
Integrated Information Infrastructure Reference Model
Part VII – Architecture Capability Framework
Architecture Board
Architecture Compliance
Architecture Contracts
Architecture Governance
Architecture Maturity Models
Architecture Skills Framework

- Part III, ADM Guidelines and Techniques, Chapter 21

Module Objectives

The objectives of this module are:

- Obtain an understanding of the security considerations that need to be addressed during application of the ADM

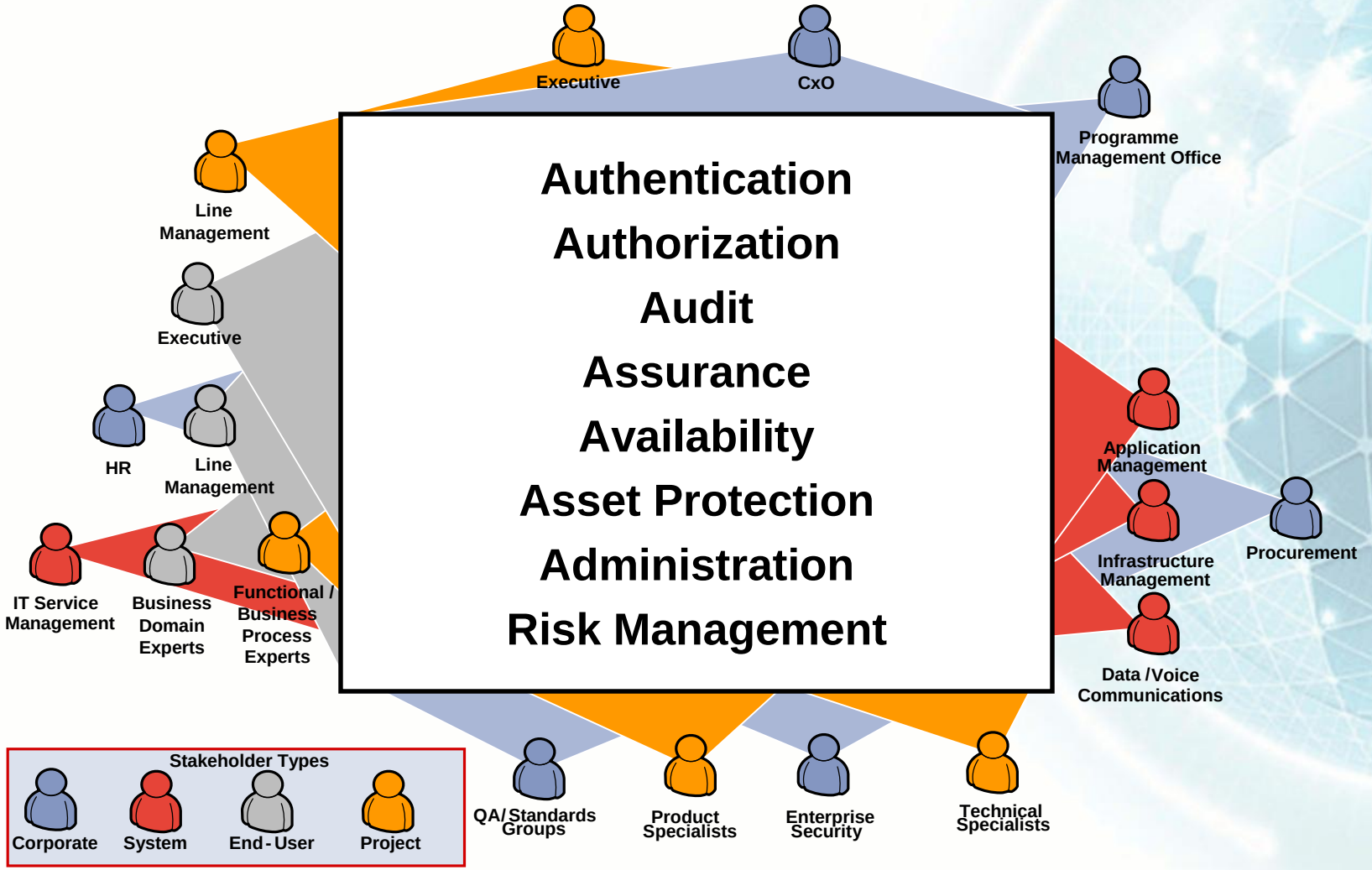
Security and the ADM

- TOGAF introduces guidance to help practitioners avoid missing critical security concerns
- The guidance is not intended to be a security architecture development methodology
- It is intended to inform the enterprise architect of the security architecture task and role
- Security objectives have been developed for each ADM Phase

Security Architecture Characteristics

- It has its own discrete security methodology
- It composes its own discrete view and viewpoints
- It addresses non-normative flows
- It introduces its own unique normative flows
- Introduces unique, single-purpose components in the design.
- It calls for its own unique set of skill requirements in the enterprise architect

