Enterprise Security Architecture for Cyber Security

M.M.Veeraragaloo

5th September 2013

Outline

- Cyber Security Overview
- TOGAF and Sherwood Applied Business Security Architecture (SABSA)
  - Overview of SABSA
  - Integration of TOGAF and SABSA
- Enterprise Security Architecture Framework

Cyber Security

1. What is Cyber Security?
2. How is Cyber Security related to information security?
3. How do I protect my company from malicious attacks?

"Cyber Security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the **availability** and reliability of the ICT, breach of the **confidentiality** of information stored in ICT or damage to the **integrity** of that information." (The National Cyber Security Strategy 2011, Dutch Ministry of Security and Justice)

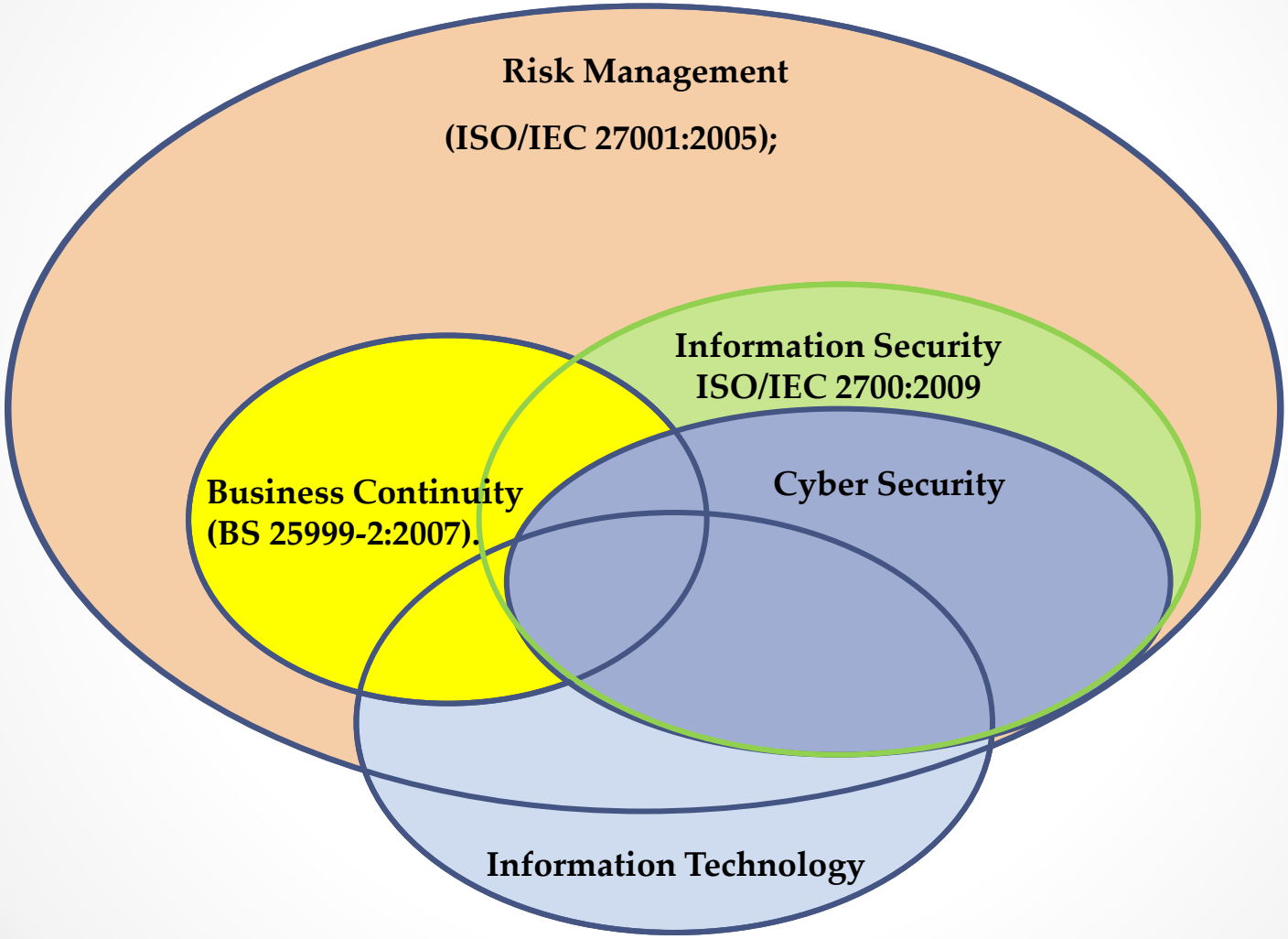
Information security - the "preservation of **confidentiality**, **integrity** and **availability** of information" (ISO/IEC 27001:2005);

The Four Types of Security Incidents

1. Natural Disaster
2. Malicious Attack (External Source)
3. Internal Attack
4. Malfunction and Unintentional Human Error

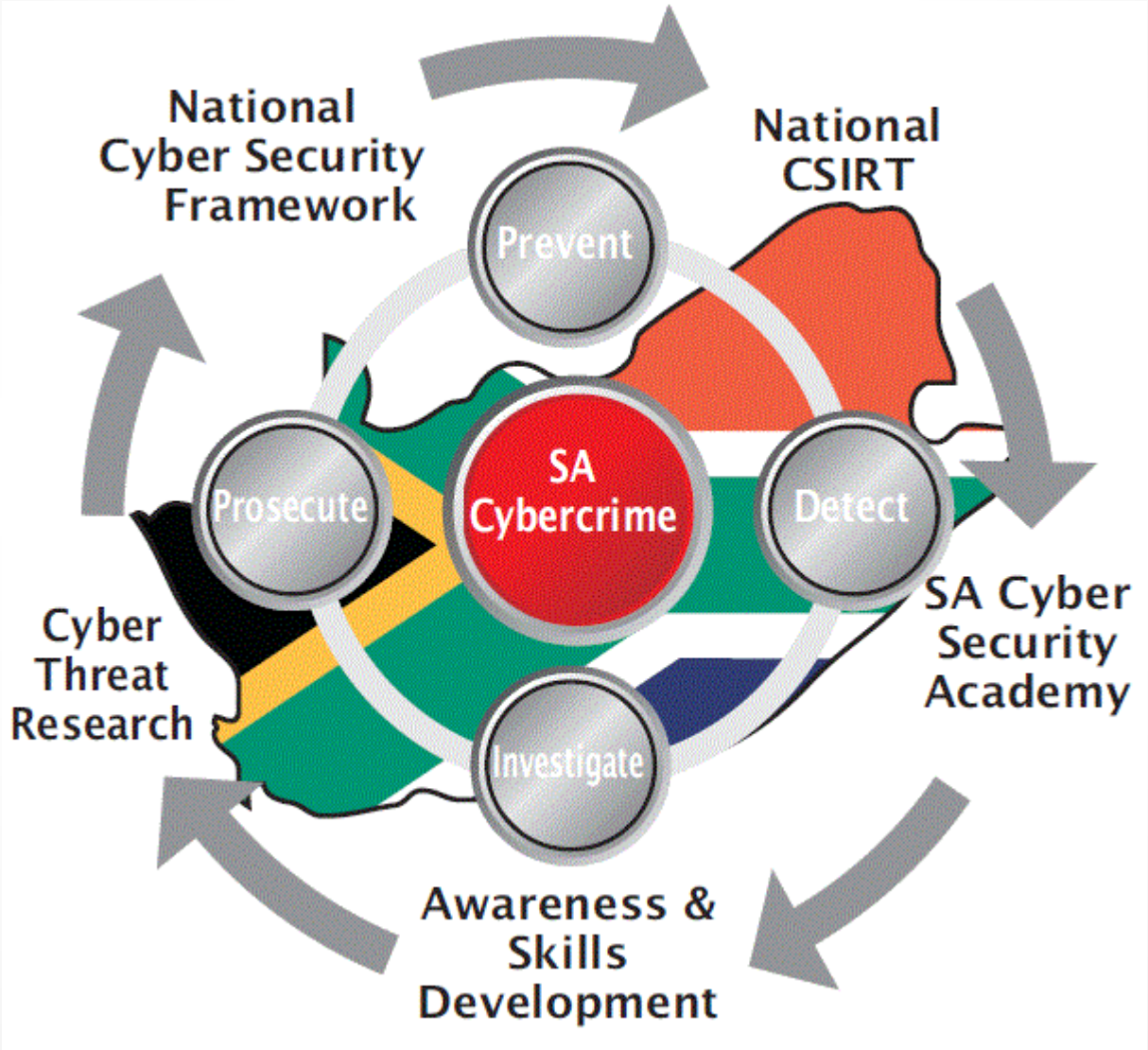
Cyber Security in Perspective

No official position about the differences between Cyber Security and Information Security



Source: 9 Steps to Cyber Security – The Manager's Information Security Strategy Manual (Dejan Kosutic)

Cyber Security in South Africa

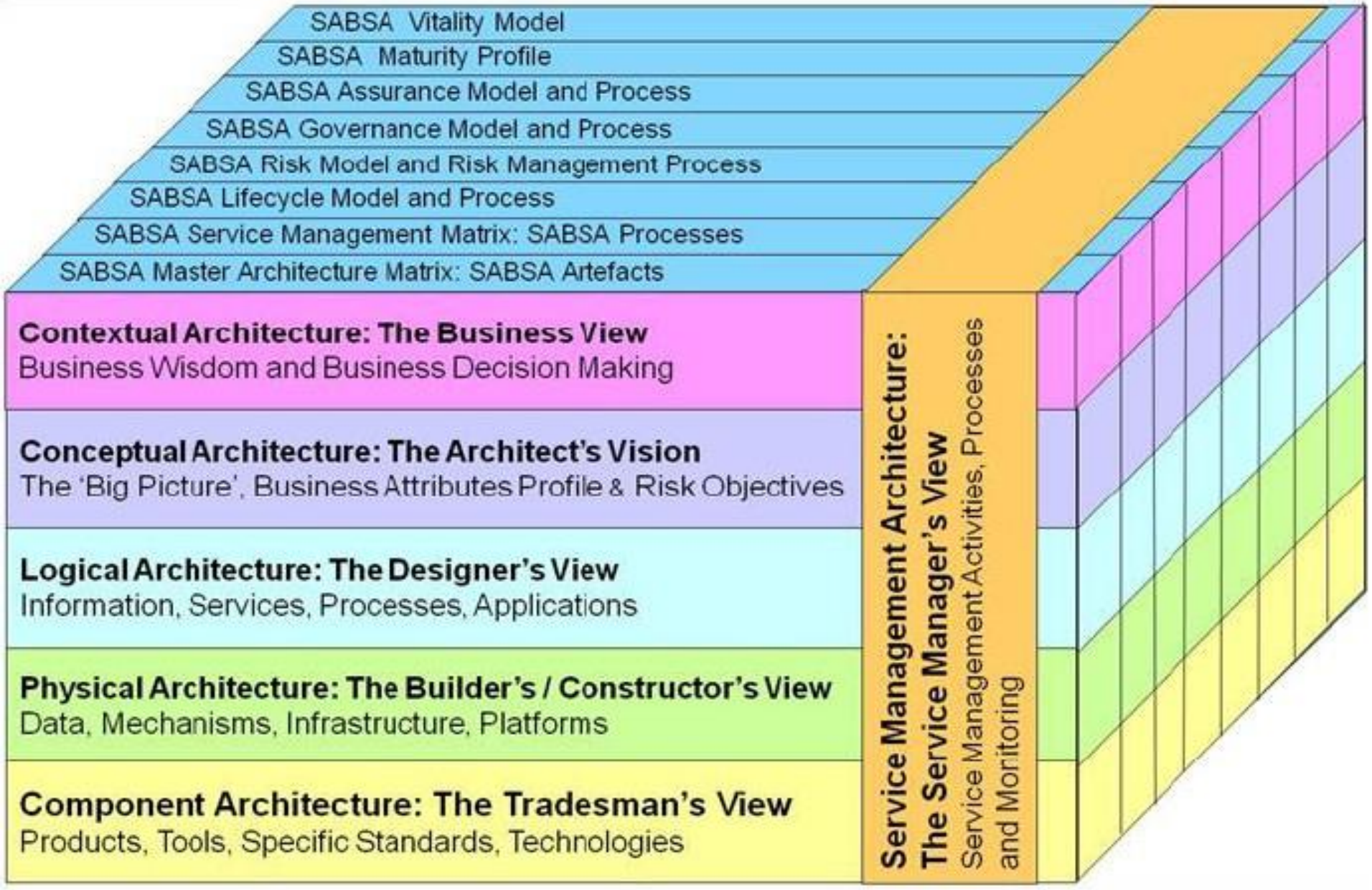


Source: SA-2012-cyber-threat (Wolf Pack) [2012/2013 The South African Cyber Threat Barometer]

