

# SABSA Foundation

SABSA Chartered Architect  
Foundation Level (SCF)  
v2.4.3

# F2 – Security Management & Design

# Module F2 – Course Outline

- Section 12 – Asset Architecture & Management
- Section 13 – Risk & Policy Management Architecture
- Section 14 – Transformation & Service Architecture
- Section 15 – Entity & Trust Framework
- Section 16 – Inter-domain Security Associations
- Section 17 – Service Sequencing & Performance

# F2 Question Domains / Materials Cross-reference

1. What (assets) – F2 sections 12
2. Why (risk & motivation factors) – F2 sections 13
3. How (process factors) – F2 section 14
4. Who (people factors) – F2 section 15
5. Where (location factors) – F2 section 16
6. When (temporal factors) – F2 section 17

# Asset Architecture & Asset Management

## Section 12

# Scope: Design Phase - Assets

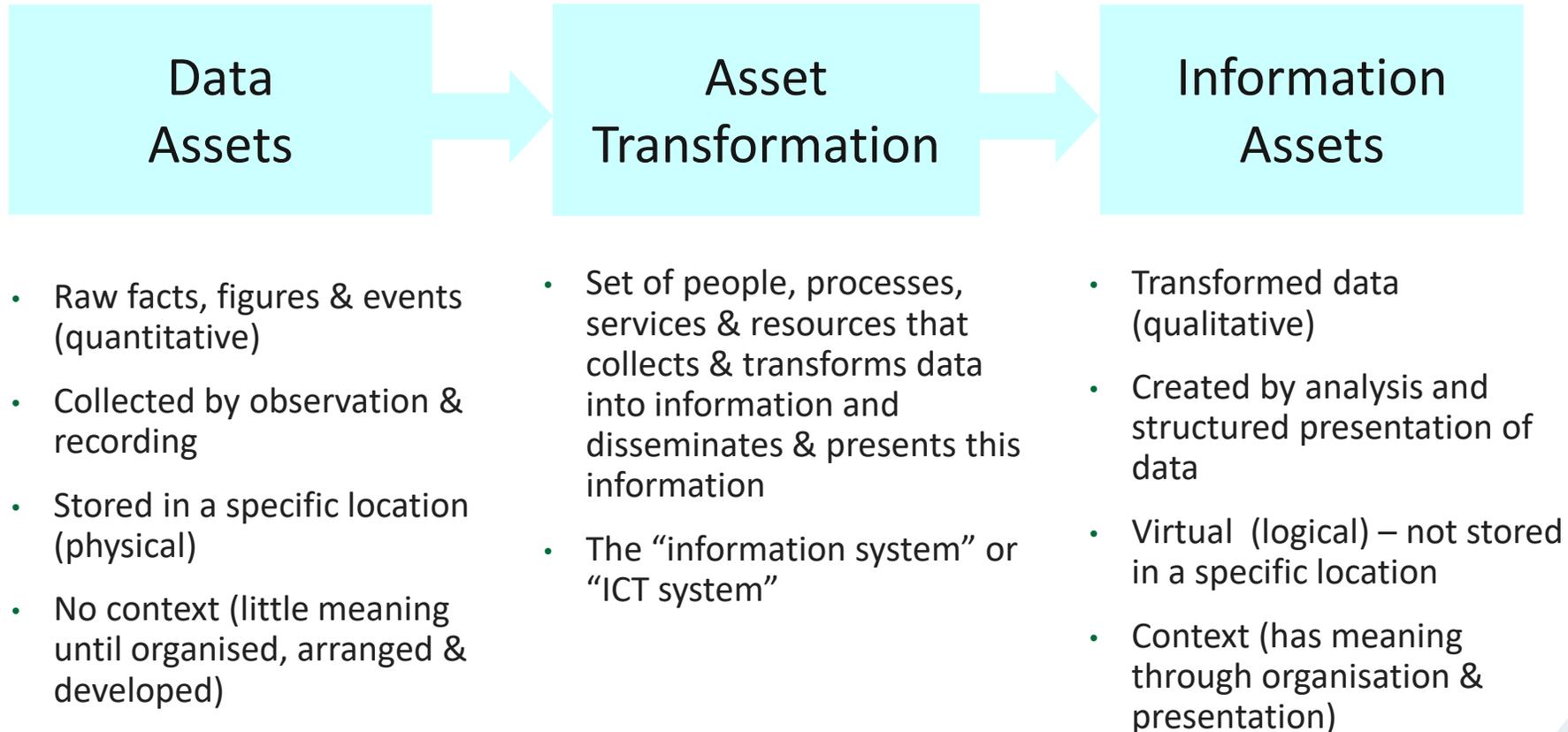
	Architecture Matrix	Management Matrix
Logical	<b>Information Assets</b>	<b>Logical Asset Management</b>
	Inventory of Information Assets Information Model of the Business	Knowledge Management; Release & Deployment Management
Physical	<b>Data Assets</b>	<b>Physical Asset Management</b>
	Data Dictionary & Data Storage Devices Inventory	Change Management; Platform & Data Storage Management
Component	<b>Component Assets</b>	<b>Component Management</b>
	Products and Tools, including Data Repositories and Processors	Product & Component Standards Management

# Section 12 Competency Objectives

## Competency / Question Domain 1 – What (Assets)

Knowledge Element	Knowledge Competency	Comprehension Competency
The SABSA Matrix	Describe the characteristics & deliverables of the SABSA Architecture Design Phase layers	Explain the constructs & characteristics of, and distinguish between assets at logical, physical & component layers
	Describe the principles of aligning & integrating SABSA's lower layers with other established frameworks & standards	Summarise approaches to aligning & Integrating architectural frameworks & standards
Service Management	Identify the role of SABSA techniques for security in Release & Knowledge Management	Explain Release & Knowledge Management in terms of SABSA assets & attributes
Start-up Approaches	List and define possible start-up approaches to SABSA Enterprise Security Architecture	Differentiate between start-up approaches & interpret the benefits and challenges of each to recommend appropriate approaches for organisational circumstances

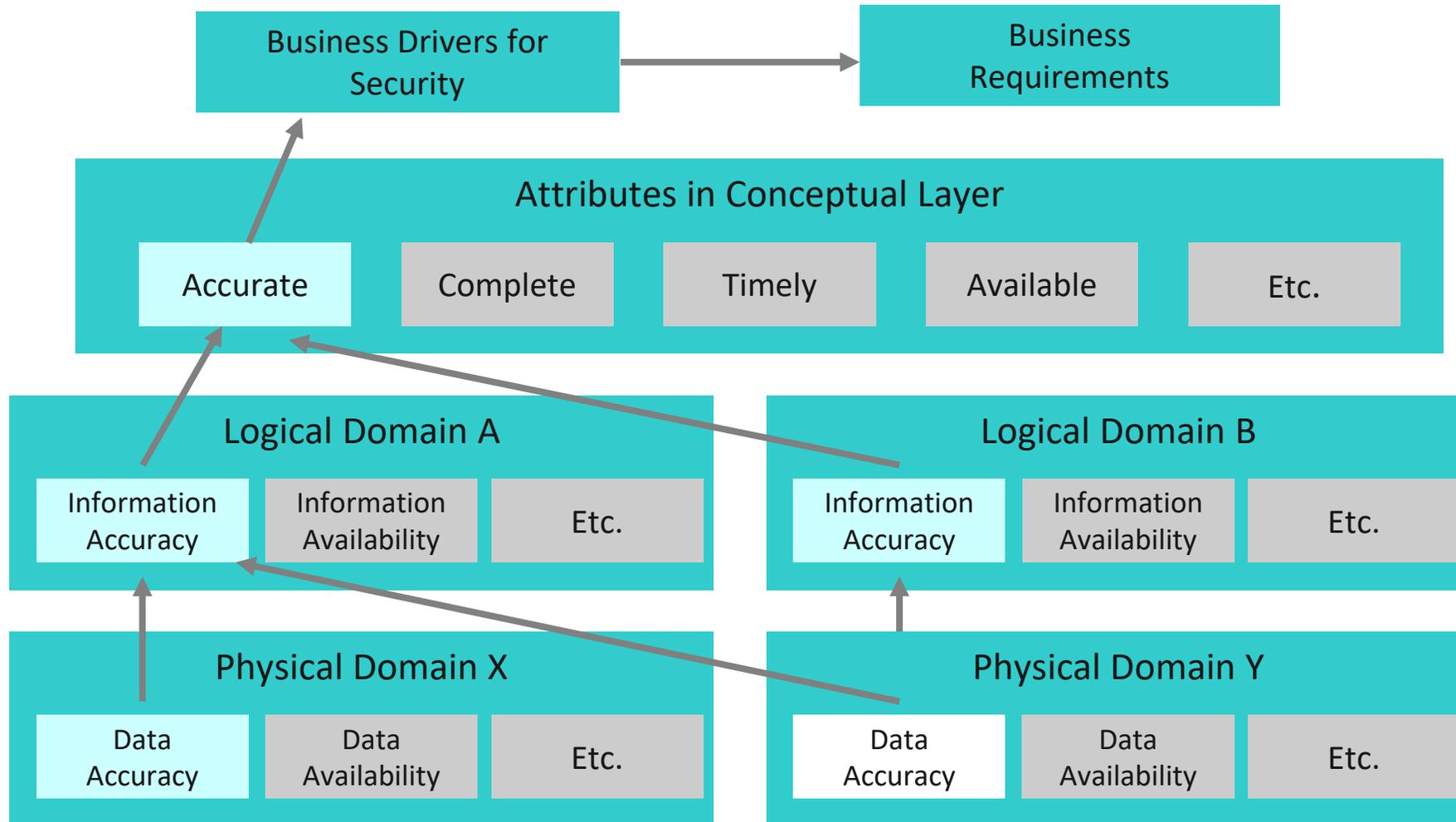
# Constructs & Characteristics of Assets



# Asset Value in SABSA

- The purpose of information is to contribute to business knowledge for decision-making
- Information value is achieved if it has certain properties such as:
  - Accuracy & Completeness
  - Timeliness & Availability
  - Relevance
- Similar properties are required for the data assets to be transformed to create the information, and the management assets of the information systems that perform the transformations
- SABSA traceably derives these properties from the Conceptual Attributes
- Attributes performance targets also provide added-value by ensuring the quantity of assets (and the quantity of asset properties) is fit-for-purpose

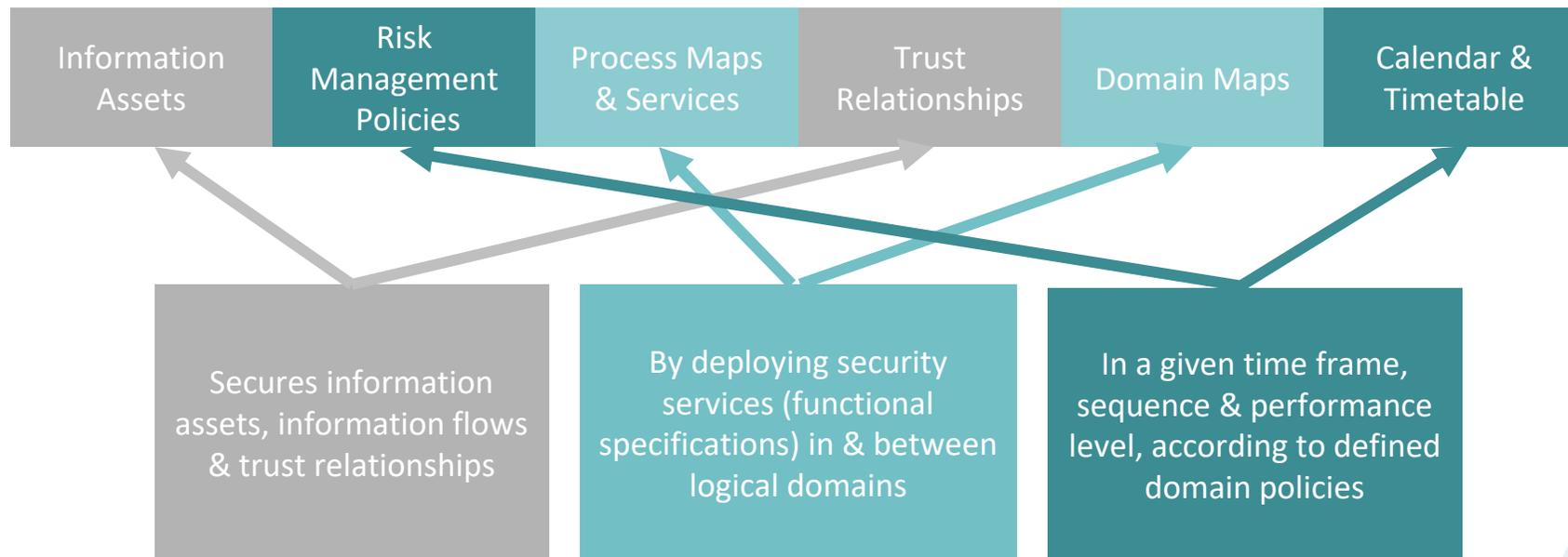
# Relationship With Conceptual Assets



# Overview of the Design Phase Logical Layer

## Logical Architecture

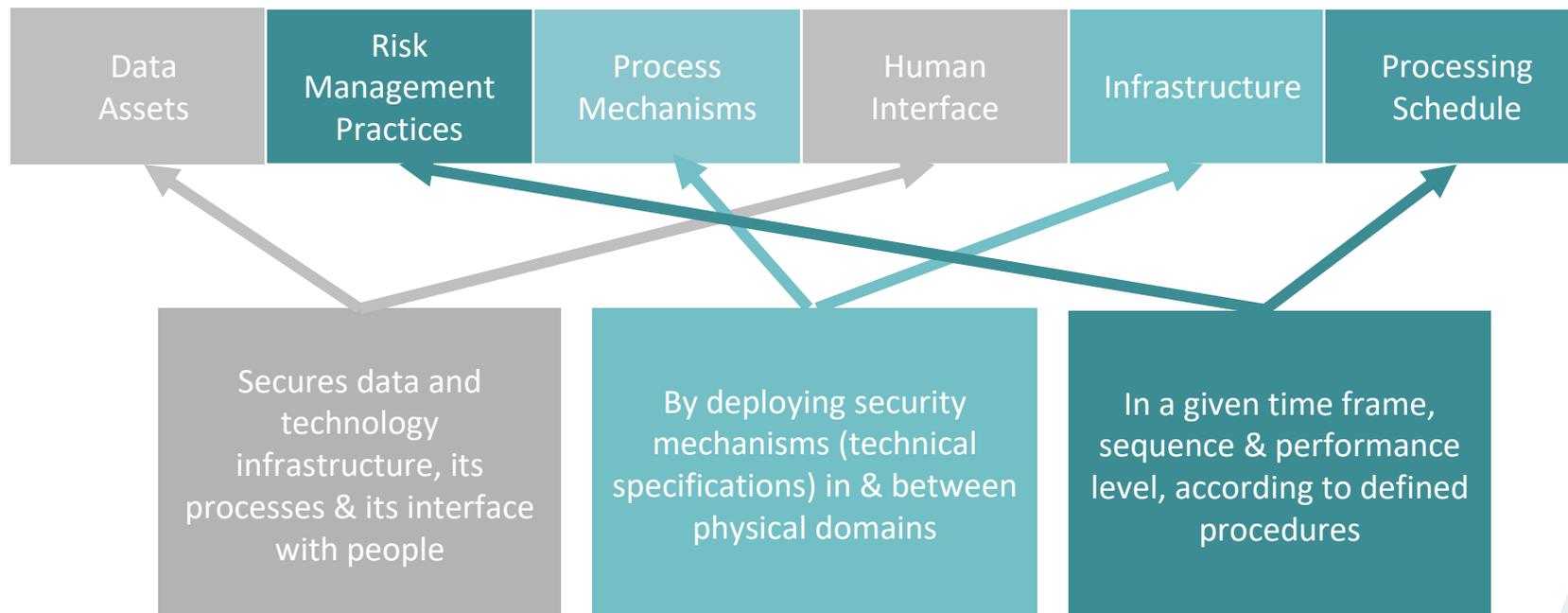
- Logical Architecture is the Designer's View of ICT Systems
- Concerned with information security & systems functionality
- Elements exist in logical domains not tied to specific physical locations



# Overview of the Design Phase Physical Layer

## Physical Architecture

- Physical Architecture is the Builder's View of ICT Systems
- Concerned with data security & infrastructure security
- Technical specifications for systems
- Elements exist in a specific physical domain and location



# Overview of the Design Phase Component Layer

## Component Architecture

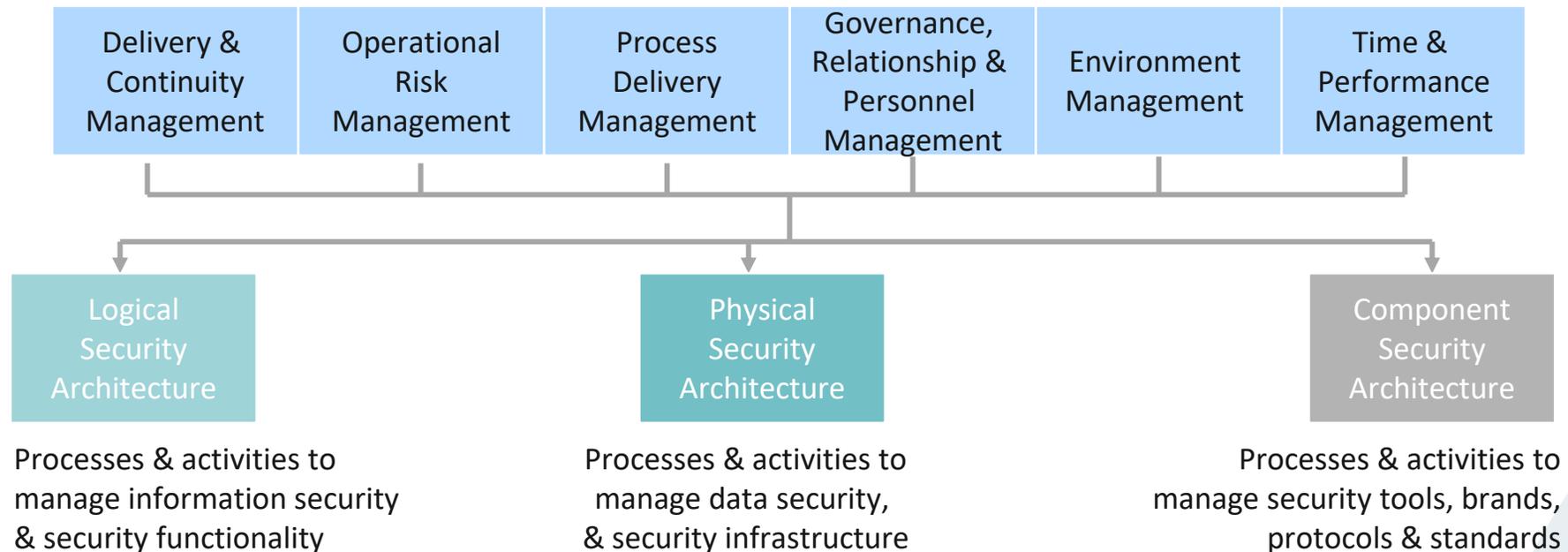
- Components are the Tradesman's View of ICT Systems
- Specialised
  - Tools
  - Brands
  - Specific granular technical specifications & standards
  - Protocols



# Overview of the Design Phase Management Layers

## Management Architecture (Overlaid)

- Management Architecture is the Manager's View of ICT Systems
- Concerned with management processes & activities



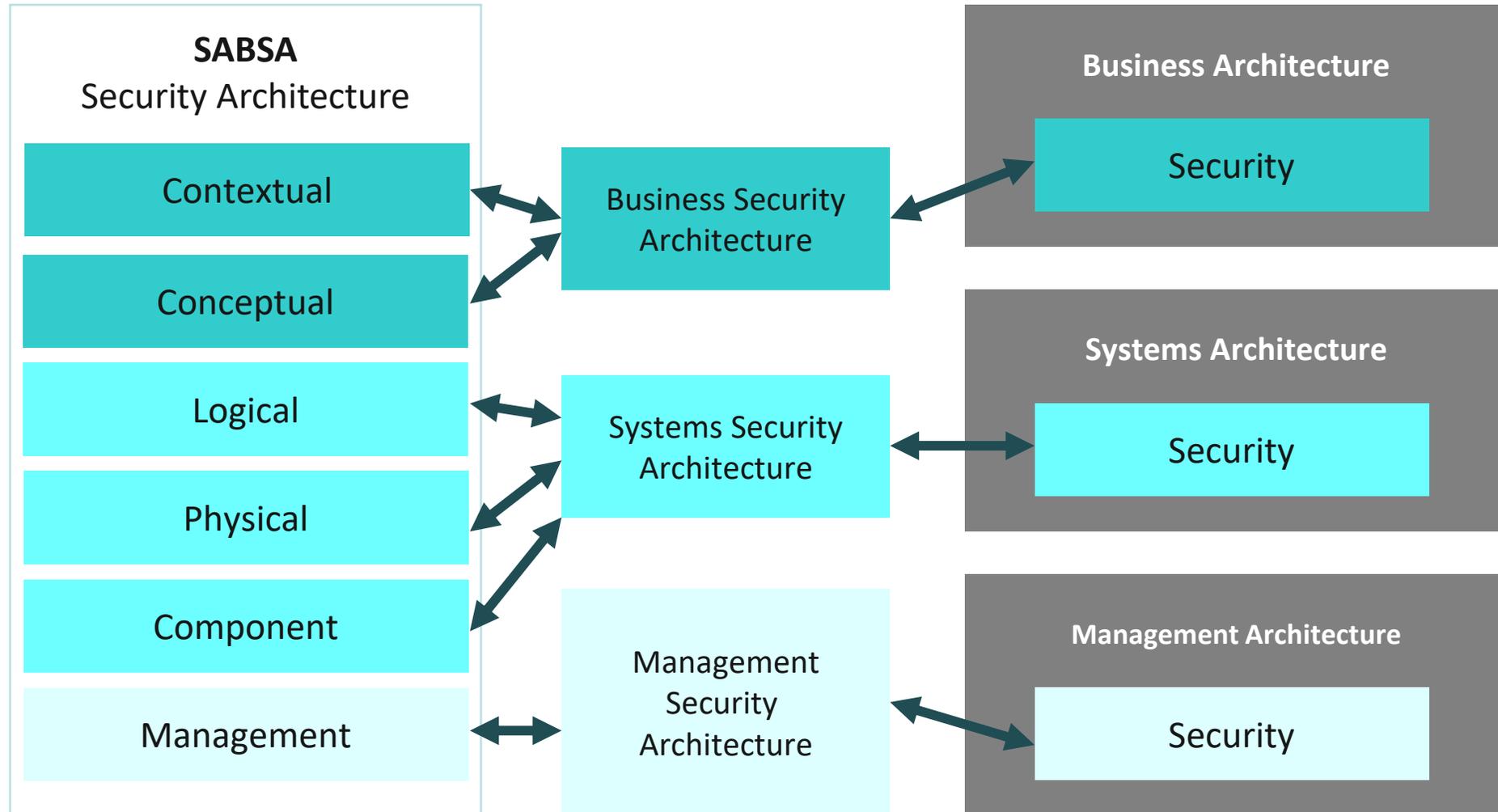
# Architectural Asset Alignment

- In section 3 of Module F1 we discussed the fact that security does not exist in isolation – it is a property of something else (assets)
- It is not possible to define the security architecture of logical, physical & component level assets until the assets themselves have been defined
- The assets are defined, organised and architected in a number of different ways according to other architectural frameworks, approaches and standards
- In the same section we discussed a guiding principle that a good architecture framework must have compatibility
- Therefore the security architect must be capable of demonstrating compatibility and alignment with the frameworks used by other architects

# Build on Existing Strengths

- Organisations may have already invested heavily in architectural frameworks
- No-one wants to reverse or waste that investment
- But frameworks leave gaps for security
- SABSA fills those gaps by being compatible and aligned
  - It doesn't replace other frameworks
  - It builds on their strengths by adding security in a fully aligned way

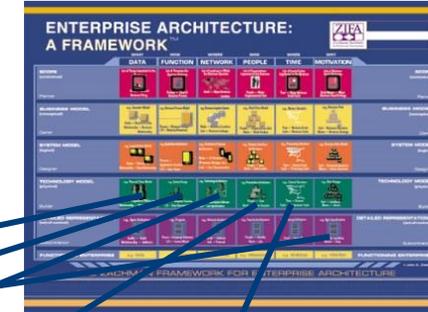
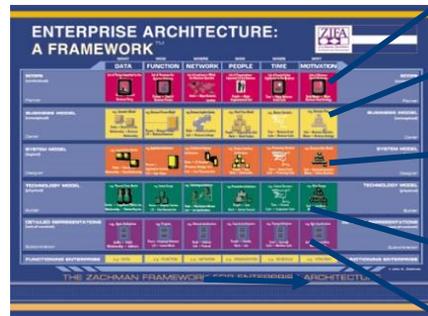
# Align & Enhance, Don't Replace



# TOGAF, SABSA and General Architecture

<b>SABSA View</b>	<b>SABSA Architecture Layer</b>	<b>SABSA Lifecycle</b>	<b>TOGAF Architecture Layer</b>	<b>General (Enterprise) Architecture</b>
Business	Contextual	Strategy and Planning	Architecture Vision/Business	Enterprise
Architect	Conceptual	Strategy and Planning	Business	Enterprise / Service
Designer	Logical	Design	Information Systems	Service / Solution Design
Builder	Physical	Design	Information Systems / Technology	Solution Build
Tradesman	Component	Design	Technology	Solution Components

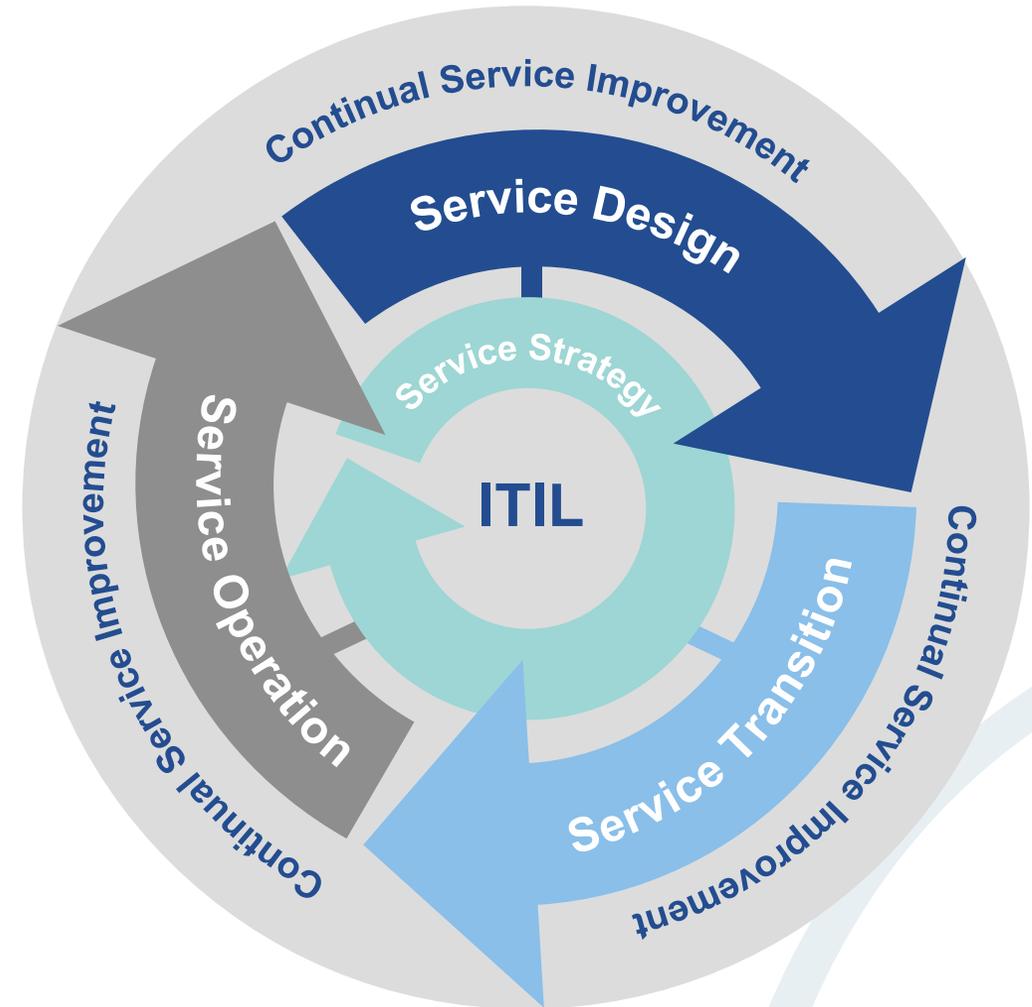
# Zachman Architecture Alignment



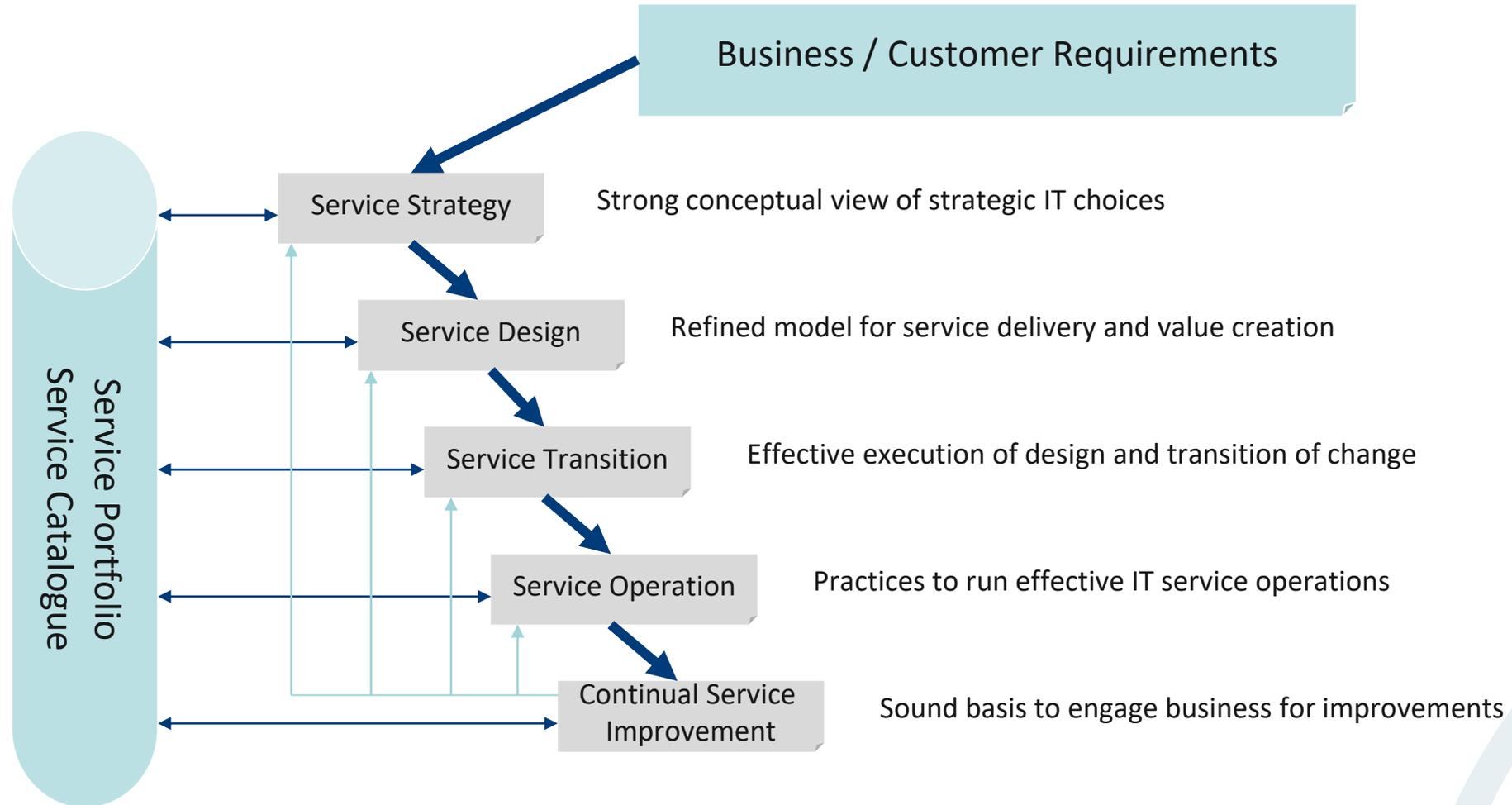
	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Goals & Decisions Business Value; Taxonomy of Business Assets, including Goals & Objectives, Success Factors, Targets	Business Risk Opportunities & Threats Inventory	Business Meta-Processes Business Value Chain; Business Capabilities	Business Governance Organisational Structure & the Extended Enterprise	Business Geography Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Business Time Dependence Time dependencies of Business Goals and Value Creation
CONCEPTUAL ARCHITECTURE	Business Value & Knowledge Strategy Business Attributes Taxonomy & Profile (with integrated performance targets)	Risk Management Strategy & Objectives Enablement & Control Objectives; Policy Architecture; Risk Categories; Risk Management Strategies; Risk Architecture; Risk Modelling Framework; Assurance Framework.	Strategies for Process Assurance Inventory of all Operational Processes (IT, industrial, & manual); Process Mapping Framework; Architectural Strategies for IT used in process support.	Security & Risk Governance; Trust Framework Owners, Custodians and Users; Service Providers & Customers; Trust Modelling Framework	Domain Framework Security Domain Concepts & Framework	Time Management Framework Through-Life Risk Management Framework; Attribute Performance Targets
LOGICAL ARCHITECTURE	Information Assets Inventory of Information Assets; Information Model of the Business	Risk Management Policies Risk Models; Domain Policies; Assurance Criteria (populated Assurance Framework).	Process Maps & Services Information Flows; Functional Transformations; Service Oriented Architecture; Services Catalogue; Application Functionality and Services	Trusts Relationships Domain Authorities; Entity Schema; Privilege Profiles; Trust Relationship Models	Domain Maps Domain Definitions; Inter-domain Associations & Interactions	Calendar & Timetable Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets Data Dictionary & Data Storage Devices Inventory	Risk Management Practices Risk Management Rules & Procedures; Risk Metadata	Process Mechanisms Working Procedures; Application Software; Middleware; Systems; Security Mechanisms; Process Control Points	Human Interface User Interface to Business Systems; Identity & Access Control Systems	Infrastructure Workspaces; Host Platforms, Layout of Devices & Networks	Processing Schedule Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	Component Assets Products and Tools, including Data Repositories and Processors	Risk Management Components & Standards Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Process Components & Standards Tools and Protocols for Process Delivery; Application Products	Human Entities: Components & Standards Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Locator Components & Standards Nodes, Addresses and other Locators; Component Configuration	Step Timing & Sequencing Components and Standards Time Schedules; Clocks, Timers & Interrupts
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management Assurance of Operational Excellence & Continuity	Operational Risk Management Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Process Delivery Management Management & Support of Systems, Applications & Services	Governance, Relationship & Personnel Management Management & Support of Enterprise-wide and Extended Enterprise Relationships	Environment Management Management of Buildings, Sites, Platforms & Networks	Time & Performance Management Management of Calendar and Timetable