Stakeholder Concerns



TOGAF®

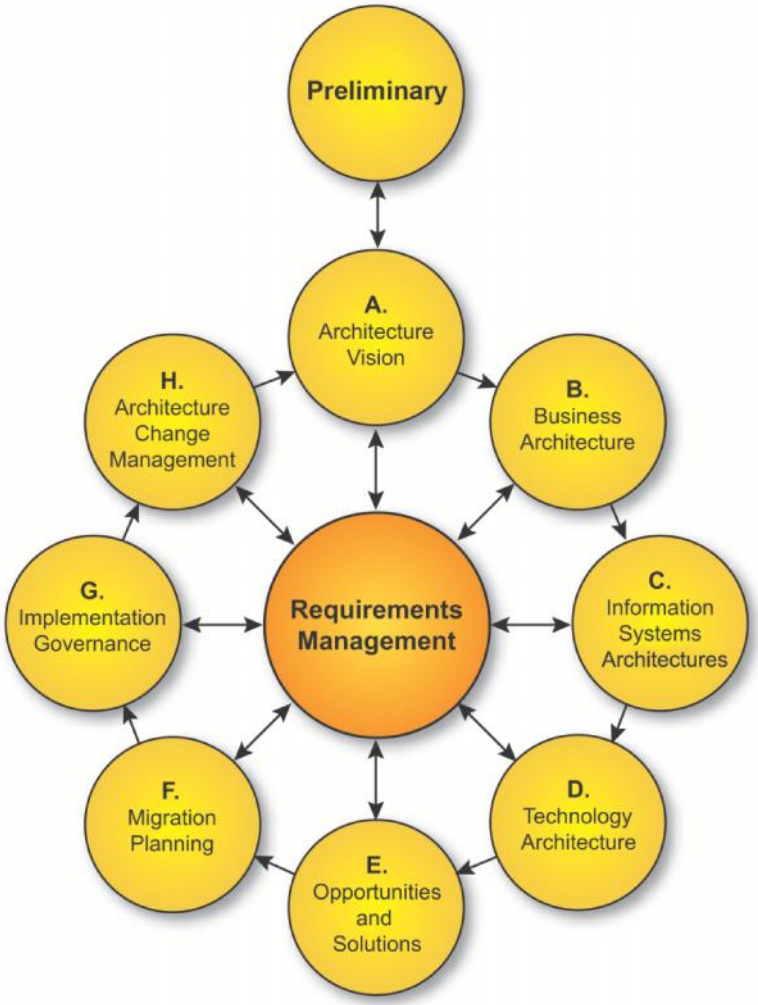
Security Areas of Concern

- **Authentication**: The substantiation of the identity of a person or entity related to the system in some way.
- **Authorization**: The definition and enforcement of permitted capabilities for a person or entity whose identity has been established.
- **Audit**: The ability to provide forensic data attesting that the system was used in accordance with stated security policies.
- **Assurance**: The ability to test and prove that the system has the security attributes required to uphold the stated security policies.
- **Availability**: The ability of the system to function without service interruption or depletion despite abnormal or malicious events.
- **Asset Protection**: The protection of information assets from loss or unintended disclosure, and resources from unauthorized and unintended use.
- **Administration**: The ability to add and change security policies, add or change how policies are implemented in the system, and add or change the persons or entities related to the system.
- **Risk Management**: The organization's attitude and tolerance for risk.

Typical Security Artifacts

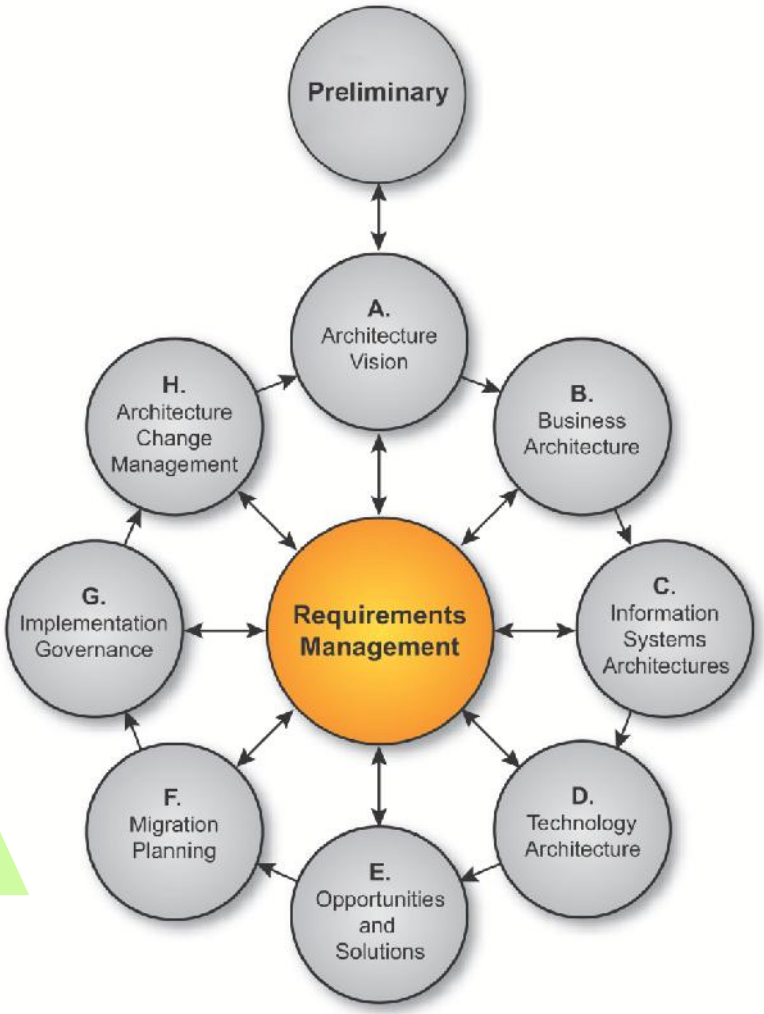
- Business rules regarding handling of data/information assets
- Written and published security policy
- Codified data/information asset ownership and custody
- Risk analysis documentation
- Data classification policy documentation

TOGAF ADM



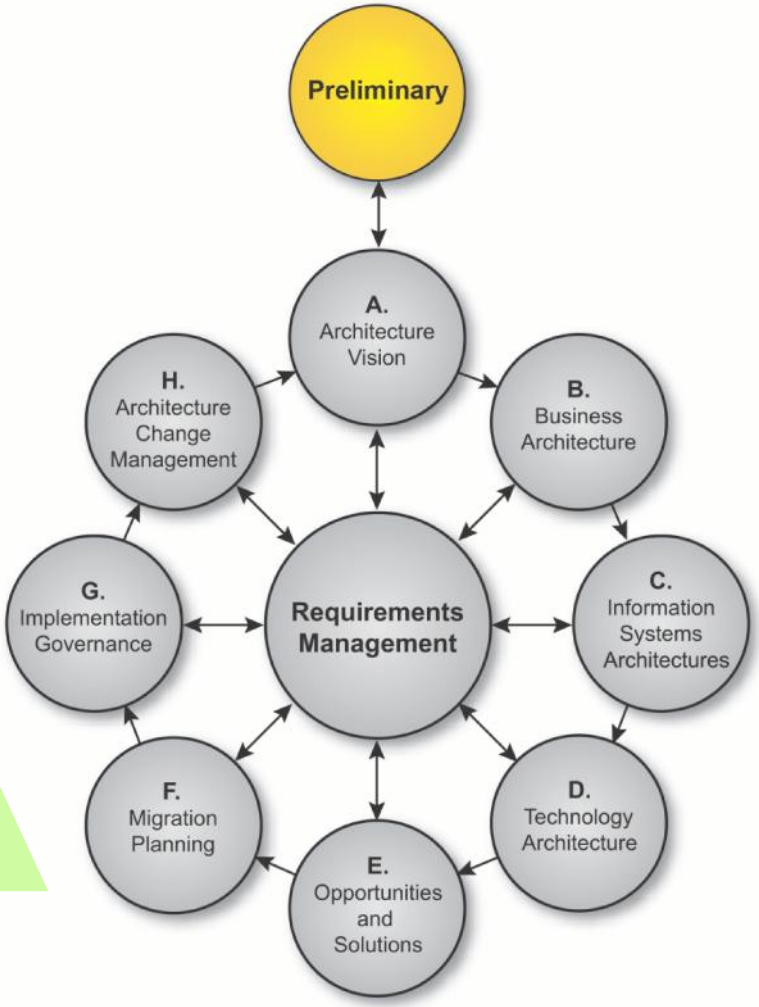
TOGAF®

ADM Requirements Management



- Security Policy and Security Standards become part of the requirements management process
- New Security requirements arise from many sources:
  - A new statutory or regulatory mandate
  - A new threat realized or experienced
  - A new architecture initiative discovers new stakeholders with new requirements