TOGAF & SABSA

SABSA Overview

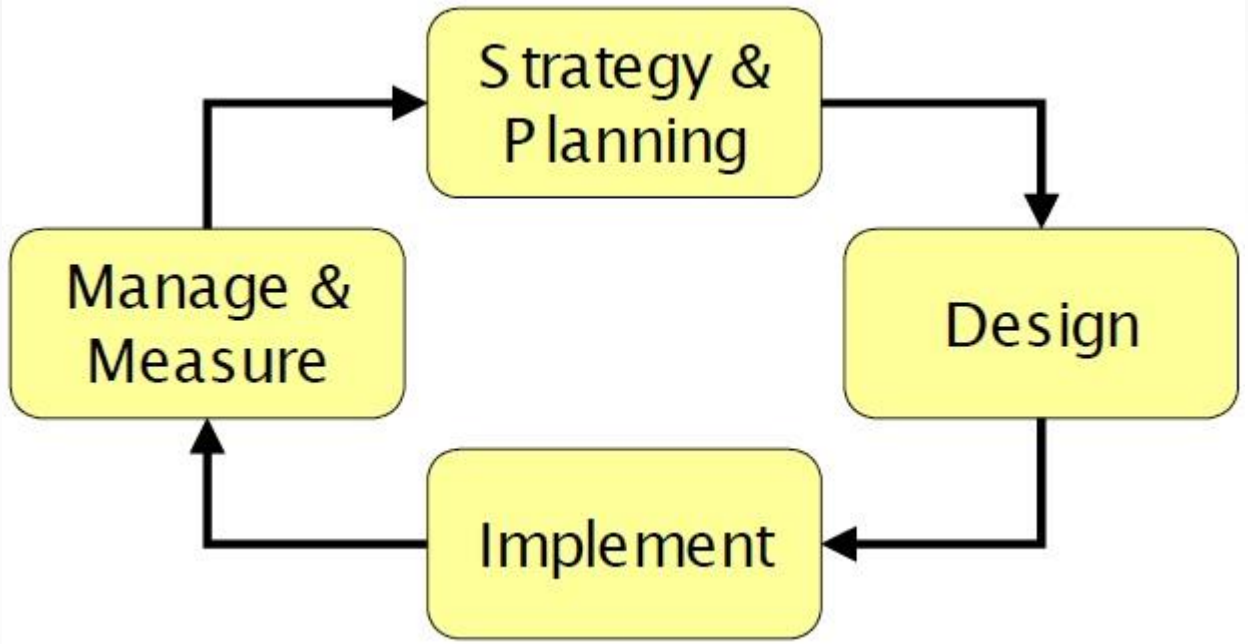
SABSA Meta Model



SABSA Matrix

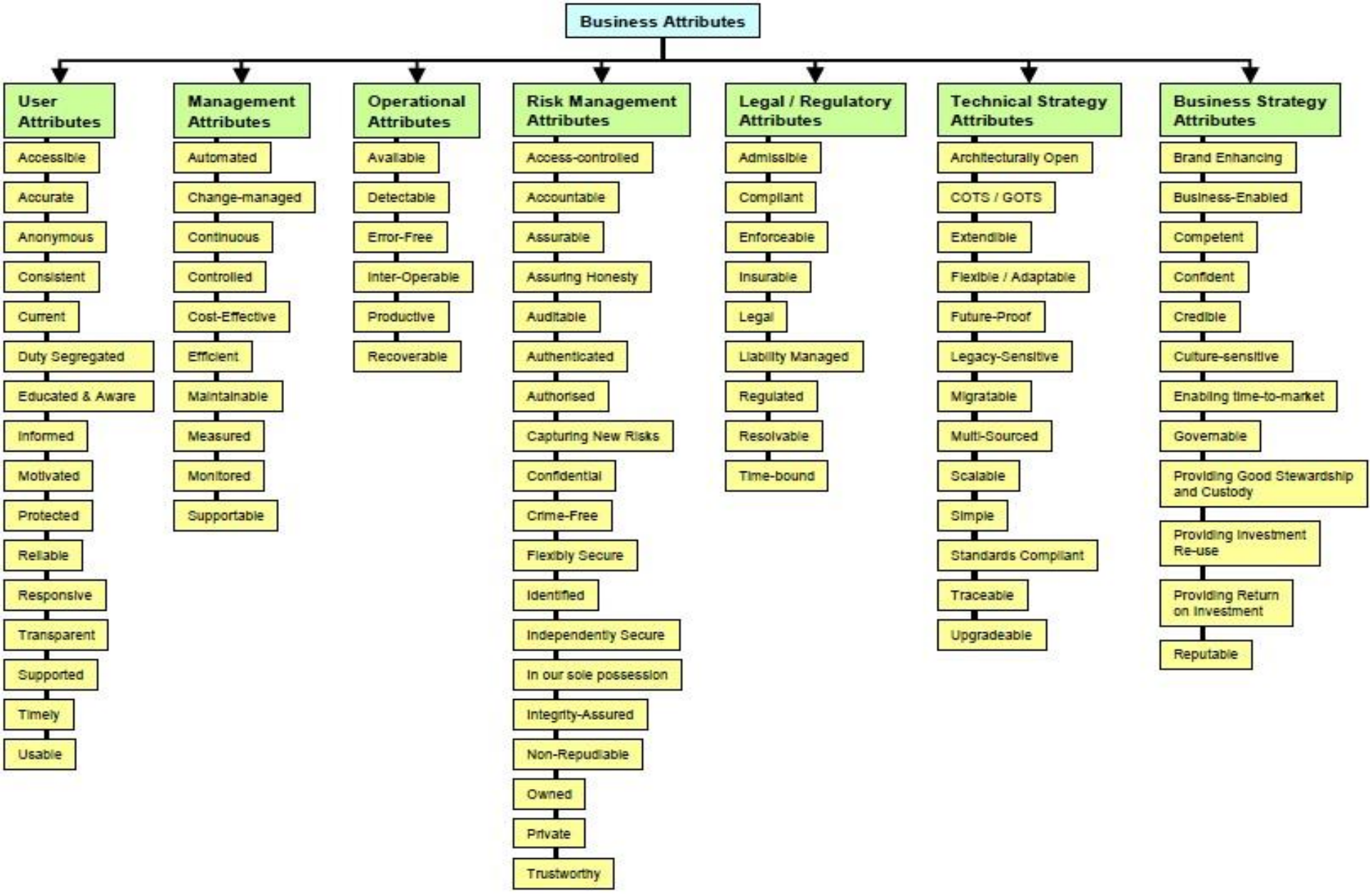
	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

SABSA Life Cycle

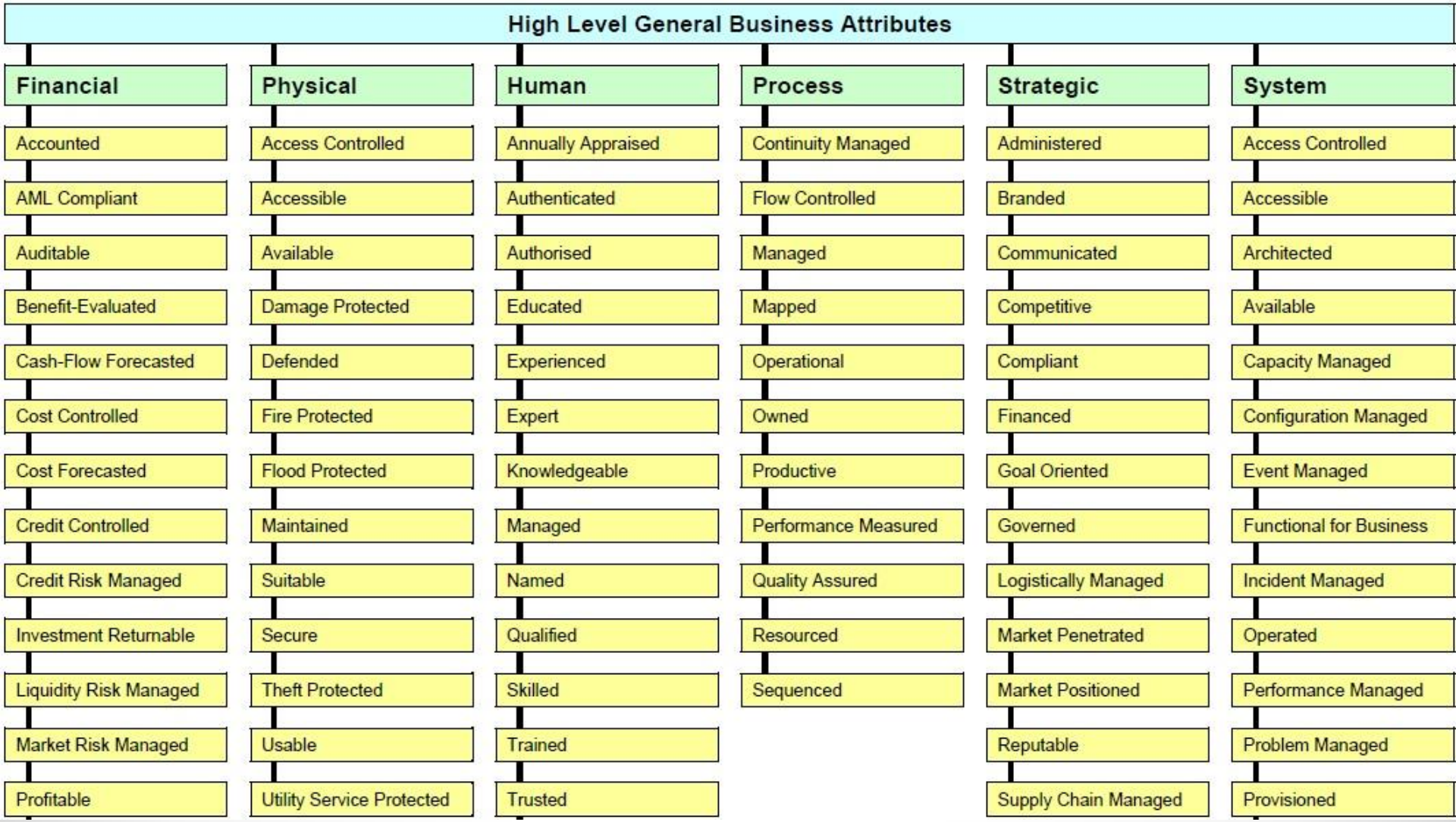


In the SABSA Lifecycle, the development of the **contextual** and **conceptual** layers is grouped into an activity called **Strategy & Planning**. This is followed by an activity called **Design**, which embraces the design of the **logical, physical**, **component**, and **service management architectures**. The third activity is Implement, followed by Manage & Measure. The significance of the Manage & Measure activity is that once the system is operational, it is essential to measure actual performance against targets, to manage any deviations observed, and to feed back operational experience into the iterative architectural development process.

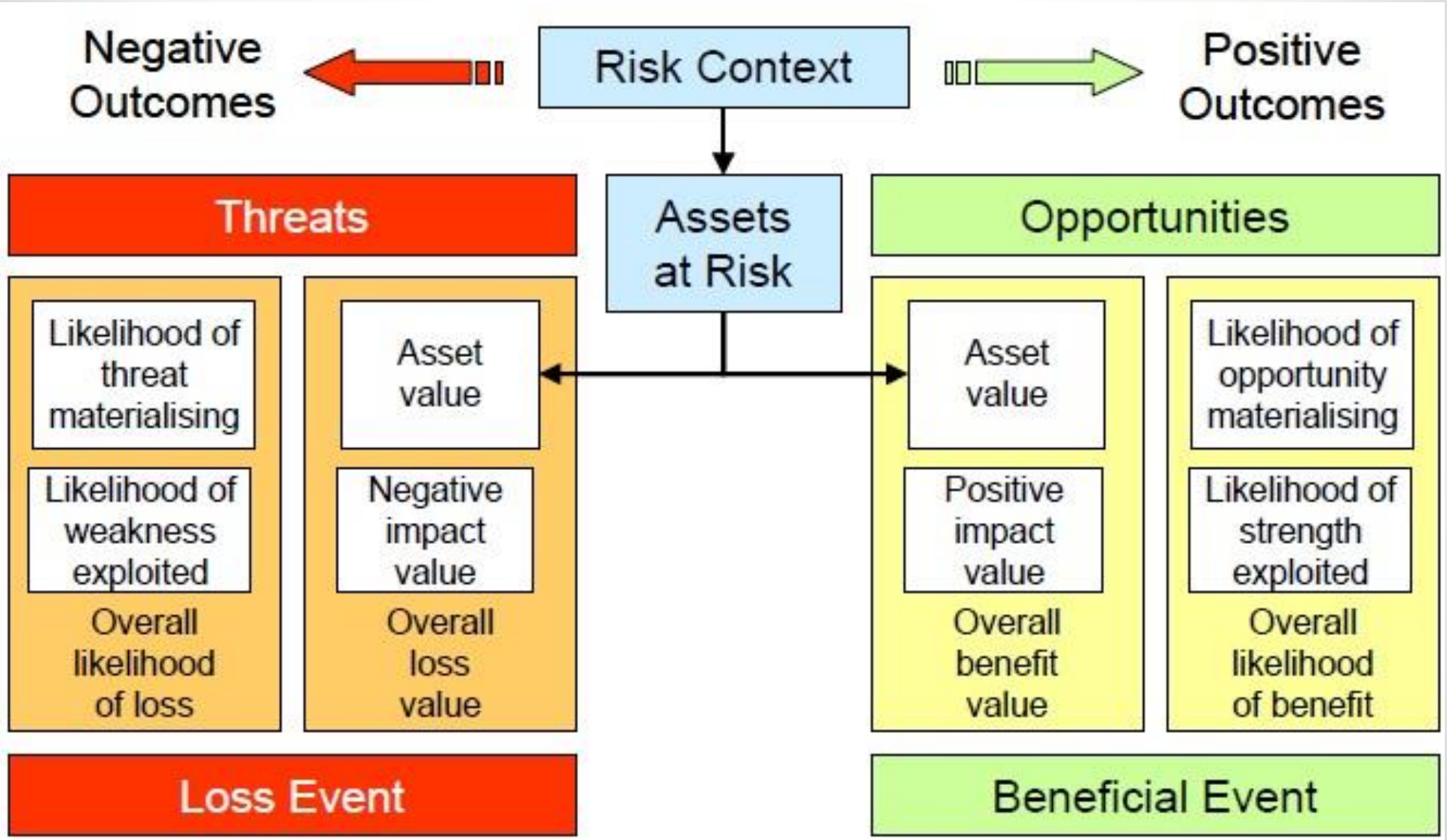
SABSA Taxonomy of ICT Business Attributes