# ITIL V3 Service Lifecycle

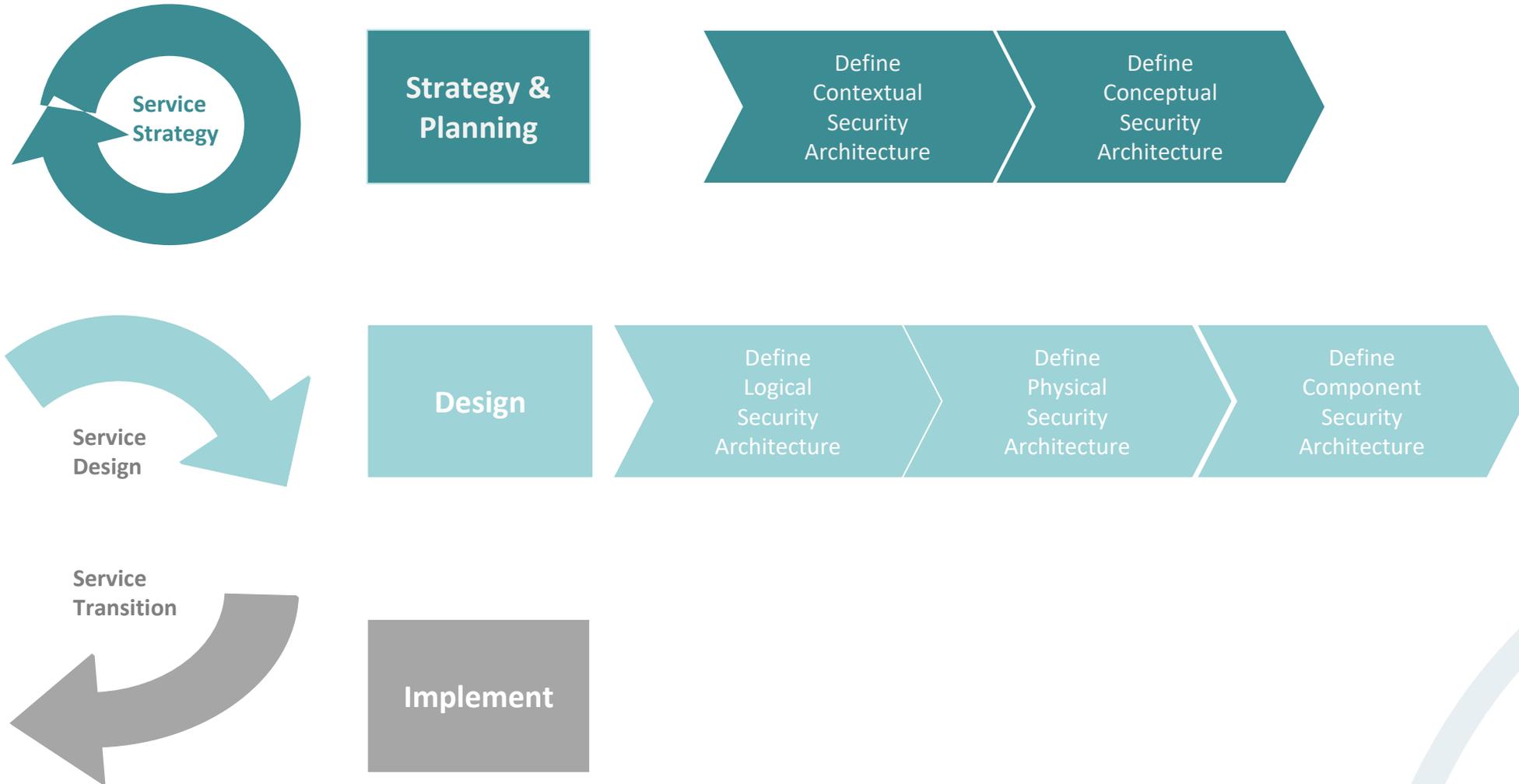
- Published mid 2007
- Changes the V2 principles of scope
- Moves to a focus on “service lifecycle”
- Positions the lifecycle within a feedback loop of continual improvement



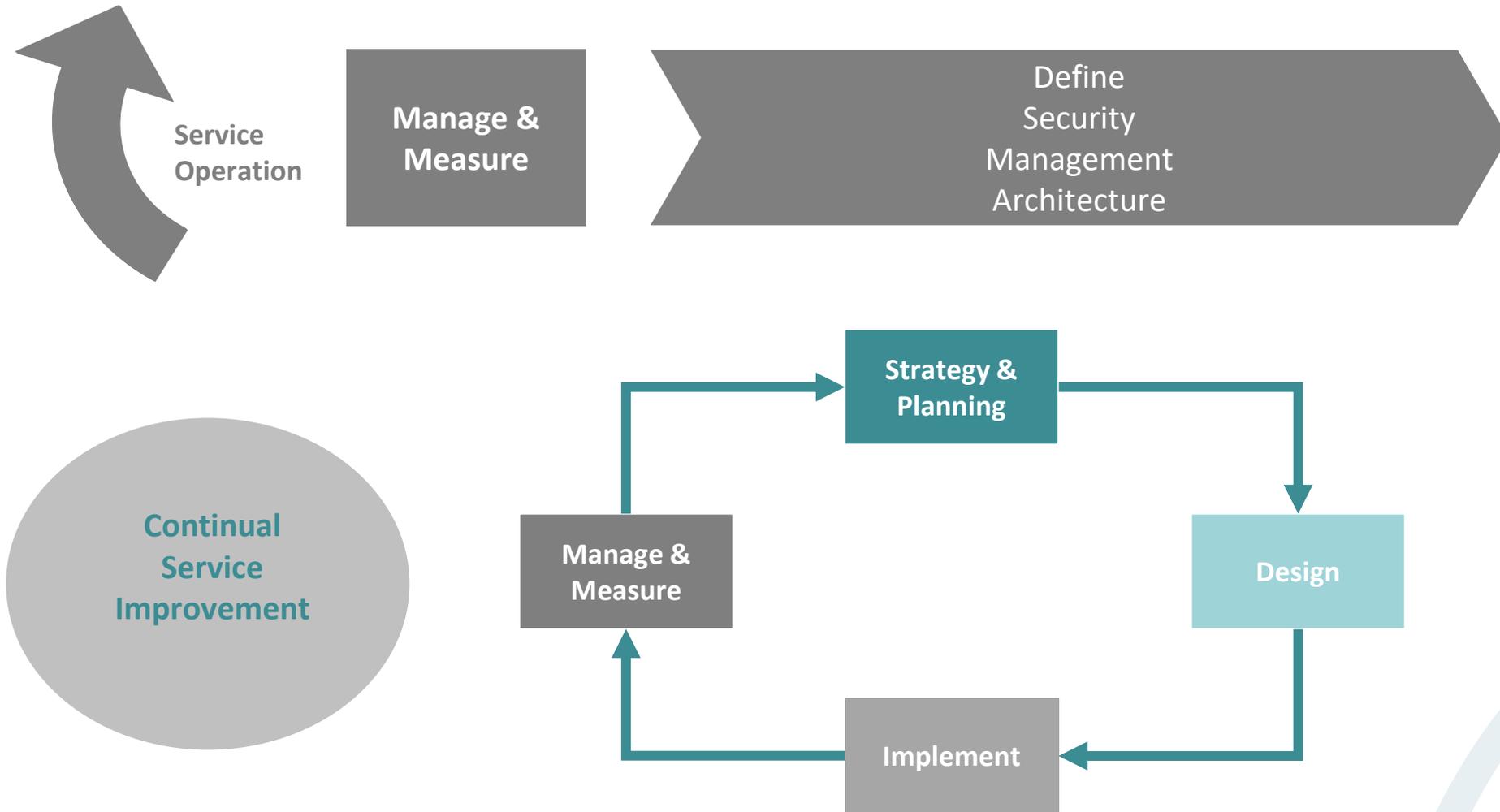
# ITIL V3 Service Lifecycle



# SABSA and the ITIL Service Lifecycle



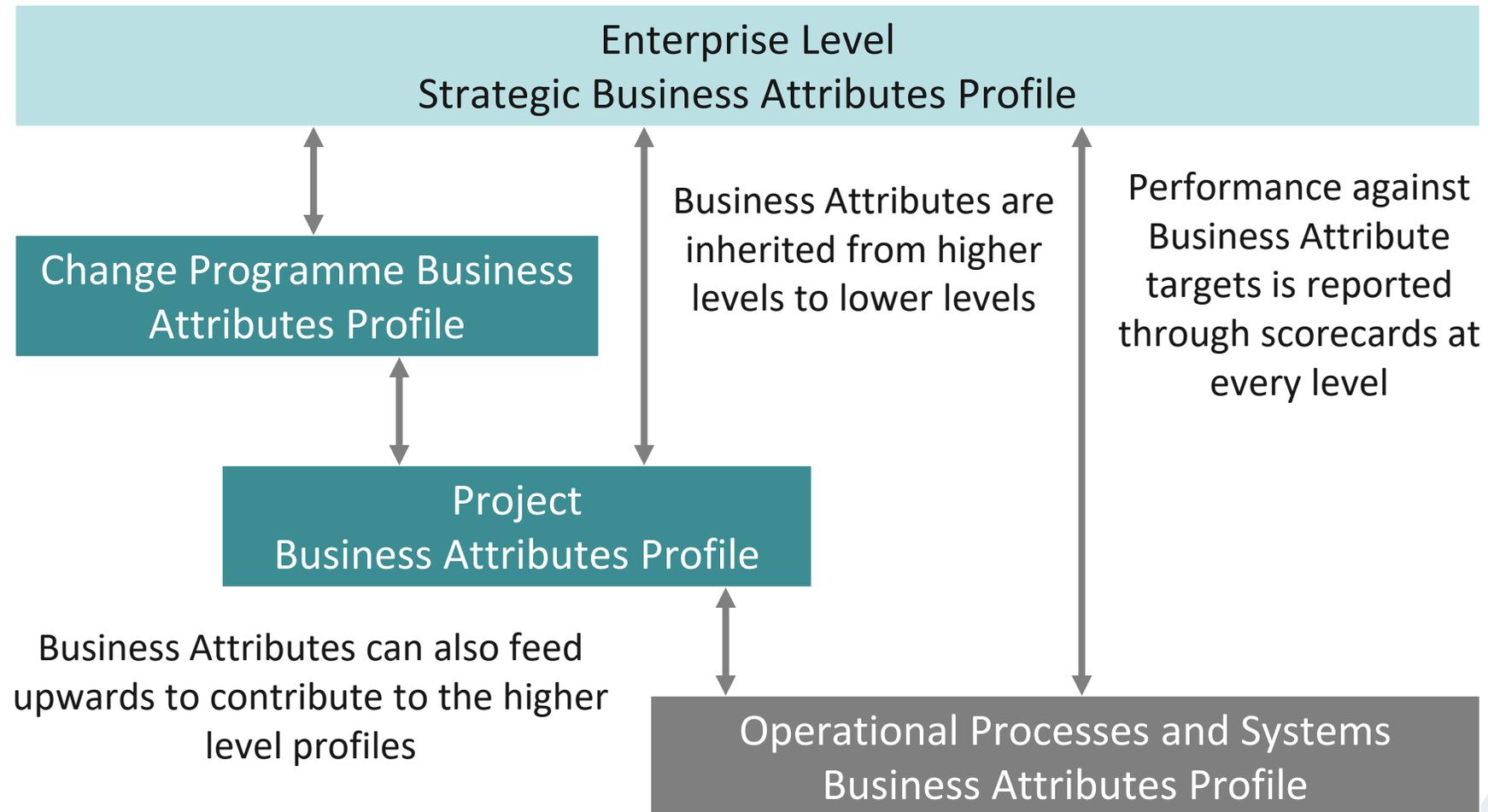
# SABSA and the ITIL Service Lifecycle



# Release & Deployment Management

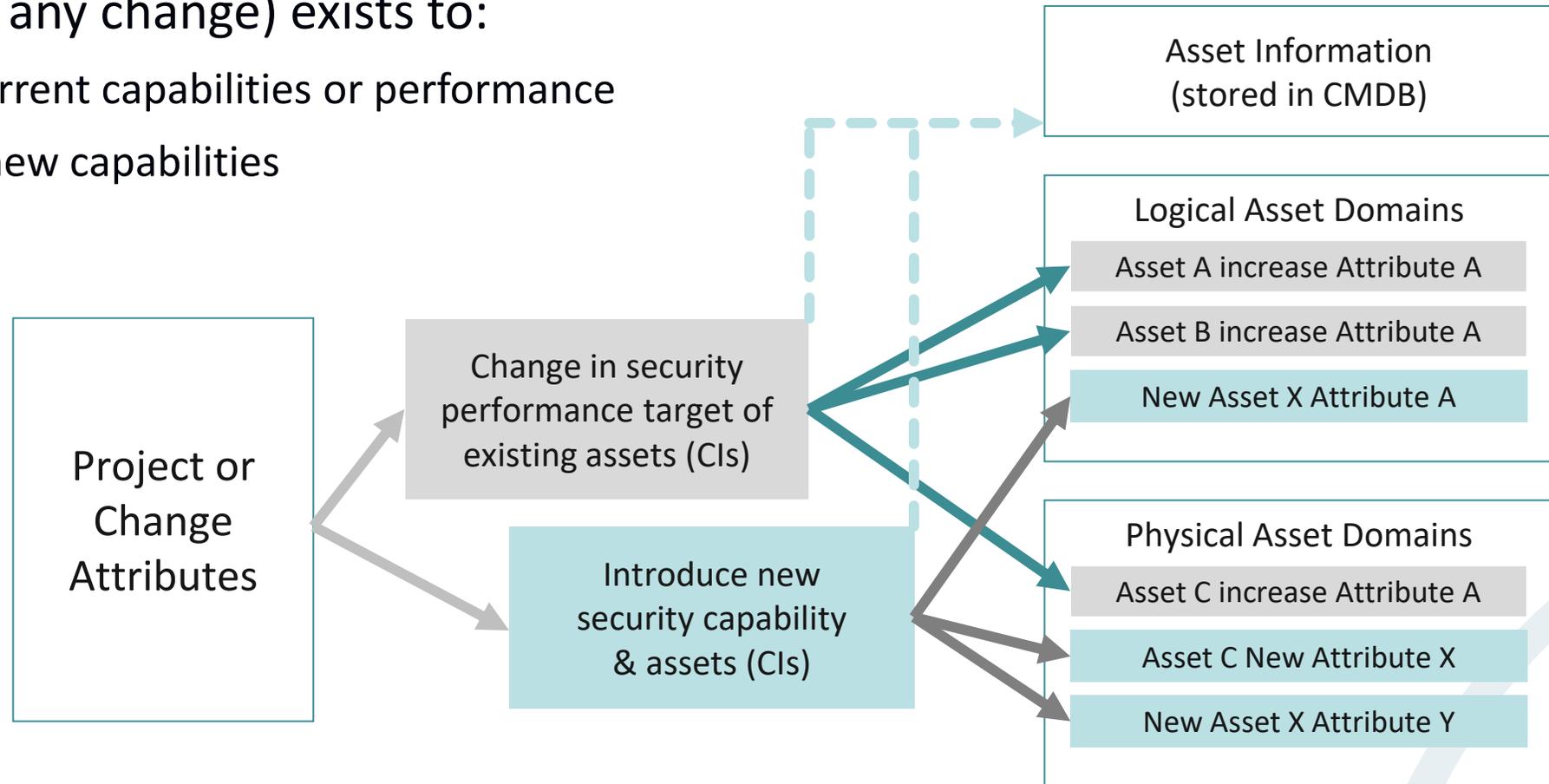
- In the Service Management field, assets (information, data, and all of the elements of the ICT system) are called *Configuration Items (CI)* and stored in a *Configuration Management Database (CMDB)*
- Objective of Release & Deployment Management is to build, test and deliver the capabilities and resources to provide the required services
- A *Release* is set of new or changed CIs that will be released into production together

# SABSA Lifecycle Domain Risk Perspectives



# SABSA in Release & Deployment

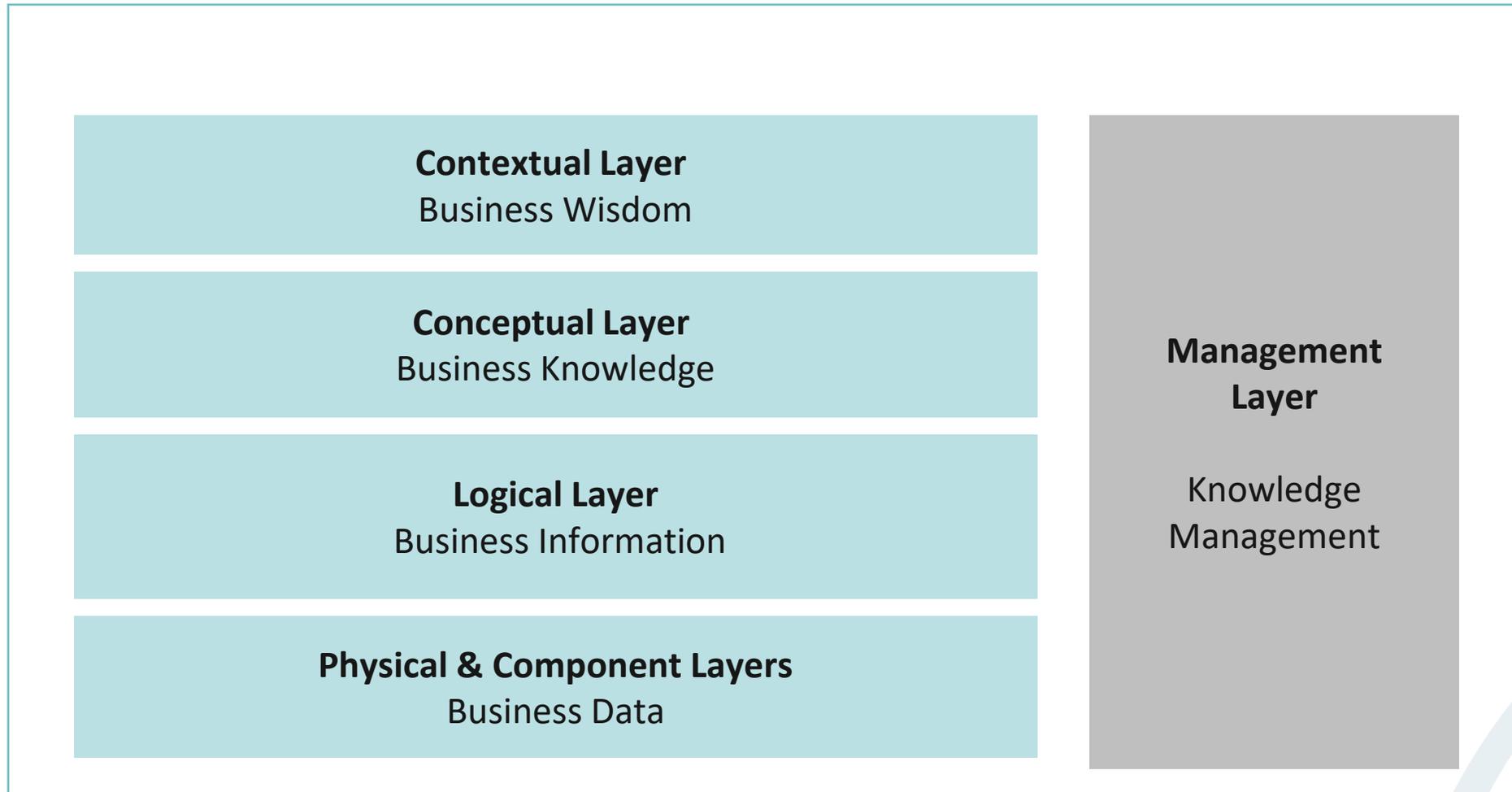
- A project (or any change) exists to:
  - Improve current capabilities or performance
  - Introduce new capabilities



# Knowledge Management

- Knowledge Management improves the quality of decision making by ensuring that reliable information is available during the service lifecycle
- Knowledge is aggregated and contextualised through the SABSA Architecture layers
- The layer-mapping technique discussed in module F1 is the mechanism for delivering knowledge for:
  - Asset risk status
  - Asset risk & enablement performance
  - Re-usability of assets to meet control & enablement objectives
  - Completeness, justification & assurance
  - Managing change

# Knowledge Management Layer-Map



# Implementation Approach

- Implementation is an important part of the lifecycle but the SABSA Matrix does not define a specific implementation layer
  - No need to re-invent Prince2 or PMI etc.
- Rare that a major strategic enterprise-wide security architecture is implemented as a single project
- More likely (and more sensible) is that the architecture provides a blue-print and a road-map that guides a whole series of separate implementation projects, each of which is driven by a specific business initiative and funded by a budget associated with that initiative

# Start-up Approaches

- Executive Interview Approach
  - Requires access to stake holders
- Analysis followed by validation
  - No access to stake holders
  - Team research & assumptions
  - Review, consensus & sign-off of strategy
- SABSA Fast-Track
  - Full scope experience & proof of concept
  - Limited financial liability & commitment
  - Requires access to full team & stake holders
- Blended Approach
  - Complex or distributed organisations often require a combination of the other three approaches

# Fast-Track Start-up Concept

- Based on intensive facilitated workshops
- Heavily customised to the specific needs of the client organisation
  - Starting position & architectural maturity
  - Key programmes & risk priorities
- Key players experience every aspect of the programme in a short time
  - Workshops often run in parallel syndicate groups to ensure scope is covered
  - Some types of people such as senior managers attend only a restricted sub-set of the workshops
- Post-workshop report
- Key objectives: straw-man models, realistic programme plan, proof-of-concept
- Scope: unlike other approaches covers full-scope of SABSA

# Fast-Track Work Programme - Advance

- Gain an initial understanding of the organisation, its goals and objectives, through research and an analysis of documents supplied in advance by the Fast-Track host
- Gain an initial understanding, through an analysis of documents supplied in advance, of the current security and technology environment or the position of any architecture program that has already commenced
- Gain an initial understanding of the roles of all of the proposed Fast-Track participants and their objectives
- Draft, prioritise and agree the specific Fast-Track objectives and deliverables
- Draft, structure and agree the five-day program and its detailed contents
- Compile and customise all presentations for delivery
- Design and produce appropriate detailed workshops

# Fast-Track Work Programme - Workshops

- Customisation of planned presentations to meet new objectives
- Development of new or replacement presentations to be introduced into the program
- Customisation of participant workshops to meet new or refined objectives
- Development of new or replacement participant workshops to be introduced into the program
- End of day status meetings to review progress against objectives and to plan mechanisms that must be introduced to meet altered priorities or objectives
- Review workshop output and document key architecture components

# Fast-Track Work Programme – Post Workshop

- Documented summary of the business case for Security Architecture development activities
- Documented summary of a plan to collect and verify the full set of security business requirements
- Documented summary of the outline presentations and draft reports developed during the on-site program, and advice on progressing these to definitive and detailed architecture plans
- Summary of existing Architecture layers and a high-level gap analysis against stated strategic architectural requirements
- Advice on a means to integrate the Security Architecture with any existing or in-progress developments of business or technology architecture
- High-level implementation and migration strategy
- Summary of Key Performance Indicators (KPI) for Security
- Documented draft project plan to communicate key tasks, milestones, and future deliverables, together with any key dependencies revealed from an analysis of the on-site program
- Documented draft project plan summary illustrating what is needed to complete the Security Architecture, when it is needed, and what resources are required

# Interview Approach – Who to Interview

- Hierarchical Structure
  - May be many Executives & Senior Managers
  - Some have multiple responsibilities
  - Some have many staff - some not
  - Too many decision makers to interview?
- Process Structure
  - Identify key processes
  - Few, clearly identified 'Chiefs'
  - Best positioned to answer



# Executive Interview Risks & Opportunities

- Risks

- Tired of being interviewed by IT
- Limited Access Time & Availability
- Language Barrier
- Failure to Attain Buy-in and Support
- Raised Expectations
- Conflicting Priorities
- Project Exposure
- One-chance Opportunity

- Opportunities

- High Level Buy-in, Endorsement & Support
- Direct Stakeholder Validation
- Positive Project Exposure & Momentum
- Establish Departmental 'Champions'
- Building Bridges to the Business Managers
- "The Value of the Process Itself Is More Important Than the Value of the Results"

# Interview Criteria & Aims

- Criteria:
  - Ensure Requirements Come From Key Business Decision Makers
  - Ensure Requirements Are Current & Future
  - Validate Our Understanding
- Aim To Understand:
  - Culture and Business Environment
  - Business Risks, Opportunities, Strategies
  - Constraints & Motivators
  - Business Relationships & Priorities
  - Attitudes & Awareness Levels

# Gaining Consensus

- Build and maintain strong relationships with the key players
- Facilitated consensus sessions or direct meetings
- Find out what makes them tick
  - Do they have any concerns?
  - Are they pre-disposed for or against any particular approaches?
  - What will you need to do to get their agreement to the conceptual security architecture?
  - What level of influence do they expect to have?
  - What type of involvement in the process do they expect?
  - Who are their key allies / opponents?
  - What specific 'buttons' do they have that you will need to 'push'?
- Foresee difficulties & manage expectations
- Pre-sell the ideas
- Politics & diplomacy

# Appendices F2-1 & F2-2

- Sample interview scripts
  - Start-up
  - Validation

# Sample Questions

## Competency Domain 1

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



# Competency Domain 1

- Which ONE of the following statements about the Fast-Track facilitated workshop approach to SABSA start-up is TRUE?
  - A. Fast-Track creates deliverables for only one SABSA Architecture Layer
  - B. Fast-Track facilitated workshops are dependent upon week-long access to Executive Management
  - C. Fast-Track requires long-term investment of finances and resources in order to deliver 'proof of concept' for the SABSA method
  - D. Fast-Track provides key participants in the architecture project with the opportunity to experience the full scope of SABSA in a short time frame

# Competency Domain 1

- A diagram that shows the location in a distributed computing environment of ICT infrastructure is described as which ONE of the following?
  - A. Component Architecture
  - B. Physical Architecture
  - C. Logical Architecture
  - D. Conceptual Architecture

# Risk & Policy Management Architecture

## Section 13

# Scope: Design Phase - Motivation

	Architecture Matrix	Management Matrix
Logical	<b>Risk Management Policies</b>	<b>Policy Management</b>
	Risk Models; Domain Policies; Assurance Criteria (populated Assurance Framework).	Risk Modelling; Management of Policy Development & Maintenance. Policy Publication & Compliance Management
Physical	<b>Risk Management Practices</b>	<b>Risk Data Management</b>
	Risk Management Rules & Procedures; Risk Metadata	Risk Procedure Management; Risk Metadata Management
Component	<b>Risk Management Components &amp; Standards</b>	<b>Risk Management Components</b>
	Risk Analysis Tools; Risk Registers; Risk Monitoring & Reporting Tools	Risk Analysis, Monitoring & Reporting Components, Systems and Standards Management

# Section 13 Competency Objectives

## Competency / Question Domain 2 – Why (Motivation)

Knowledge Element	Knowledge Competency	Comprehension Competency
Risk & Policy Management Architecture	List the requirements for architected controls	Explain the association of architected controls To SABSA Contextual & Conceptual layers
	Identify the role in controls architecture of Pure Risk, Appetite Thresholds, Actuarial Data, & Dynamic Thresholds	Summarise the possible applications of Pure Risk, Appetite Thresholds, Actuarial Data & Dynamic Thresholds
SABSA Assurance Framework	List & label Risk Levels, Policy Levels, Control Levels & Management Activities in Risk & Policy Management	Associate & relate to SABSA Architecture Layers Risk, Policy & Control Levels and Management Activities
	Describe the structure & objectives of the SABSA Assurance Framework	Explain the application of the SABSA Assurance Framework & its relationship with Risk Level

# Relationship With Conceptual Risk & Policy

- Business risks & opportunities exist traceably through every layer of the architecture
- Responsibility for managing enterprise risks & opportunities is delegated to Domains
- Each Domain Policy Authority:
  - Operates within the risk appetite parameters of the super domain
  - Is compliant with the super domain policy
  - Has vested interest in risk performance within their own domain
  - Deploys specific controls & enablers to manage risk according to the architecture layer at which their domain exists
    - e.g. network risk is managed by network controls & enablers deployed in the network domain according to the network security policy