Preliminary Phase

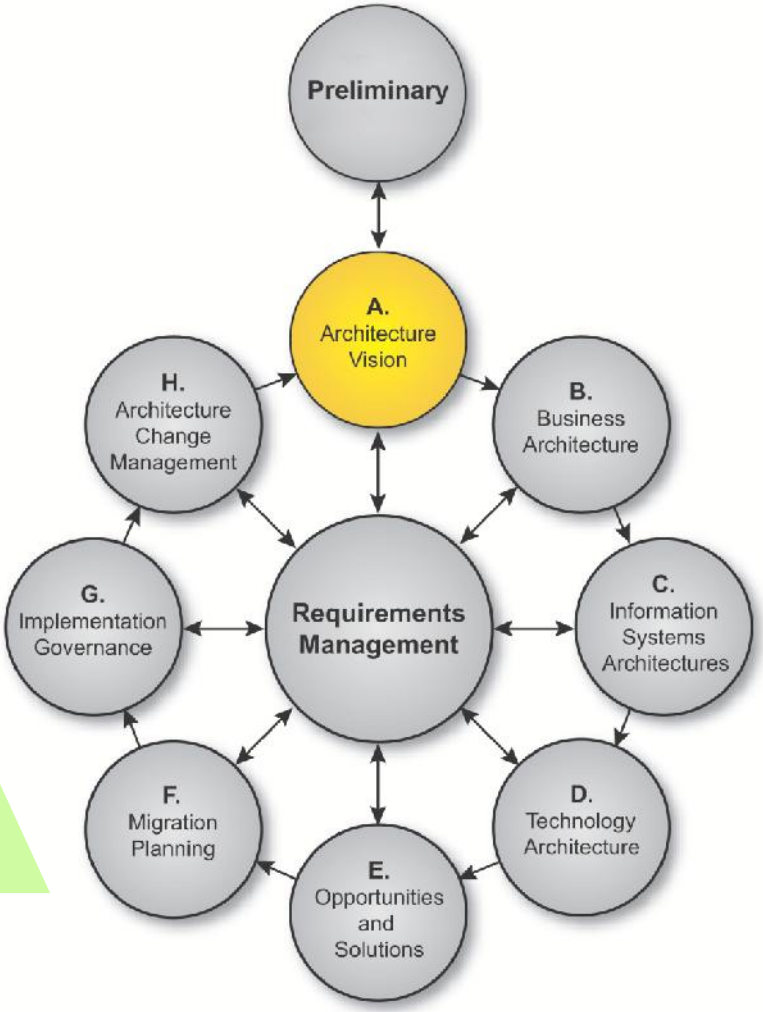


- Scope the enterprise organization units impacted by the security architecture
- Define and document applicable regulatory and security policy requirements
- Define the required security capability as part of the Architecture Capability
- Implement security architecture tools

Preliminary Phase – Inputs/Outputs

- Inputs:
  - Written security policy
  - Relevant statutes
  - List of applicable jurisdictions
- Outputs:
  - List of applicable regulations
  - List of applicable security policies
  - Security team roster
  - List of security assumptions and boundary conditions

Phase A
Architecture Vision



- Obtain management support for security measures
- Define necessary security-related management sign-off milestones
- Determine applicable disaster recovery or business continuity requirements
- Identify anticipated physical/ business, regulatory environments in which the systems will be deployed
- Determine the criticality of the system: safety-critical, mission-critical, non-critical

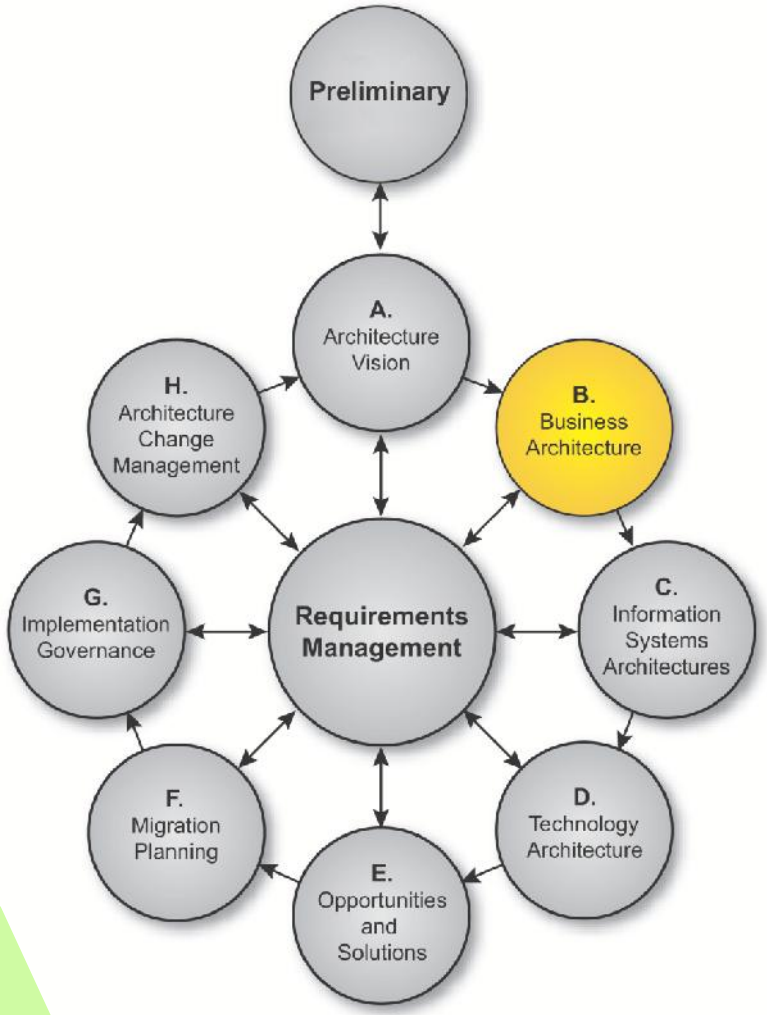
TOGAF®

Phase A
Architecture Vision – Inputs/Outputs

- Inputs
  - List of applicable security policies
  - List of applicable jurisdictions
  - Complete disaster recovery and continuity plans

- Outputs
  - Physical security statement
  - Business security statement
  - Regulatory security statement
  - Security policy cover letter signed by CEO or delegate
  - List of architecture development checkpoints
  - List of disaster recovery and business continuity plans
  - Systems criticality statement