SABSA Taxonomy of General Business Attributes

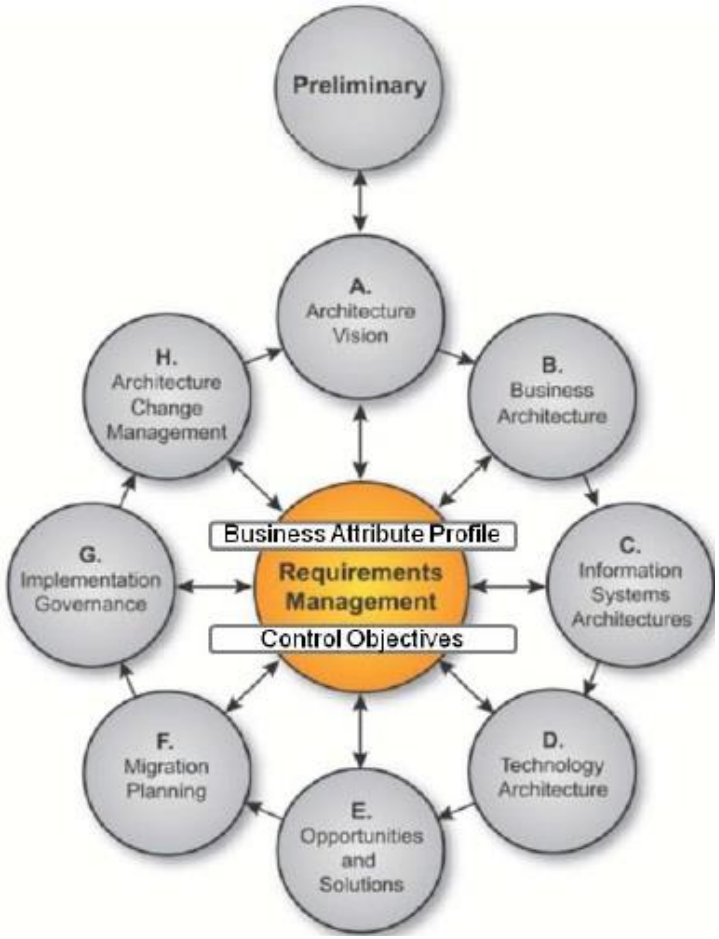


SABSA Operational Risk Model



SABSA integrated with TOGAF

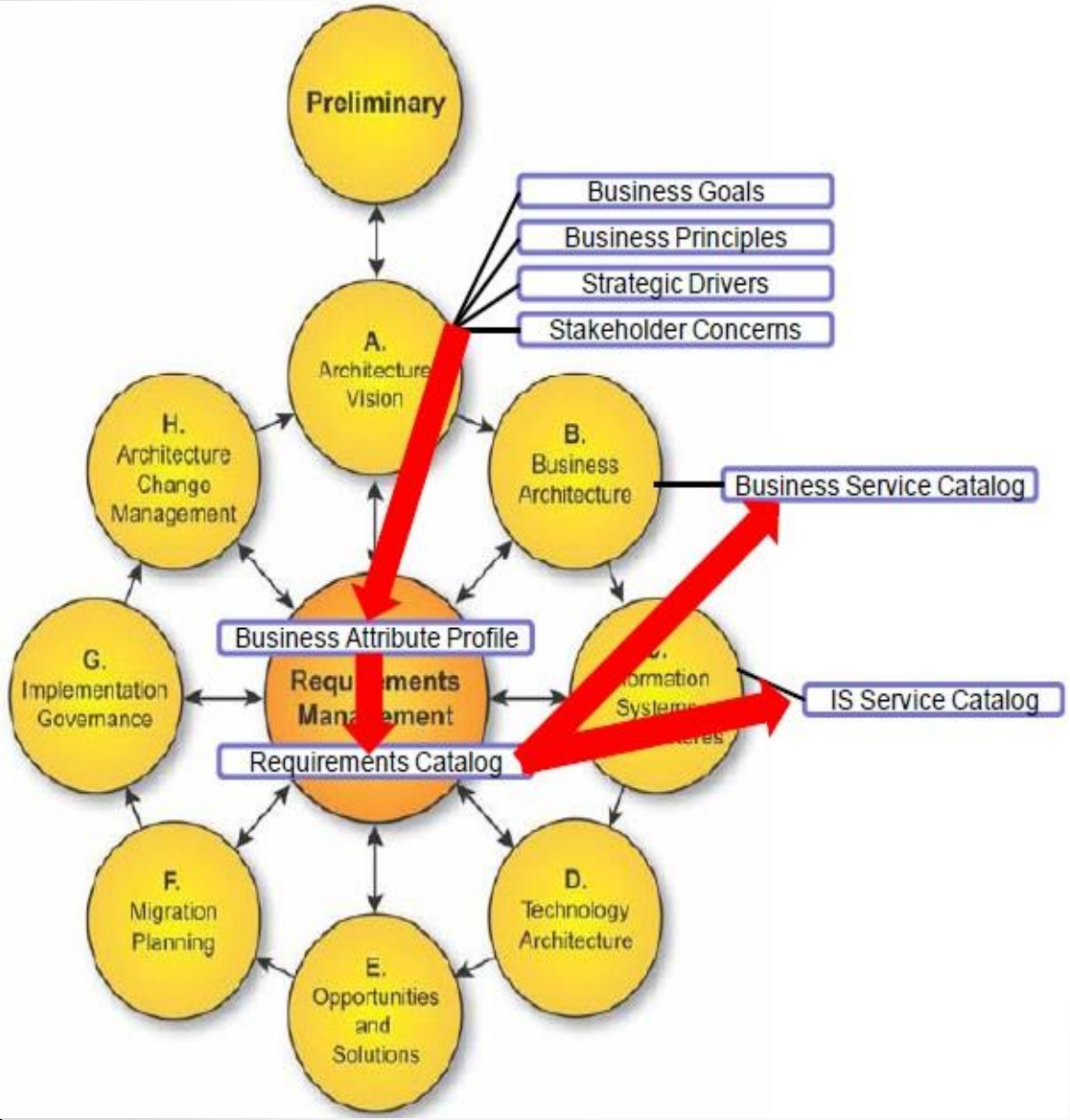
A Central Role for Requirements Management



	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture

Linking the Business Requirements (Needs) to the Security Services – which TOGAF does in the "Requirements Management" Phase and SABSA does via the Business Attributes Profile. These Artefacts needs to be linked to ensure traceability from Business Needs to Security Services.

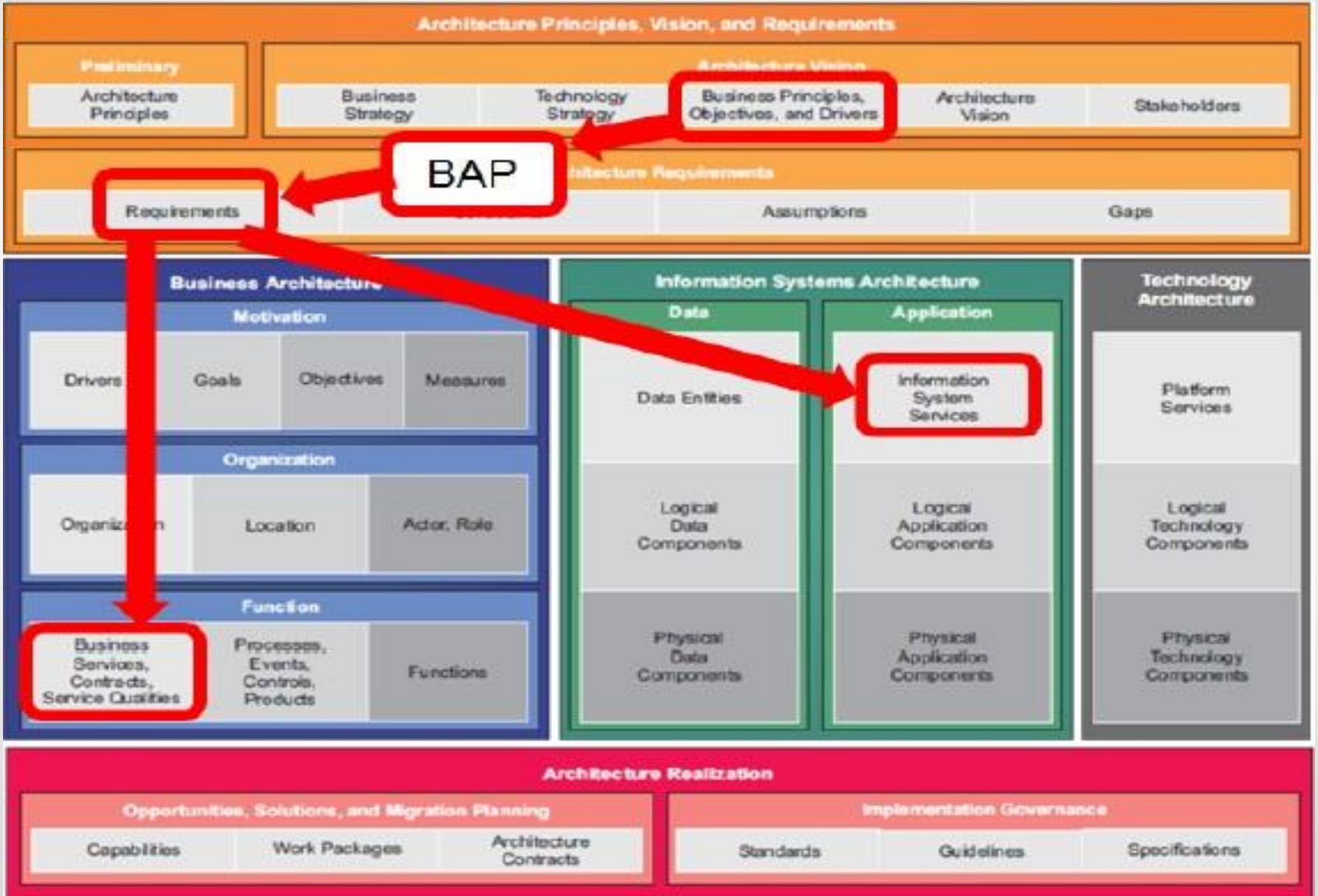
Requirements Management in TOGAF using SABSA Business Attribute Profiling



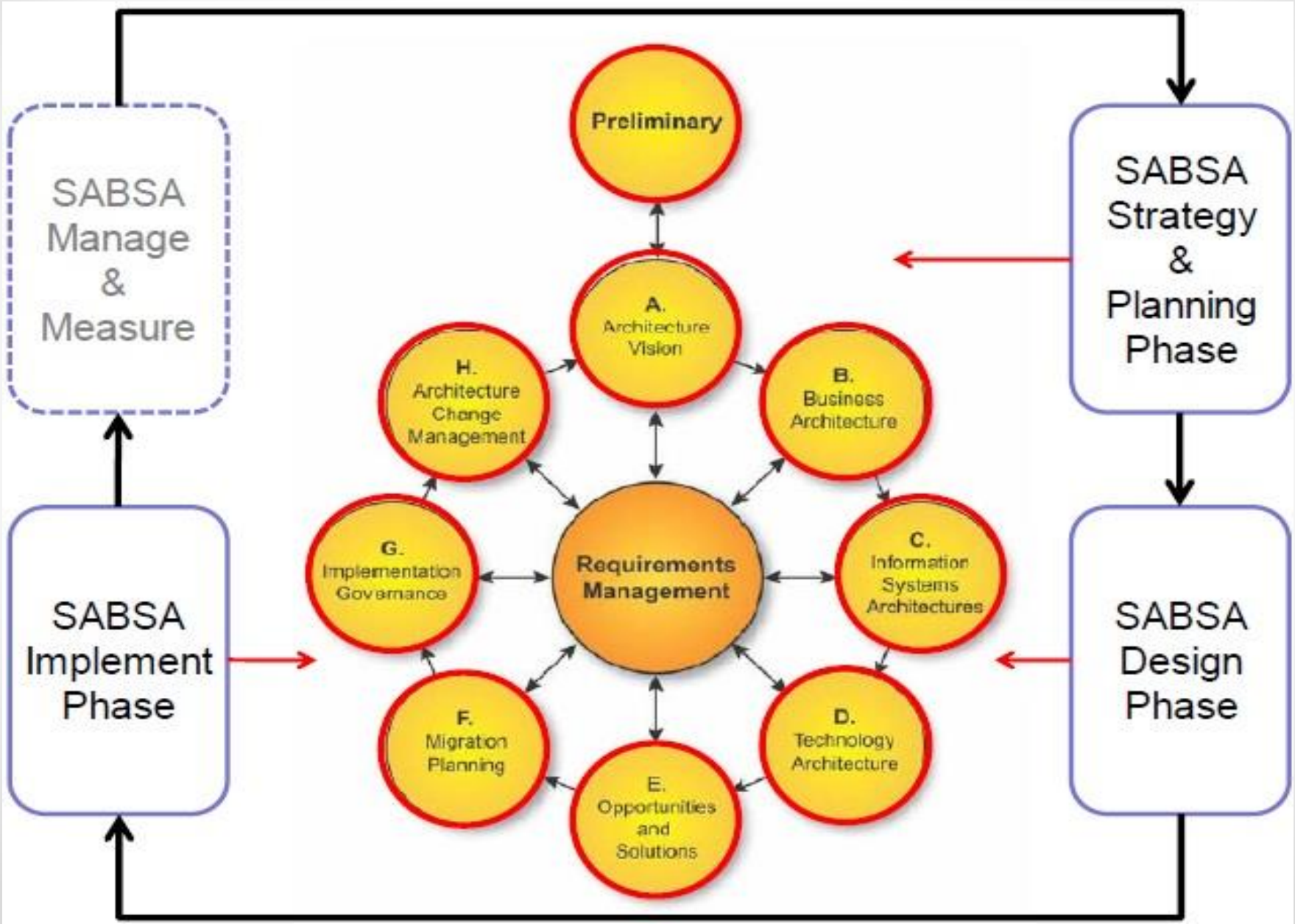
Business Attribute Profiling: This describes the level of protection required for each business capability.

- **Requirements Catalog**: This stores the architecture requirements of which security requirements form an integral part. The Business Attribute Profile can form the basis for all quality requirements (including security requirements) and therefore has significant potential to fully transform the current TOGAF requirements management approach.
- **Business and Information System Service Catalogs**: TOGAF defines a business service catalog (in Phase B: Business Architecture) and an information system service catalog (Phase C: Information Systems Architecture). The creation of the information system services in addition to the core concept of business services is intended to allow more sophisticated modelling of the service portfolio.
- **The Security Service Catalog**: As defined by the SABSA Logical Layer, this will form an integral part of the TOGAF Information System Service Catalogs.