# Complexity of Control Considerations

- Legislation
- Sectoral regulation
- Sectoral standards
- Quality management
- Management style
- Corporate culture
- Risk management
- Technical standards
- IT & Architecture frameworks
- Development lifecycles
- Management frameworks



# Standards Are Not Enough

- Most suggest what may be managed but few advise how
- Some contain control objectives, controls libraries or both
- Almost every organisation needs to adapt them to their specific business sector, culture, terminology, and national legislative and regulatory requirements
- To succeed we need an overarching framework and methodology that ties it all together to design, deliver, and support end-to-end secure processes



# Requirement for Controls Architecture

- Few controls standards are written from the Architect's holistic and structured point of view
- Example: ISO 27001 / ISO 27002 – 11.4 Network Access Control

<p>11.4.1 <b>Policy on use of Network Services</b></p>	<p>Users shall only be provided with access to the services that they have been specifically authorised to use</p>	<p>Policy is at logical layer but requires physical procedures, component configuration standards &amp; operating instructions at the management layer. Implies an authorisation service, mechanisms components &amp; activities</p>
<p>11.4.2 <b>User authentication for external connections</b></p>	<p>Appropriate authentication methods shall be used to control access by remote users</p>	<p>Implies an authentication service, Mechanisms components &amp; activities on at least three different domain levels (external users &amp; networks, &amp; internal networks) plus a means of associating the domains together. Doesn't cover internal users</p>
<p>11.4.3 <b>Equipment identification on networks</b></p>	<p>Automatic equipment identification shall be considered as a means to authenticate connections from specific locations &amp; equipment</p>	<p>Implies physical identification mechanisms &amp; components, the means to verify the identities, &amp; management activities at each layer</p>

# Risk & Policy Management Architecture

Risk Level	Policy Level	Control Level	Management Activity Controls
Business Risks & Opportunities to Logical Domains	Appetite & strategy articulated in Logical Policy	Security Services	Management of Security Services
Risks & Opportunities to Physical Environment & Infrastructure Domains	Managed by Physical Procedures derived from Policy	Security Mechanisms	Management of Infrastructure & Environment
Risks & Opportunities to System Components & Configurations	Managed by Standards for Tools & Products	Security Components	Management of Components, Products & Standards

# Architectural Control Distribution Case Study

Business Context:	Interactions between Government Departments			
Business Drivers for Security:	Information confidentiality in storage & in transit Information integrity in storage & in transit			
Business Attributes:	Confidential	Integrity-Assured	Identified	Authenticated

## Architecture Controls & Enablers

Logical Services: credentials issuance, session authentication, message origin authentication, message integrity, message content confidentiality, non-repudiation, replay protection, stored data integrity protection, stored data confidentiality

Physical Mechanisms: SSL, VPNs, disk encryption, file hashing, message hashing, HSMs, crypto servers, smartcards

Components: x.509 certificates, algorithms (AES, SHA-1, etc) & keys

## Management Controls & Enablers

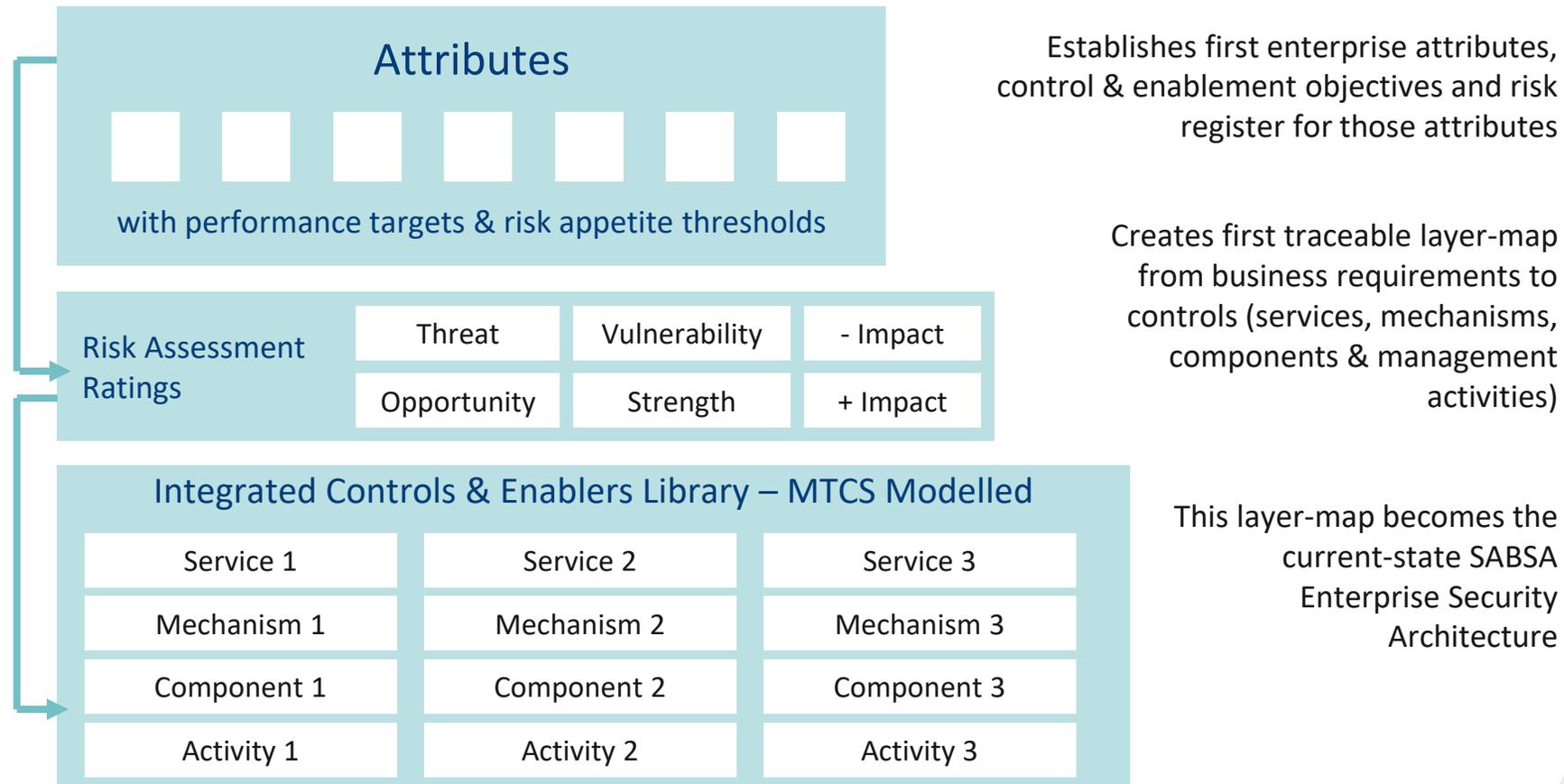
Logical Activities: Registration process, authorisation process, credentials management, certificate policy statement definition

Physical Activities: certification practice statement definition, token management, provisioning, platform management, environment management, network management

Component Activities: user credential management, certificate management, key management

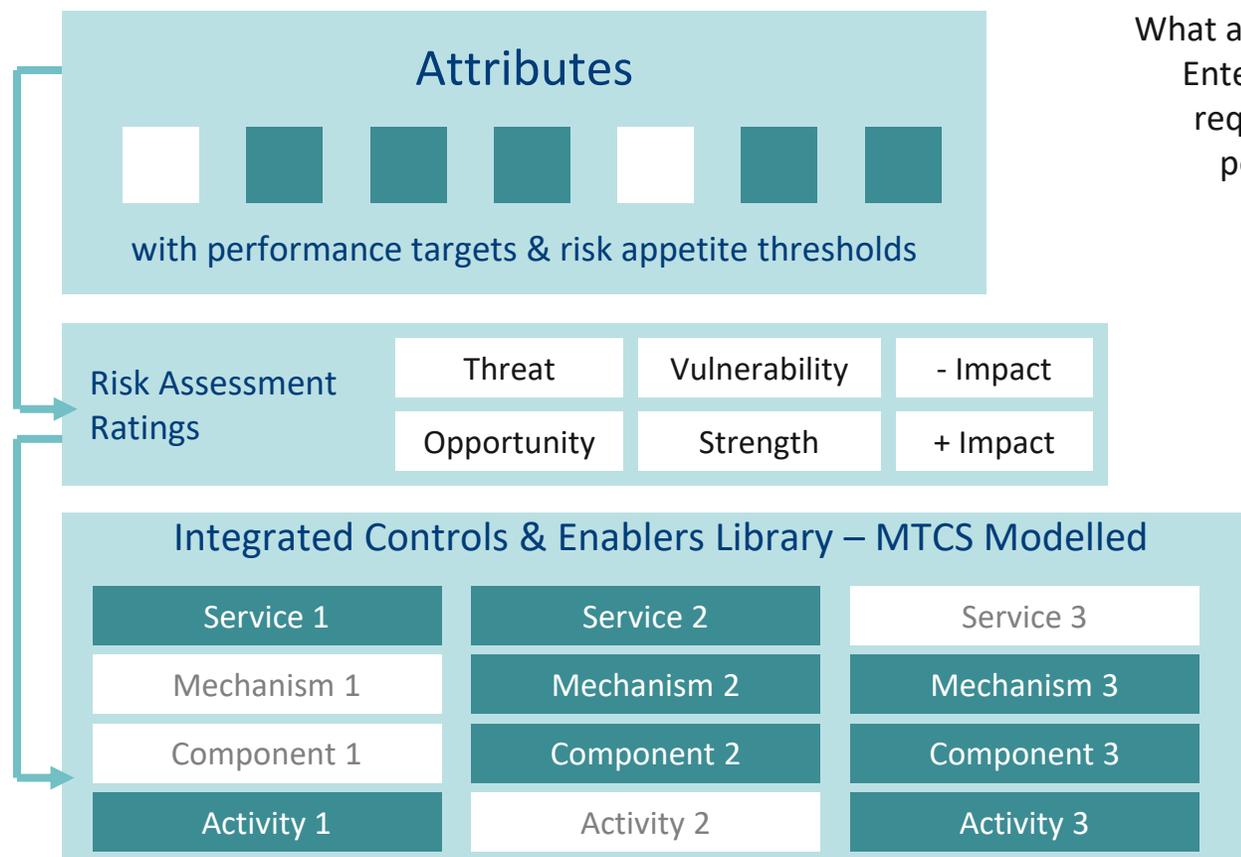
# ORM Architecture Inheritance & Re-use

## SABSA Risk Assessment #1 / Pilot / Establishment Project



# ORM Architecture Inheritance & Re-use

## Subsequent SABSA Risk Assessments / Project – Re-use



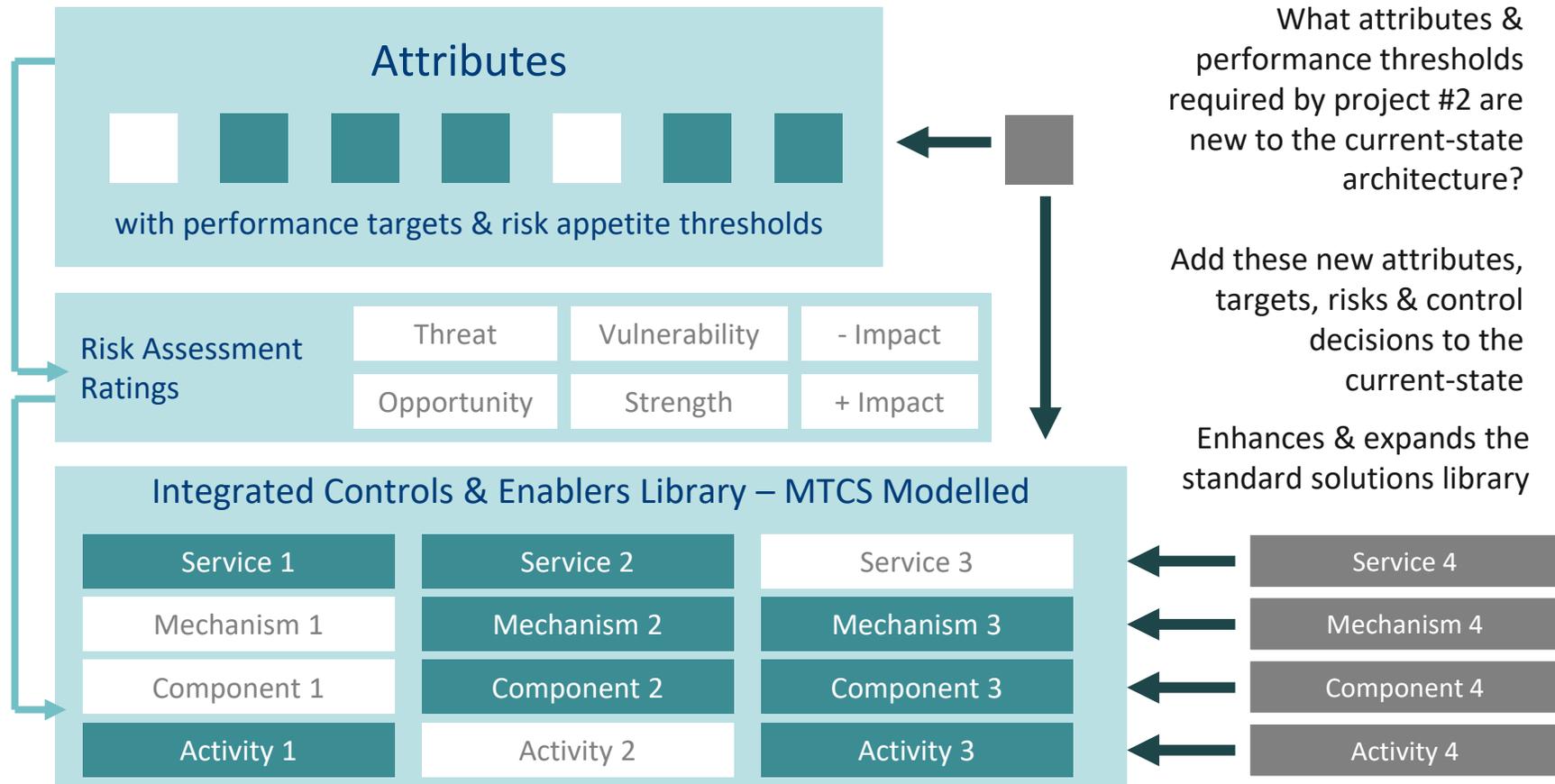
What attributes from the current-state Enterprise Security Architecture are required for project #2 with similar performance bands / thresholds?

We have already analysed and modeled the appropriate controls to achieve these attributes at those performance levels

We have already solved this problem – inherit all entries in layer-map linked to the attributes: re-use our now 'standard' solutions

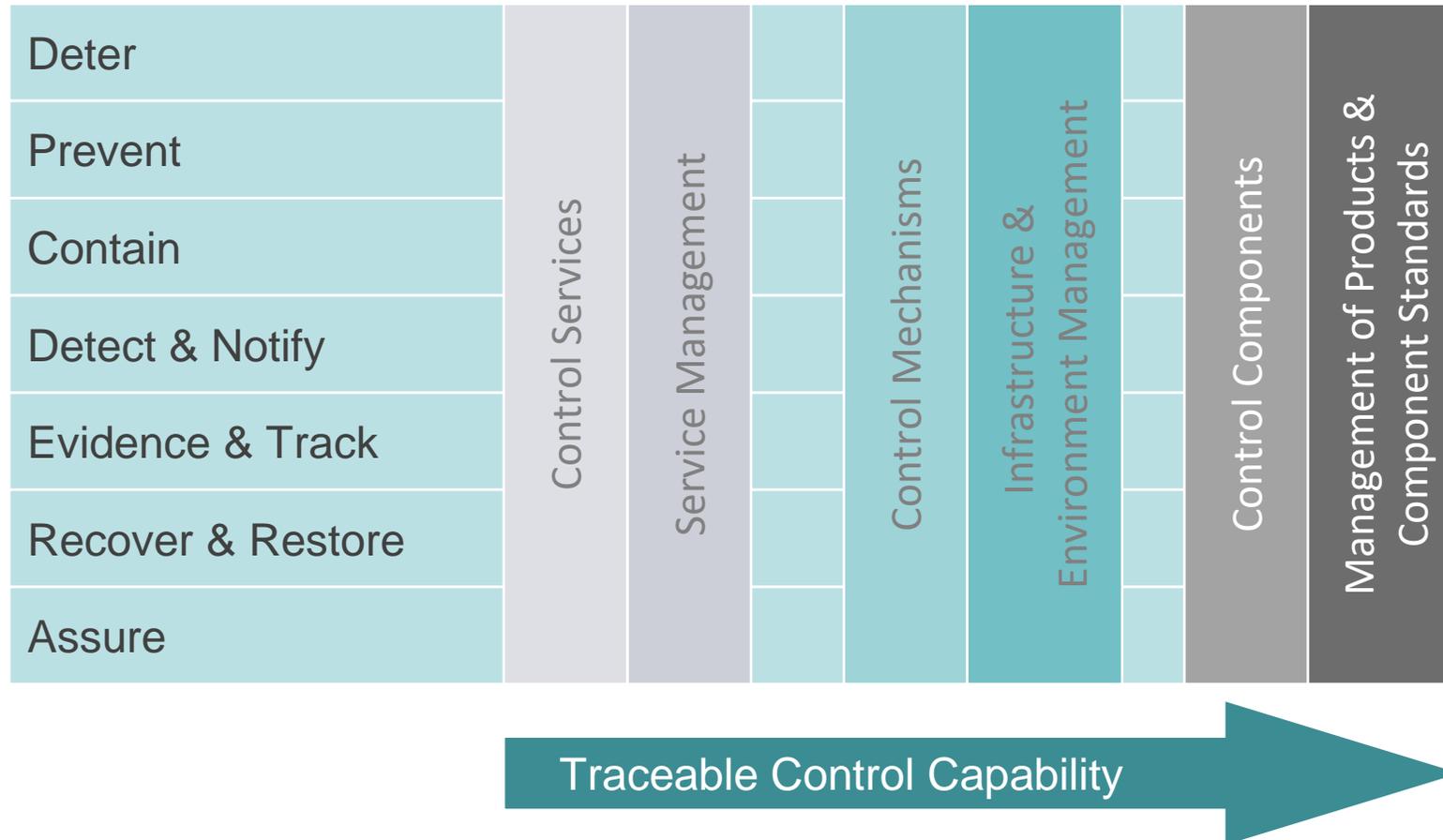
# ORM Architecture Inheritance & Re-use

## Subsequent SABSA Risk Assessments / Projects – Enhance



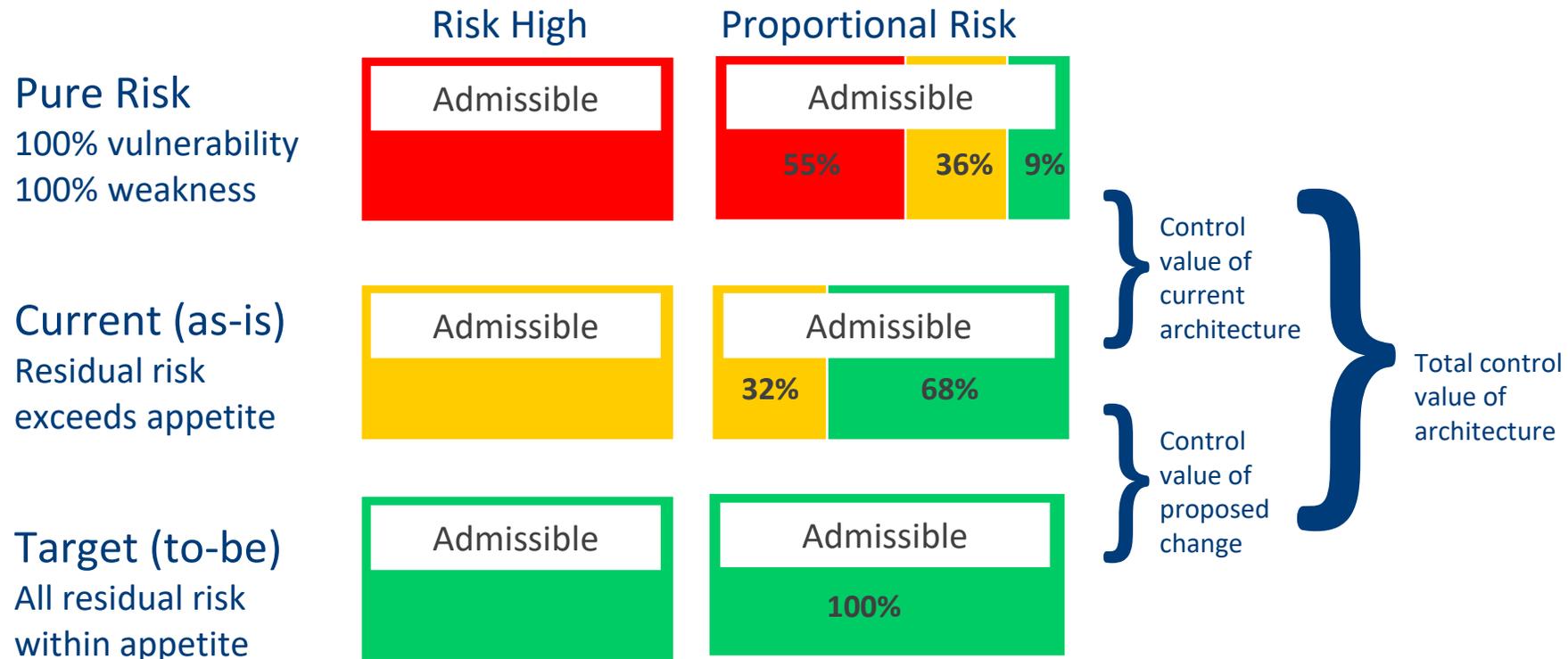
# Strength-in-Depth Capability Engineering

Application of the SABSA Multi-tiered Control Strategy to each architected control layer



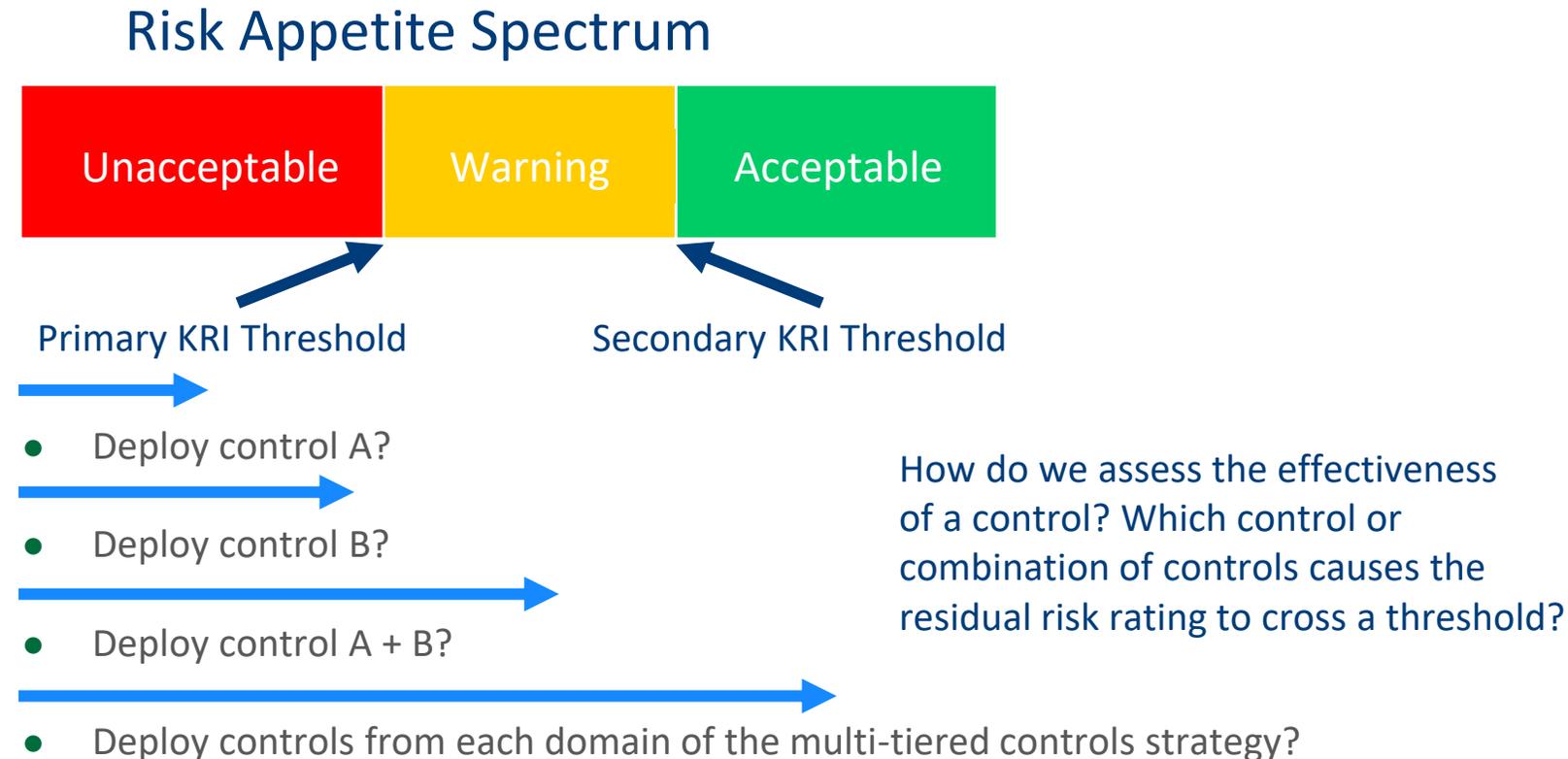
# Risk Assessment in Controls Architecture

## The Role of Pure Risk in Control Value Assessment



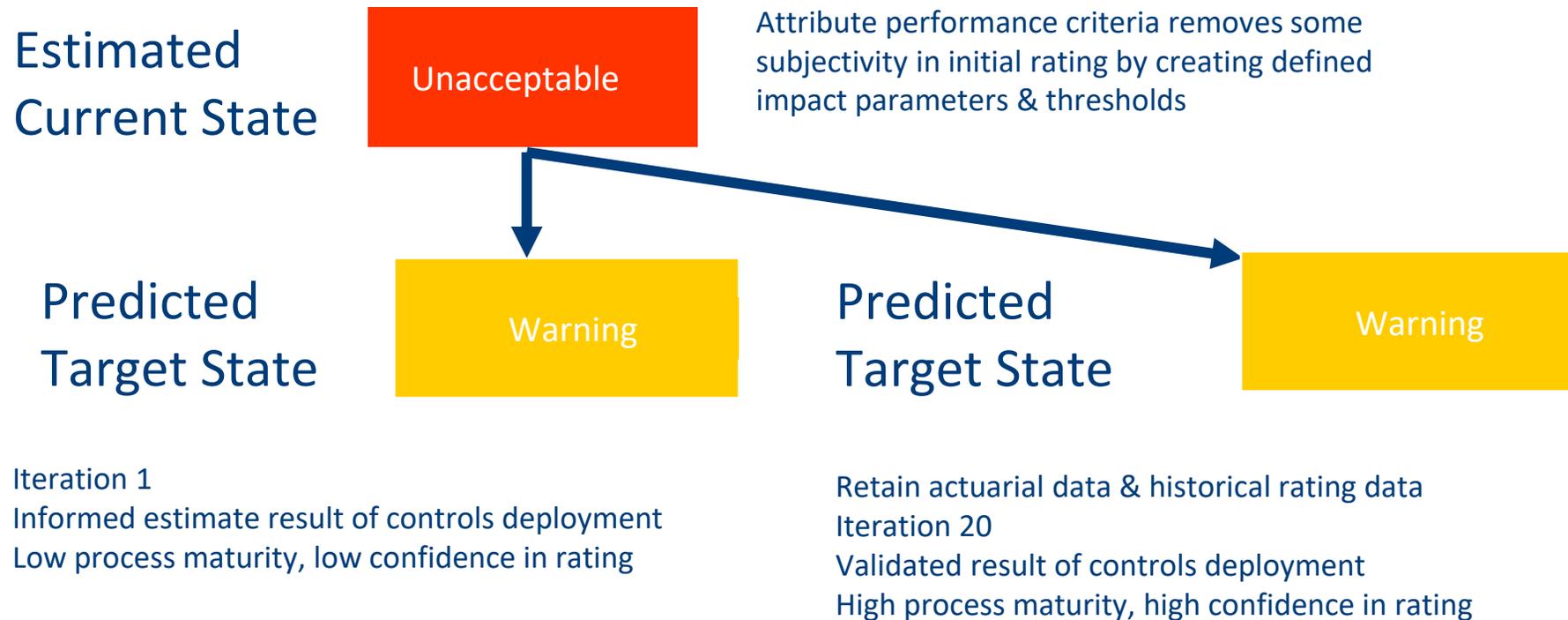
# Risk Assessment in Controls Architecture

## The Role of Appetite Thresholds in Control Value Assessment



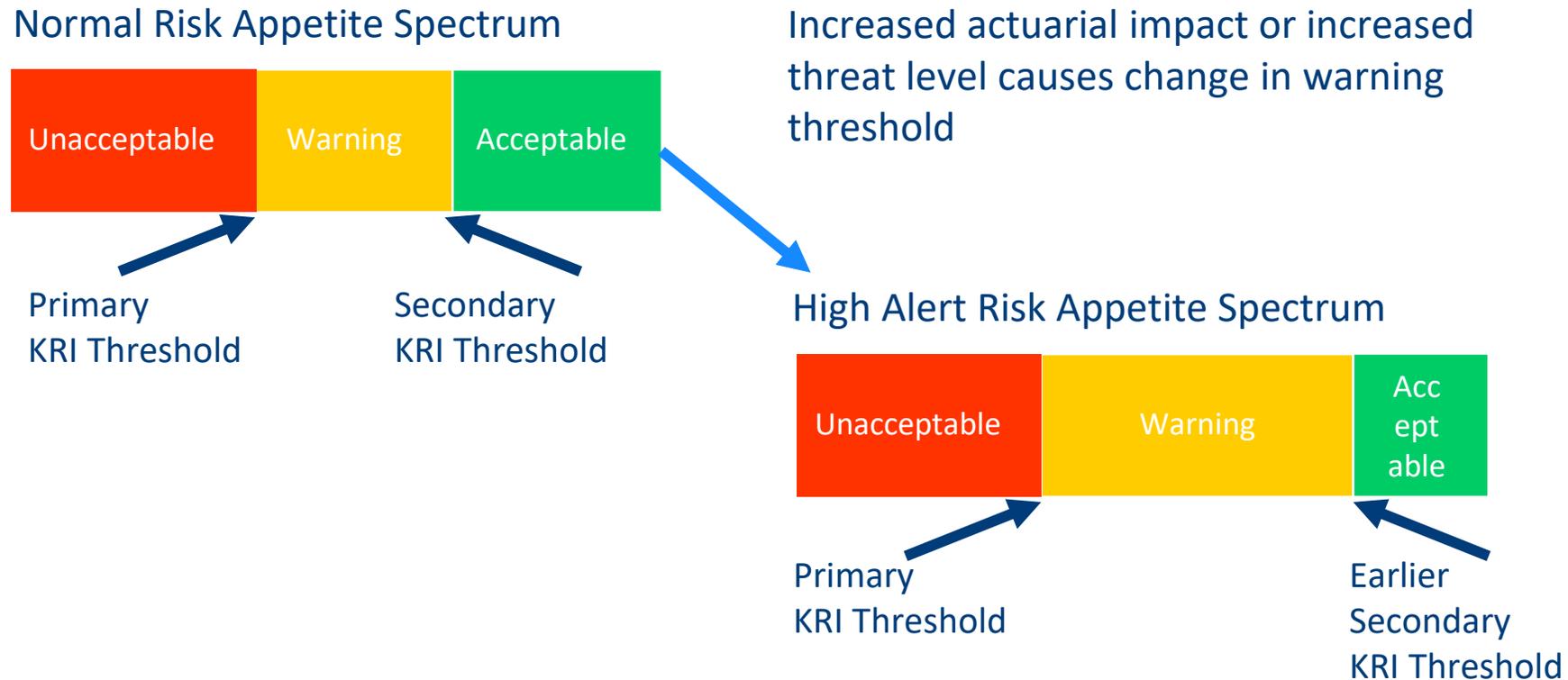
# Risk Assessment in Controls Architecture