Phase B
Business Architecture

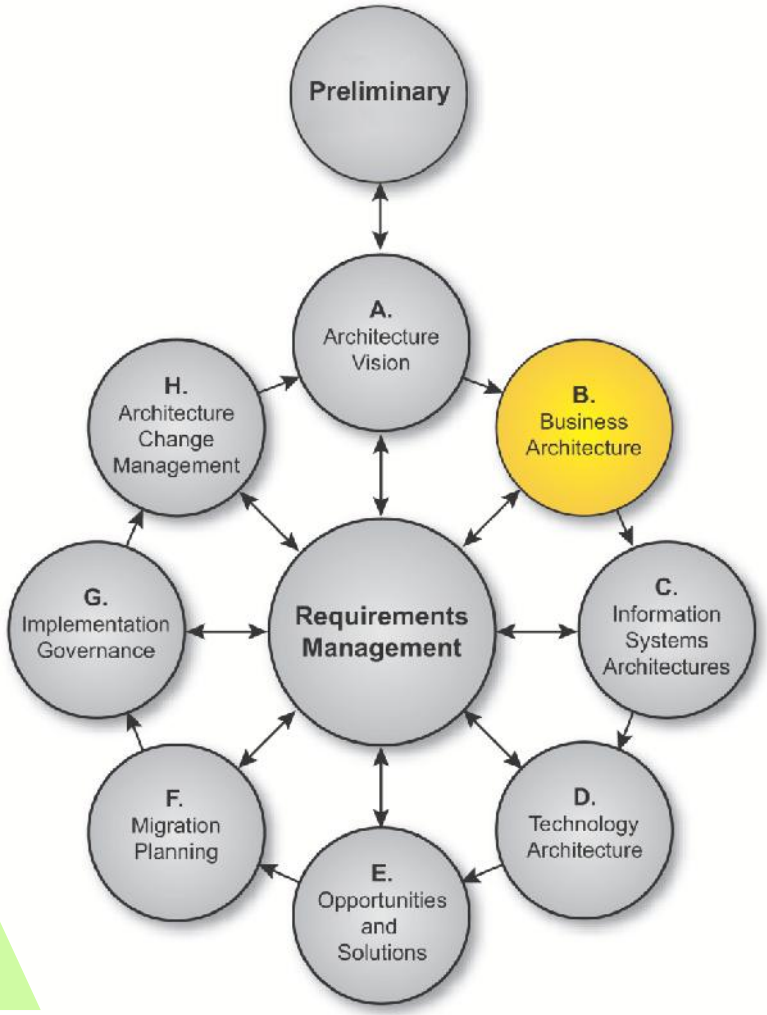


- Determine who are the legitimate actors who will interact with the system
- Assess and baseline current security-specific business processes
- Determine whom/how much it is acceptable to inconvenience with security measures
- Identify and document interconnecting systems beyond project control
- Determine the assets at risk if something goes wrong
- Determine the cost of asset loss/impact in failure cases
- Identify and document the ownership of assets

Continued

TOGAF®

Phase B
Business Architecture



- Determine and document appropriate security forensic processes
- Identify the criticality of the availability and correct operation of the overall service
- Determine and document how much security (cost) is justified by the threats and value of the assets
- Reassess and confirm Architecture Vision decisions
- Assess alignment or conflict of identified security policies with business goals
- Determine “what can go wrong?”

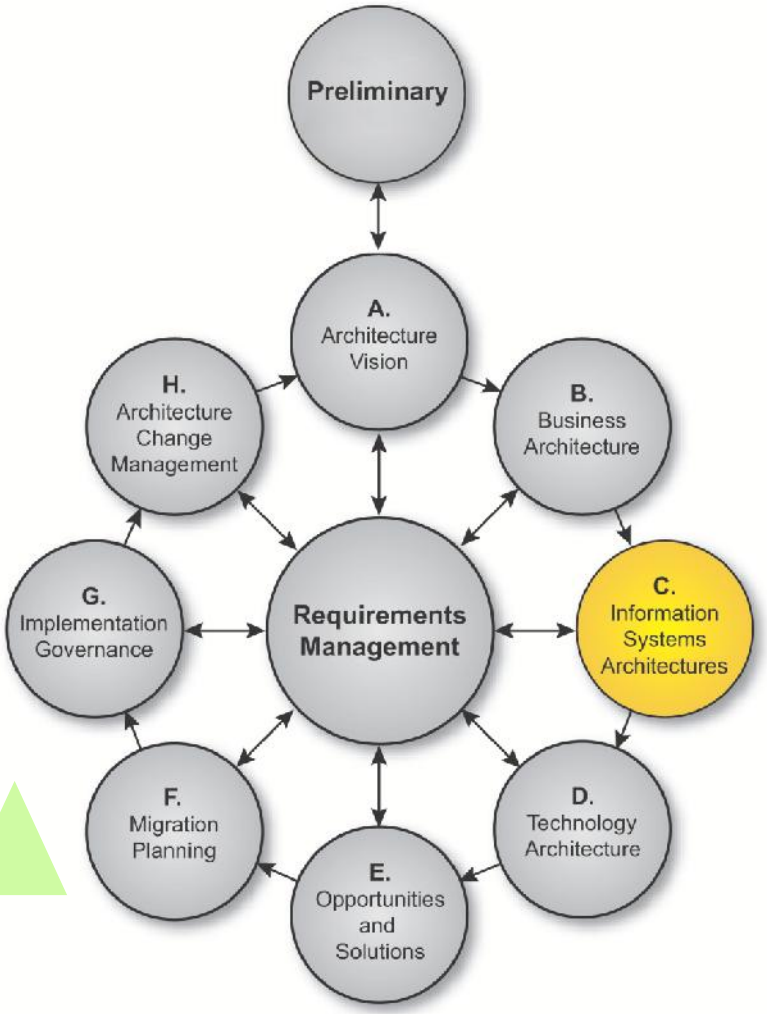
TOGAF®

Phase B: Business Architecture – Inputs/Outputs

- Inputs
  - Initial business and regulatory security statements
  - List of applicable disaster recovery and business continuity plans
  - List of applicable security policies and regulations

- Outputs
  - List of forensic processes
  - List of new disaster recovery and business continuity requirements
  - Validated business and regulatory environment statements
  - List of validated security policies and regulations
  - List of target security processes
  - List of baseline security processes
  - List of security actors
  - List of interconnecting systems
  - Statement of security tolerance for each class of security actor
  - Asset list with values and owners
  - List of trust paths
  - Availability impact statement(s)
  - Threat analysis matrix