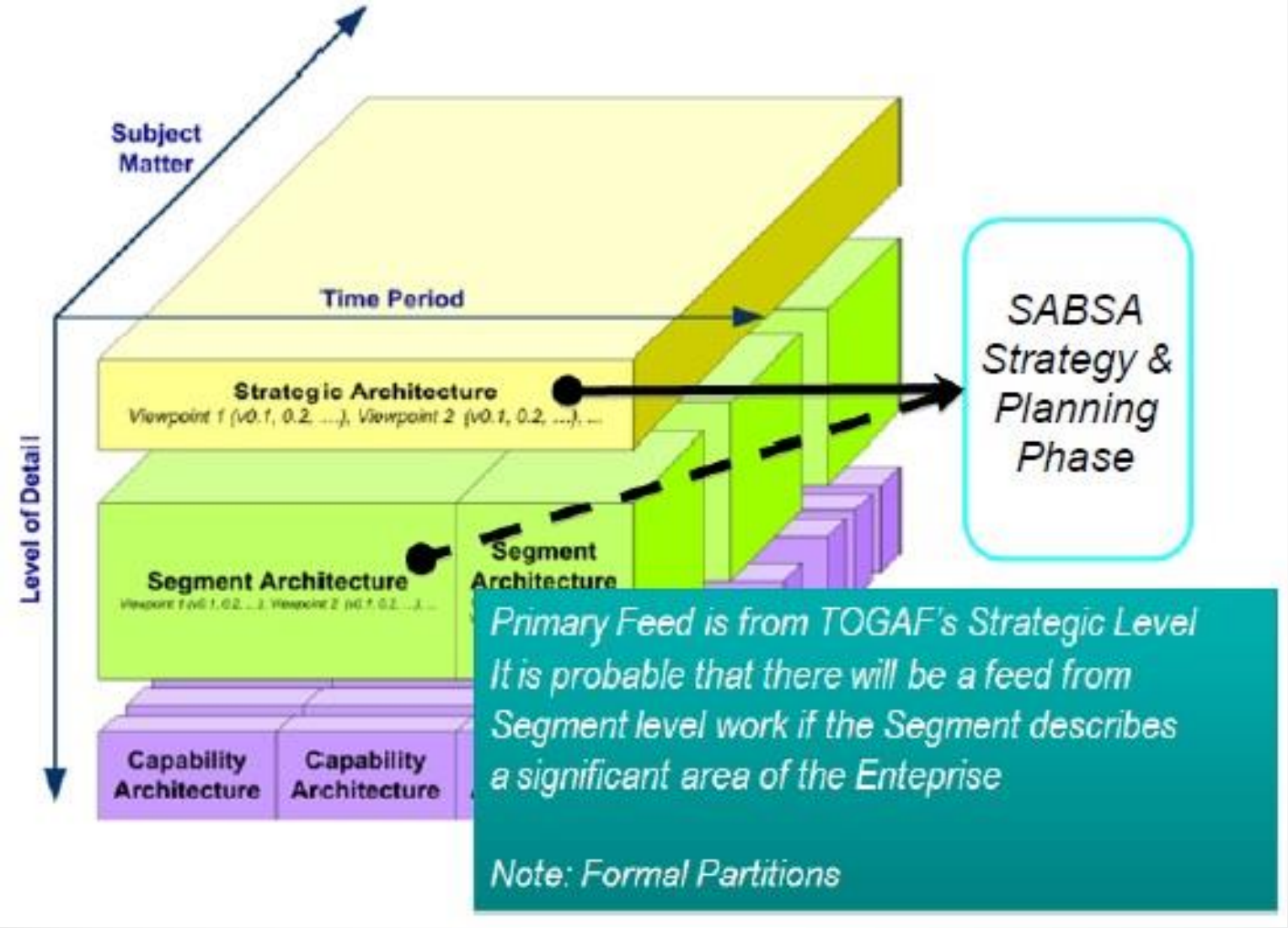
The Business Attribute Profile Mapped onto the TOGAF Content Meta Model



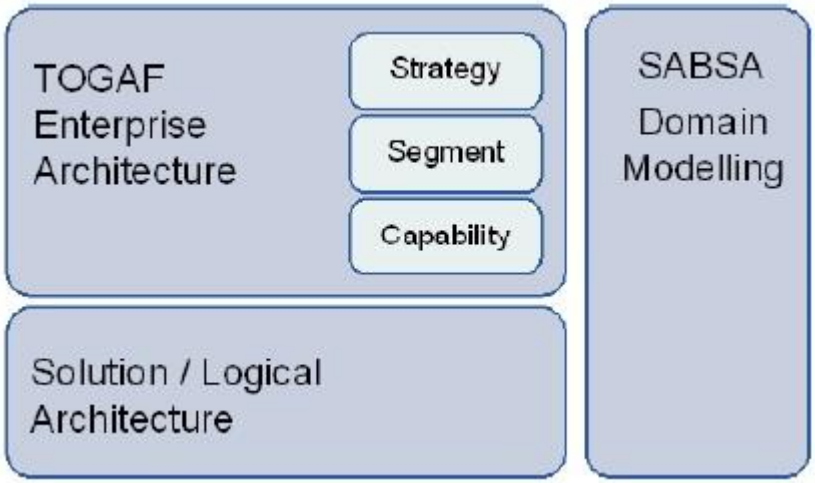
SABSA Life Cycle and TOGAF ADM



Mapping TOGAF and SABSA Abstraction Layers

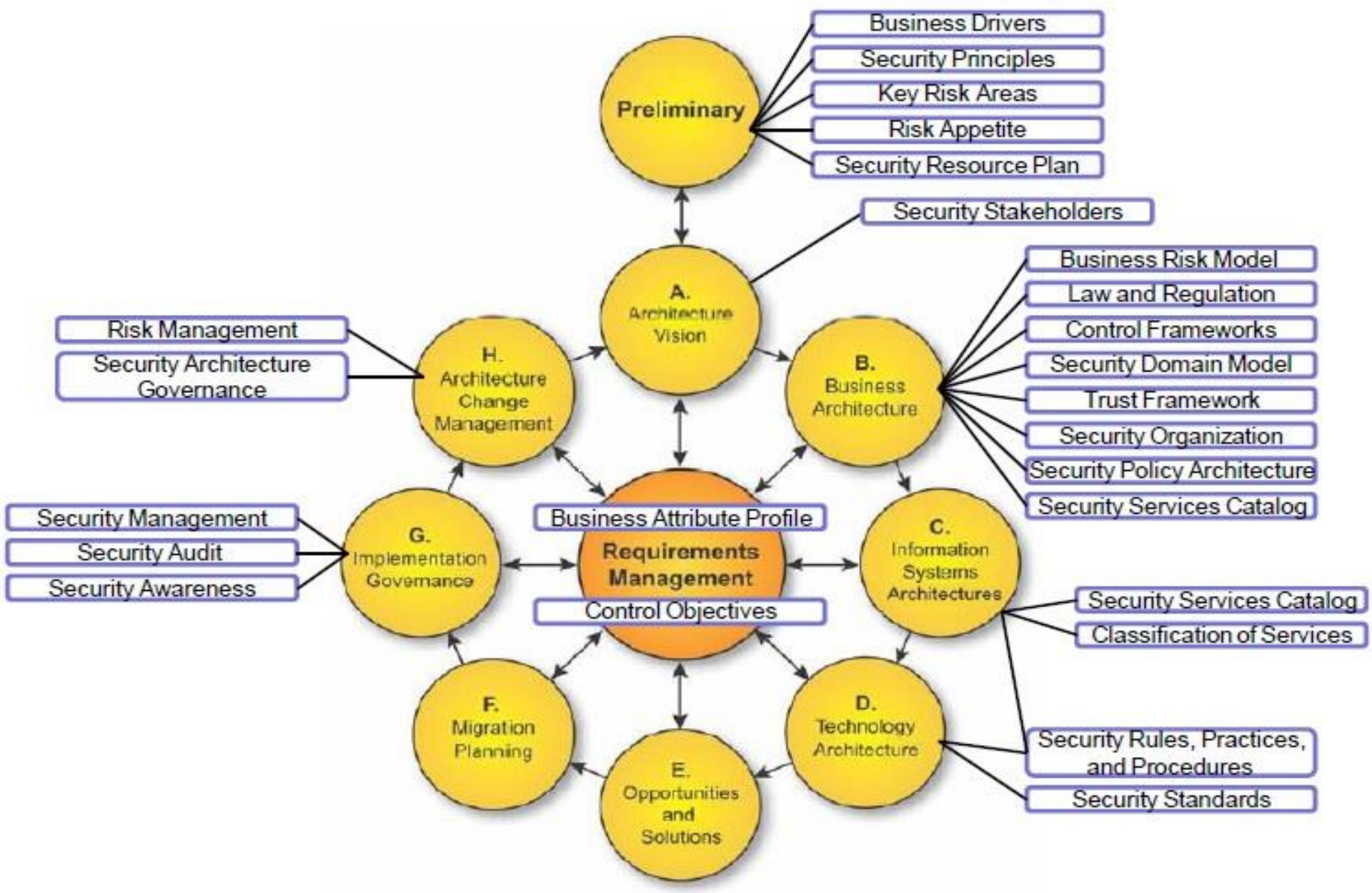


Mapping of TOGAF to SABSA Strategy and Planning Phase

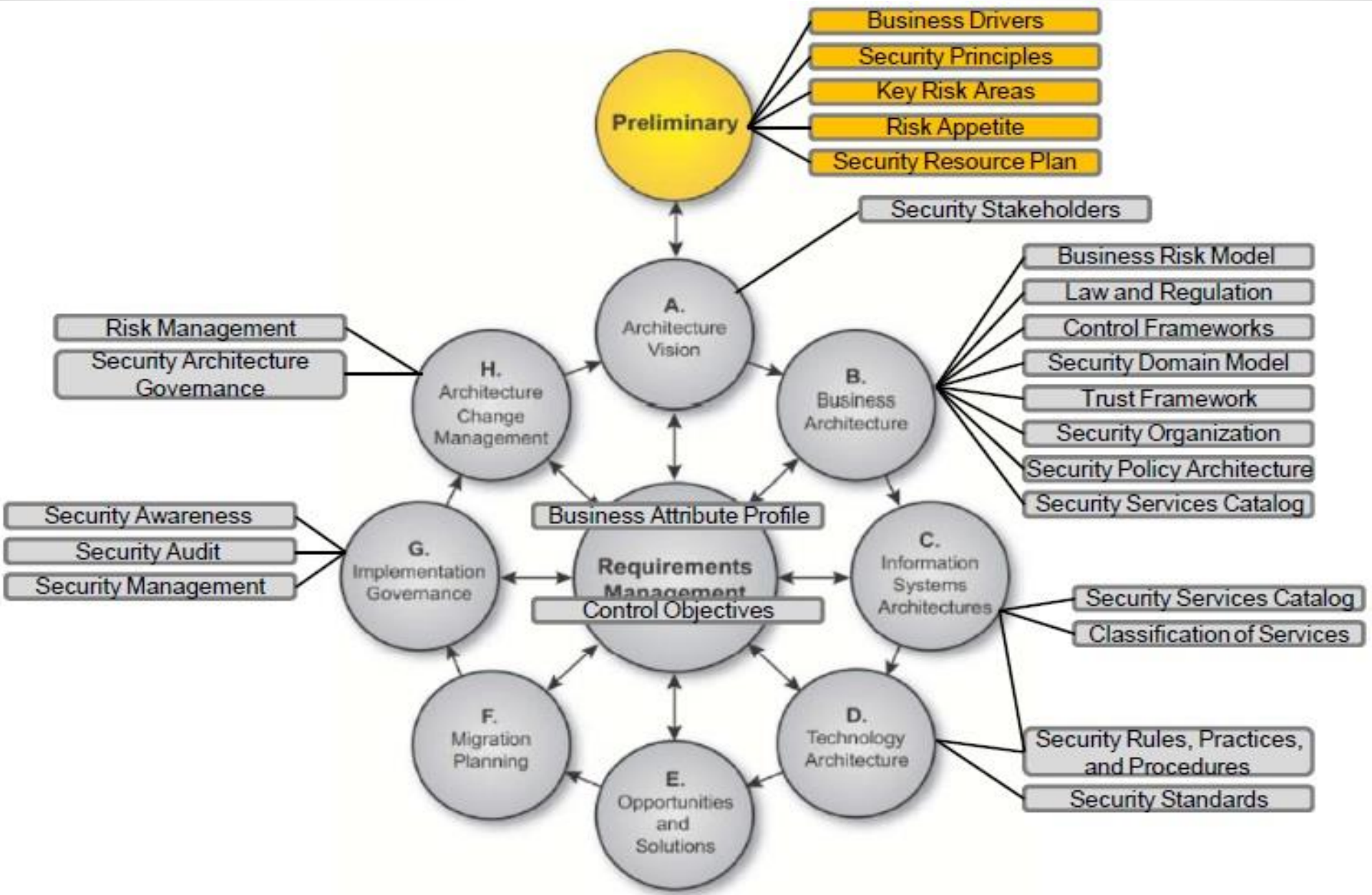


As the SABSA phases extend beyond the core phases of the TOGAF ADM, the scoping provided by the SABSA Domain Model extends beyond these core phases of TOGAF, both in terms of solution design and system and process management during the operational lifecycle.

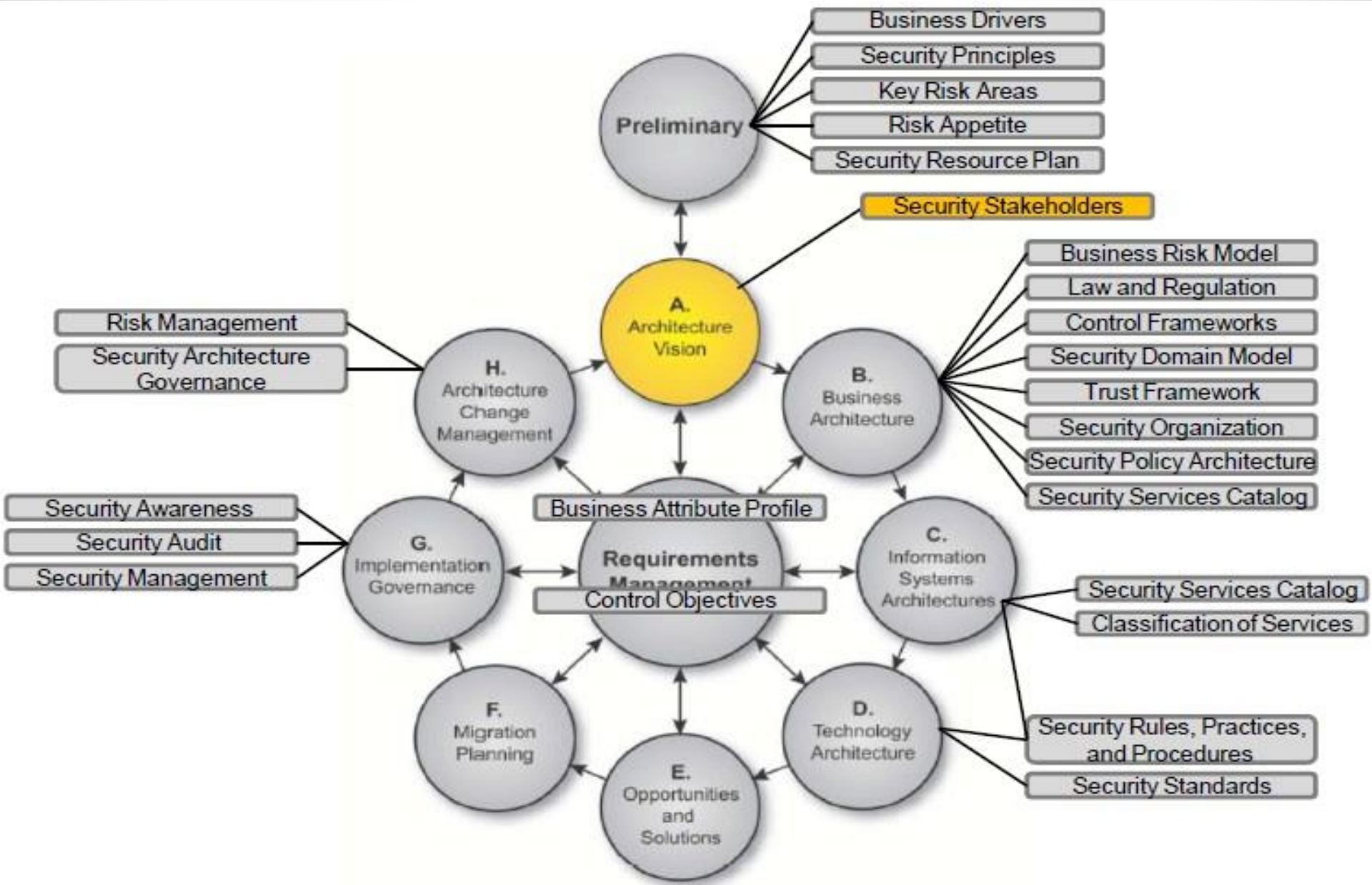
Overview of Security Related Artifacts in the TOGAF ADM