## The Role of Actuarial Data in Control Value Assessment



# Dynamic Risk & Policy Management

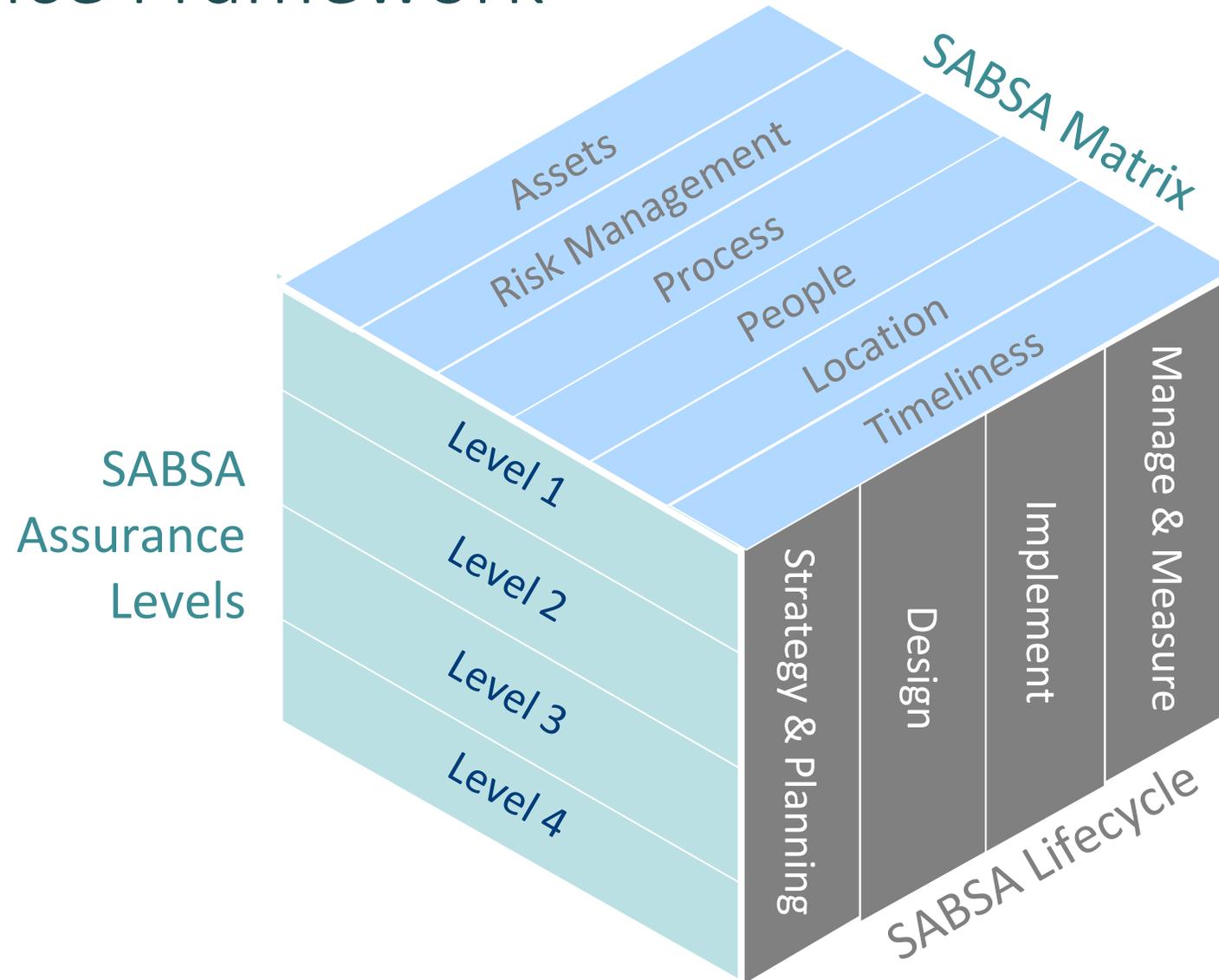
## Example: credit card security alert thresholds



# SABSA Assurance Defined

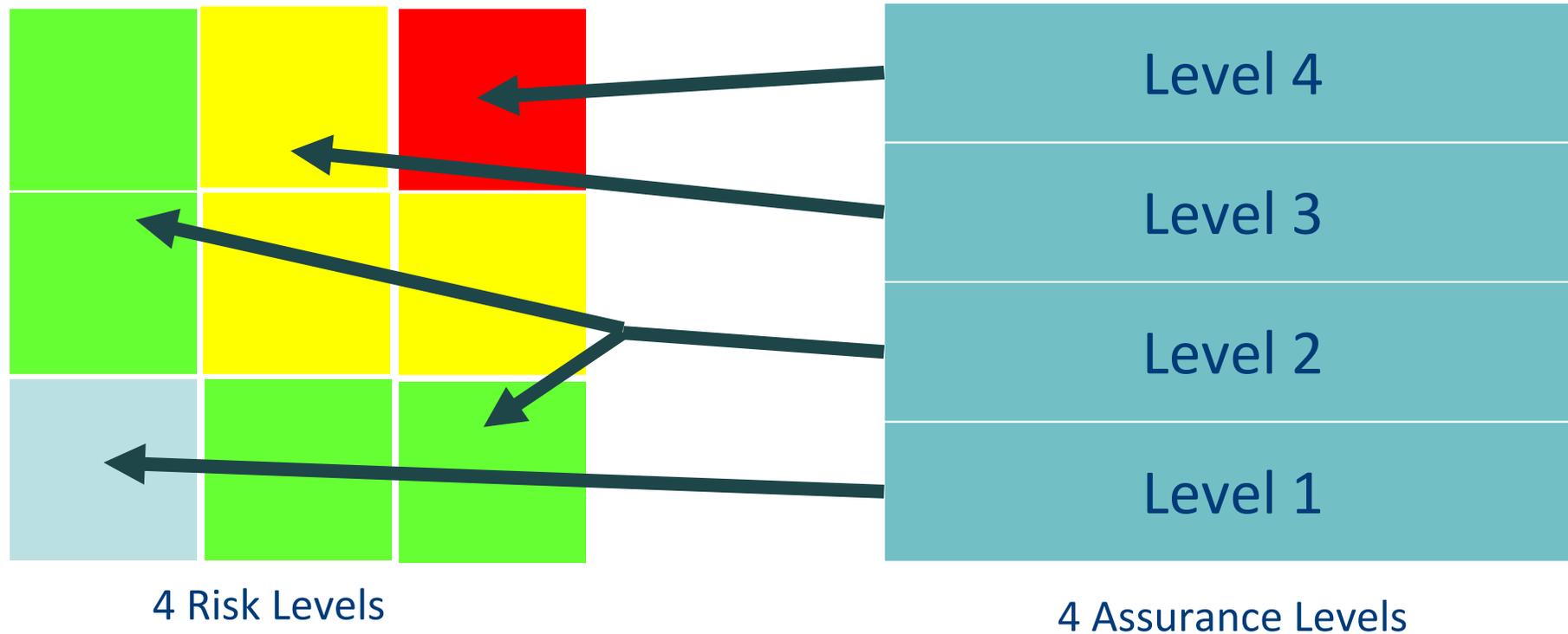
- Assurance
  - Providing confirmation and confidence that the enterprise risks are being adequately managed and that residual information risk is within the risk appetite or risk tolerance of the organisation
- Assurance Management
  - The process of managing assurance, including governing, planning and executing an enterprise assurance programme
  - The process of providing assurance that the enterprise security architecture is
    - Business-driven
    - Complete
    - Consistent
    - Robust
    - Fit-for-purpose in every way
- Assurance Management Activities
  - The set of activities that comprise 'assurance management'
    - Audits, Tests, Reviews, Checks & Balances

# SABSA Assurance Framework



# Determining the Assurance Levels

## Assurance Levels Correlate to Risk Levels



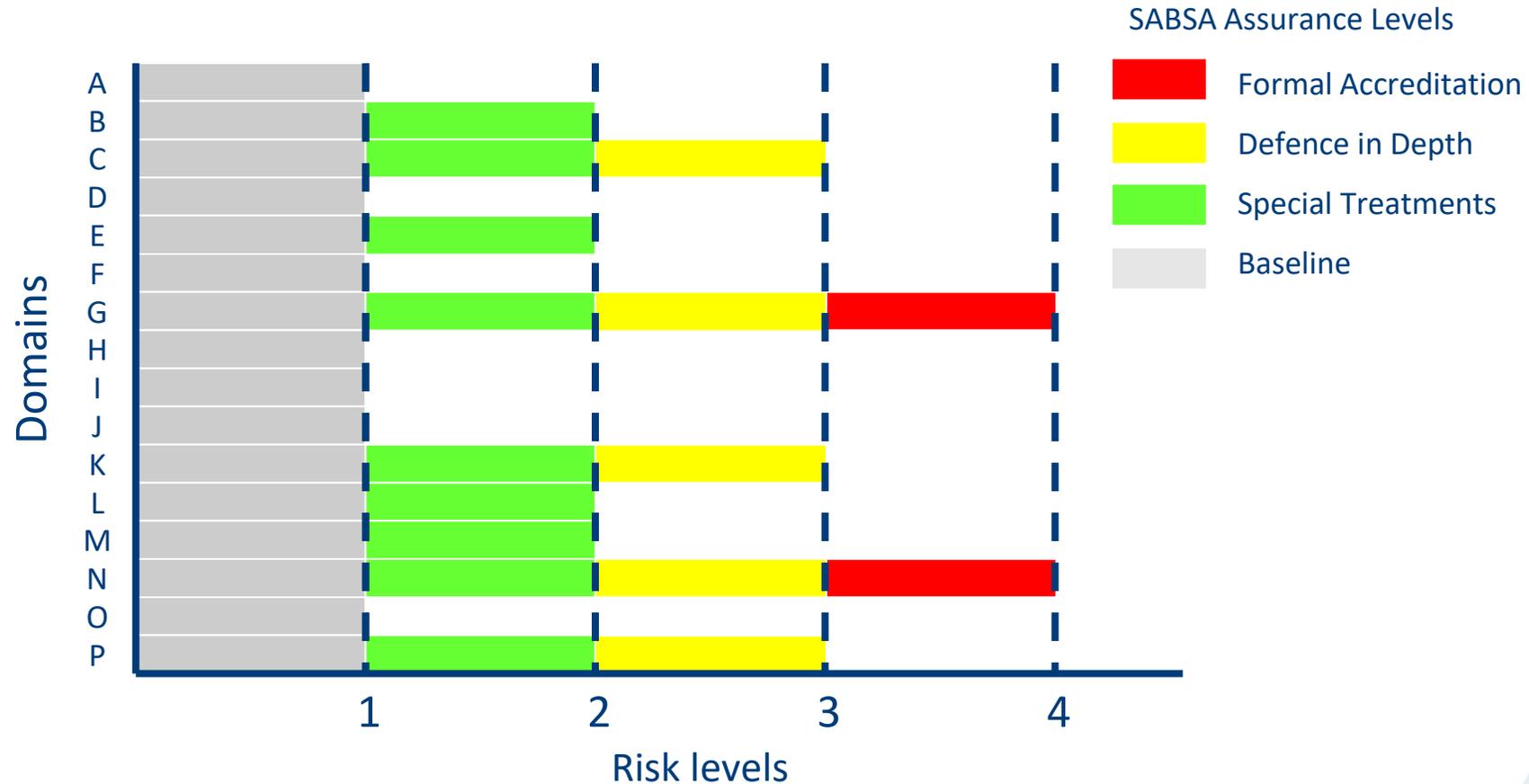
# Constructing a SABSA Assurance Matrix

Two-dimensional view through the SABSA Assurance Framework cube

Lifecycle View (one of four)	Assets	Risk Man'ment	Process	People	Location	Timeliness
Level 1						
Level 2	<i>Assurance Services</i>			<i>Assurance Services</i>		
Level 3						
Level 4						

# SABSA Assurance Levels

## Relationship Between Assurance Level & Risk Level



# Policy Compliance & Auditing

- Services provided by the “Assurance Role” defined in section 9 of module F1
- The higher the risk level, the more assurance services are required
- Specialist skills & tools required at each architecture layer & domain level
- Traceable auditing concept to support through-life risk management
  - The elements at each architecture layer are complete, fit-for-purpose, effective, and trace from each layer of the Motivation Column to the next
  - The Risk Management activities at each Management Architecture layer are complete, fit-for-purpose, effective, and trace from each layer of the Motivation Column to the next
  - The Risk Management monitoring & reporting activities follow the Domain responsibility model
  - The aggregation of Risk Status is effective between domain levels
  - The controls & enablers in each domain are risk proportional & effective

# Sample Questions

## Competency Domain 2

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



# Competency Domain 2

- Which ONE of the following statements about SABSA Assurance is FALSE?
  - A. Assurance Management in SABSA is defined as the process of managing assurance, including governing, planning and executing an enterprise assurance programme
  - B. The SABSA Assurance Framework is often presented as a cube in which the headings of all three axes can be customised
  - C. SABSA Assurance Management provides assurance that the Enterprise Security Architecture as a whole, and its individual elements, are business-driven, complete, consistent, robust and fit-for-purpose
  - D. When populating a SABSA Assurance Matrix, risk exposure levels in a domain determine the Assurance levels required

# Competency Domain 2

- With regard to the SABSA Policy Architecture Framework which of the following statements is FALSE?
  - A. The Contextual layer contains separate enterprise-wide policies for risk categories such as Business Continuity, Physical Security and Health & Safety
  - B. The Conceptual layer contains the Enterprise Information Security Policy as one of several related Operational Risk Management categories
  - C. The Logical layer contains policies for each domain in the enterprise domain model, each owned by a domain authority
  - D. The Physical layer contains procedures as the mechanisms to implement policy within each domain

# Transformation & Service Architecture

## Section 14

# Scope: Design Phase - Process

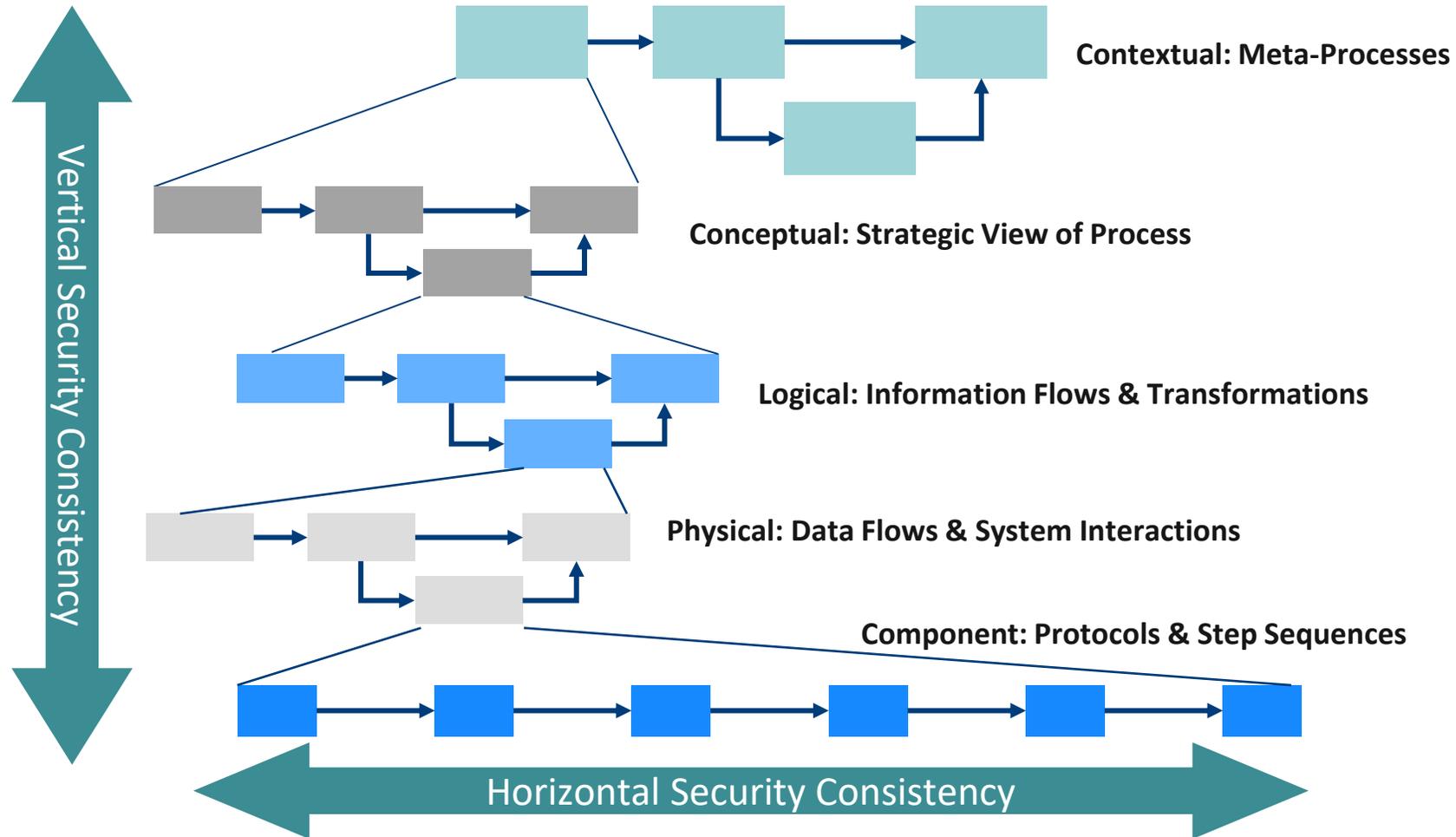
	Architecture Matrix	Management Matrix
Logical	<b>Process Maps &amp; Services</b>	<b>Delivery Management</b>
	Information Flows; Functional Transformations; Service Oriented Architecture; Services Catalogue; Application Functionality and Services	SLA Management; Supply Chain Management; BCM; Financial Management; Transition Management
Physical	<b>Process Mechanisms</b>	<b>Operations Management</b>
	Working Procedures; Application Software; Middleware; Systems; Security Mechanisms; Process Control Points	Job, Incident, Event, and Disaster Recovery Management
Component	<b>Process Components &amp; Standards</b>	<b>Component Deployment</b>
	Tools and Protocols for Process Delivery; Application Products	Product & Component Selection, Procurement. Project and Standards Management

# Section 14 Competency Objectives

## Competency / Question Domain 3 – How (Process)

Knowledge Element	Knowledge Competency	Comprehension Competency
Process Analysis	Describe the concept of top-down Process analysis	Explain the implications & applications of top-down process analysis in SABSA
Security Services	Define security service & security service types	Contrast the applications of primary, Secondary, implicit & explicit services
	Describe the implications of static & Dynamic information, information flows & transactions on security service specification	Contrast & summarise the placement of Security Services in architecture layers
	Identify the position in the architecture Matrix of services, mechanisms, components & management activities	Traceably associate services, mechanisms, components & management activities
Service Value & SLAs	Describe the principle of Security Service Value	Explain the application of the Service Value concept together with roles & responsibilities, and domain models from F1 to define an SLA

# SABSA Top-Down Process Analysis

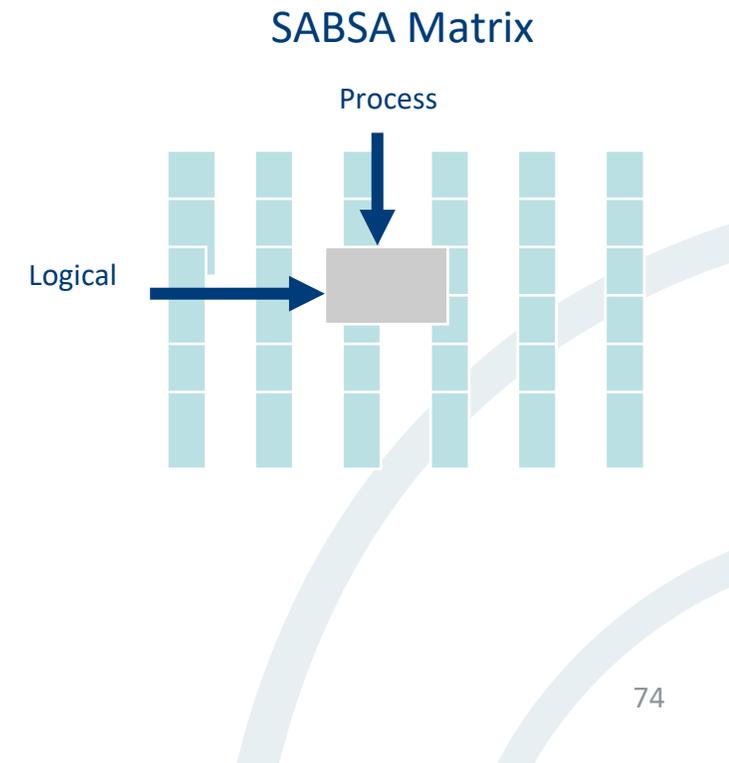


# Vertical Consistency

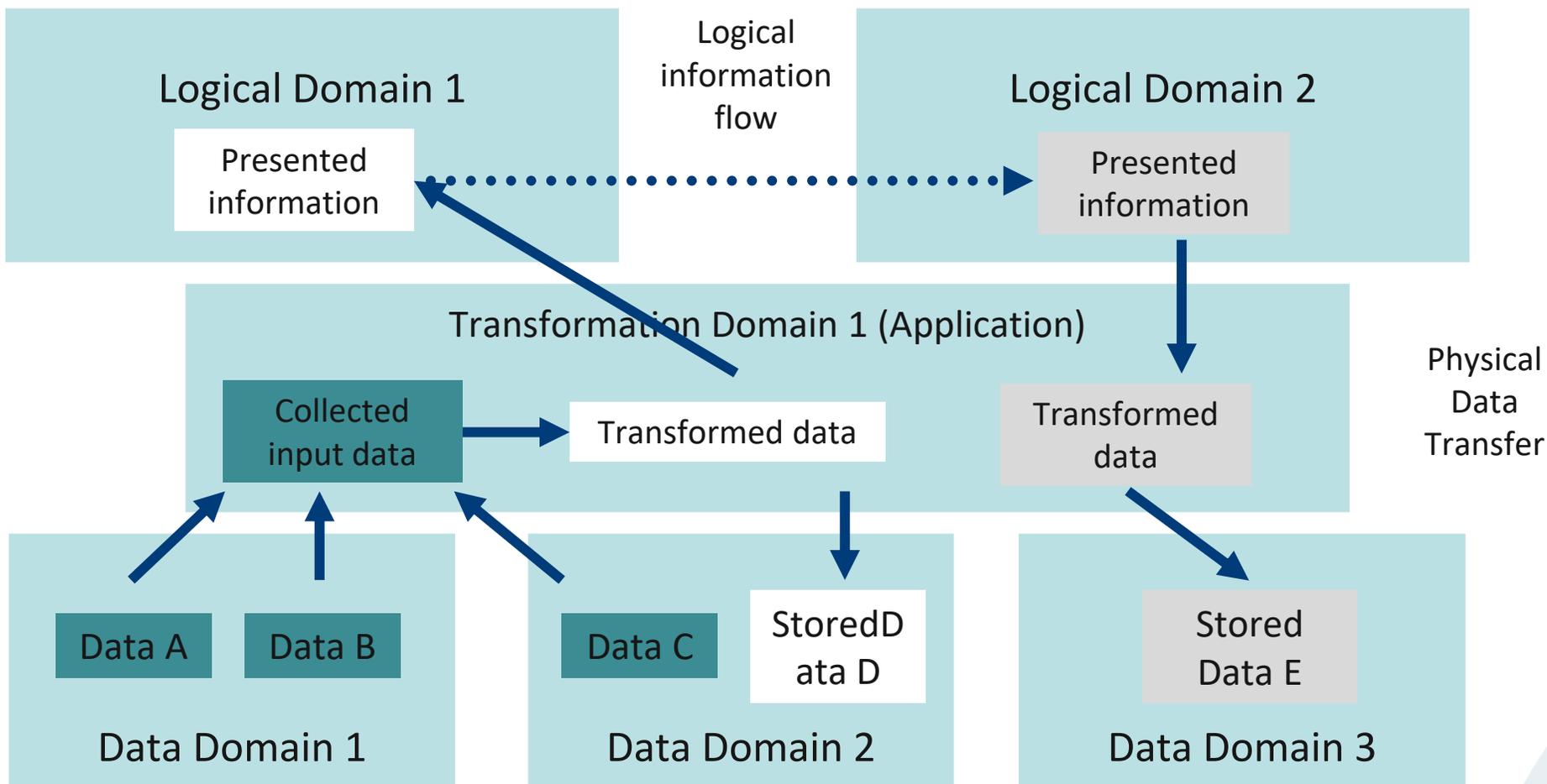
- A requirement for a business process is expressed as an attribute with a performance target
- A process is 'executed' by a series of progressively more granular steps down through each of the architecture layers
- Vertical consistency means that the conceptual attribute required at the top of the process model must be accurately represented at each layer (or the requirement is not met)
- Security Services are the means of specifying and providing the required functionality

# SABSA Concept of a Security Service

- Business-driven requirements organised into a consistent, logical / functional specification
- Arranged as a Services-Oriented Architecture
- Specified independently of the technical (physical) mechanisms used to deliver them
- Examples:
  - Entity authentication service
  - Stored data confidentiality service
  - Transaction source verification service
  - Entity unique identification service
  - Monitoring service
- Derived exclusively from the contextual and conceptual layers above, especially
  - Attribute profile (with performance metrics)
  - Control & Enablement objectives (to defined risk appetite)
  - Domain model (organisation & infrastructure policy architecture)
  - Trust model (inter-domain service requirements)



# Information Flows & Transformations



# Contains Static & Dynamic Information

Information Type	Properties	Example	Services Example
Static Information	Does not move or change in the short term	<ul style="list-style-type: none"> <li>Master records and files (such as customer information)</li> <li>Executable object code</li> <li>Configuration information for systems and applications</li> </ul>	<ul style="list-style-type: none"> <li>Confidentiality protection</li> <li>Integrity protection</li> <li>Availability protection</li> </ul>
Dynamic Information	Dynamic Information	<ul style="list-style-type: none"> <li>Free format messages such as used in e-mail</li> <li>Structured application Messages such as database queries using SQL</li> <li>Transaction information</li> <li>System and service management information</li> </ul>	<ul style="list-style-type: none"> <li>Confidentiality protection</li> <li>Integrity protection</li> <li>Availability protection</li> <li>Authenticity of source</li> <li>Non-repudiation</li> </ul>

# Business Transaction Services

- Business transactions are a special case of dynamic information. Protecting them implies some specific security services:
  - Business user / entity identification: to identify uniquely every business user & entity
  - Business user / entity authentication: to verify the identity of every business user & entity, as a pre-requisite to granting access to business resources and services.
  - Business user / entity authorisation: to ensure that every business user & entity has been authorised for access to the functions and information needed to carry out legitimate business activities, and that access to other, unauthorised functions and information is specifically prevented.
  - Business transaction integrity protection: to ensure that business transactions are completed as expected, and that they are protected from unauthorised modification, duplication, replay, delay or deletion.
  - Business transaction authentication: to ensure that all business transactions are initiated by authenticated entities.
  - Business transaction non-repudiation: to give assurance that all entities involved in a business transaction cannot later deny having participated to the transaction.

# Primary Security Services

- Primary security services are wholly embedded within a domain element
- Self-contained within the element to provide security functionality that secures the element



Example: A primary service wholly contained within an application element secures the application to specified functionality (such as confidentiality)

# Secondary Security Services

- Secondary security services operate between elements in a domain
- They secure the communications between the elements



Example: A secondary service between elements in an application domain secures the communication between them to specified functionality (such as confidentiality). The service is not wholly self-contained within the code of a single element but has a secondary deployment such as in layer 7 of the OSI stack.