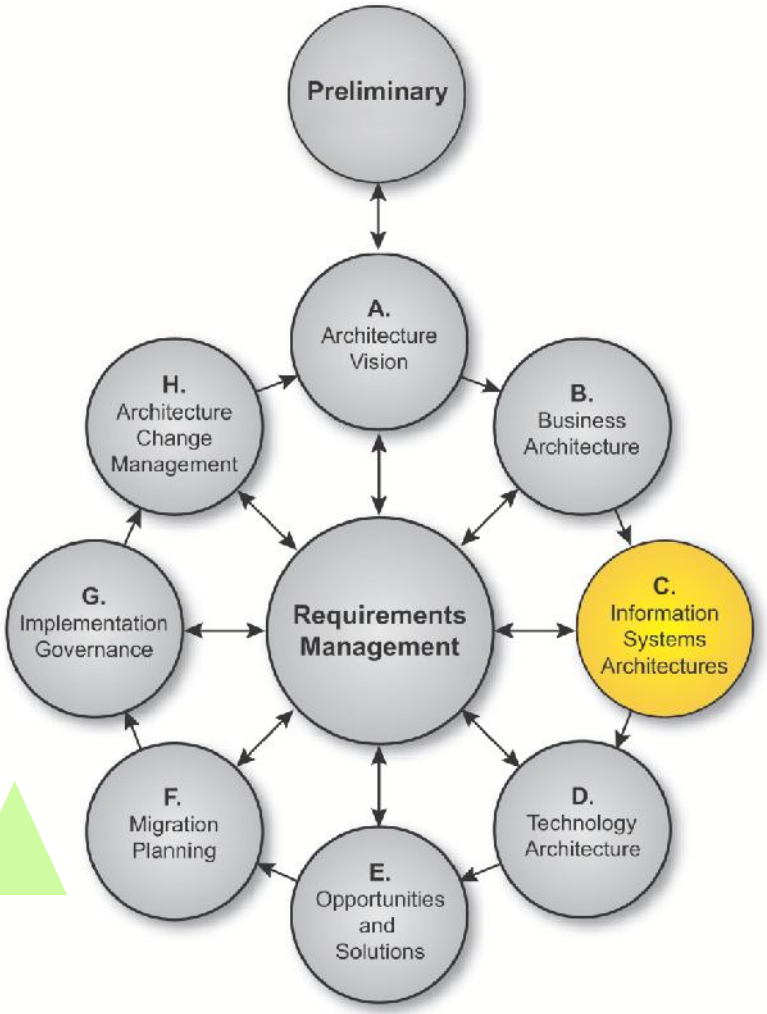
Phase C
Information Systems Architectures



- Assess and baseline current security-specific architecture elements
- Identify safe default actions and failure states
- Identify and evaluate applicable recognized guidelines and standards
- Revisit assumptions regarding interconnecting systems beyond project control
- Determine and document the sensitivity or classification level of information stored/created/used
- Identify and document custody of assets

Continued

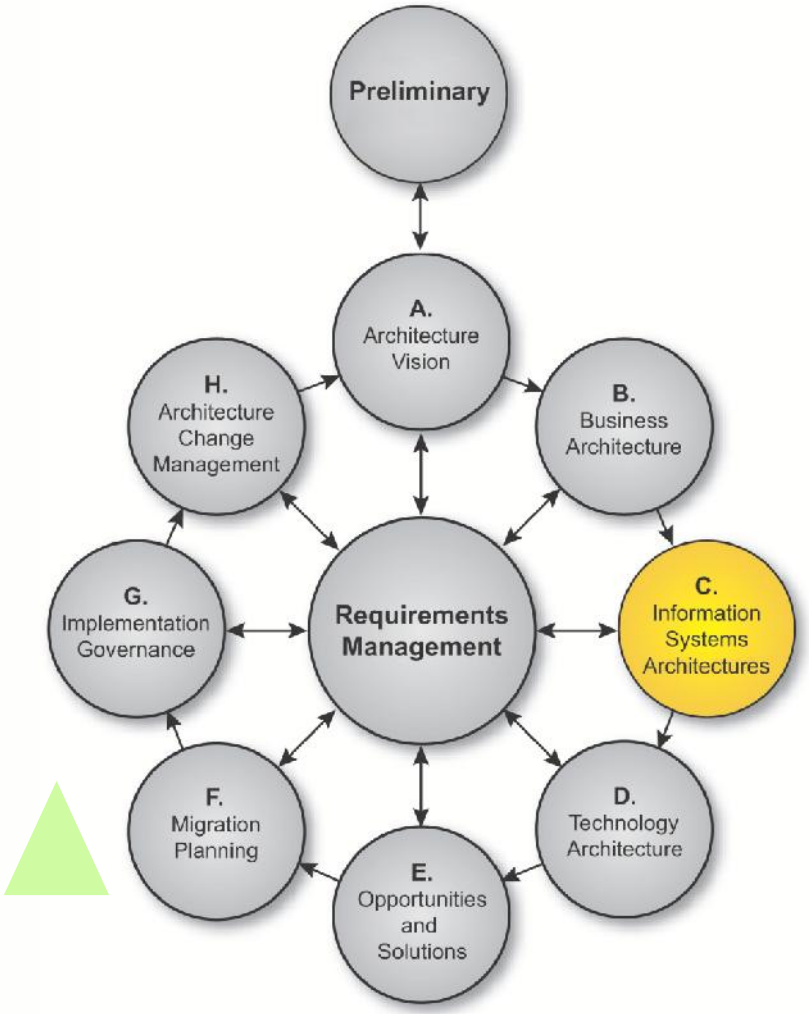
Phase C
Information Systems Architectures



- Identify the criticality of the availability and correct operation of each function
- 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
- Identify lifespan of information used as defined by business needs and regulatory requirements

Continued

Phase C
Information Systems Architectures



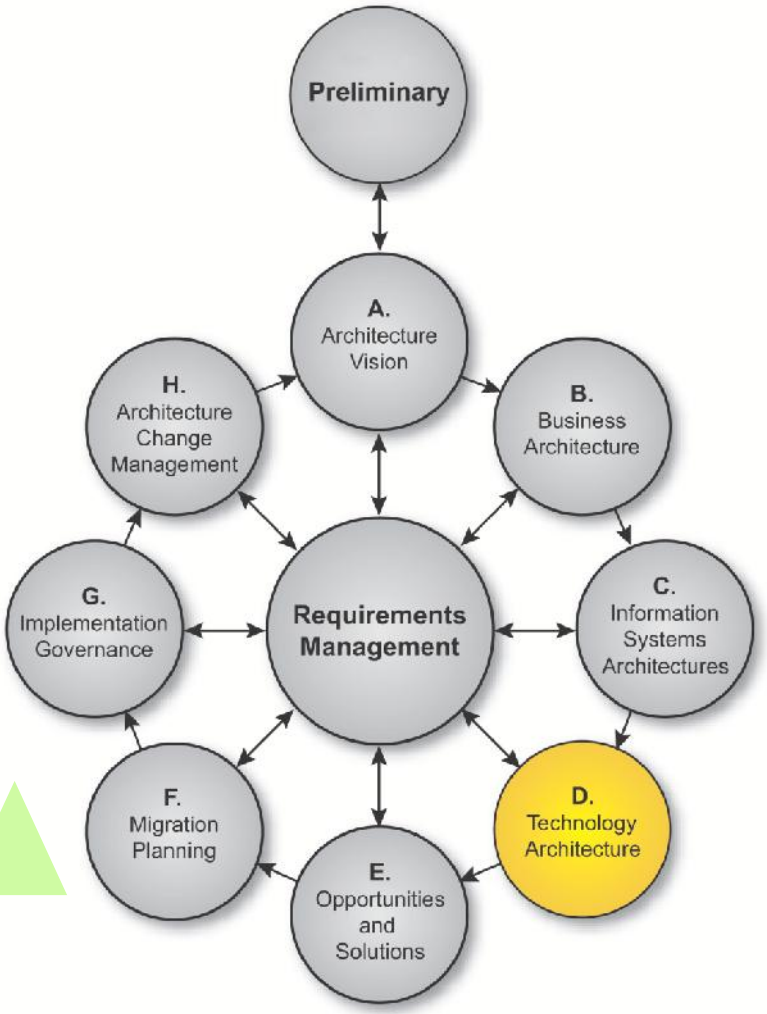
- Determine approaches to address identified risks
- Identify actions/events that warrant logging for later review or triggering forensic processes
- Identify and document requirements for rigor in proving accuracy of logged events (non-repudiation)
- Identify potential/likely avenues of attack
- Determine "what can go wrong?"