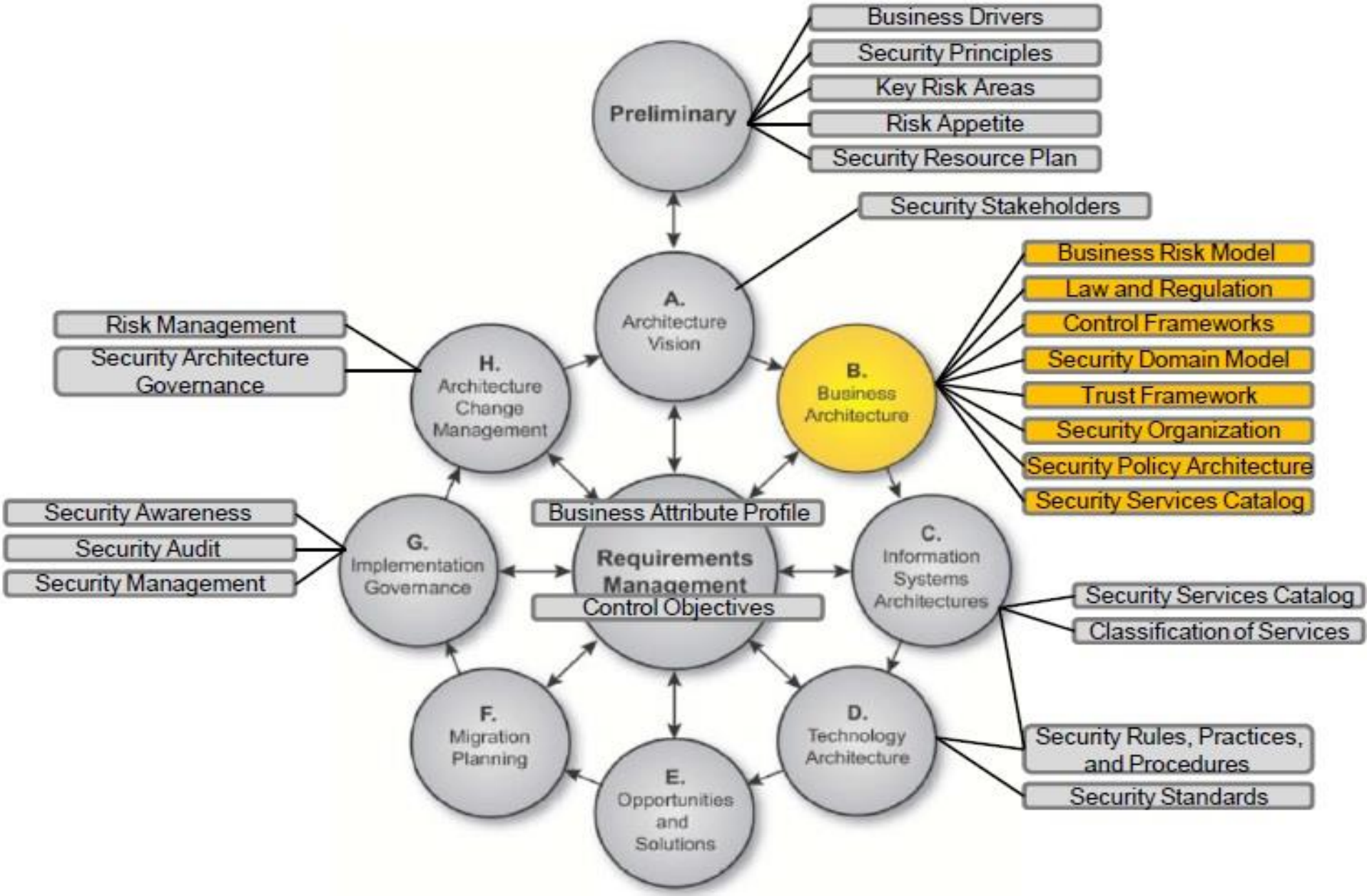
Preliminary Phase – Security Artifacts



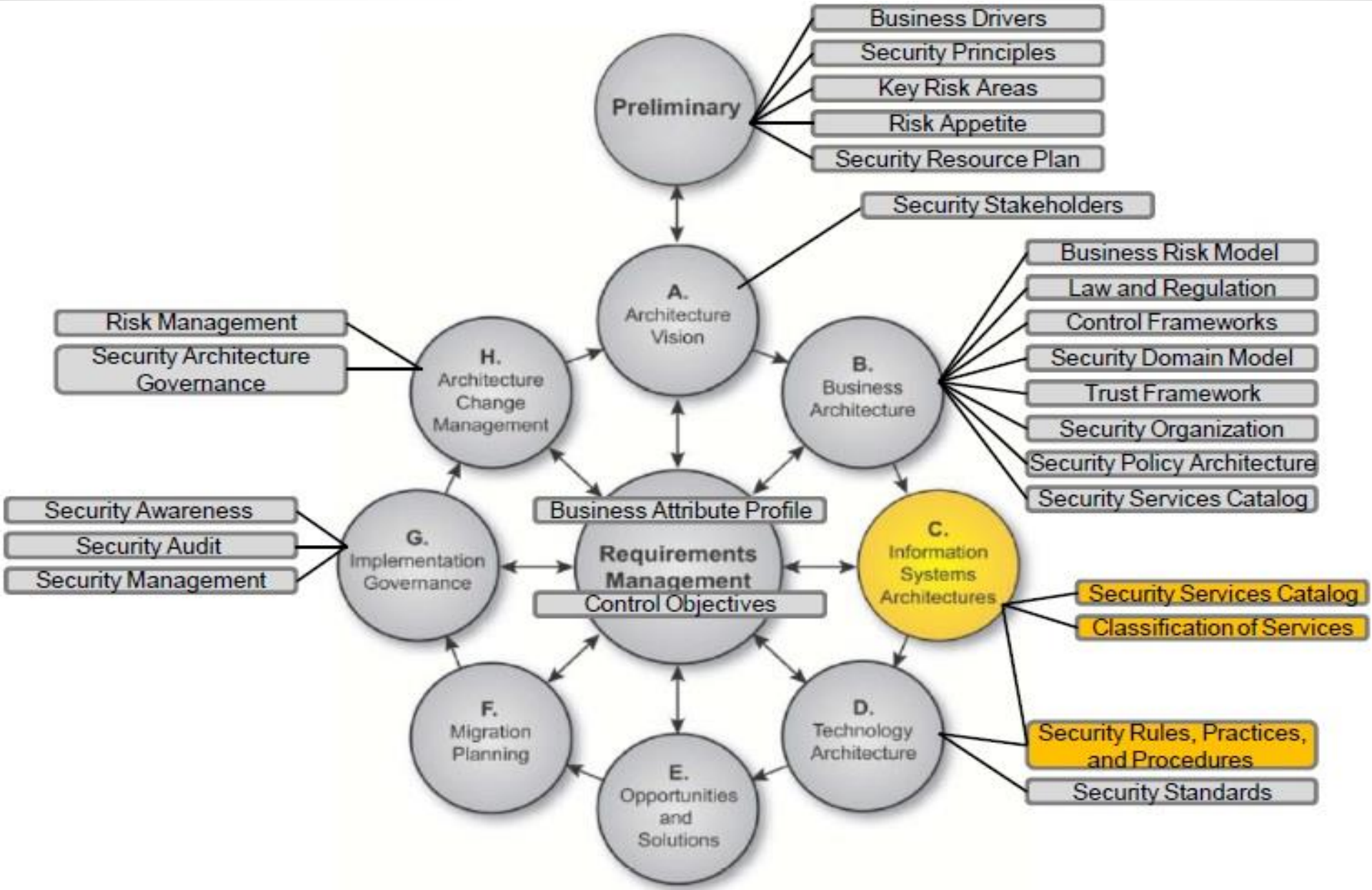
Phase A - Architecture Vision – Security Artifacts



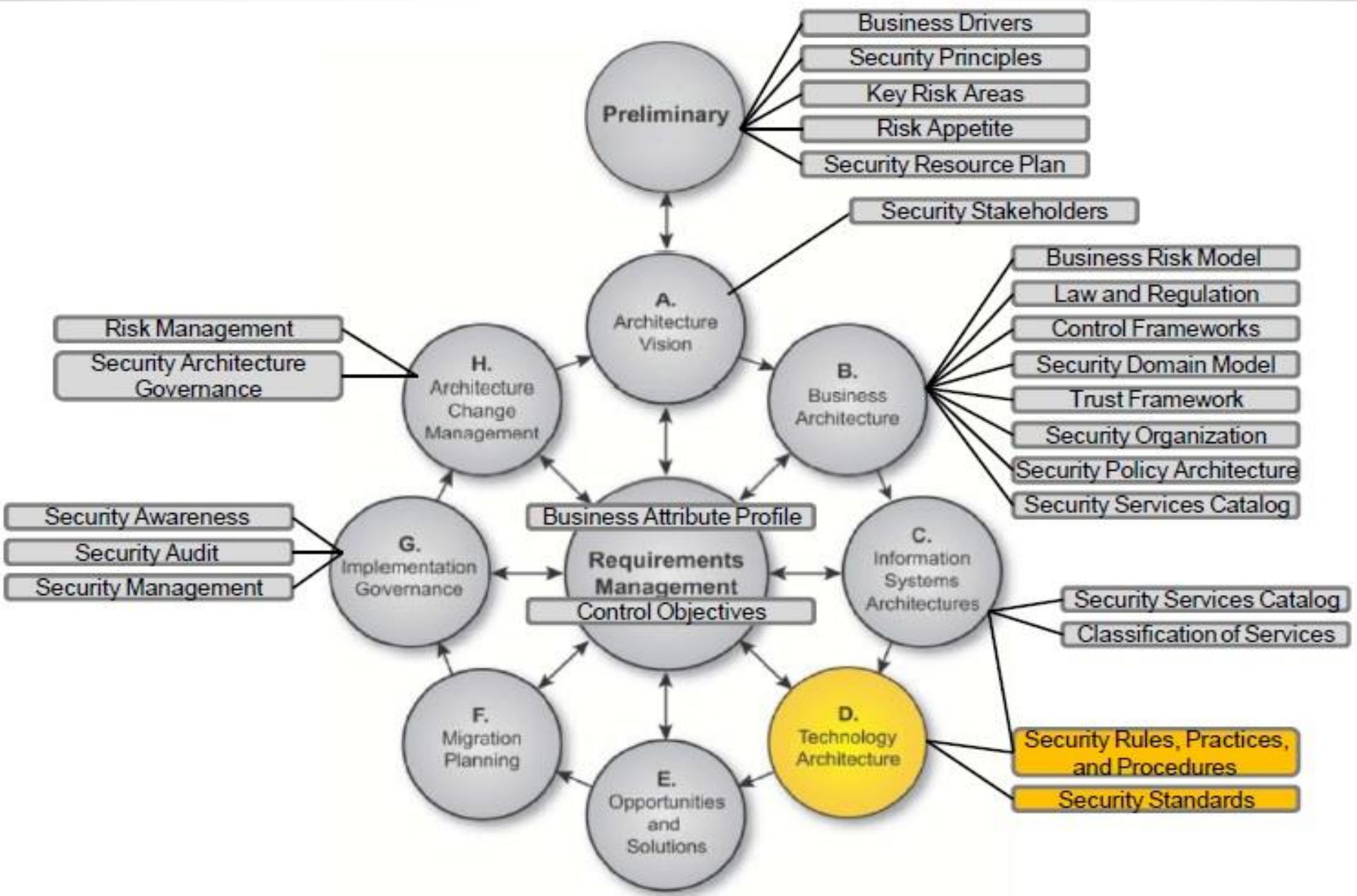
Phase B – Business Architecture – Security Artifacts



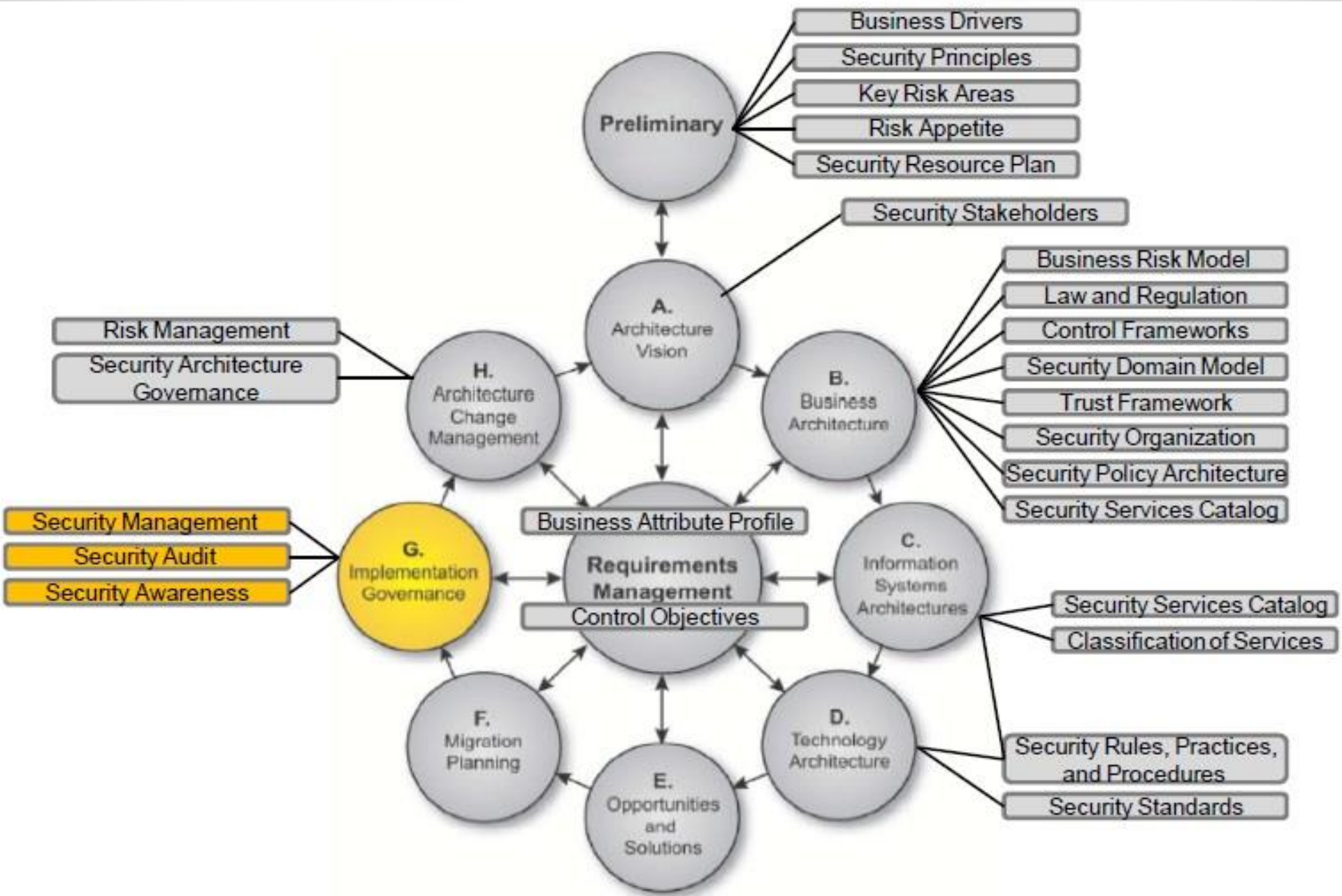
Phase C – Information Systems Architecture – Security Artifacts