# Implicit Security Services

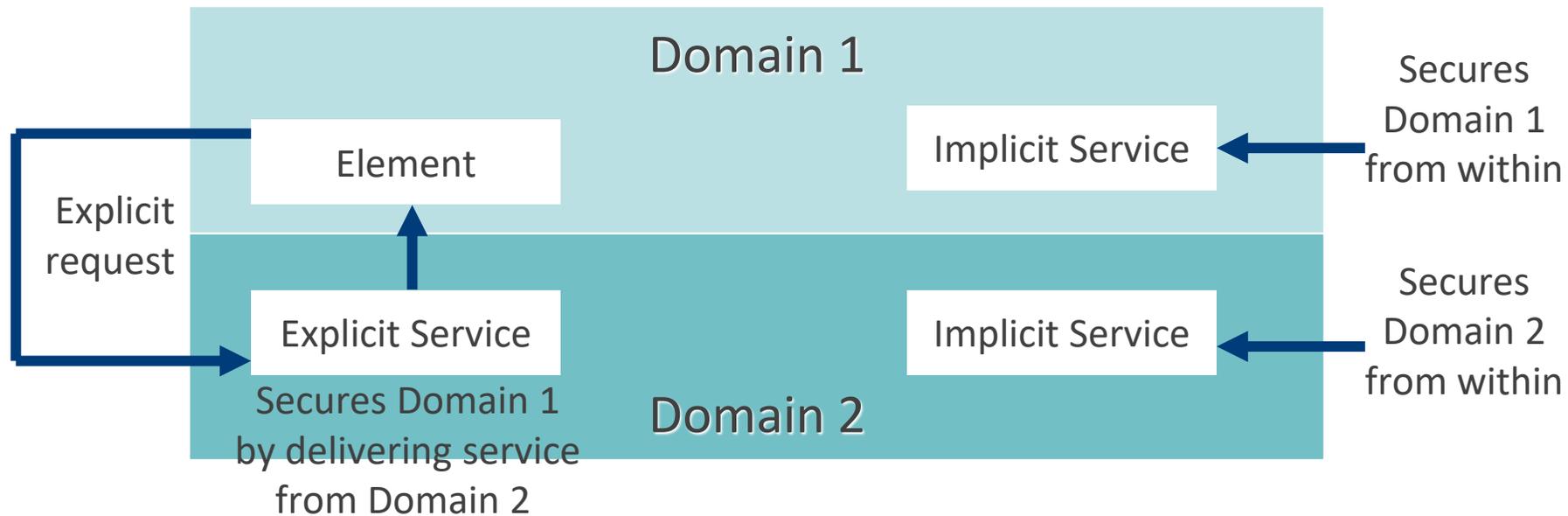
- Implicit security services are implicit in a domain – they secure the domain from within



Example: Both primary and secondary services in our previous examples are  
Providing 'applications security' from within the applications domain

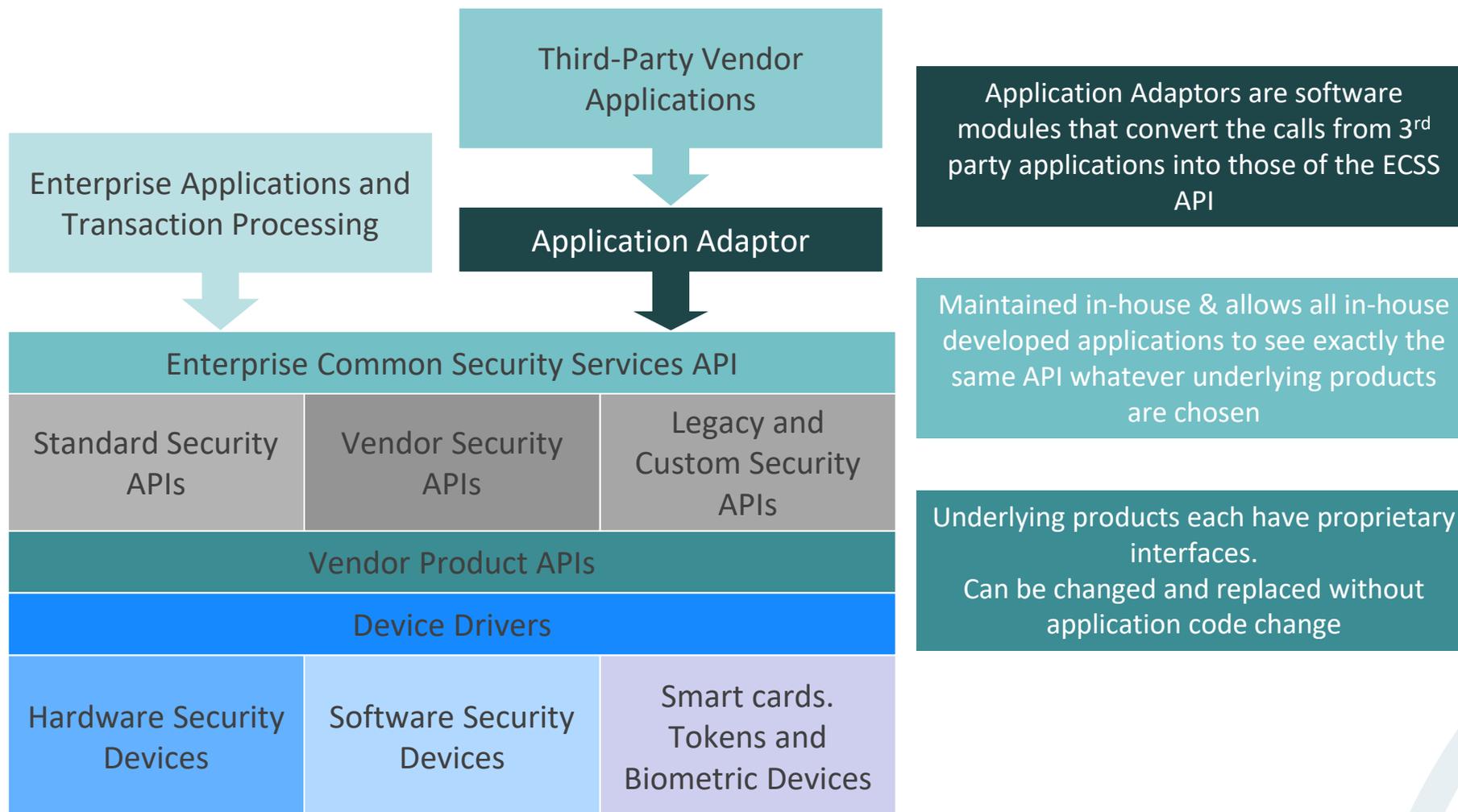
# Explicit Security Services

- Explicit security services are explicitly requested from one domain to another

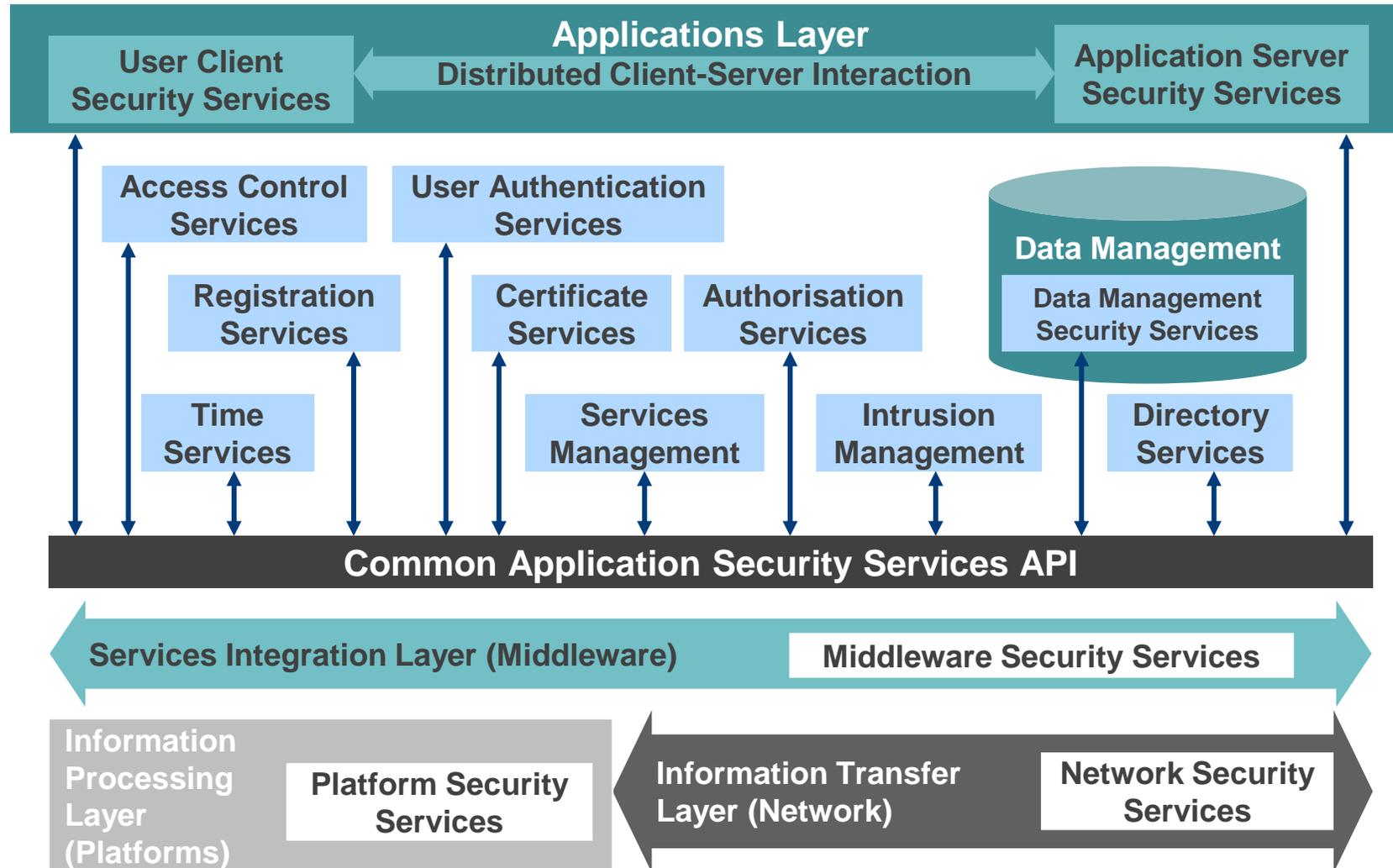


Example: Applications domain requests service from common services domain through an API

# Enterprise Common Security API



# Architectural Layering of Security Services



# Placing Services in the Architectural Layers

- Application security services – within the application code or located so that services can be called through an API from another location such as middleware
- Middleware security services – within the middleware layer itself
- Data management security services – provided within the databases and possibly considered as part of the middleware security services
- Network security services – within the network
- Platform security services – within the individual platforms

# Application Security Service Types

- Primary
  - Authorisation
  - Authentication
  - Access control
  - Audit
  - Administration
  - Application-to-application communications security
- Secondary – Applications layer of communications
  - Confidentiality
  - Integrity
  - Authenticity
  - Non-repudiation

# Middleware Security Service Types

- Explicit (by explicit API call)
  - All those listed for the applications
- Implicit
  - Entity authentication for entities making use of the middleware infrastructure
  - Entity authorisation and role management
  - Logical domain access control based upon entity roles
  - Physical middleware node-to-node mutual authentication
  - Physical middleware node-to-node confidentiality of transmitted data
  - Physical middleware node-to-node protection of message and object integrity
  - Traffic flow confidentiality, preventing the application traffic flows from being analysed for source, destination, volumes and timing
  - Real-time security monitoring, intrusion detection and reporting

# Data Management Security Service Types

- Access control to data at the object level, using labelling mechanisms within the metadata as a means to match data object classification to subject access privileges, based upon subject roles
- Authorisations based upon business need and the segregation of 'write' access (for making transactions and other updates) as against 'read-only' access for information retrieval, analytics, etc
- Data availability protection, using a variety of back-up and restoration techniques
- Data integrity protection within databases, to maintain a high level of confidence in the quality, accuracy and cleanliness of stored data
- Data confidentiality protection, ensuring that stored data is only revealed to authorised subjects.
- Authentication of SQL requests and responses (and other database access mechanisms: OQL, Java, Smalltalk, C++, etc), especially for remote database access (RDA).

# Data Management Security Service Types

- The process for designating the sensitivity and criticality of data (data classification)
- The designation of stewardship roles and the execution of these roles
- The use of standard naming conventions for data objects as a part of an integrated data architecture
- The support for standard data formats to provide inter-operability with other organisations (such as support for XML formats)

# Information Transfer Layer Services (Network Security)

- The sub-net: (OSI layers 1 and 2) provides physical transmission, transmission media access control, link level protocols (framing protocols such as HDLC, Token Ring or Ethernet) for error detection and correction, flow control, etc, and bridges and switches for network segmentation and traffic control.
- The Network Layer: (OSI layer 3) provides network naming, addressing, directory and routing control, and network protocols (packet protocols such as IP) for transfer of data units between physical platforms. The network layer also provides remote access services using dial-up sub-net connections and PPP or SLIP protocols.
- The Transport Layer: (OSI layer 4) provides end-to-end flow control, error control and session management for transfer of data units between applications (such as is provided by TCP).

# Misunderstandings in Network Security

- Authentication failures are not reported to the application (the decision making authority)
- No guarantee of application PDUs having a one-to-one mapping with network protocol PDUs
  - Buffering, line speeds, traffic density, multiplexing etc
  - Fragment application PDUs over several network packets
  - Aggregate application PDUs into a single network packet
  - Application needs to authenticate entities such as whole single transactions
  - No one-to-one relationship: not clear what has failed
- Business applications require records – network protocols throw records away

# Network Security Services

- Network security policy
- Network domain segregation
- Network component redundancy and resilience
- Network entity authentication
- Network entity authorisation
- Network boundary access control
- Connectivity control
- Network management security
- Network resource integrity protection
- Network security monitoring and intrusion detection
- Network security incident handling
- Network vulnerability research

# Processing Layer Services

- Physical security of the installation site to prevent theft, unauthorised physical access to the platform or malicious destruction.
- Environmental protection of the installation: electrical power protection, fire prevention, detection and quenching, flood prevention, structural stability, humidity and temperature control, etc.
- Local user authentication.
- Local user access control
- Local audit trails
- Cryptographic services provided by local cryptographic sub-systems (h/w and/or s/w)
- Remote interaction with central security services such as cryptographic key management, digital certificates, role-based access control, etc.

# Processing Layer Schedules

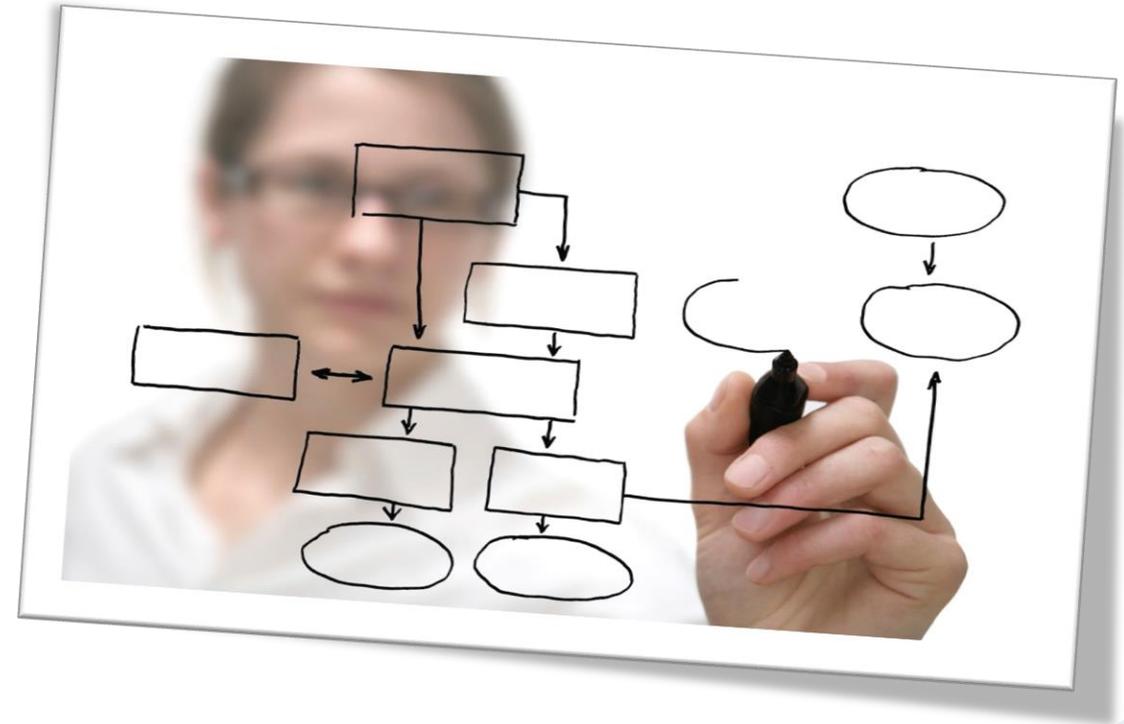
- Anti-virus services for prevention, containment, detection, reporting, restoration and recovery of virus and other malicious software attacks.
- Content filtering services to support the implementation of 'acceptable use' policies with regard to pornography and other socially unacceptable materials.
- Change control.
- Configuration control.
- Regular scanning to detect unauthorised changes to the configuration.
- Back up and recovery planning.
- Systems management (including operations management, security administration and many other services).

# Appendices F2-3, F2-4, F2-5

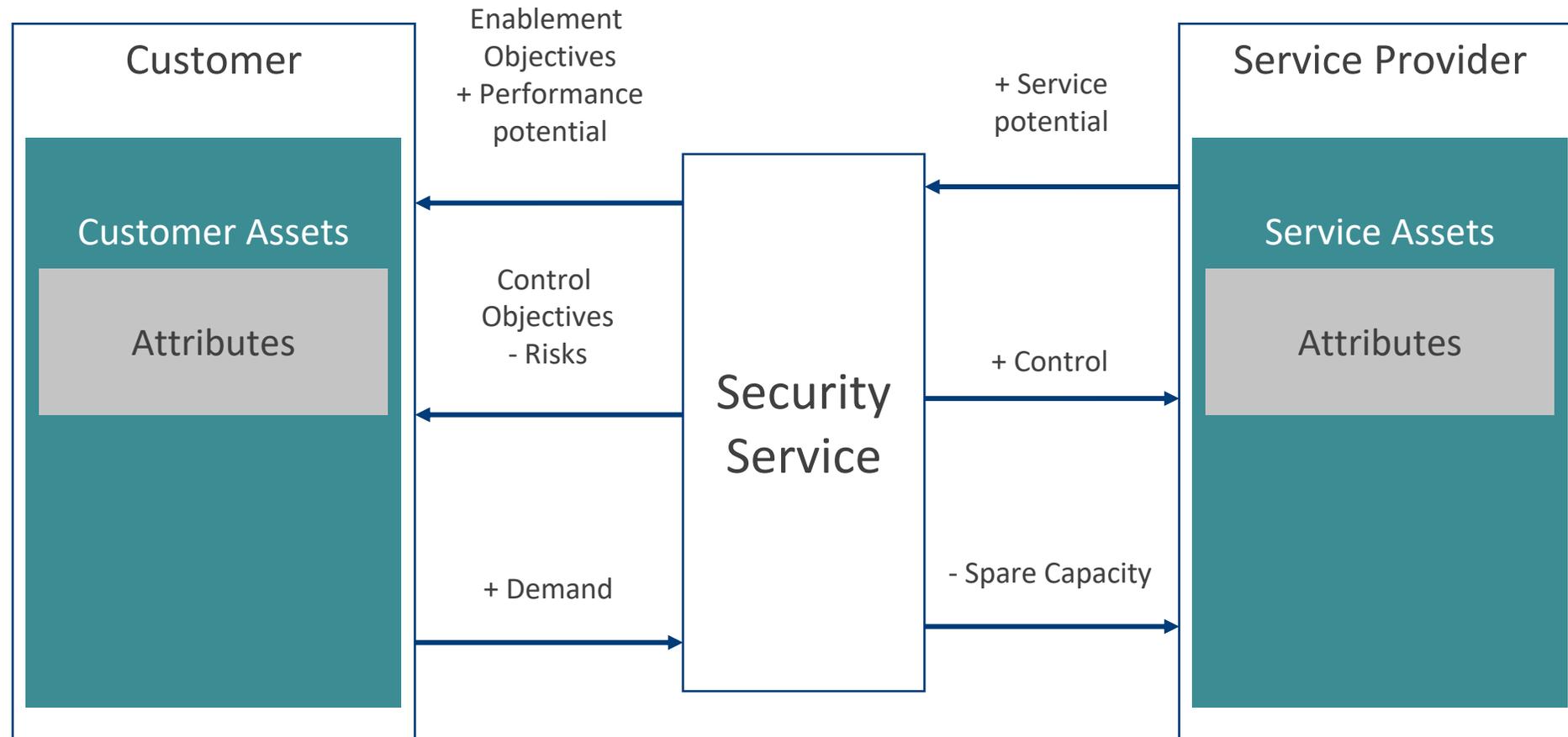
- Sample security services
- Sample security mechanisms
- Sample security components

# Workshop F2-1

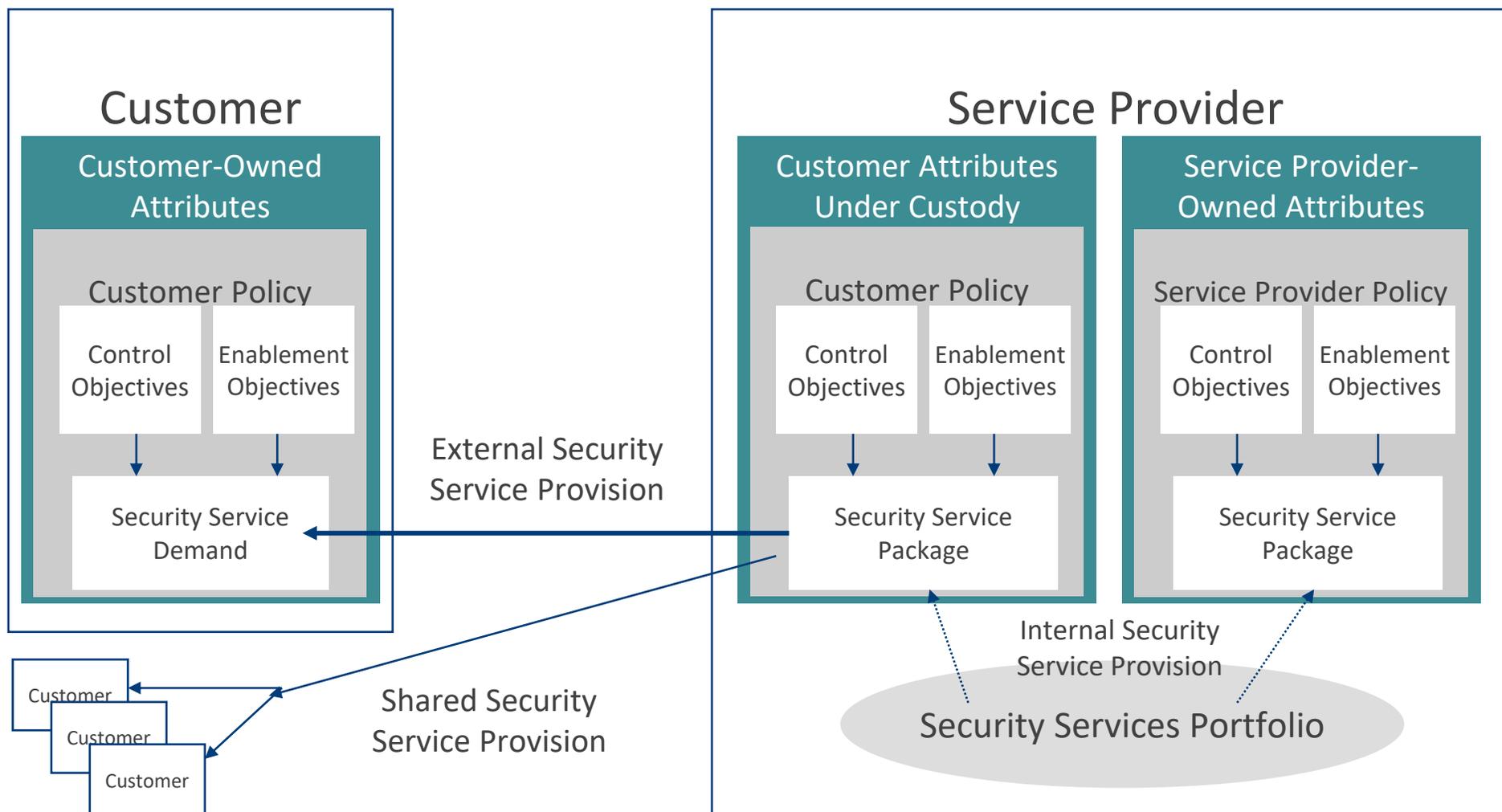
## Placement of Security Services



# SABSA Concept of Security Service value



# SABSA Security Service Value Relationships



# ITIL Concept of Service Management

- Service Management is a set of specialised organisational capabilities for providing value to customers in the form of services
- Service Management involves matching business requirements to available service provider resources and capabilities
- Its aim is to make capabilities and resources available to the customer in the highly usable form of services at acceptable levels of quality, cost, and risk

# SABSA Concept of Security Service Management

- Security Service Management is a set of specialised organisational capabilities for providing value to customers in the form of security services
- Security Service Management involves matching business requirements for controls and enablers to available security service provider resources and capabilities
- Its aim is to make security capabilities and resources available to the customer in the highly usable form of security services that meet control and enablement objectives

# ITIL Functions, Roles & Processes

- Functions

- The means to structure an organisation to implement specialisations
- Organisational units specialised to perform certain types of work and responsible for specific outcomes
- Self-contained with capabilities and resources necessary to their performance and outcomes

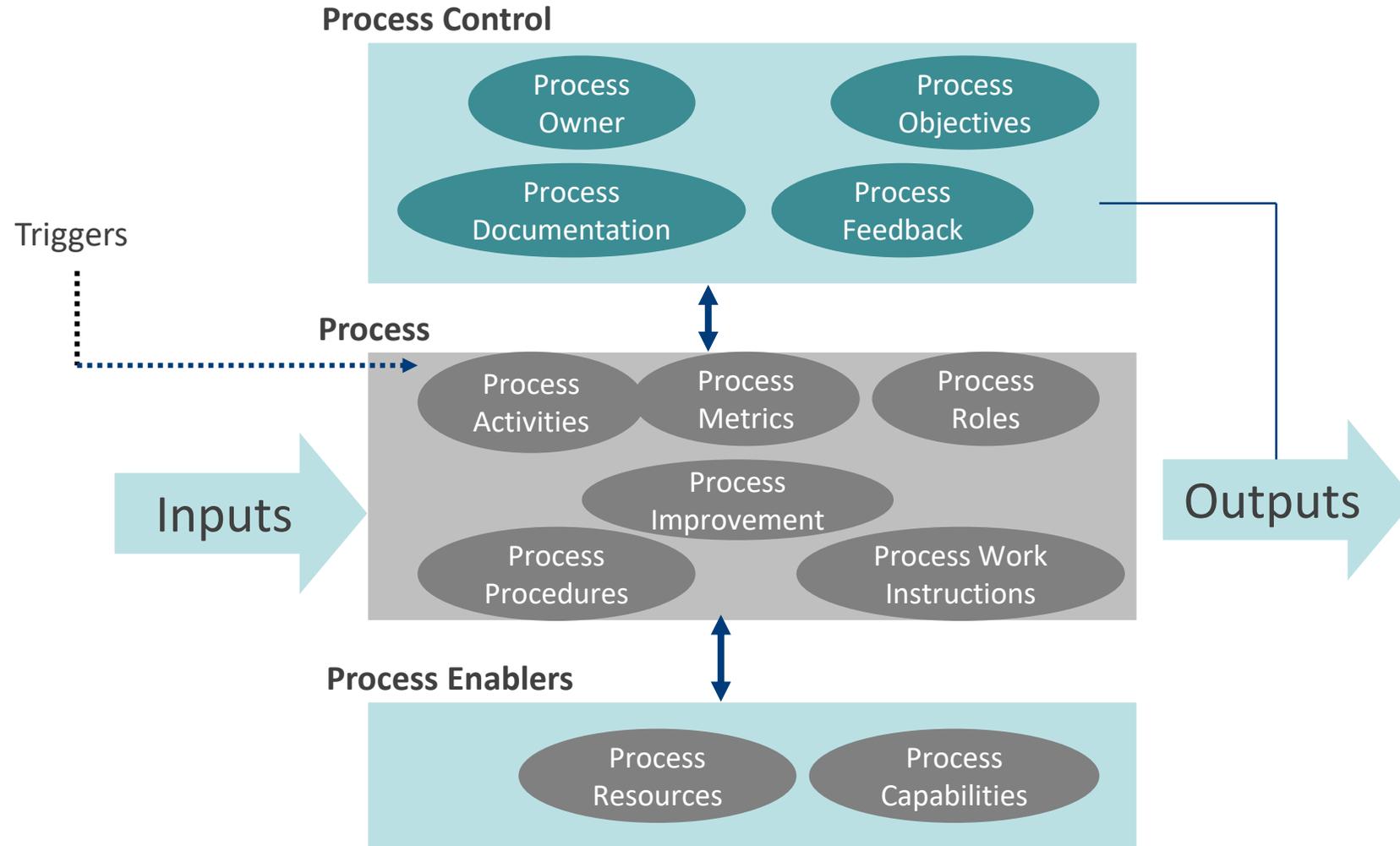
- Processes

- A set of co-ordinated activities combining resources and capabilities to produce outcomes of value to the stakeholder or customer

- Roles

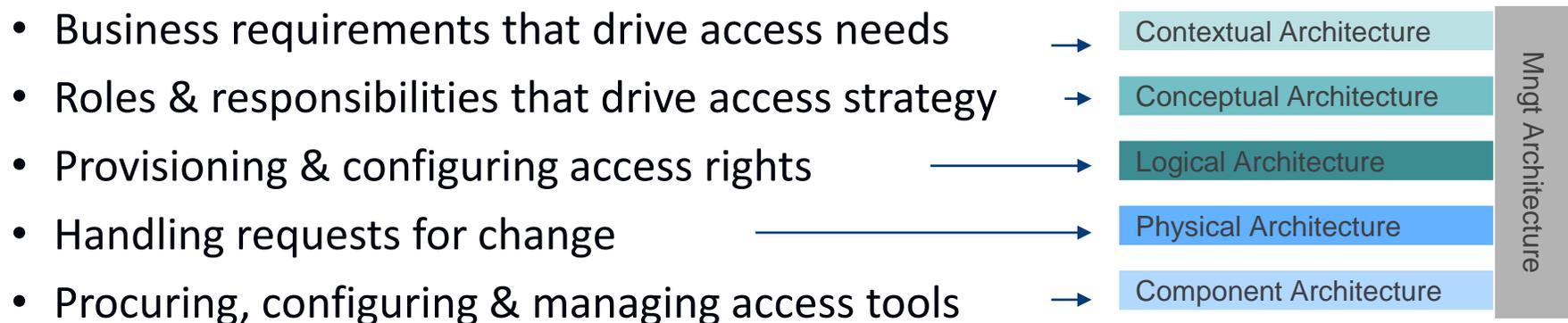
- A set of responsibilities defined in a process and assigned to a person or a team
- One person or team may have multiple responsibilities in multiple processes

# ITIL Concept of Process



# Architected Security Processes

- Security Management usually has a valid meaning and set of security-relevant activities at every layer
- Definition of all of these activities is required to achieve properly architected security services
- E.g. “Access Management” is located by ITIL as part of the Service Operations lifecycle phase
- But an architected process means traceability through the layers

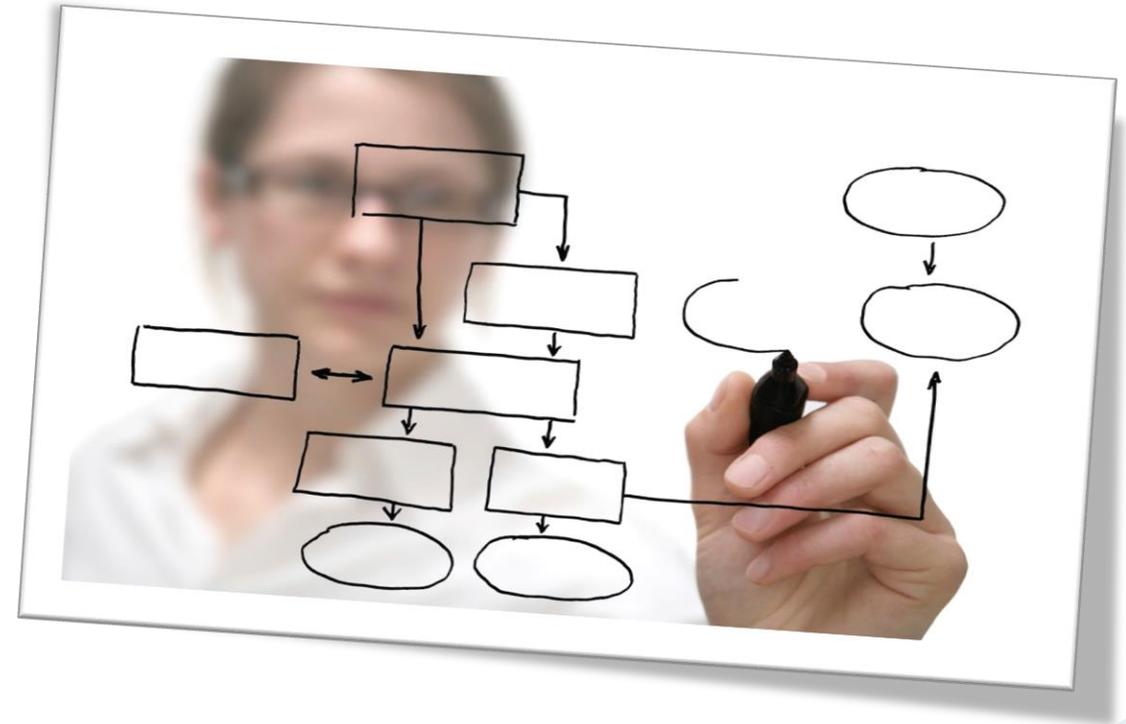


# Security Architecture – Process Issues

- To achieve end-to-end process security the architecture layers must be properly integrated and aligned
- Responsibility for process activities may change through the layers
- Objectives may have layer-specific interpretations but must aggregate into the higher-level security objective of the overall process owner
- Process documentation must be available at multiple levels
- The means of obtaining process feedback and measuring performance may not be consistent from layer to layer
- Process enablers may differ from layer to layer
- To ensure Security Service Levels meet the highest level requirements, each layer may require a unit-based Security SLA