Phase C: Information Systems Architectures – Inputs/Outputs

- Inputs
  - Threat analysis matrix
  - Risk analysis
  - Documented forensic processes
  - Validated business policies and regulations
  - List of interconnecting systems
  - New disaster recovery and business continuity requirements

- Outputs
  - Event log-level matrix and requirements
  - Risk management strategy
  - Data lifecycle definitions
  - List of configurable system elements
  - Baseline list of security-related elements of the system
  - New or augmented security-related elements of the system
  - Security use-case models
  - List of applicable security standards:
  - Validated interconnected system list
  - Information classification report
  - List of asset custodians
  - Function criticality statement
  - Revised disaster recovery and business continuity plans
  - Refined threat analysis matrix

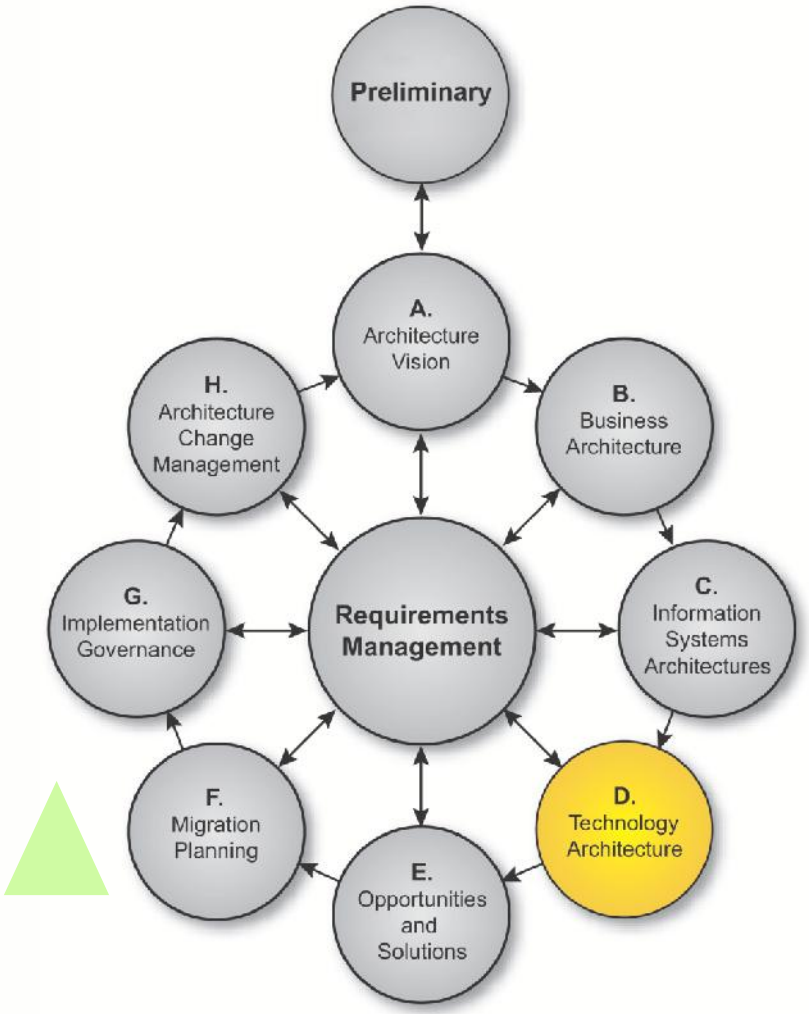
Phase D
Technology Architecture



- Assess and baseline current security-specific technologies
- Revisit assumptions regarding interconnecting systems beyond project control
- Identify and evaluate applicable recognized guidelines and standards
- 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

Continued

Phase D
Technology Architecture



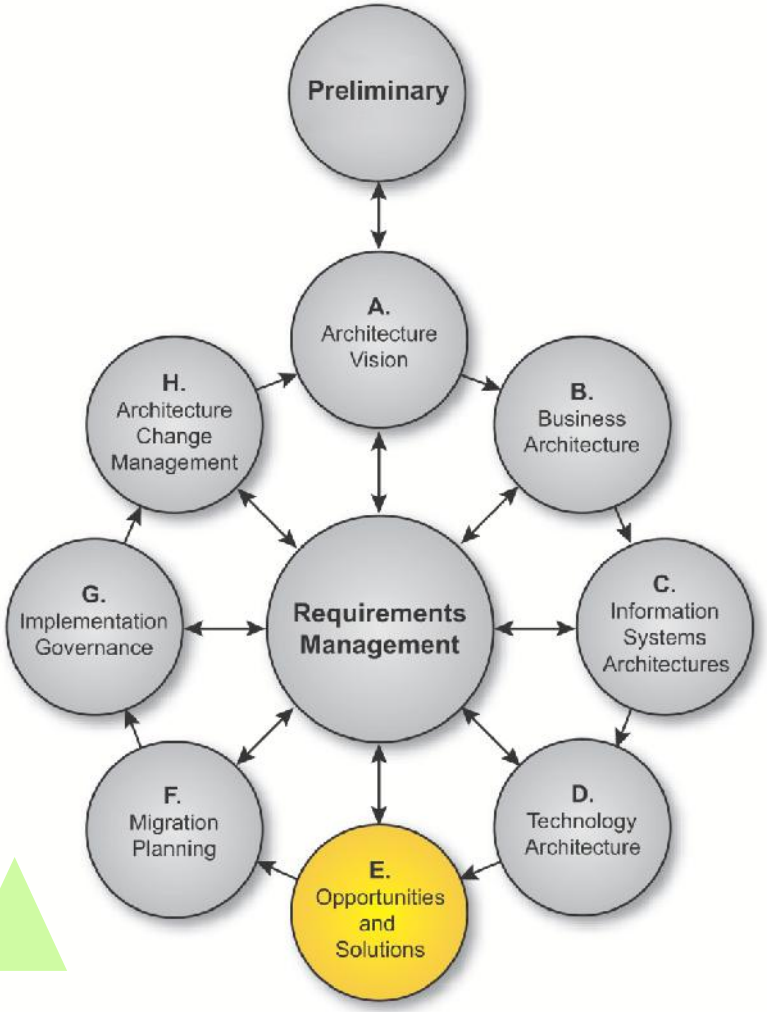
- Identify the trust (clearance) levels for the system
- Identify minimal privileges required for any entity to achieve a technical or business objective
- Identify mitigating security measures, where justified by risk assessment
- Determine "what can go wrong?"