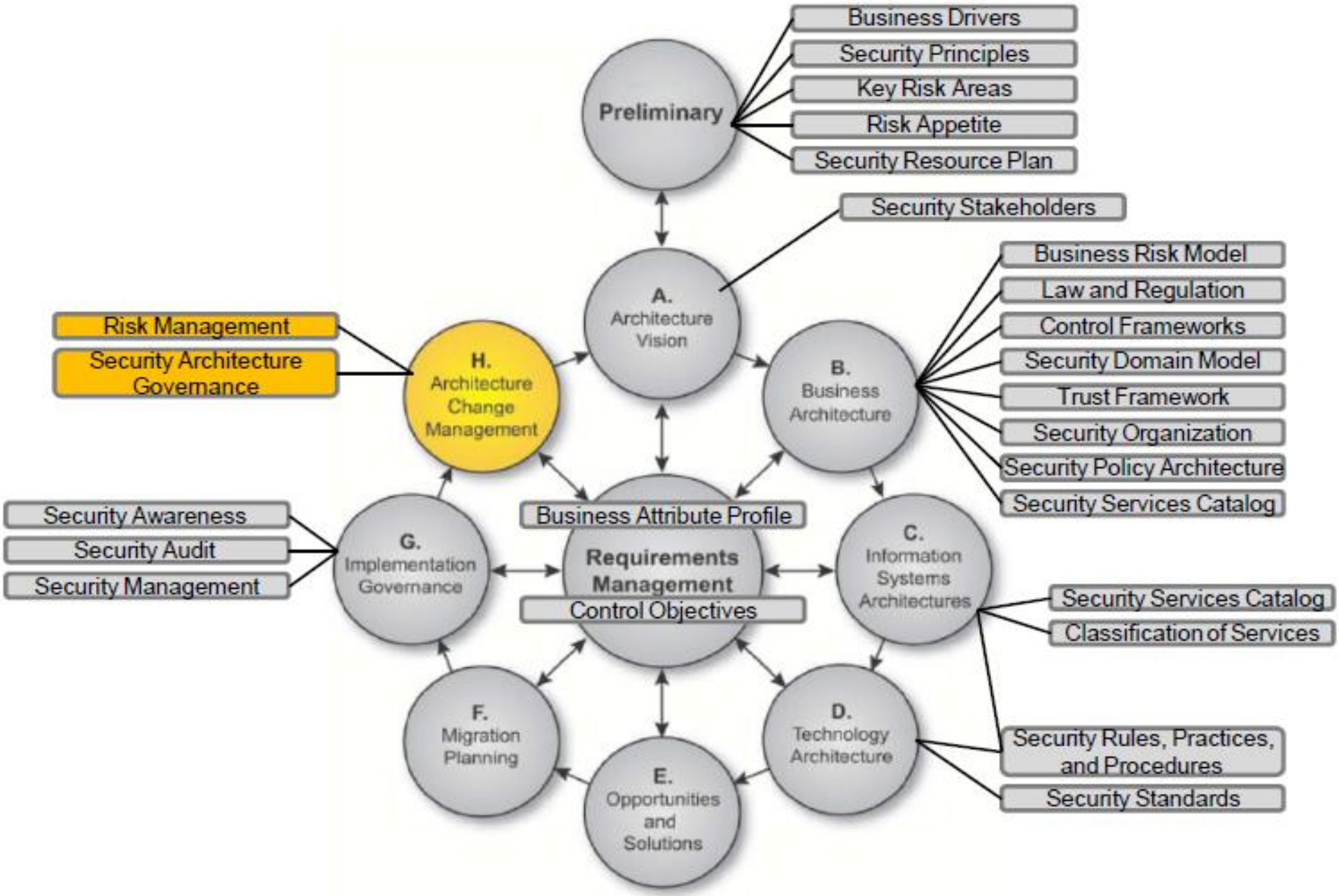
Phase D – Technology Architecture – Security Artifacts



Phase G – Implementation Governance – Security Artifacts

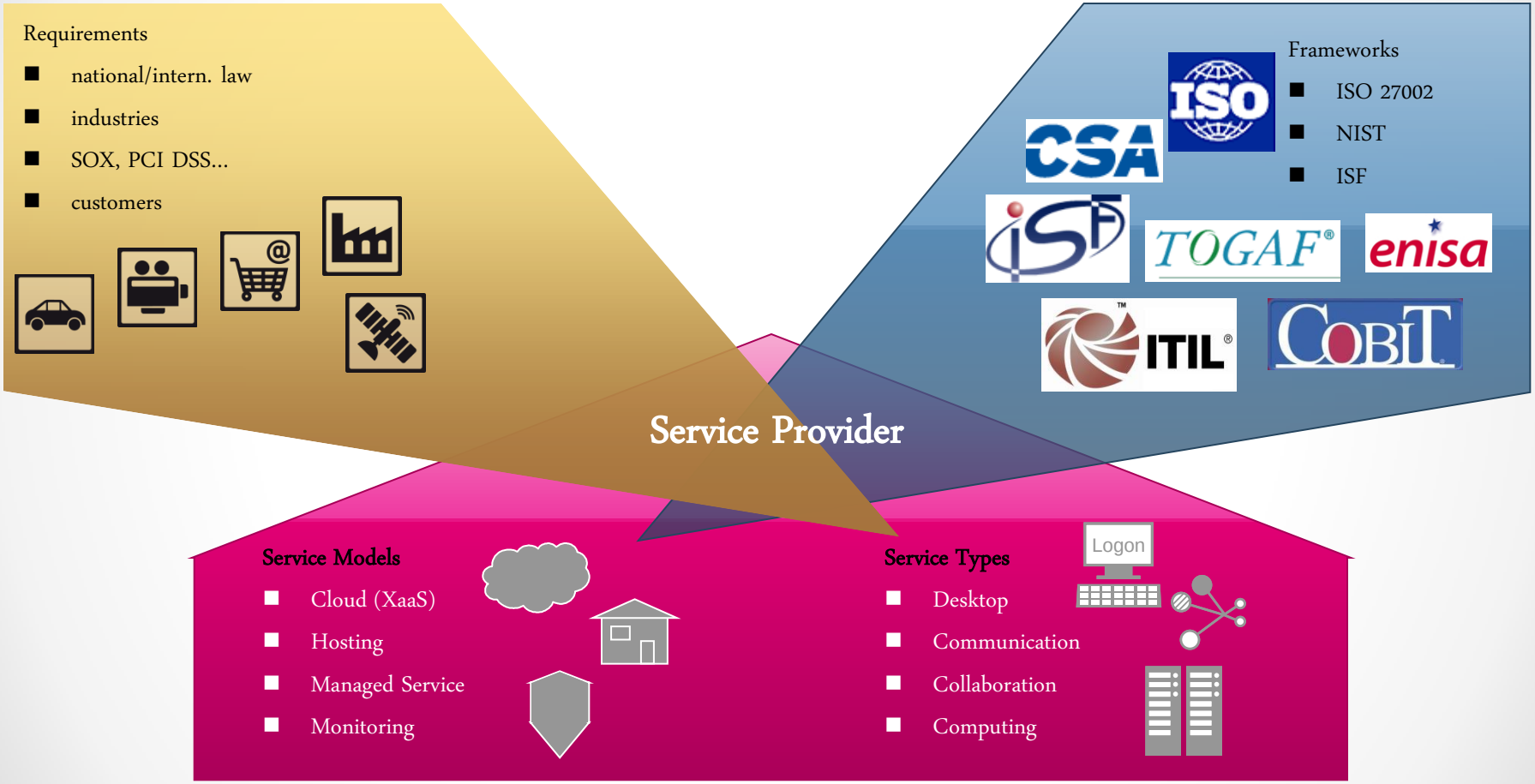


Phase H – Architecture Change Management – Security Artifacts



Enterprise Security Architecture - Framework

ICT service providers must consider the whole market. Four dimensions to put in one line



ICT service providers must consider the whole market. Four dimensions to put in one line

4) Mapping Model to demonstrate fulfillment of all types of security requirements

3) Hierarchy of Security Standards delivering information on each level of detail

Enterprise Security Architecture

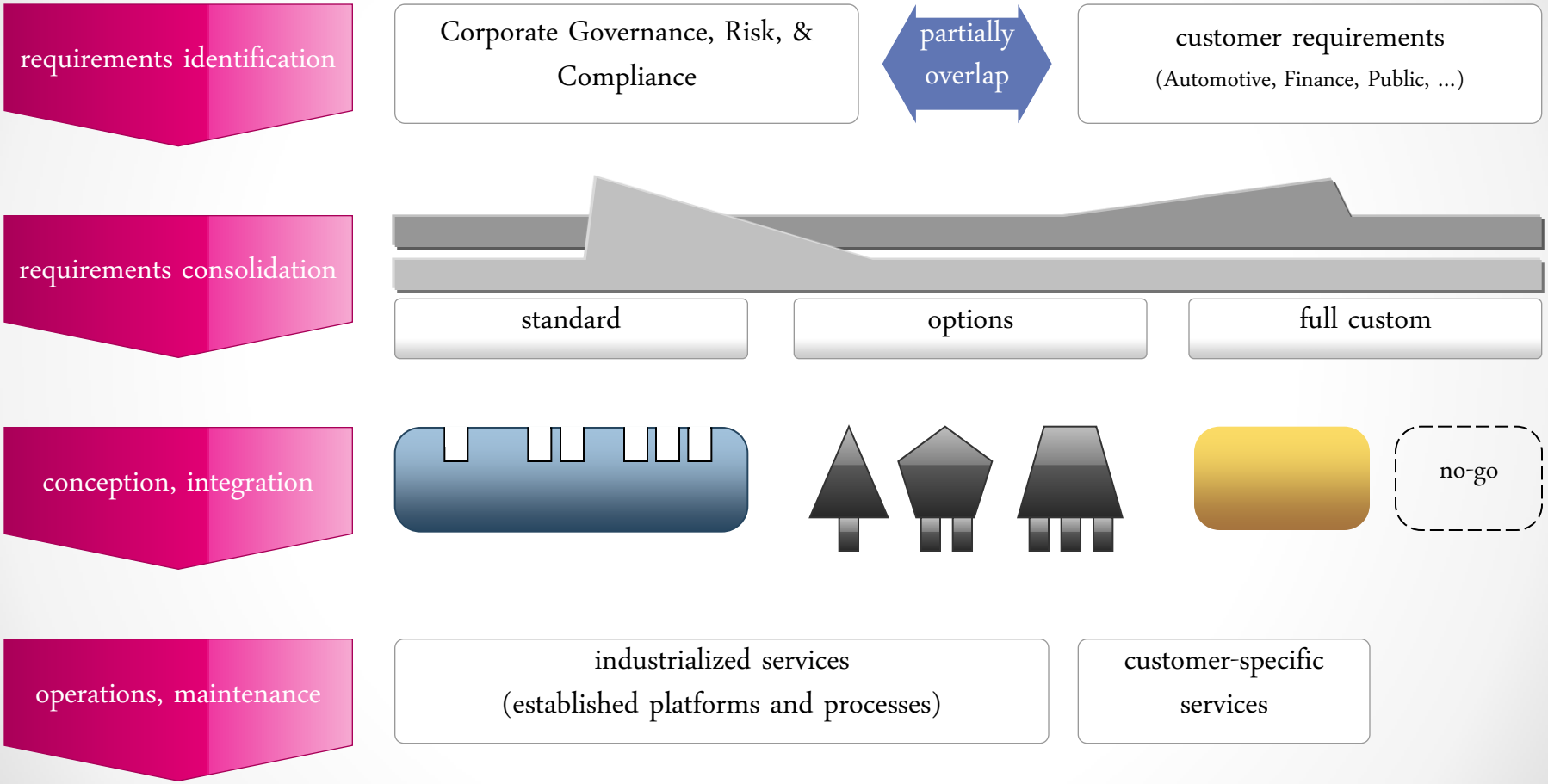
» shaping the security of ICT service provisioning «

deliver assurance to customers and provide directions for production

1) Produce Standardized Security measures for industrialized ICT production

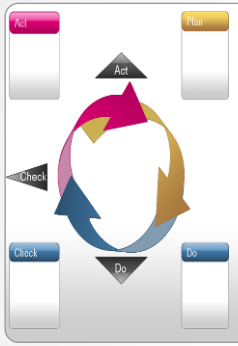
2) Modular and Structured approach that serves all possible models and offerings

From Requirements to ICT Services. Standardisation is Key



Framework for Enterprise Security Architecture

Requirements (corporate and customer)



Framework for ESA

Enablement (ISMS)

- security management process and reference model (mainly ISO 27001)

Enforcement (Practices)

- controls / techniques (mainly ISO 27002)
- specific standards

impact analysis for non-framework requirements

Enterprise Security Architecture

Industrialized ESA Services

- processes including roles for new business, changes and operational services
- technology platform
- evidence (monitoring, analytics and reporting)

custom services

(specific service and realization for a customer)