# Workshop F2-2

## SLA Planning



# Sample Questions

## Competency Domain 3

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



# Competency Domain 3

- Which ONE of the following is the MOST CORRECT statement of Security Service value from the customer's perspective?
  - A. Value is created by services that meet the customer's enablement objectives to reduce the customer's risk exposures
  - B. Value is created by services that meet the customer's control objectives to increase the customer's opportunities
  - C. Value is created by services that meet the customer's enablement and control objectives
  - D. Value is created by a standardised service package that can be provided to all customers simultaneously

# Competency Domain 3

- Which ONE of the following statements about the provision of infrastructure security services is TRUE?
  - A. Applications security is provided exclusively by implicit security services placed within the middleware layer
  - B. Applications security is provided exclusively by explicit security services placed within the middleware layer and accessed through an API
  - C. Applications security is provided by a combination of both implicit and explicit security services placed within the middleware layer
  - D. Applications security is provided by a combination of security services placed in the applications layer and explicit security services placed within the middleware accessed through an API

# Entity & Trust Framework

## Section 15

# Scope: Design Phase - People

	Architecture Matrix	Management Matrix
Logical	<b>Trust Relationships</b>	<b>Enterprise-wide User Management</b>
	Domain Authorities; Entity Schema; Privilege Profiles; Trust Relationship Models	Trust Modelling; IA Management; Management of User Privileges; Account Admin & Provisioning
Physical	<b>Human Interface</b>	<b>User Support</b>
	User Interface to Business Systems; Identity & Access Control Systems	Service Desk; Problem and Request Management
Component	<b>Human Entities: Components &amp; Standards</b>	<b>Personnel Component Management</b>
	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Recruitment; Disciplinary; Training & Awareness Delivery; Component & Standards Management

# Section 15 Competency Objectives

## Competency / Question Domain 4 – Who (People)

Knowledge Element	Knowledge Competency	Comprehension Competency
SABSA Trust Model	Describe the SABSA concept of Trust & Trust Models	Explain the implications & applications of top-down process analysis in SABSA
	Identify the roles of participants in a SABSA Trust Model	Distinguish between the claimant, reliant & trust broker parties & the role of registration
	Describe the process of, and rationale for, decomposing complex two-way trust	Relate SABSA trust modeling to vertical process consistency
	Describe chains of trust & trust hierarchies	Explain applications of the trust modeling technique in SABSA architecture

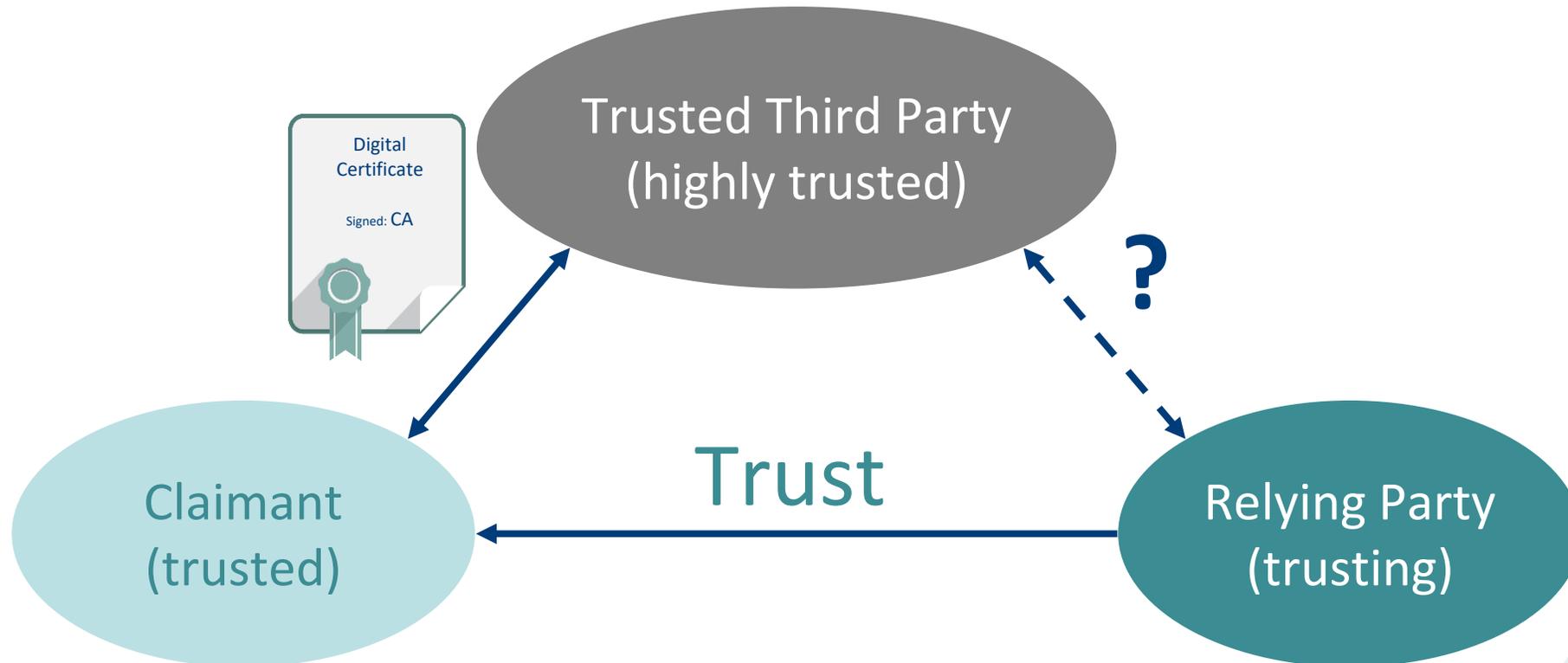
# The Trust Concept

- Trust is an important concept relevant to business relationships
- Trust is a relational business attribute not a technical one
- Technical services are often used to support trusted interoperation between trusted entities
- An entity that has been successful in creating some business reputation & credibility is 'trusted'
- Recognised by a 'trusting' entity

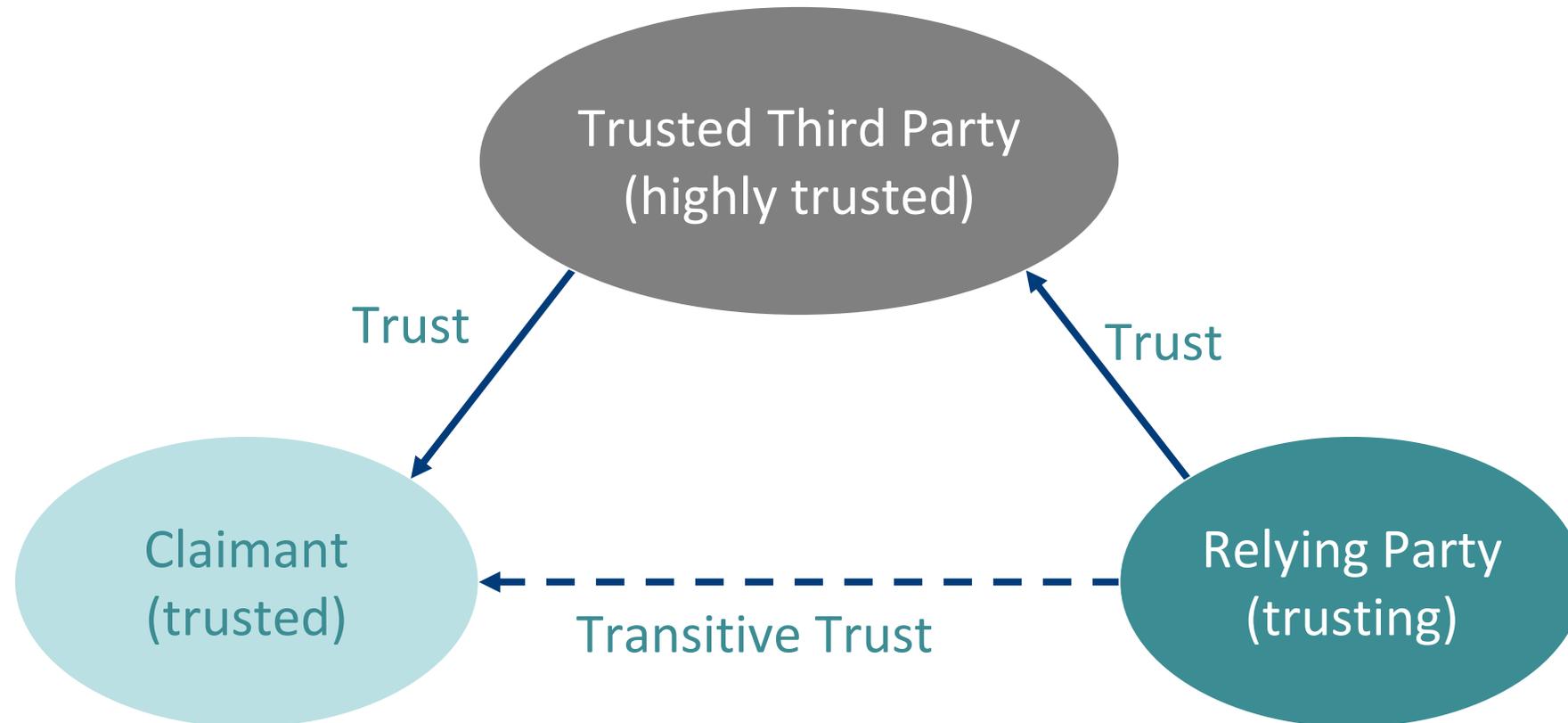
# One-way Trust – Who is the Customer?



# Getting the Trust Model Right



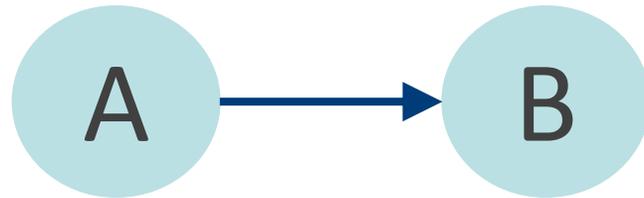
# Correct Transitive Trust Model



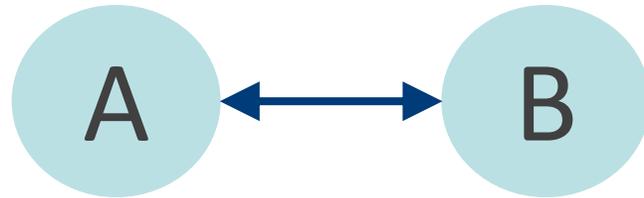
# Trust Models

- For two or more entities to interact and exchange information they must first trust one another
- Trust is established through registration by a mutually trusted third party within a given domain (logical or physical)
- All registered entities within a given domain trust one another within the domain policy
- The technical mechanism needed to support trusted interaction is ‘mutual authentication’

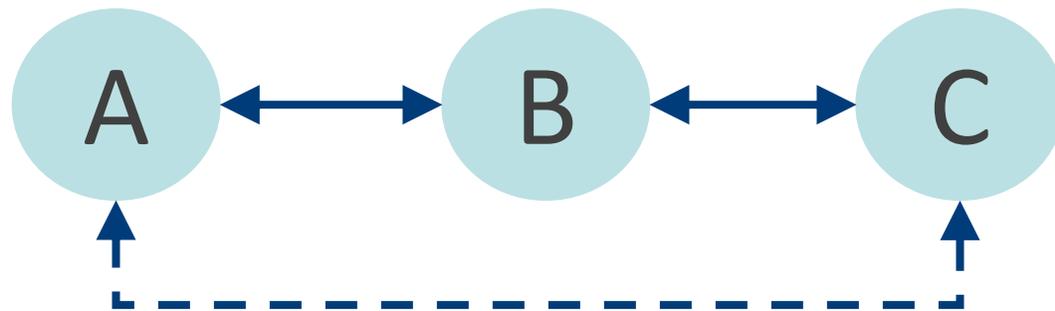
# Relationships & Trust



One-Way Trust



Two-Way Trust



Transitive or  
Pass-Through Trust

# Trust Has Variable Characteristics



## Buying a hotdog

I might wonder whether it is fit to eat and may not buy for this reason alone.

However, I will not worry about whether the stall-holder owns the hotdog and has the right to sell it, nor question whether they will be there tomorrow in case I want to complain.

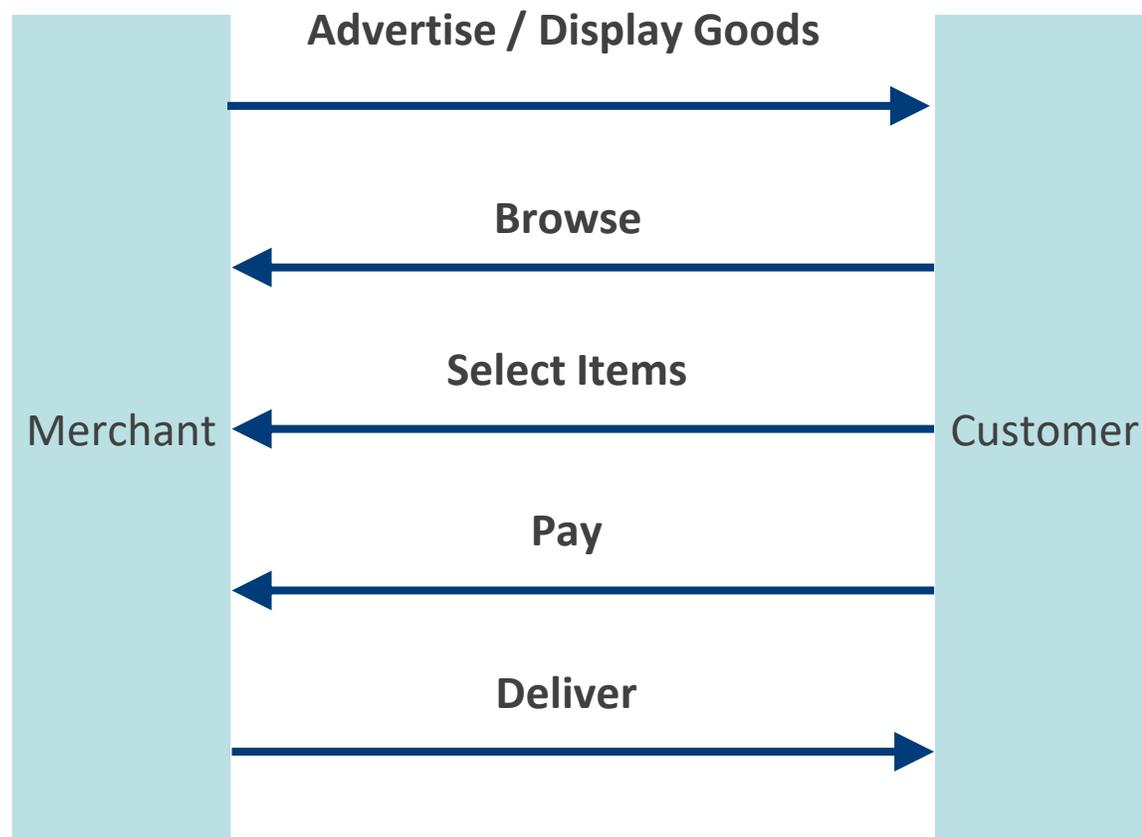


## Buying a house

I will employ a lawyer and surveyor at significant cost to investigate every detail of the ownership, construction, planning regulations and prospects for my future peaceful residence in the house.

Only when I have developed a high level of trust in the vendor and their claims will I sign the contract - and that will be filled with conditions and get-out clauses in case the information turns out to be false.

# Trust Modelling

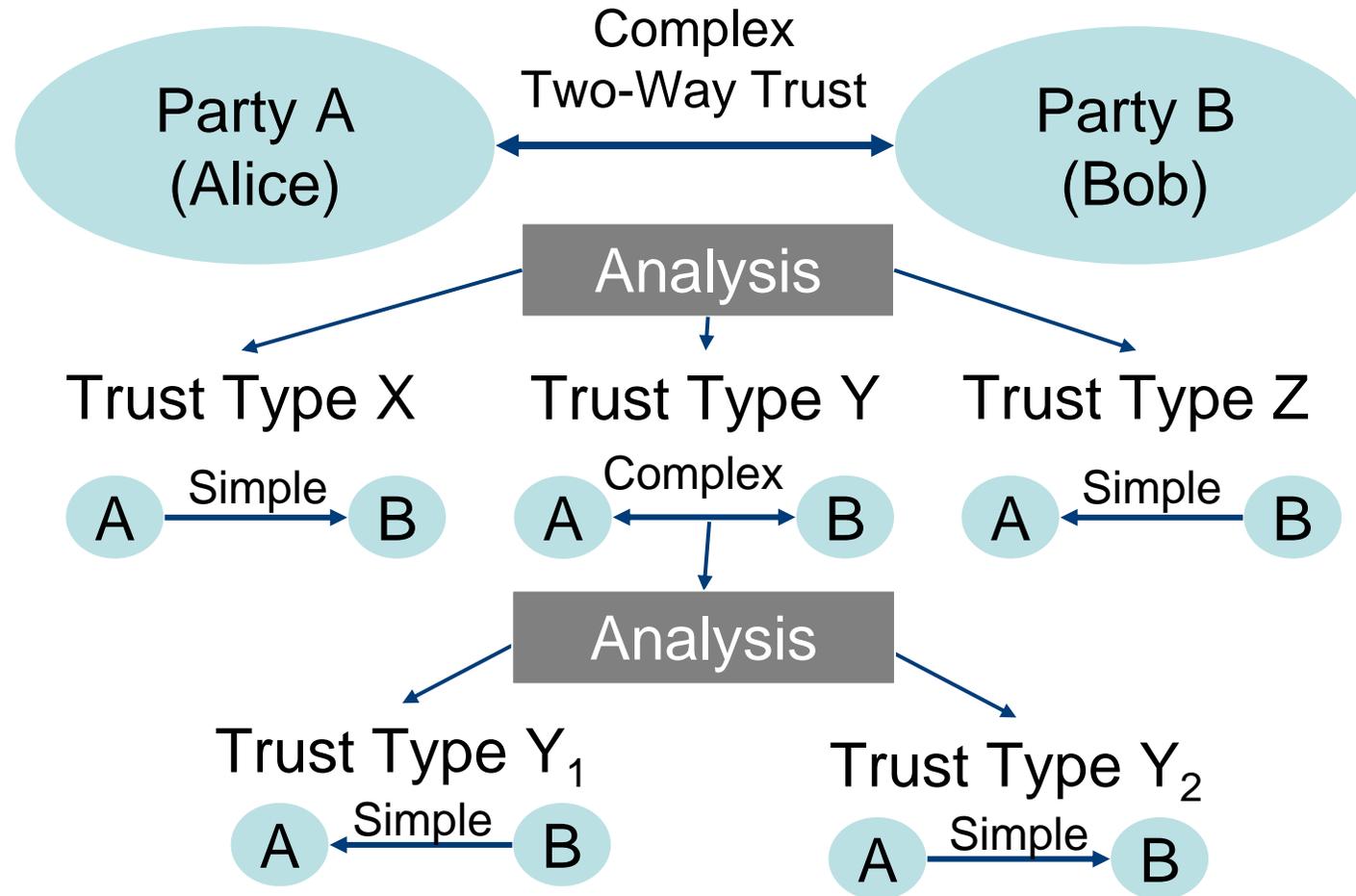


What needs to be protected here?  
What is the 'security' that we require?  
What function does it serve?

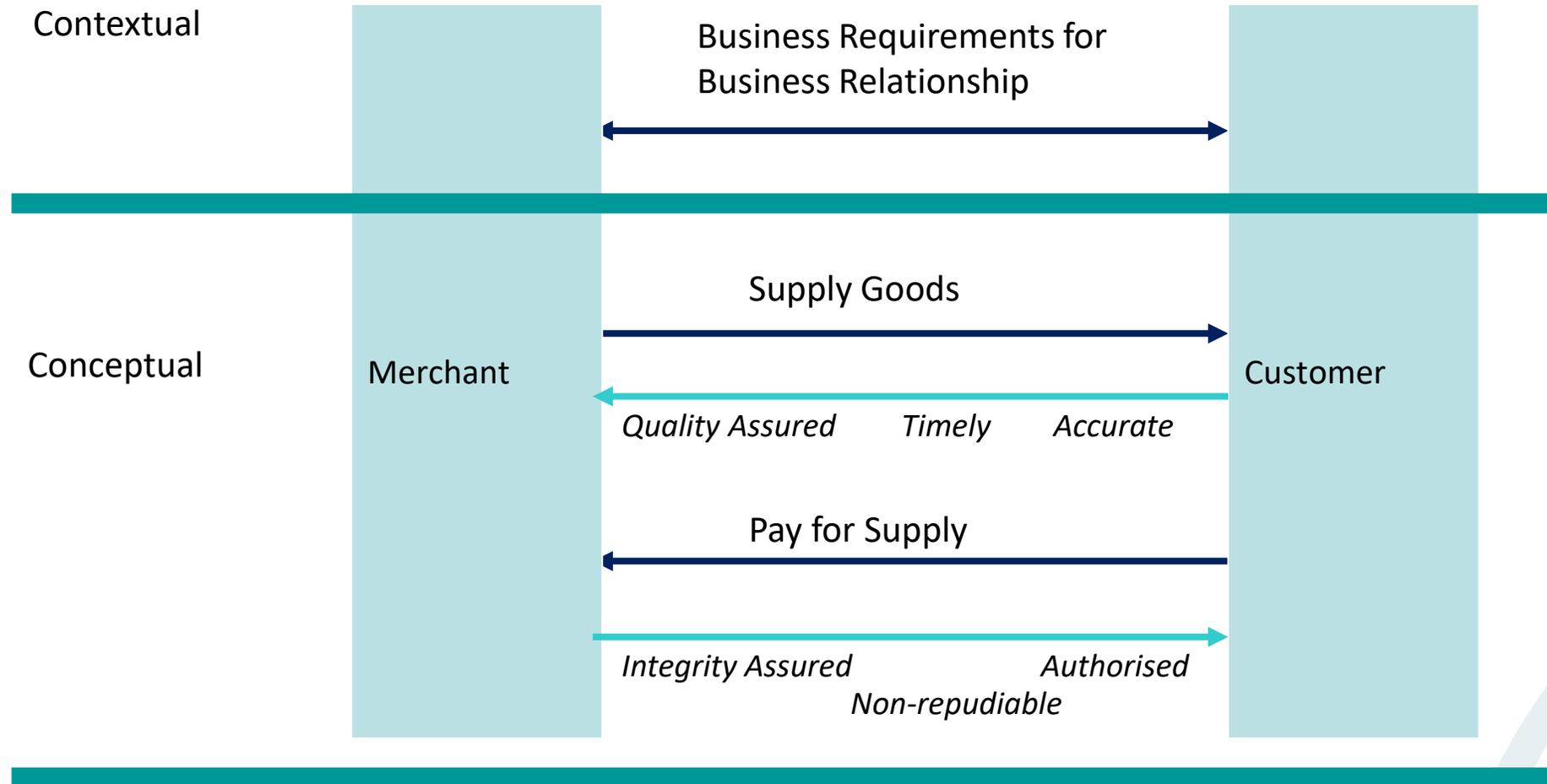
Trust Modelling in SABSA is about a clear specification of the business requirements for Trust, Security & Control.

What does security look like in this context?  
How much of it should there be?  
In which direction is it to be deployed?  
Who is the policy authority?

# Decomposition of Two-way Trust

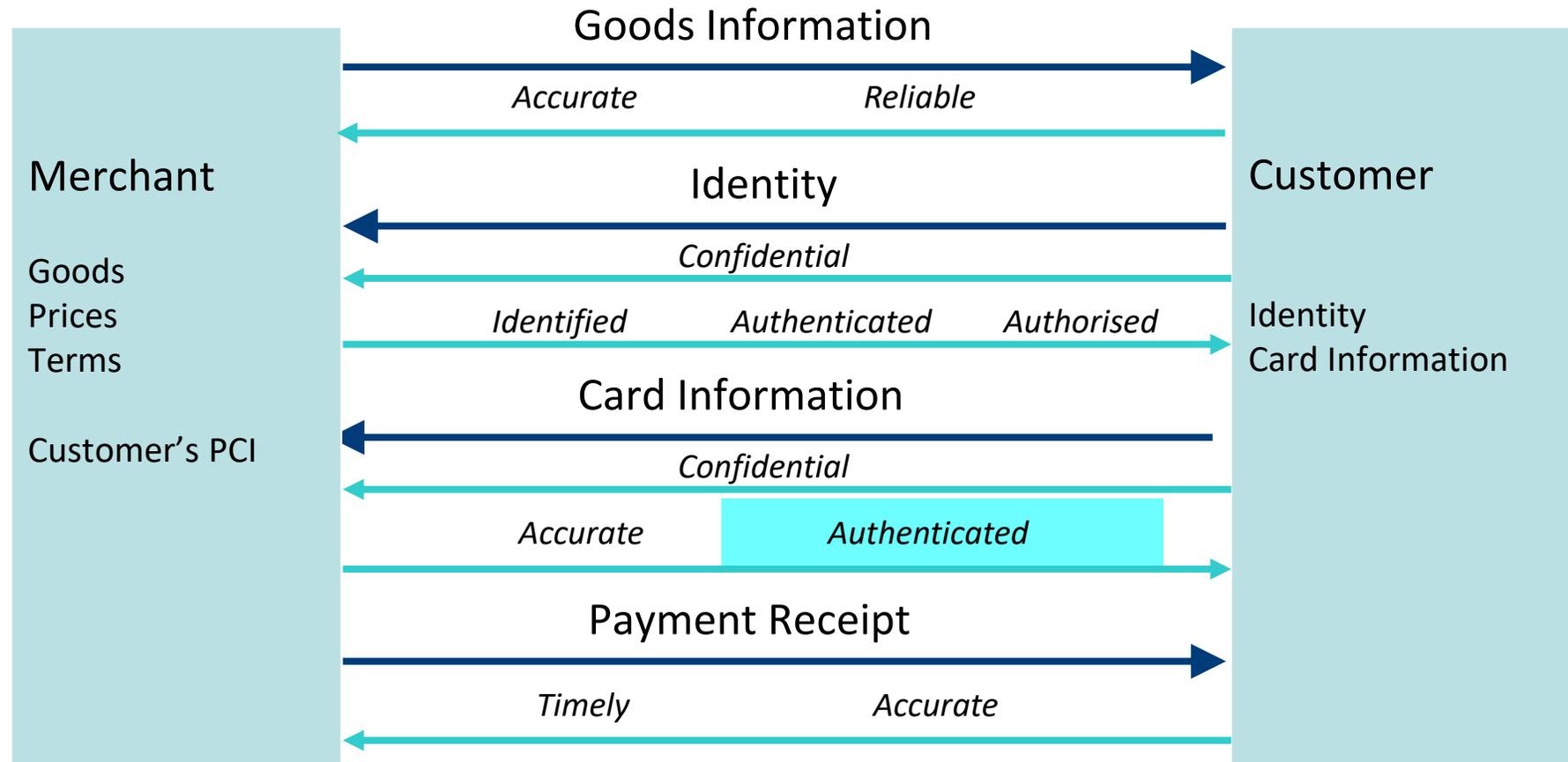


# Trust Model Decomposition



# Trust Model Decomposition

## Logical Decomposition – Attributes to Information Flows

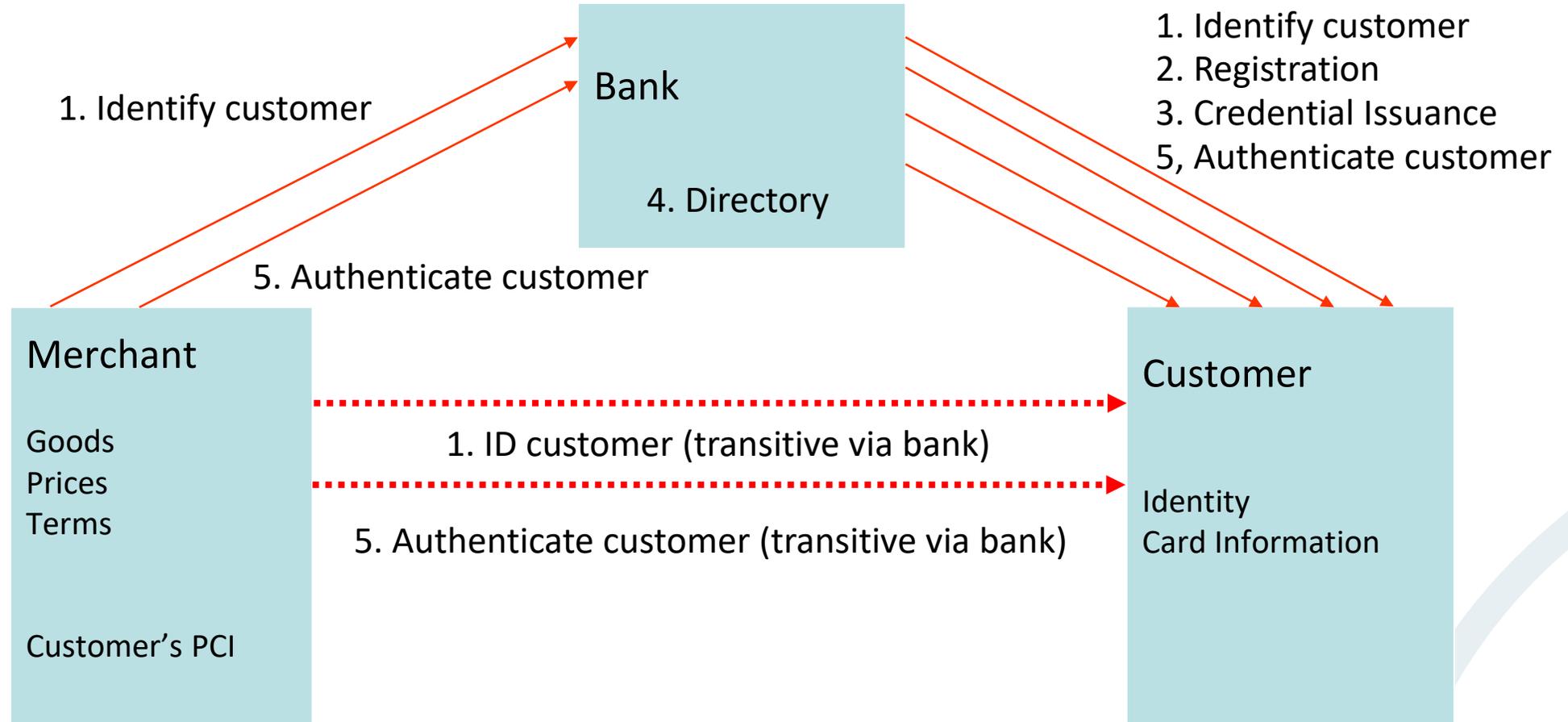


# Trust Model Decomposition

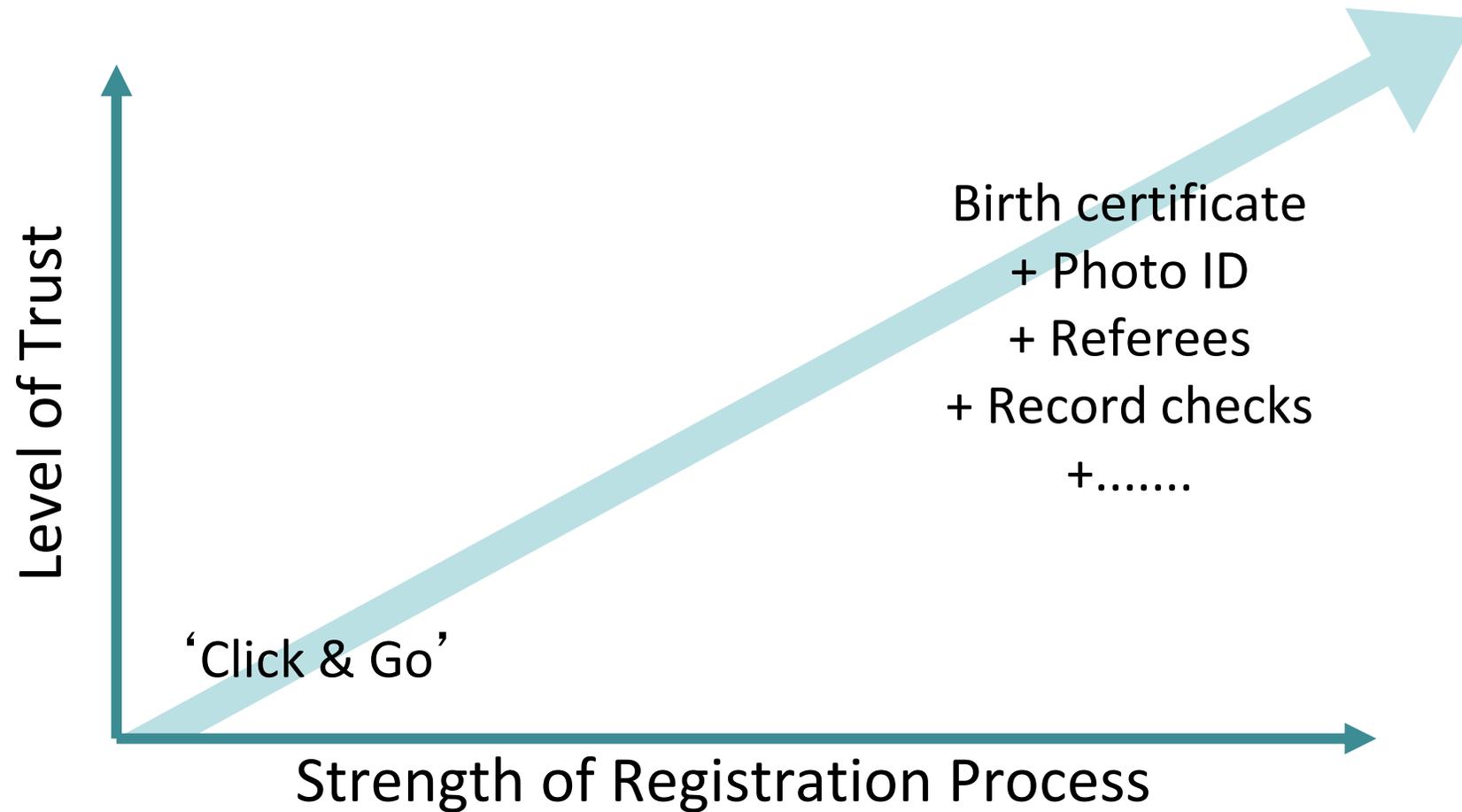
- The Attribute “Authenticated” requires certain functionality:
  - Identity / naming service
  - Registration service
  - Directory service
  - Credentials issuance service
  - Authentication / verification service
- The direction of the trust arrow is the direction of the dependency upon security / control
  - We trust because we build the capability to provide sufficient trust, not because we ‘don’t know what to do’ (I.T. Trust)