TOGAF®

Phase D: Technology Architecture – Inputs/Outputs

- Inputs
  - List of security-related elements of the system
  - List of interconnected systems
  - List of applicable security standards
  - List of security actors
  - Risk management strategy
  - Validated security policies
  - Validated regulatory requirements
  - Validated business policies related to trust requirements
- Outputs
  - Baseline list of security technologies
  - Validated interconnected systems list
  - Selected security standards list
  - Resource conservation plan
  - Security metrics and monitoring plan
  - User authorization policies
  - Risk management plan
  - User trust (clearance) requirements

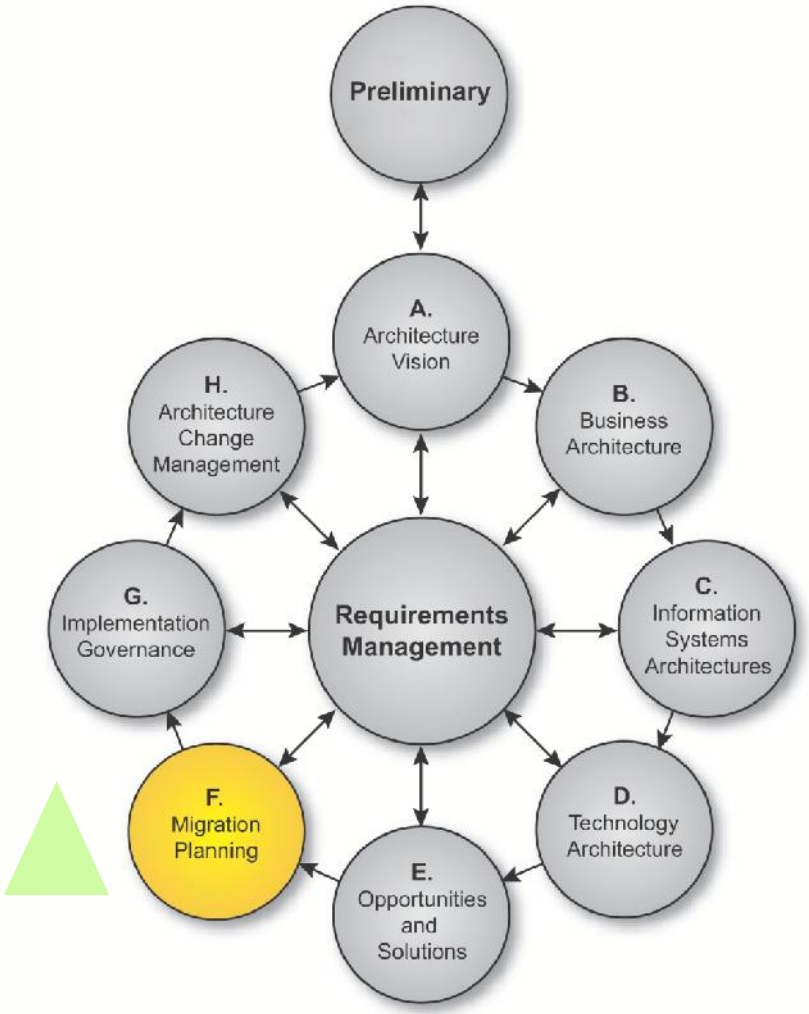
Phase E
Opportunities and Solutions



- Identify existing security services available for re-use
- Engineer mitigation measures addressing identified risks
- Evaluate tested and re-usable security software and resources
- Identify new code/resources/assets appropriate for re-use
- Determine “what can go wrong?”

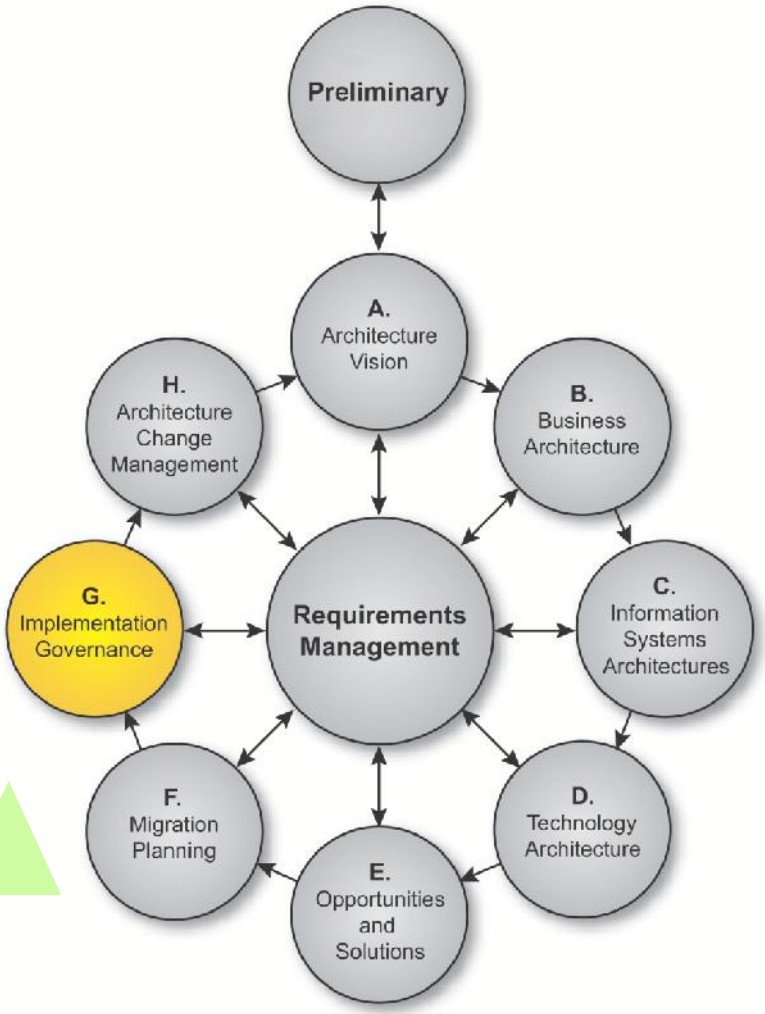
TOGAF®

Phase F
Migration Planning



- Assess the impact of new security measures upon other new components or existing systems
- Implement assurance methods by which the efficacy of security measures will be measured and communicated on an ongoing basis
- Identify correct secure installation parameters, initial conditions, and configurations
- Implement disaster recovery and business continuity plans
- Determine "what can go wrong?"