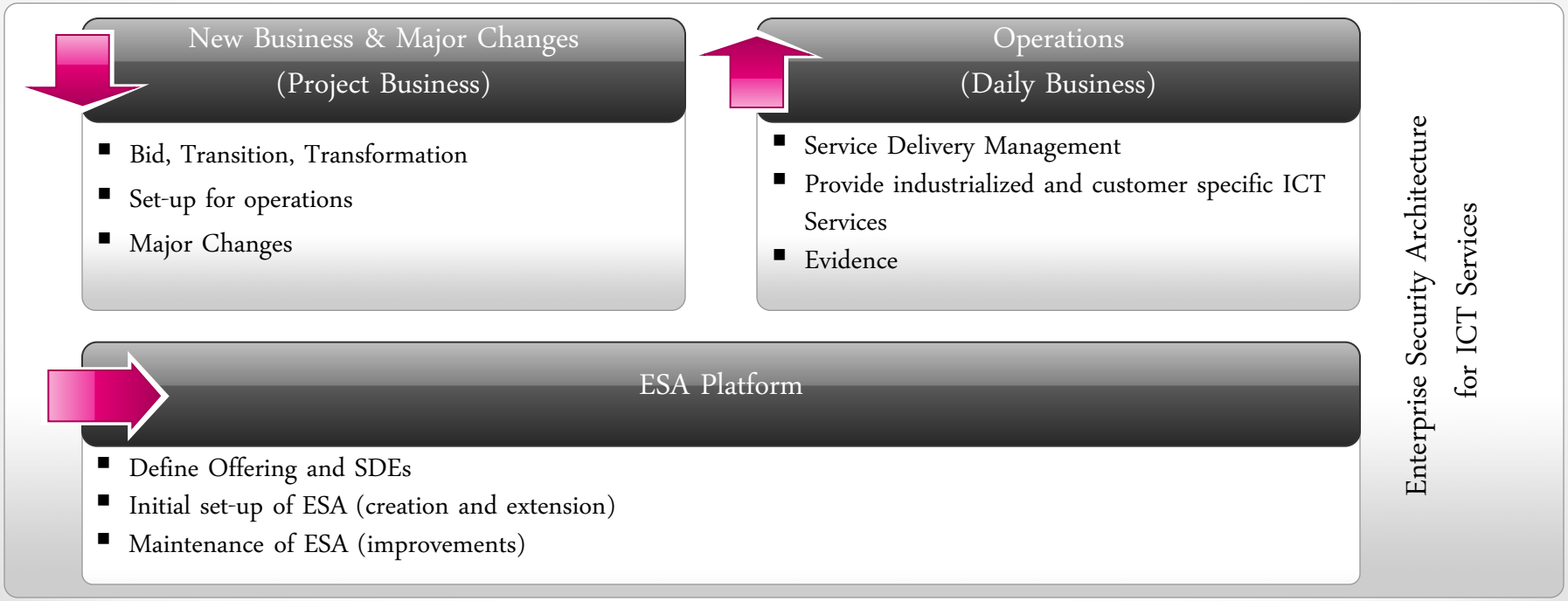
Framework for ESA.
The Enablement Framework with ISMS activities.

Activities of the Enablement Framework

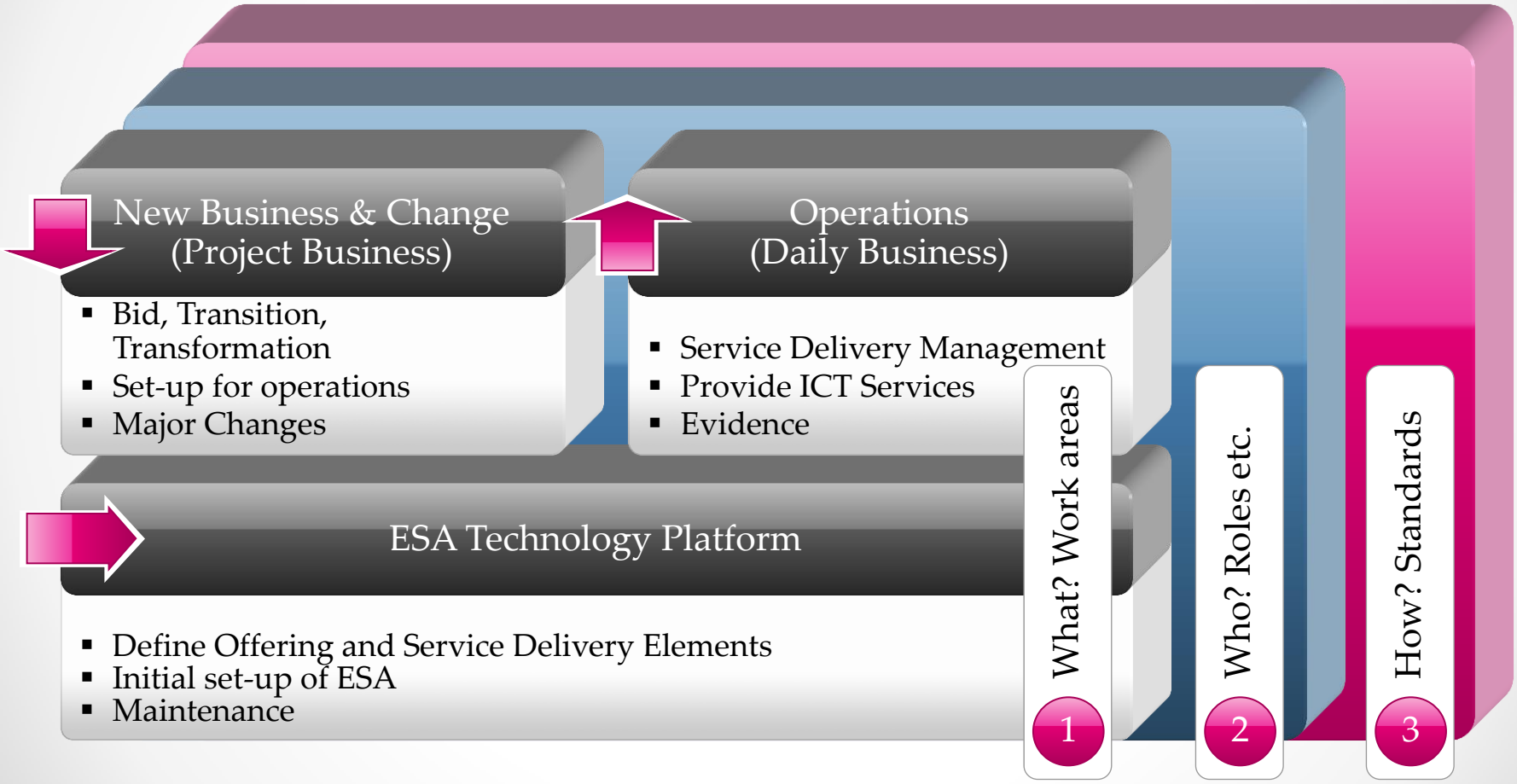
P1 Define scope and ISMS policy	D1 Implement risk handling plan & controls	C1 Monitoring & review security incidents	A1 Implement identified improvements in ISMS
P2 Define risk assessment approach	D2 Define process for monitoring the effectiveness of controls	C2 Evaluate effectiveness of the controls implemented	A2 Implement appropriate corrective and preventative controls
P3 Identify risks, derive control obj. & controls	D3 Develop security awareness	C3 Review risk assessment approach	A3 Communicate activities & improvements
P4 Approve residual risks	D4 Lead ISMS and steer funds	C4 Perform and document ISMS audits	A4 Ensure improvements achieve targets
P5 Draw up statement of applicability (SoA)	D5 Implement methods to identify / handle security incidents	C5 Carry out management evaluations	

Considering: Plan – Build – Run. Sales, Service, Production, (Integration).

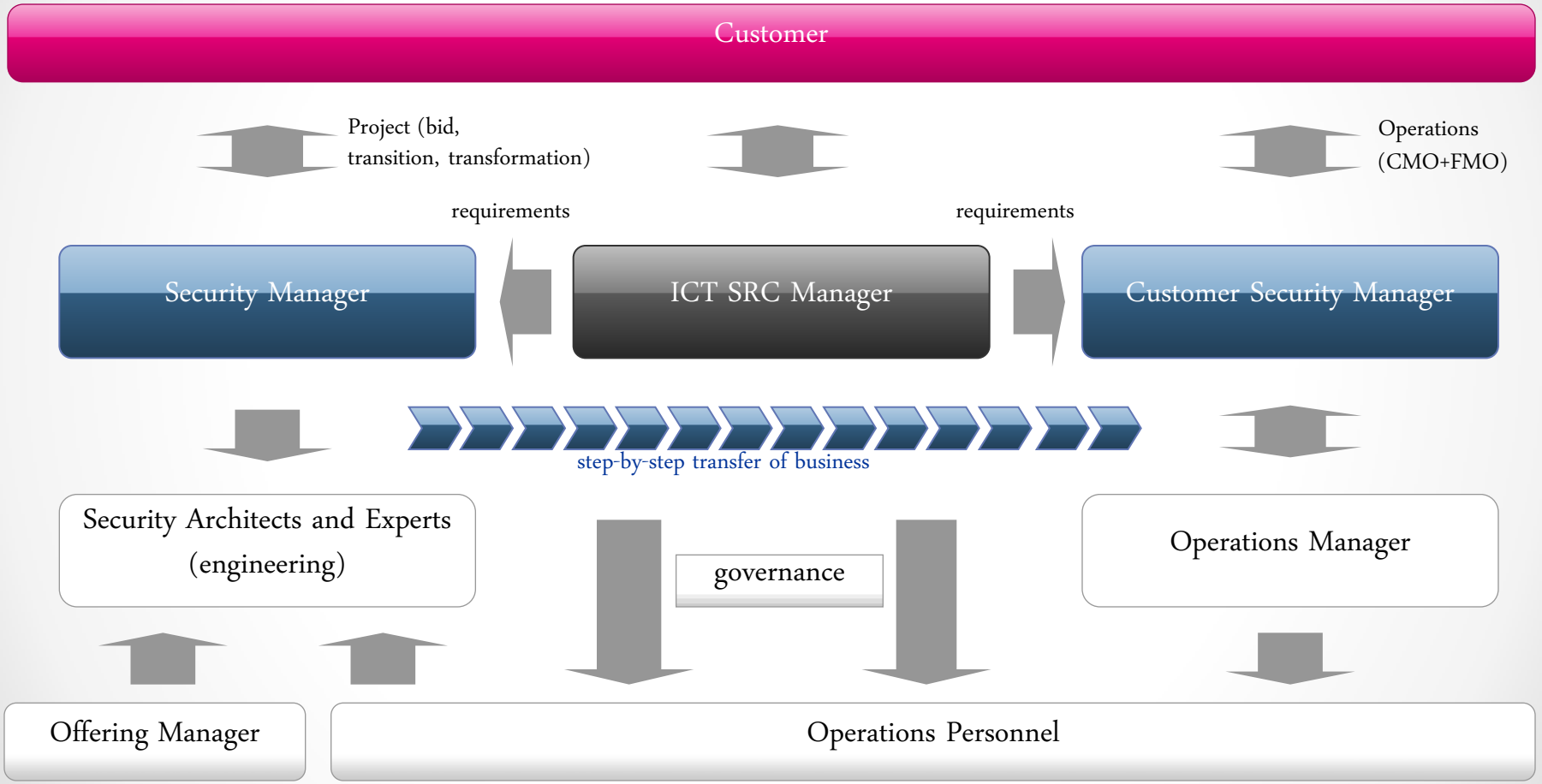
ESA reflects three types of business:
Customer Projects – Operations – Platform Preparation



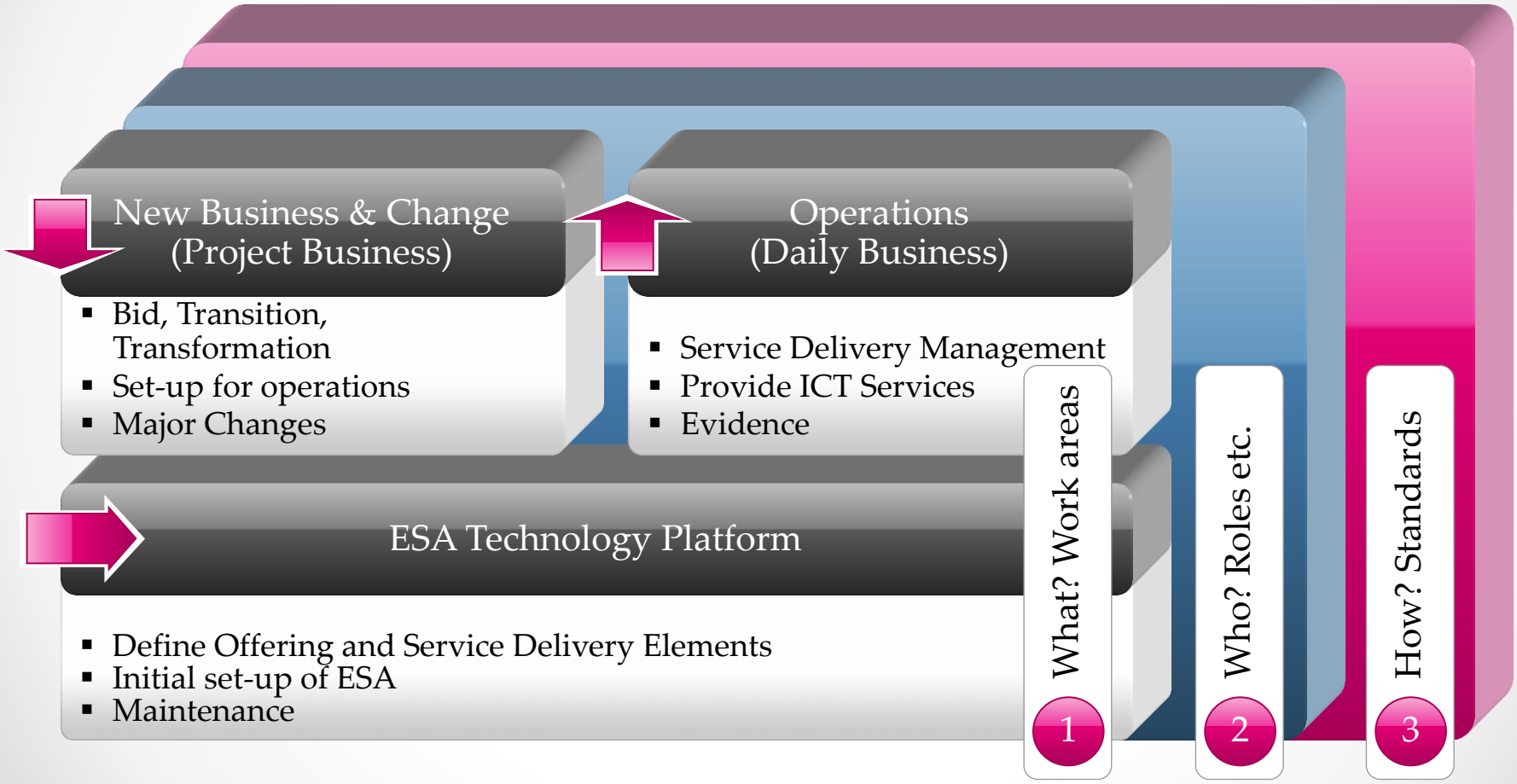
Considering: Plan – Build – Run. Sales, Service, Production, (Integration).