# Trust Model Decomposition

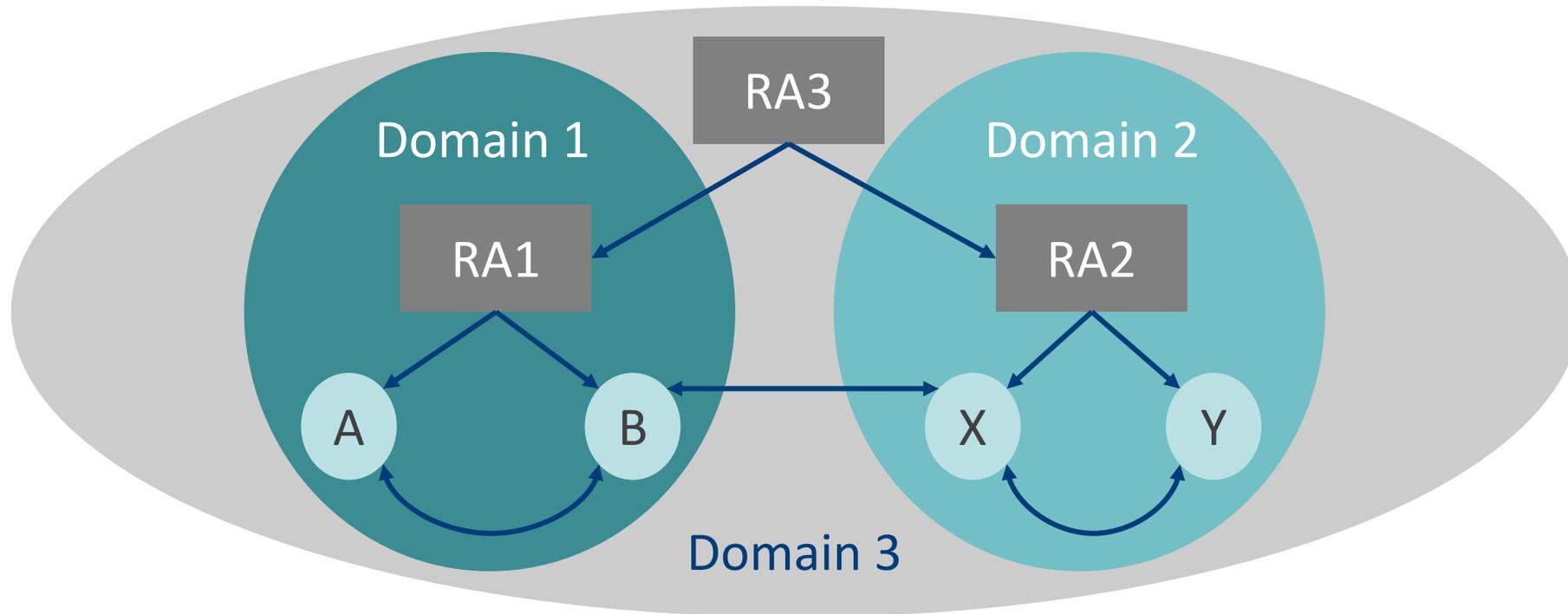
## Logical Decomposition – Attributes to Services



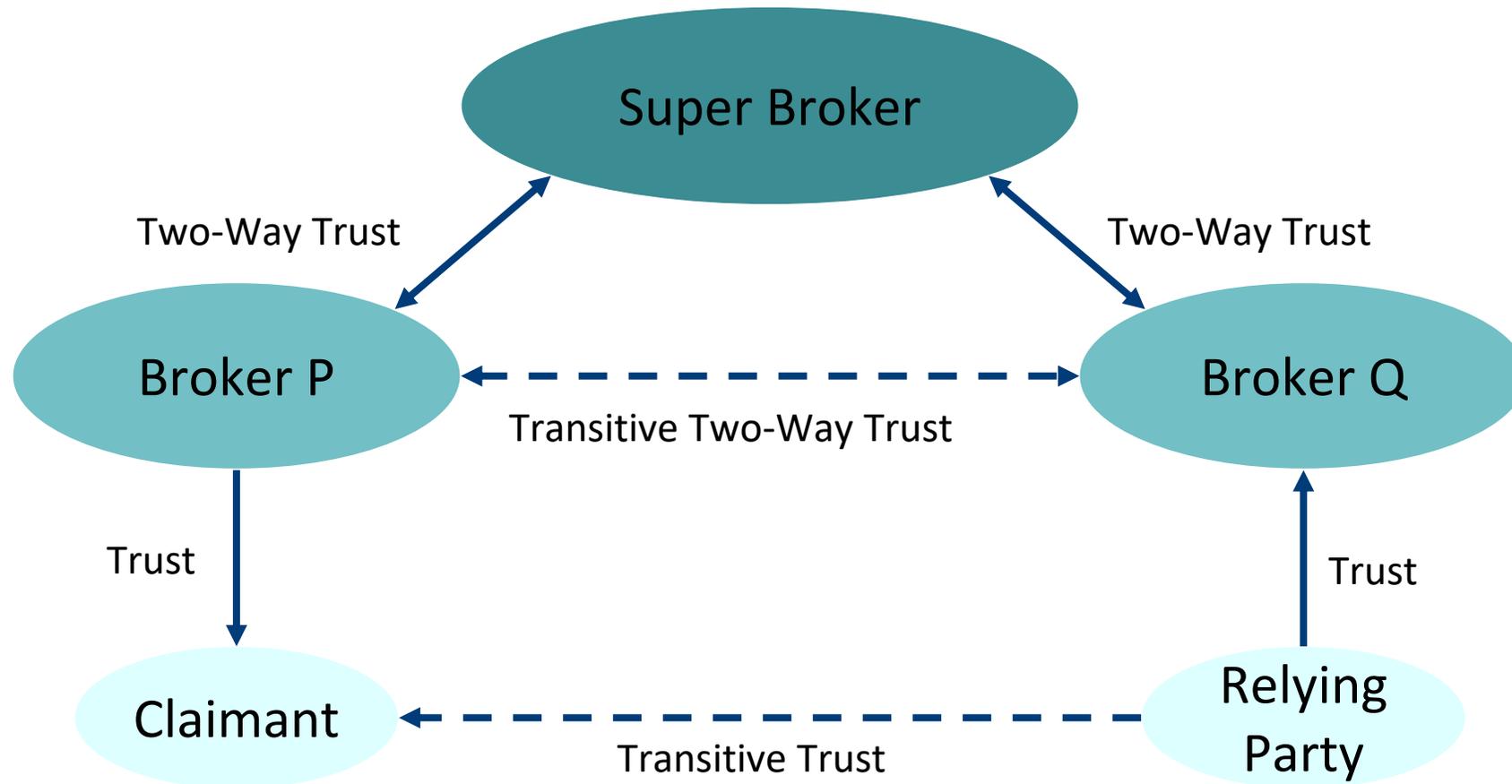
# Trust Strength is Determined by Registration



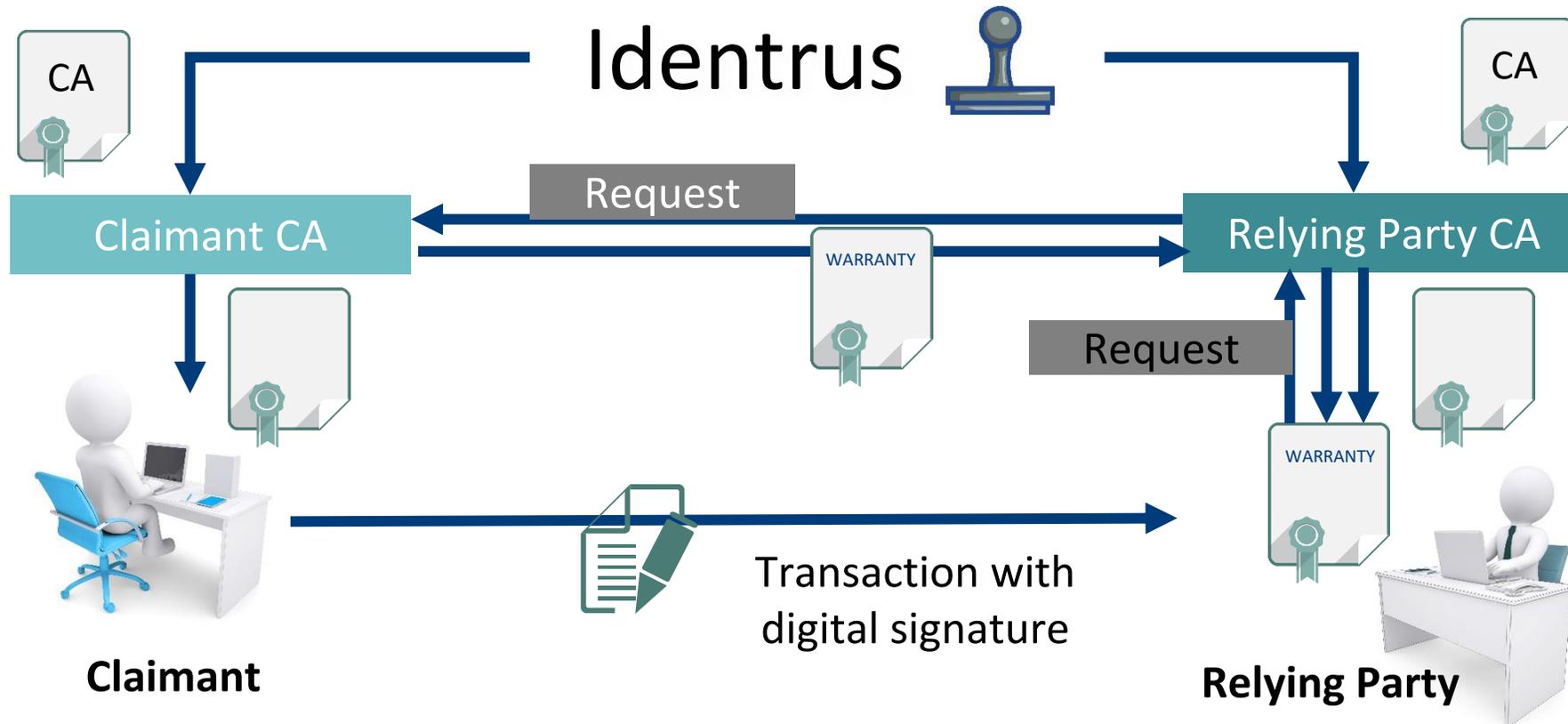
# Chains of Trust Between RAs



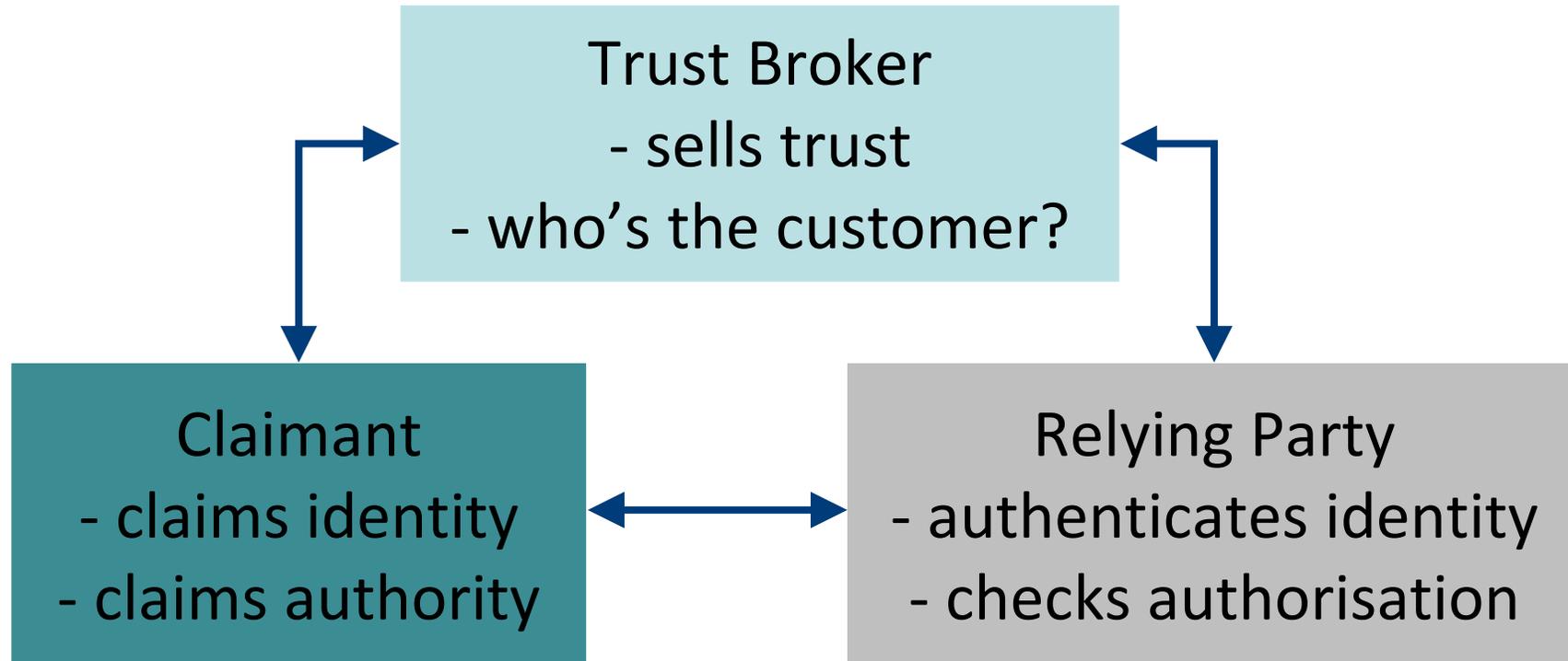
# Trust Hierarchies



# Identrus Model for Trust Brokers



# Business Models for Trust Brokering

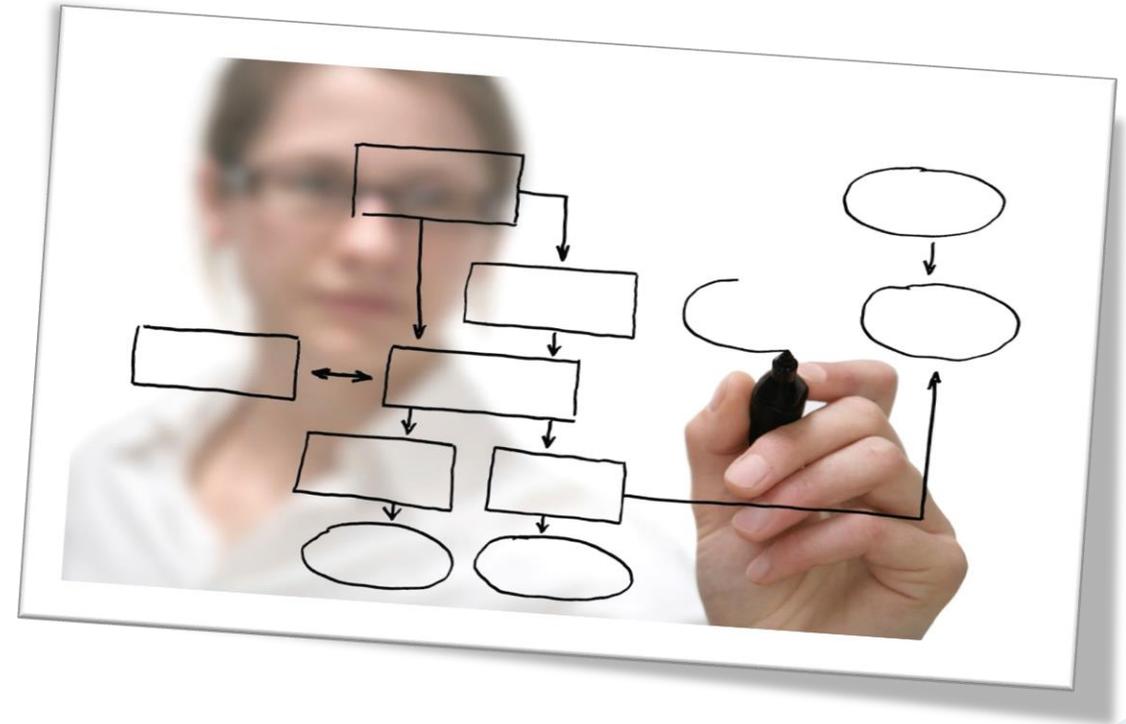


# Business Entity Relationships

- Various levels of trust and information flows
- Unilateral relationships
  - One party broadcasts or publishes information, others may receive it at their choice
- Bilateral relationships
  - Two parties make a specific contract
- Multilateral relationships
  - Group membership controlled by agreed rules

# Workshop F2-3

## Trust Modelling



# Sample Questions

## Competency Domain 4

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



# Competency Domain 4

- Alice, Bob and Charlie are the entities in a Trust Relationship. Charlie is the trusted third party who accredits credentials. Alice presents to Bob credentials that have been accredited by Charlie. Which party is MOST RELIANT on the trust asserted by the accreditation (who is the customer of trust)?
  - A. Alice
  - B. Bob
  - C. Charlie
  - D. Alice, Bob & Charlie equally

# Competency Domain 4

- Which ONE of the following statements about Authority Roles is TRUE?
  - A. The Certification (credentials issuing) Authority establishes trust and authorises participation in a domain
  - B. The Registration Authority issues credentials to trusted parties
  - C. The Certification (credentials issuing) Authority makes trust decisions on behalf of the domain owner
  - D. The Registration Authority establishes trust and authorises participation in a domain

# Inter-domain Security Associations

## Section 16

# Scope: Design Phase - Location

	Architecture Matrix	Management Matrix
Logical	<b>Domain Maps</b>	<b>Service Catalogue Management</b>
	Domain Definitions; Inter-domain Associations & Interactions	Configuration (CMBD) Management; Capacity Planning; Availability Management
Physical	<b>Infrastructure</b>	<b>Resources Management</b>
	Workspaces; Host Platforms, Layout of Devices & Networks	Physical & Environmental Security Management; Real Estate & Facilities Management
Component	<b>Locator Components &amp; Standards</b>	<b>Component Environment Management</b>
	Nodes, Addresses & Other Locators; Component Configuration	Physical & Environmental Security Component & Standards Management

# Section 16 Competency Objectives

## Competency / Question Domain 5 – Where (Location)

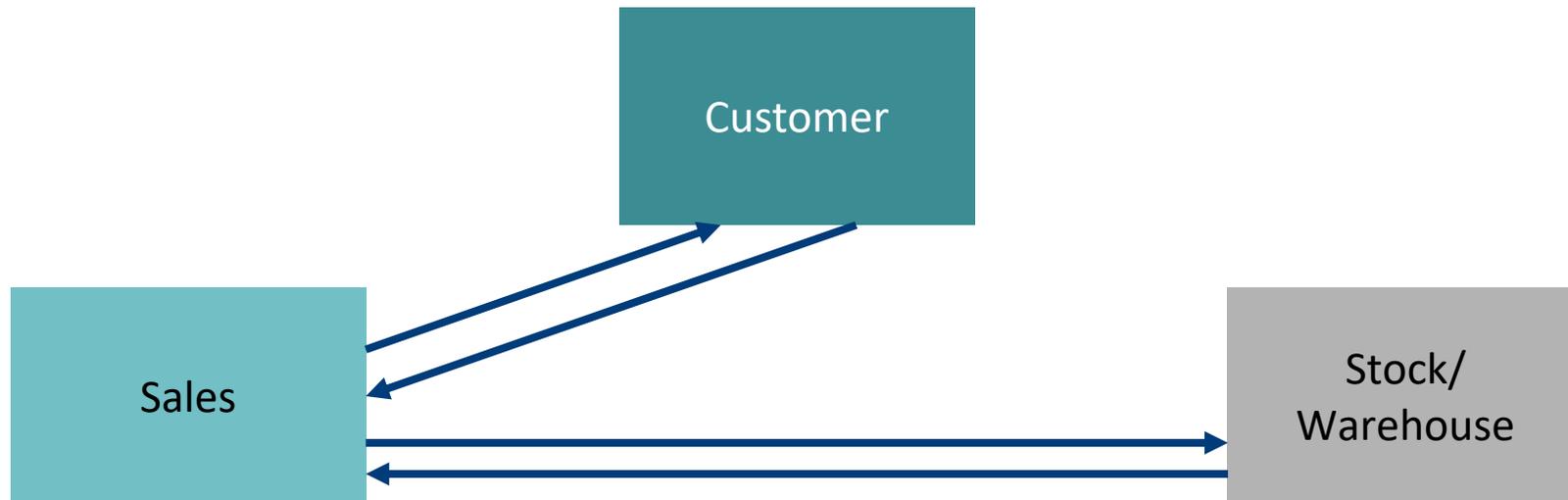
Knowledge Element	Knowledge Competency	Comprehension Competency
Domain Associations	Define the Security Associations concept & its objectives	Explain the application of security associations in achieving end-to-end security
	Describe the Extended Domain concept	Explain applications of the Extended Domain Concept
	Describe the importance of inter-domain modeling	Explain the application of inter-domain modeling

# Engineering Objectives

- The Attributes profile created in the Conceptual Architecture represents the business requirements for security end-to-end of business processes
- The security designers and engineers must therefore have a method to model and check that their solutions fit together as an end-to-end engineered complex system
- The SABSA method for achieving this is called Security Associations Modeling

# Entity Relationship Level

- Consider the 'simple' process of a customer making an enquiry to purchase some goods
- Entity view

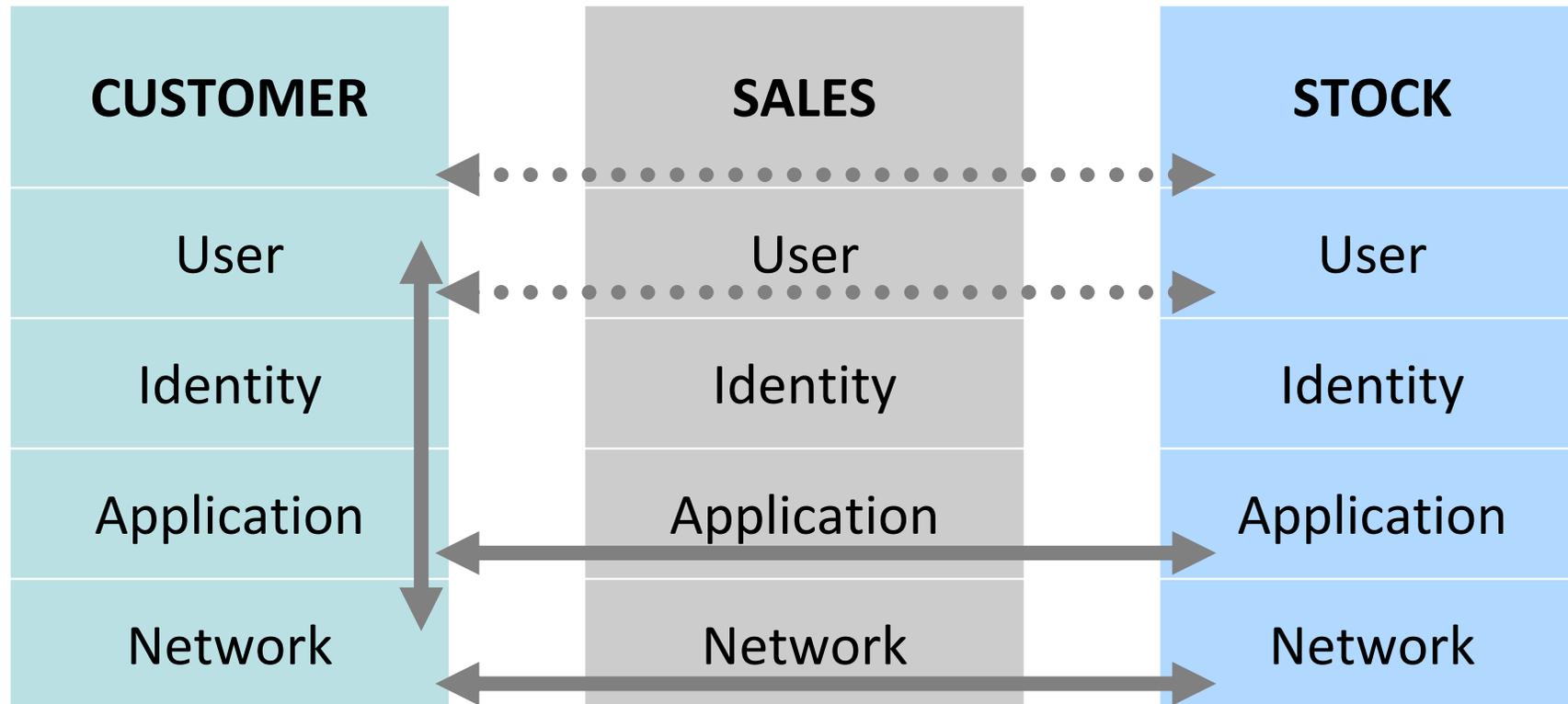


# Logical Representations

- Application
- Proxy
- System Identity (or identities)
- Client computer
- Server computer
- Network address
- Digital certificate
- Web site / page

# Entity Relationships

- Logical Representation view (illustration not definitive list of domains)



# Security Associations

- Standards define Security Associations as the set of shared information that describes the security relationship between two entities, such as
  - Cryptographic keys
  - Sequence numbers
  - Trusted time
  - etc
- In SABSA, the security association is a Logical representation of the business requirements for trust and security:
  - Intra-domain (between entities in a single domain)
  - Inter-domain (between entities in different domains)
- A fully engineered set of security associations combine to deliver the required Attribute end-to-end of the business process, irrespective of which domain boundaries are crossed, or how many

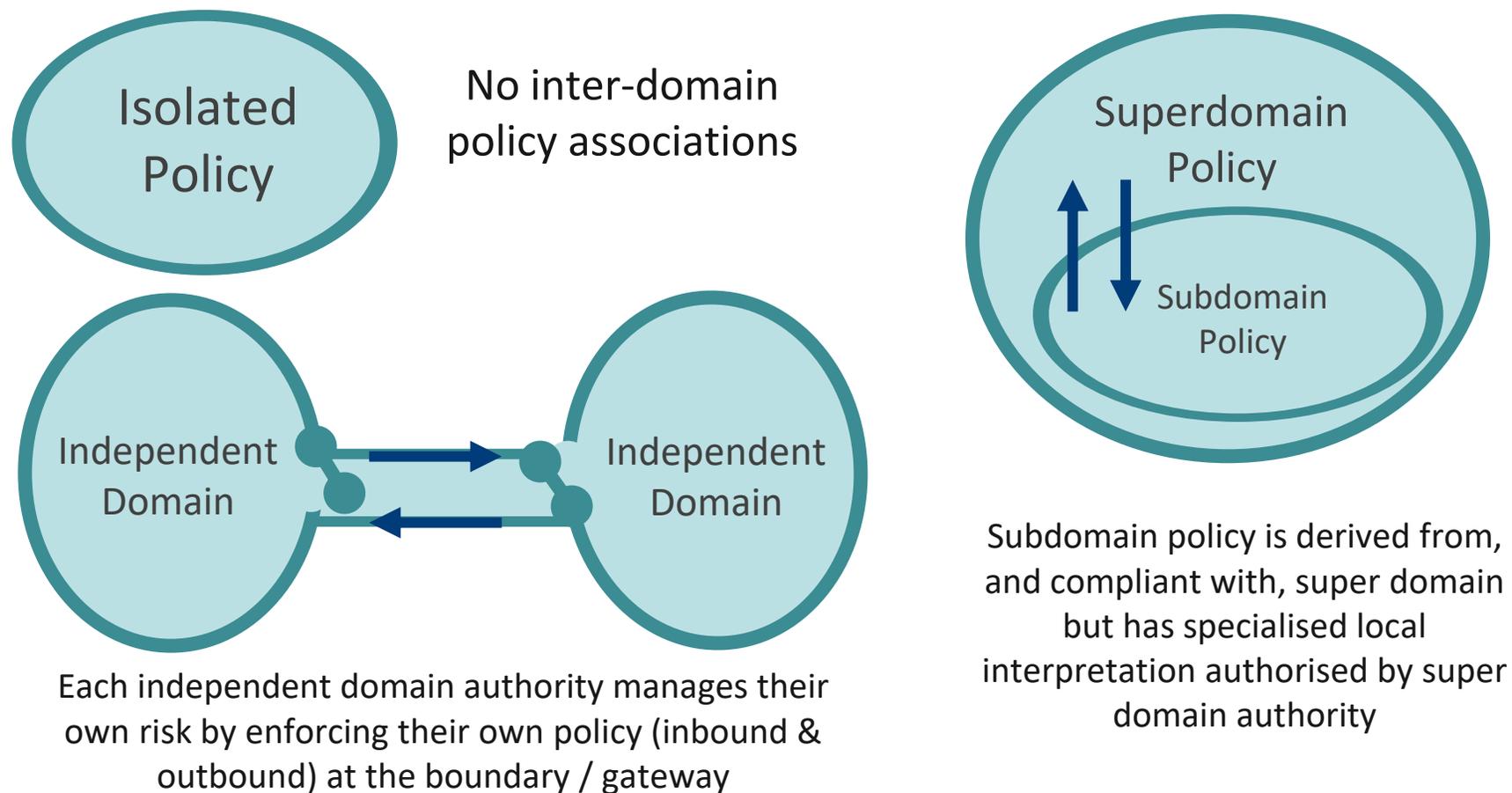
# End-to-End Security Objective

- An attribute is a requirement specified end-to-end across an entire business relationship
- The relationship is, at a lower layer, comprised of multiple business processes and information flows that often cross multiple policy domains
- Domains exist at both logical and physical levels
- Therefore Security Associations exist at many levels
- Logical domain associations - Associations in and between
  - Business units & lines of business
  - User communities & groups
- Physical domain associations - Associations in and between
  - Territories & jurisdictions
  - Buildings and sites
  - Infrastructure layer domains (networks, platforms, middleware etc.)