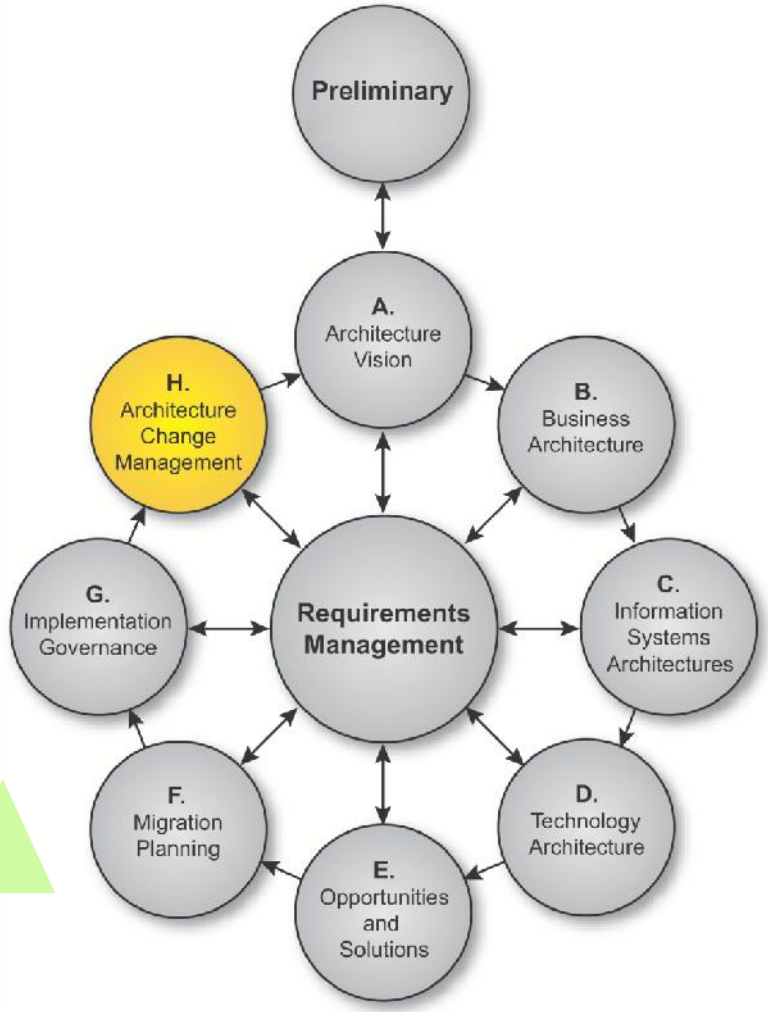
Phase G
Implementation Governance



- Establish design and code reviews
- Implement methods and procedures to review evidence that reflects operational stability and adherence to security policies
- Implement training to ensure correct deployment, configuration and operations
- Determine “What has gone wrong?”

TOGAF®

Phase H
Architecture Change Management



- Determine “What has gone wrong?”
- Incorporate security-relevant changes to the environment into the requirements for future enhancement

Summary

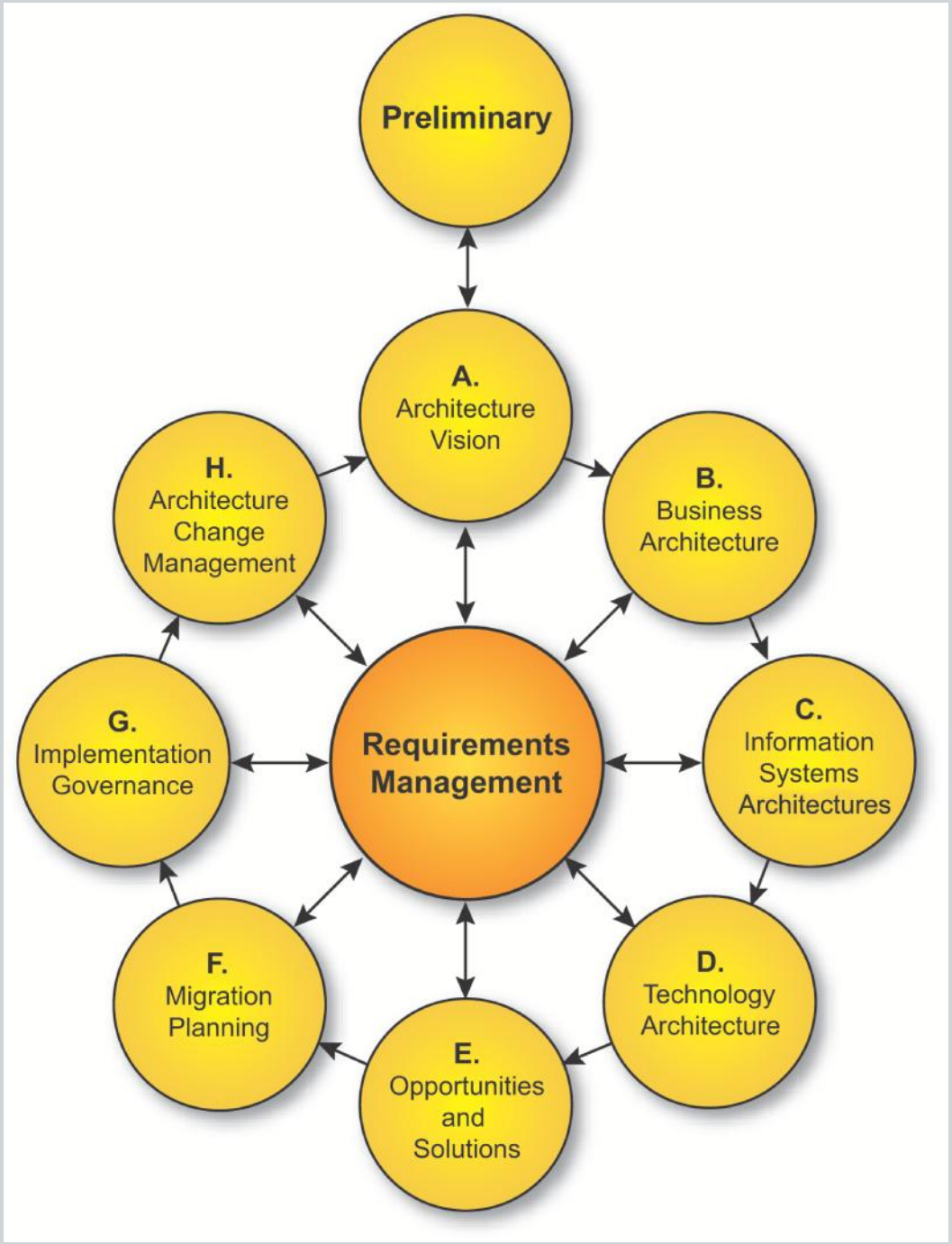
- TOGAF introduces guidance on Security and the ADM to help practitioners avoid missing a critical security concern
- The guidance is not intended to be a security architecture development methodology
- It is intended to inform the enterprise architect of the security architecture task and role

Exercise

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**

For each of these discuss its impact on the ADM.



Adapting the ADM: Security

TOGAF®