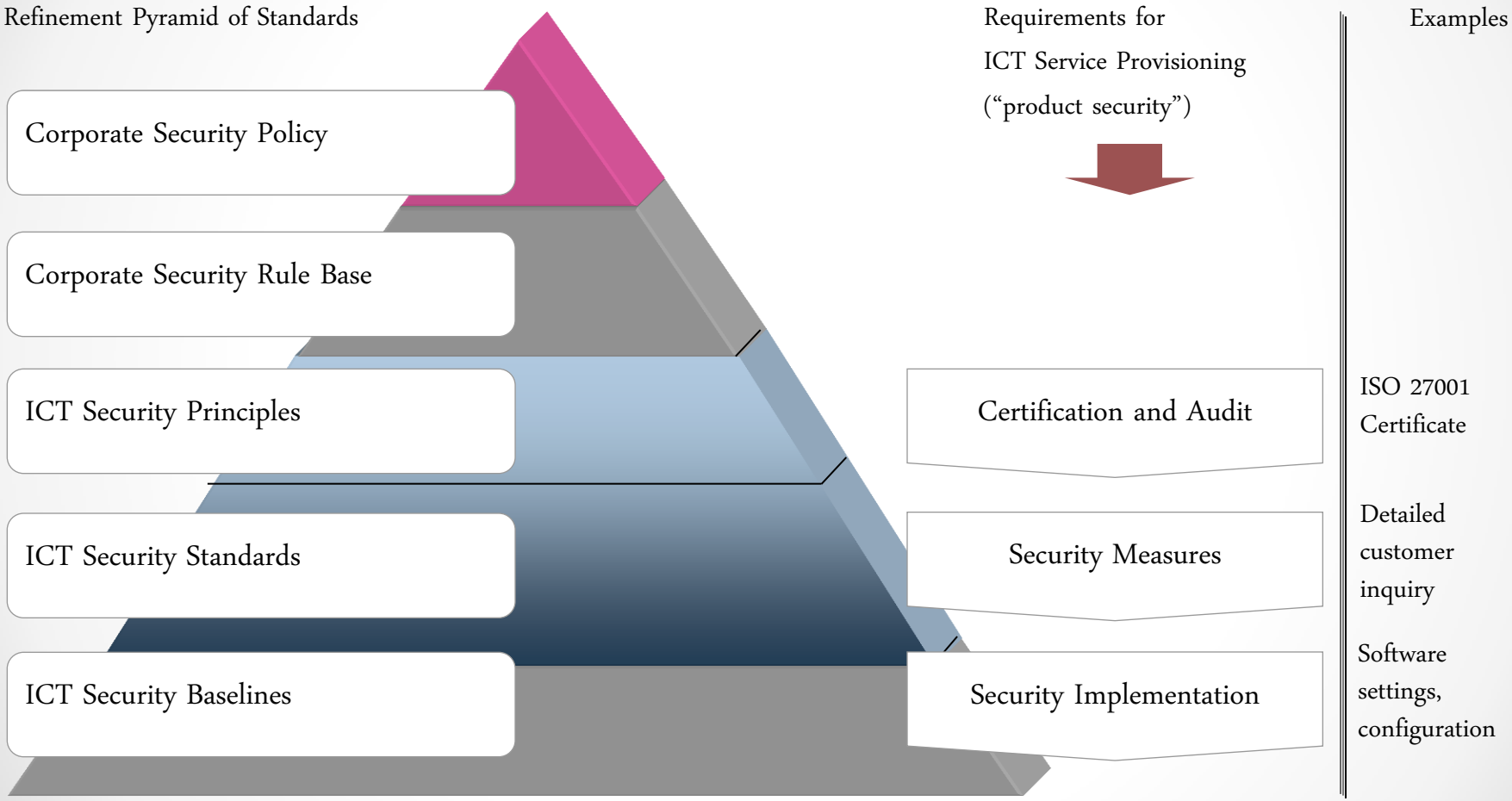
Cooperation: Implementation of Roles. Customer Projects, Portfolio, and Operations.



Considering: Plan – Build – Run. Sales, Service, Production, (Integration).

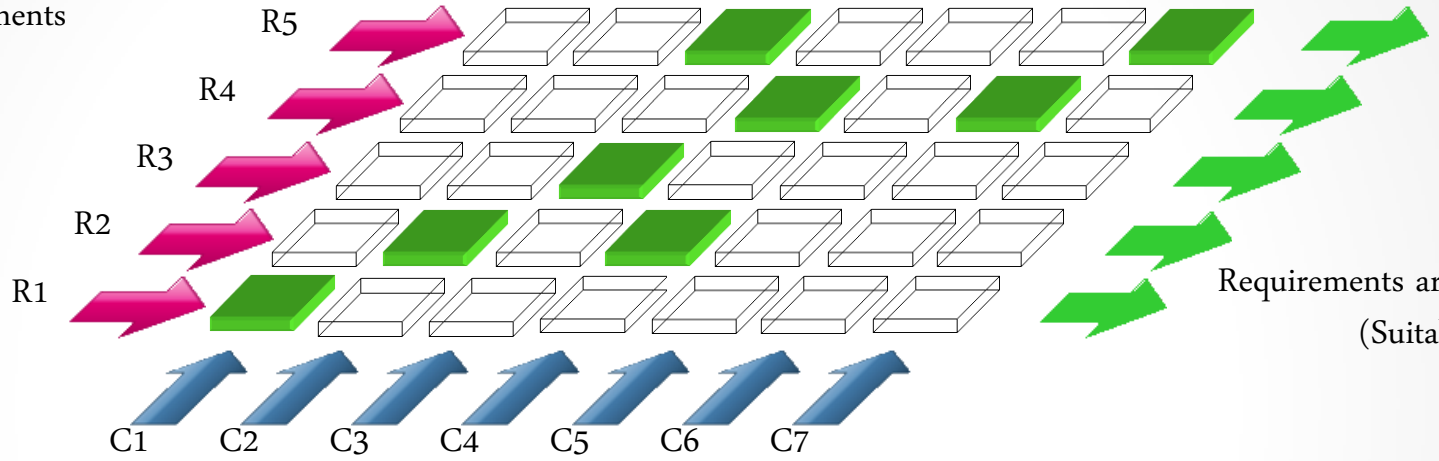


Corporate and Product Security incorporated in one Hierarchy



Demonstrating that Customer Requirements are met

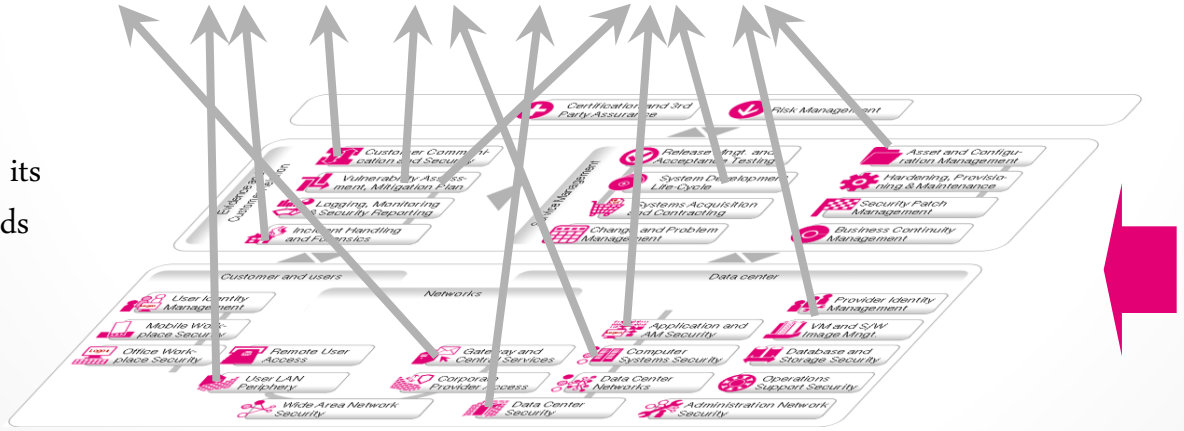
Customer Requirements



Requirements are met (Suitability)

Set of Controls (contractual)

Controls of ESA and its ICT Security Standards



Service type:

- Desktop
- Communication
- Collaboration
- Computing

Security Taxonomy

Certification and 3rd Party Assurance

Risk Management

Evidence and Customer Relation

- Customer Communication and Security
- Vulnerability Assessment, Mitigation Plan
- Logging, Monitoring & Security Reporting
- Incident Handling and Forensics

Service Management

- Release Mngt. and Acceptance Testing
- System Development Life-Cycle
- Systems Acquisition and Contracting
- Change and Problem Management
- Asset and Configuration Management
- Hardening, Provisioning & Maintenance
- Security Patch Management
- Business Continuity Management

Customer and users

- User Identity Management
- Mobile Workplace Security
- Office Workplace Security
- Remote User Access
- User LAN Periphery

Networks

- Gateway and Central Services
- Corporate Provider Access
- Wide Area Network Security

Data Center

- Provider Identity Management
- Application and AM Security
- VM and S/W Image Mngt.
- Computer Systems Security
- Database and Storage Security
- Data Center Networks
- Operations Support Security
- Data Center Security
- Administration Network Security

EAS – Meta Model

"Model World"
Architecture Repository

"Standardized"
Content, e.g. business processes, applications etc.

Industry Glossaries

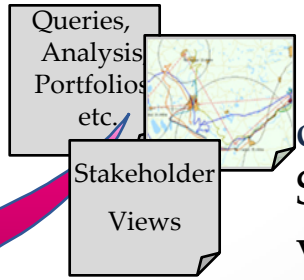
Industry Reference Models

Application Models

Application Glossaries

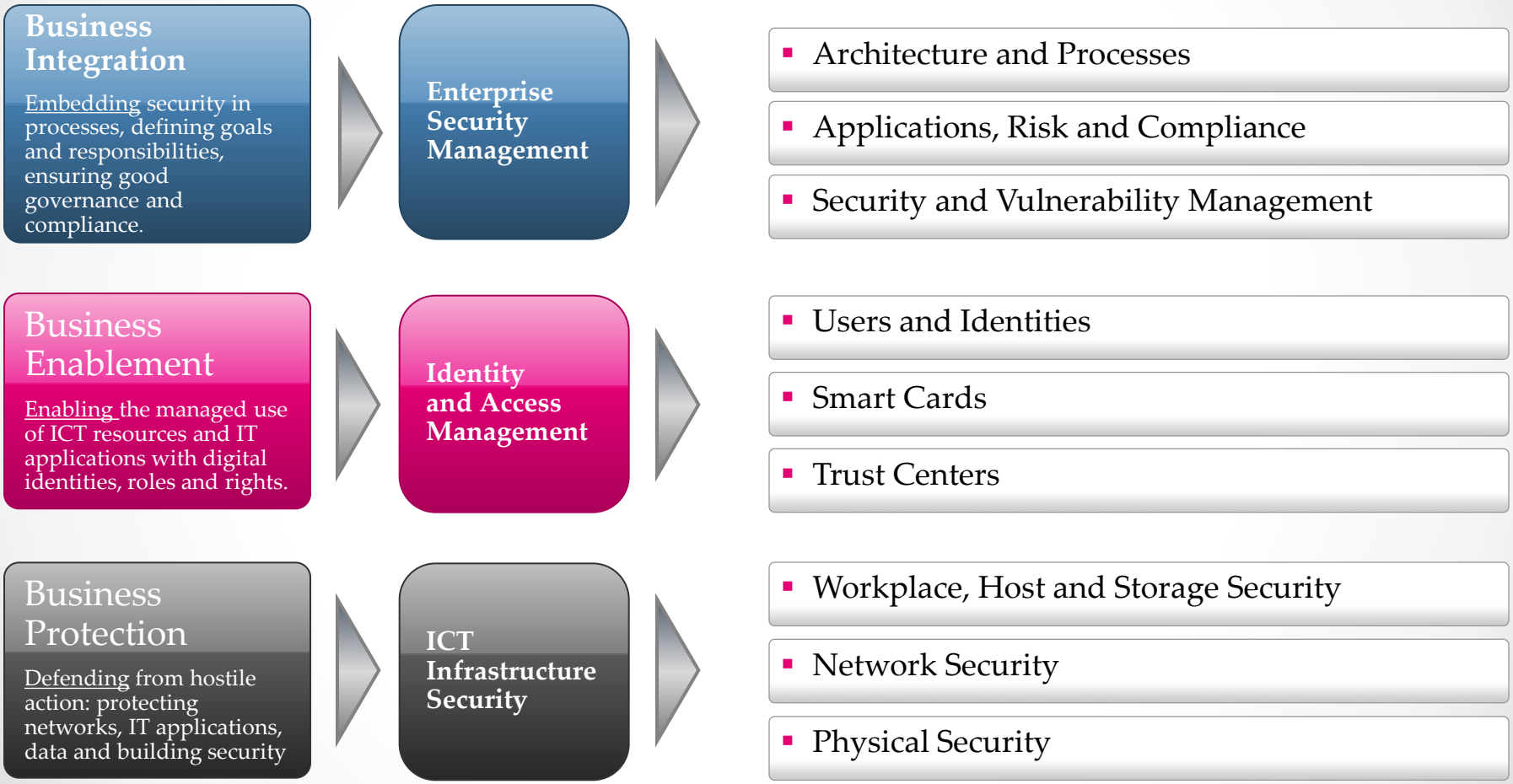
"Meta-Model"
Common Language

"Real World"
Enterprise applications teams & information



"Integrated and consistent Views"
Stakeholder specific views & reports

ICT Security Services and Solutions



If you have one last breath use it to say...