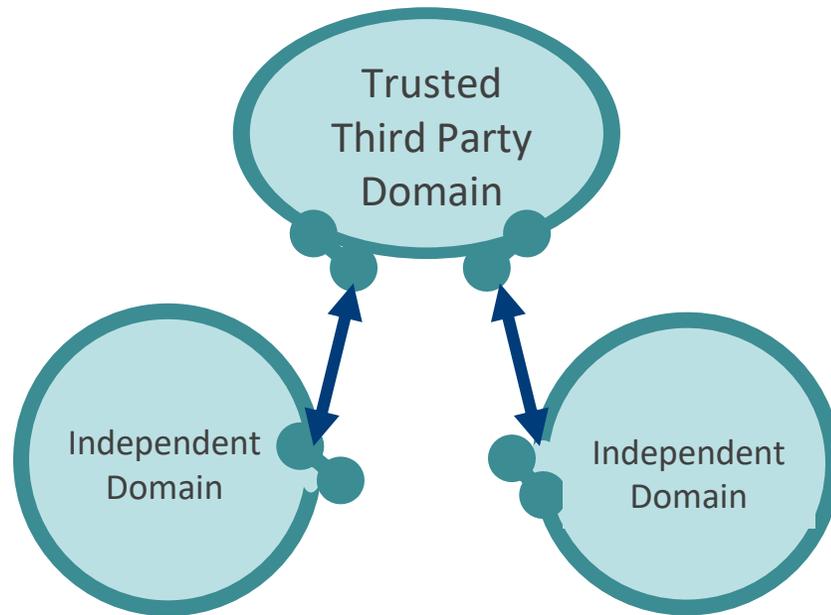
# Security Associations Represent Policy & Define Service Requirements

- Associations are achieved by deploying appropriate services
- Services are a logical abstraction of requirements specified independently of what physical mechanism might be used to deliver them
- They are driven from the Architecture layers above, most specifically from the Business Attributes Profile, the Control Objectives and the Architecture Strategies
- Intra-domain Associations are used to define the services required to meet the policy of a single domain authority
- Inter-domain Associations are used to define the services required between domains according to a specific relationship

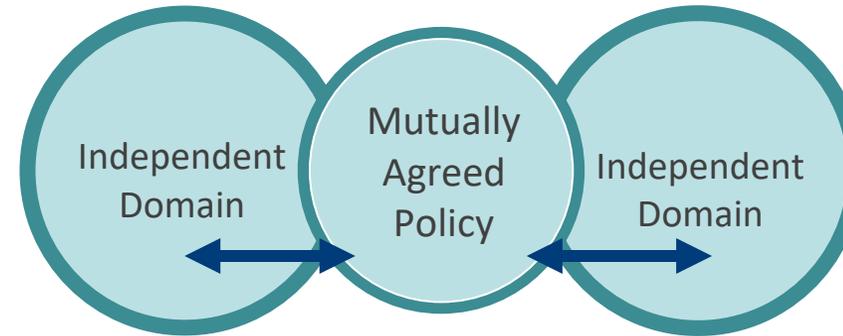
# Simple Inter-domain Policy Associations



# Complex Inter-domain Policy Associations



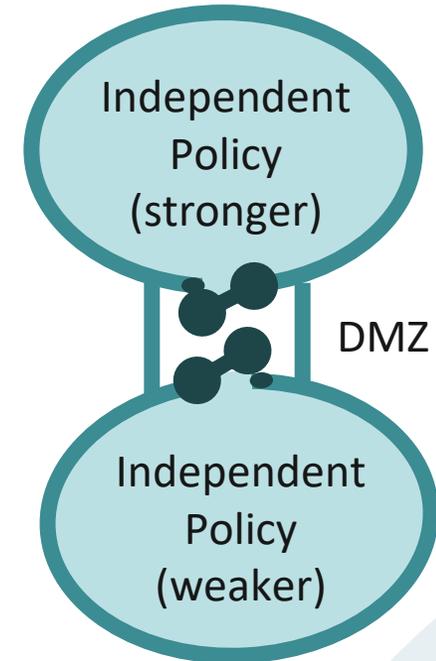
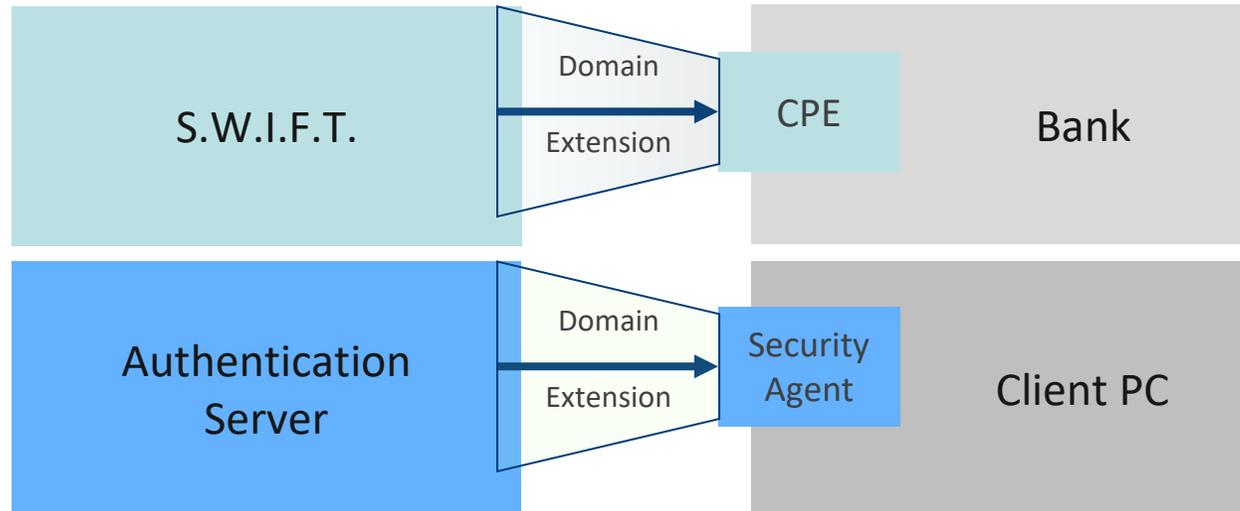
A special type of subdomain:  
the Trusted Third Party mandates  
policy for all associations – no  
local interpretation is permitted



The two independent domain authorities  
act collectively to agree / negotiate a  
common policy for a shared domain.  
Challenging: the common policy must  
contain every possible circumstance  
and/or very specific risk conflict resolution  
processes & procedures

# Extended Domain Concept

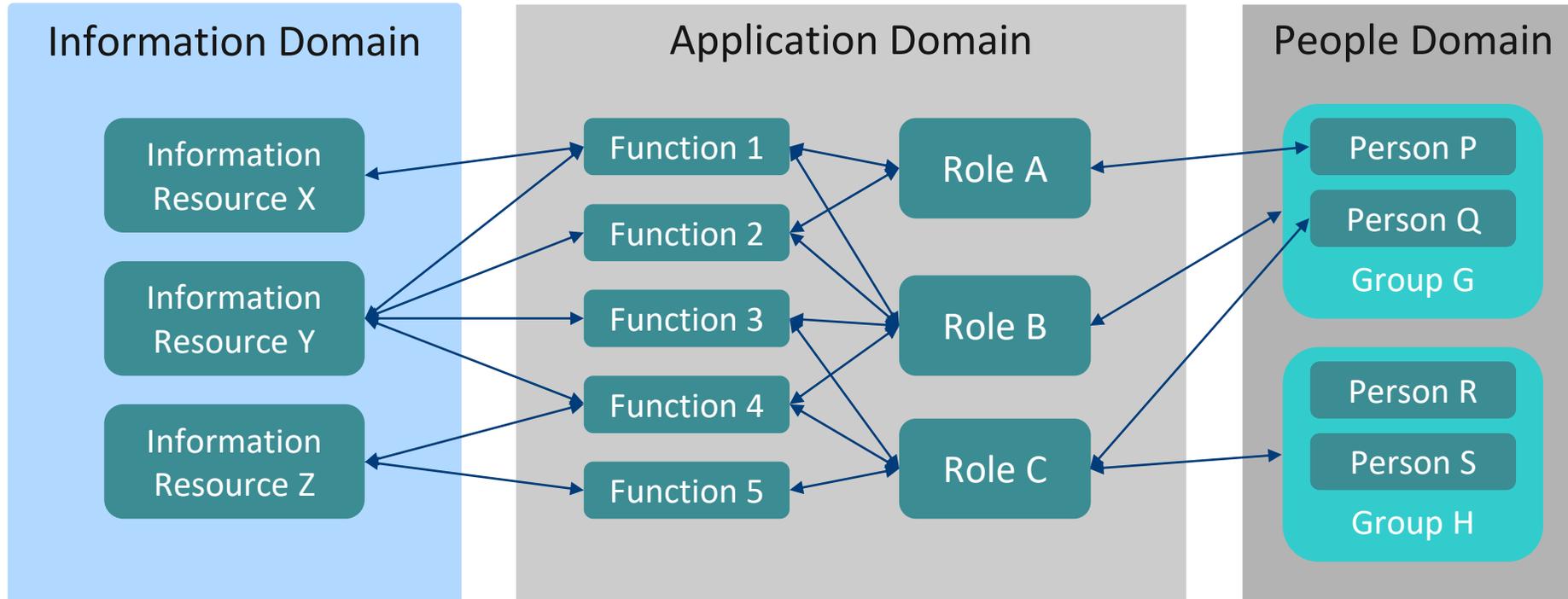
- The extended domain concept is used when one domain policy authority must exert control over another in order to successfully manage their own risk
- Effectively the dominant policy authority extends his domain into another – the stronger domain implants its policy into the 'territory' of another as a special sub-domain



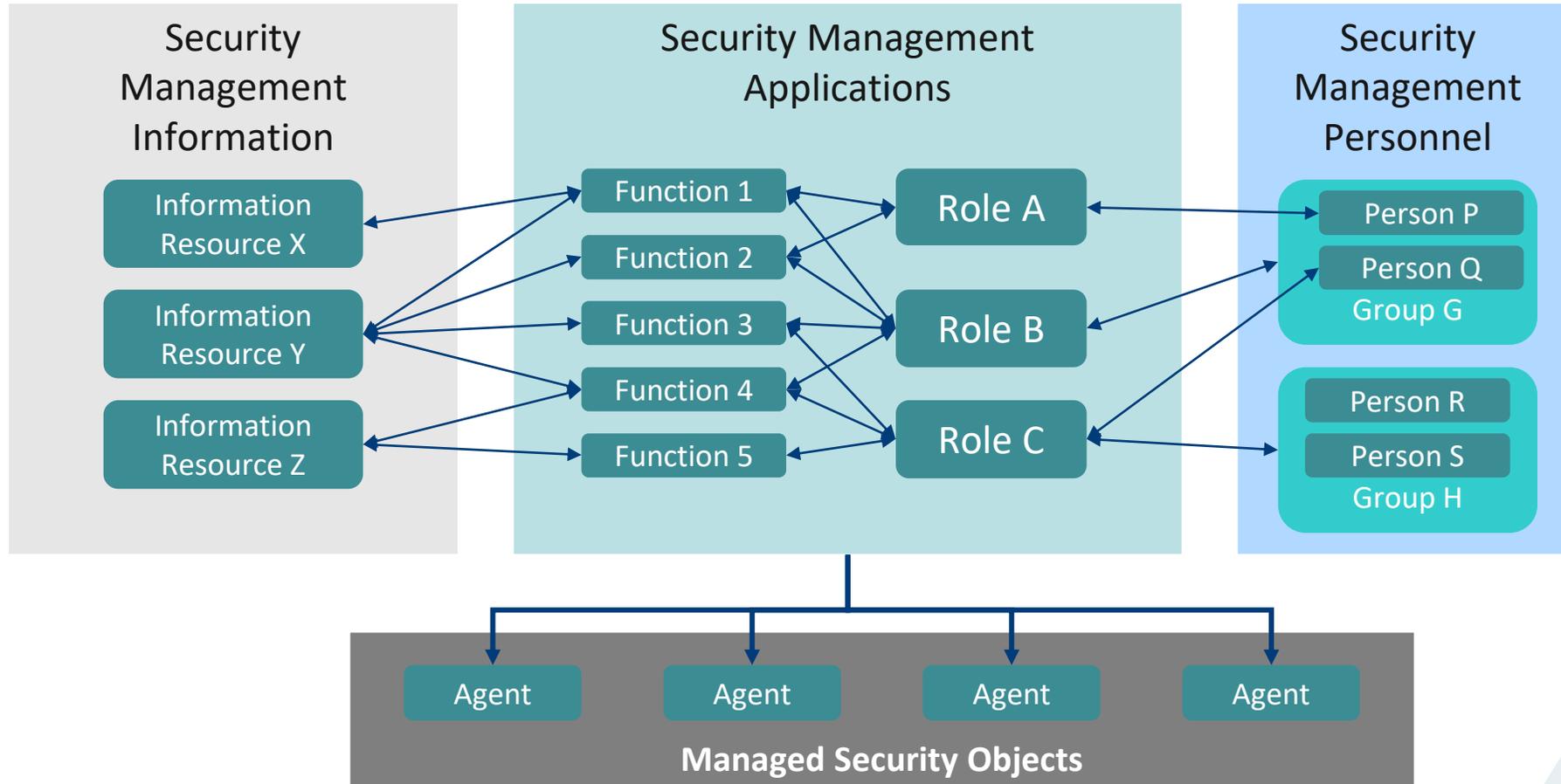
# Application Domains

- Each application is a logical domain, subject to a security policy for that application.
- This application domain has sub-domains, which are best mapped onto the roles, each role being a logical sub-domain
- The real users are actually part of another domain, which you can call the 'people domain', and the information resources used by the application are part of an 'information domain'.
- There are mappings from these external domains into the application domain to associate people and information resources with the roles.
- The 'extended application domain' includes these external logical components. Thus an 'extended application domain' comprises:
  - Roles – what are the roles and functions and information associated with each role, and what are the user-to-role mappings?
    - Functions associated with each role.
    - Users – which users?
    - High-privilege users – administrators, managers, auditors, operators, maintenance staff, etc.
    - User groups – what are the groups?
    - Information resources accessed by each role.

# Application Domain Diagram



# Extended Security Management Domain

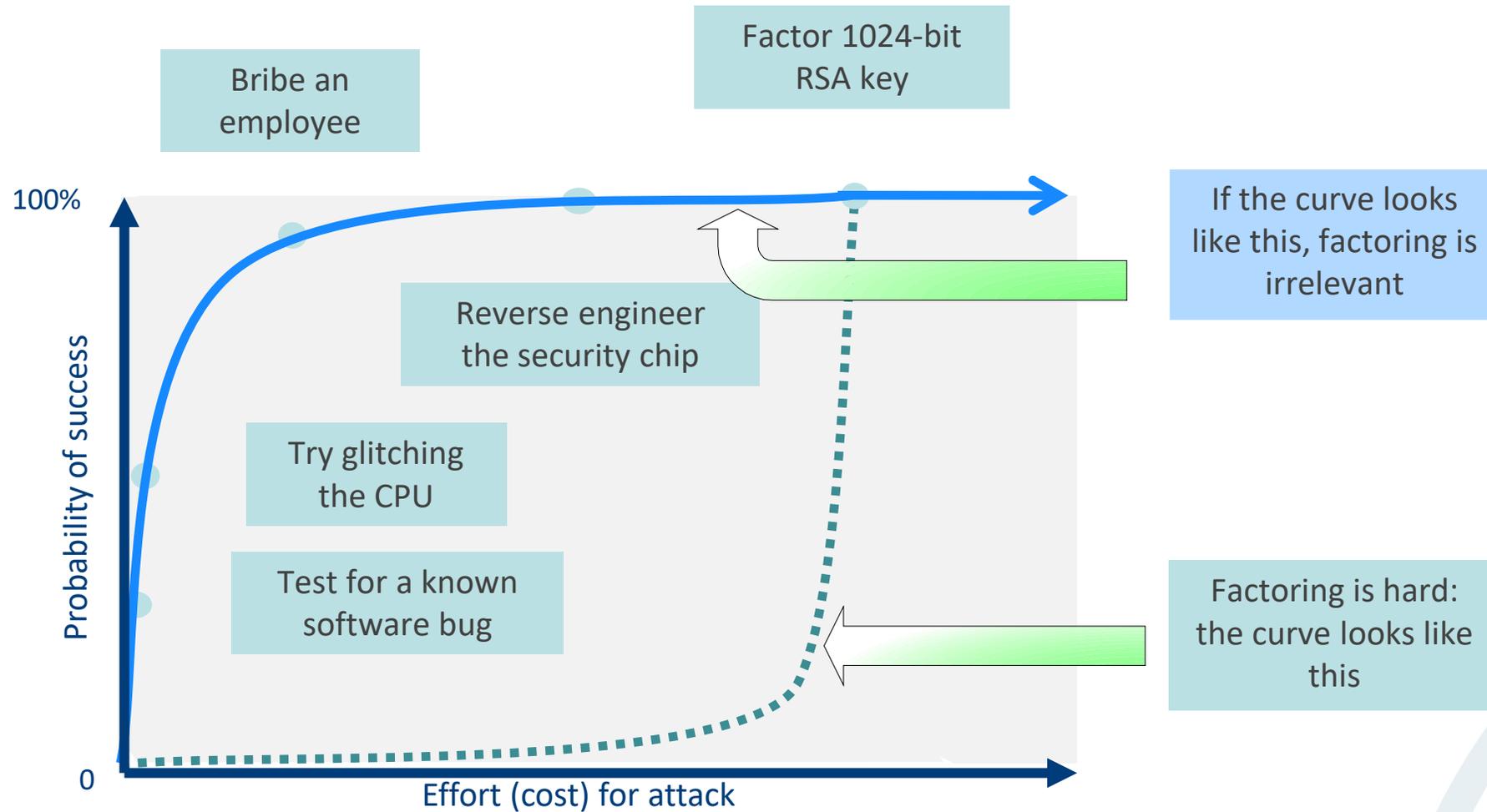


# Inter-domain Associations Case Study

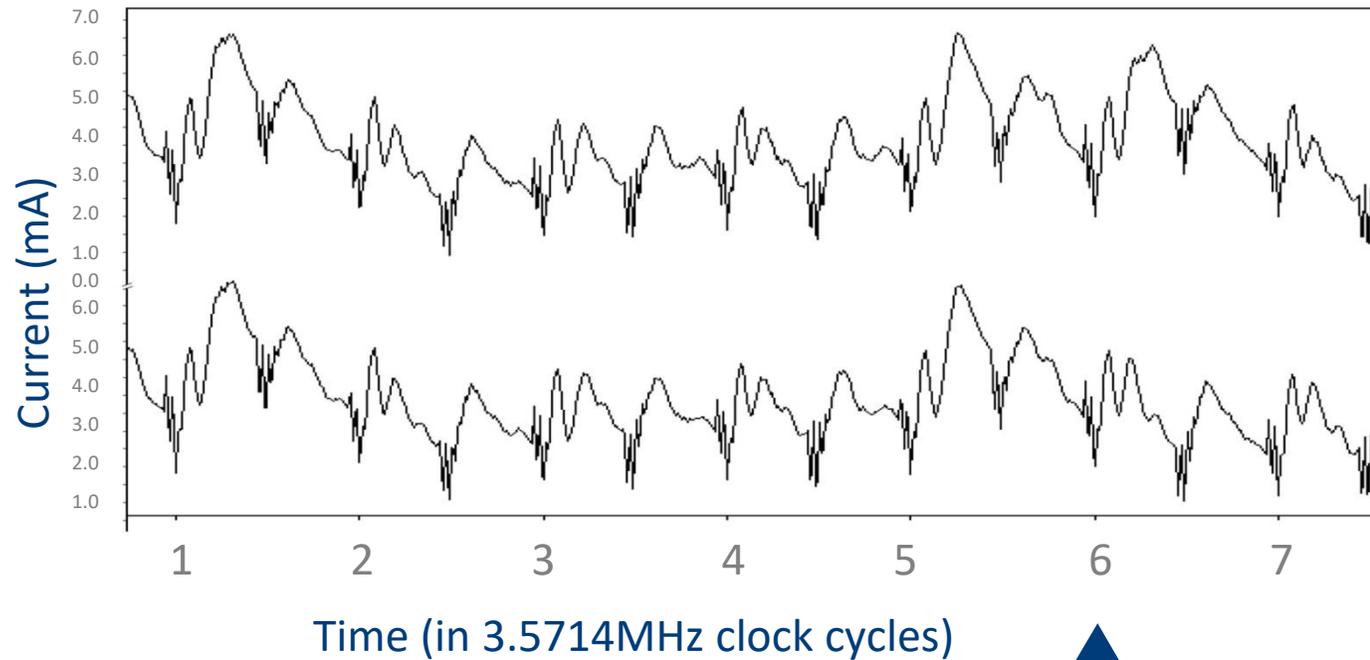
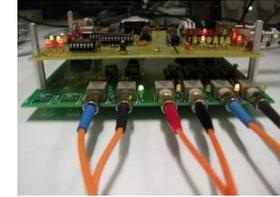
Courtesy of Paul Kocher, “Insecurity as an Emergent Property”, COSAC 2006  
(Case Study of Chip & Pin Credit Cards)

- All major operating systems have significant (or catastrophic) security bugs
- Users won't accept the reduced functionality of older systems
  - Companies and governments have to use modern technology to keep up with their rivals

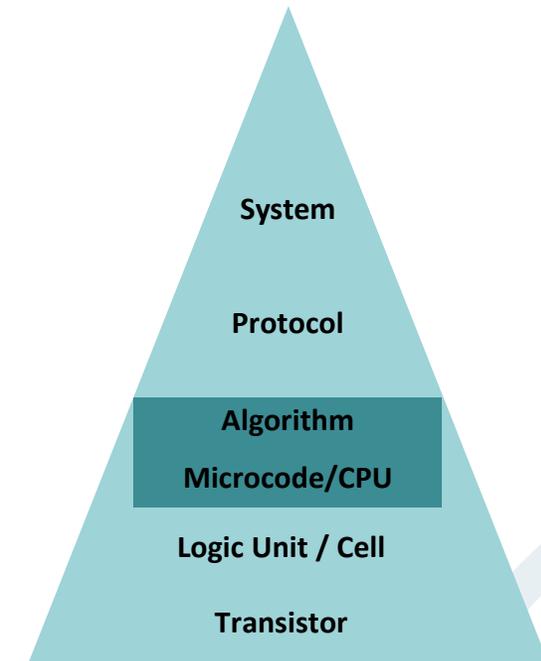
# Interactions & Complexity Create Low-hanging Fruit



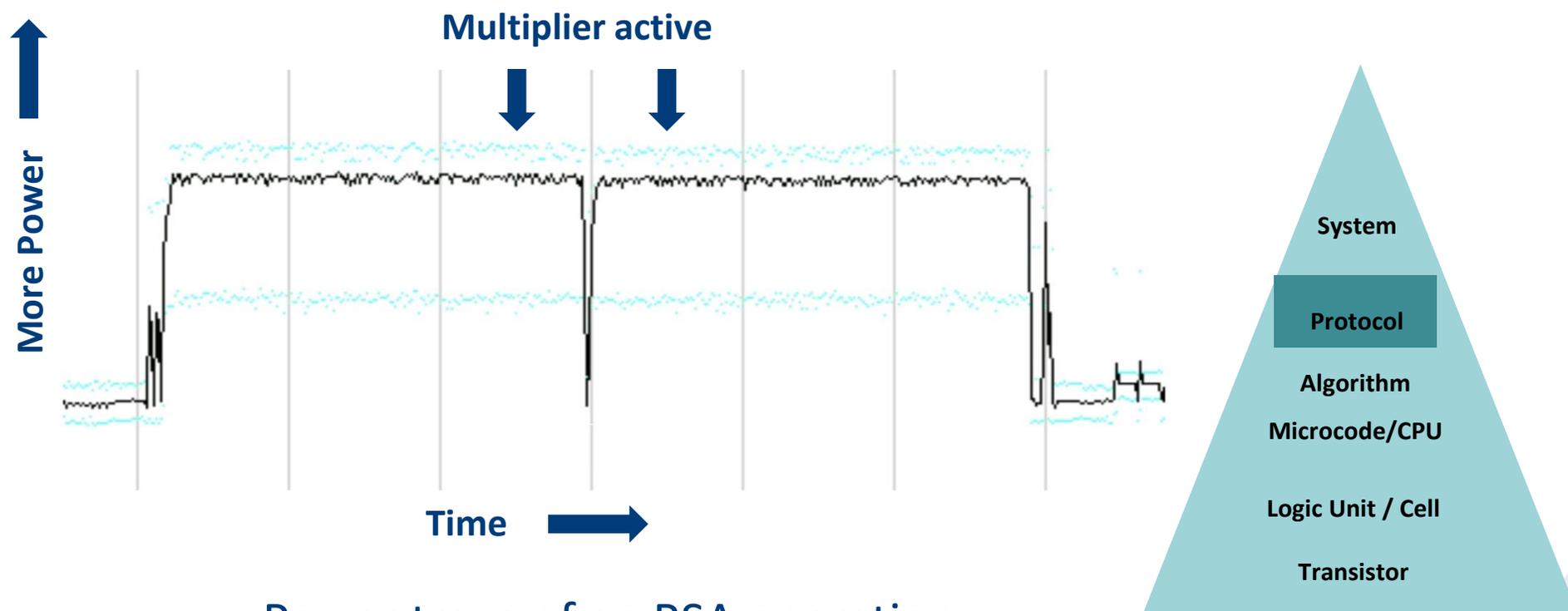
# Simple Power Consumption



Courtesy of Paul Kocher

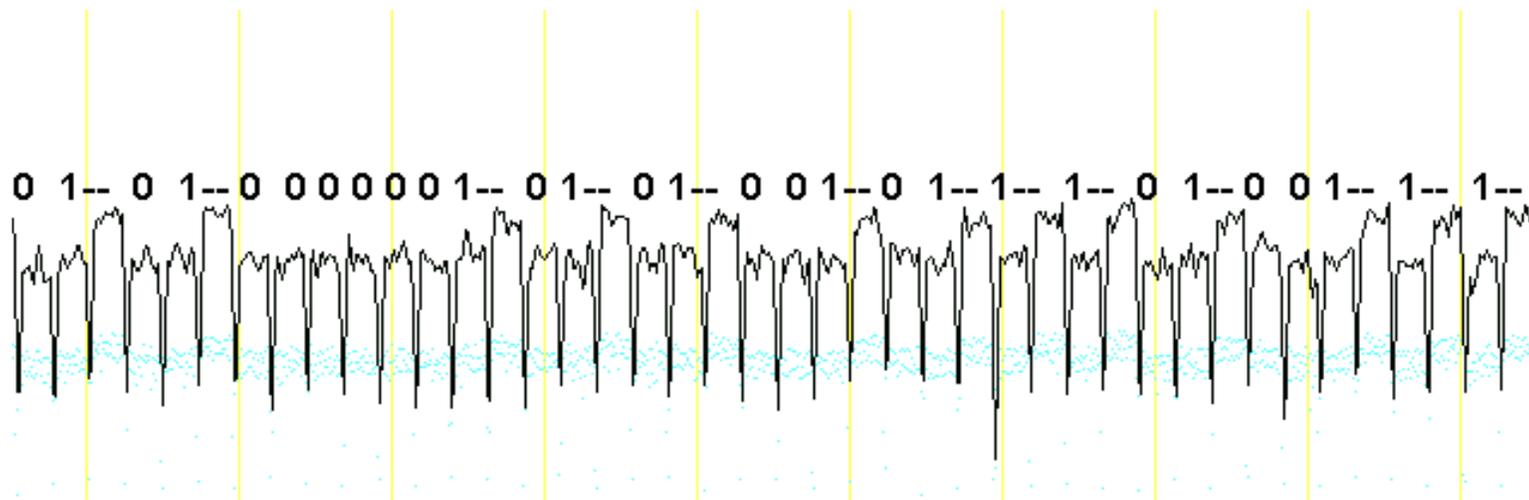


# Affecting Crypto & Software

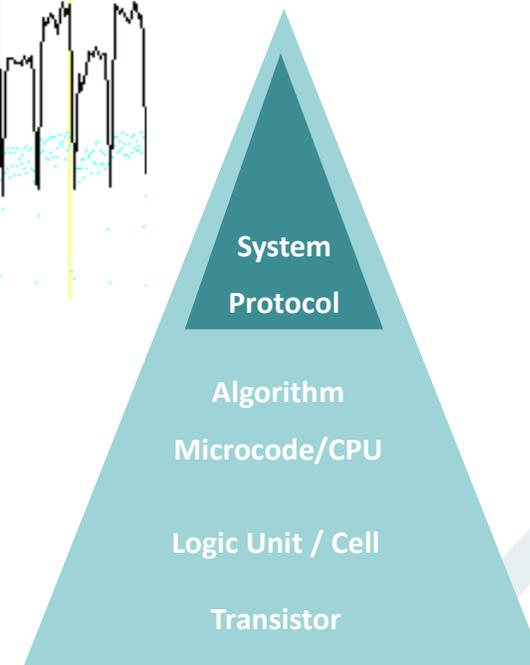


Power trace of an RSA operation  
(using Chinese Remainder Theorem)

# Affecting Crypto & Software

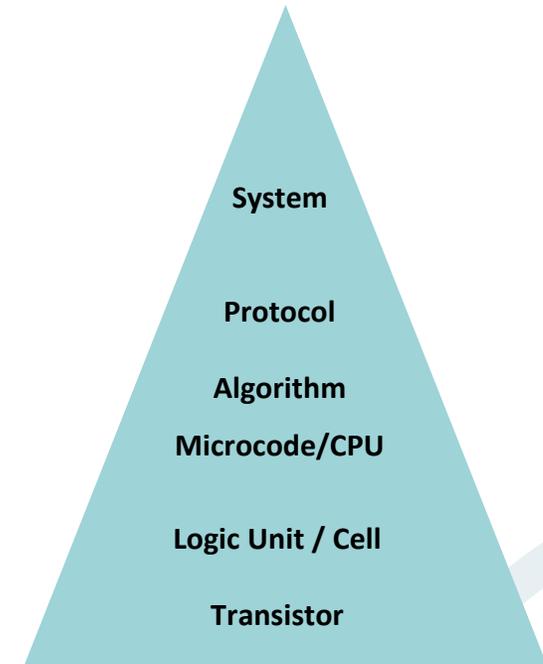


Zooming in on the multiply and reading off key bits



# What Happened?

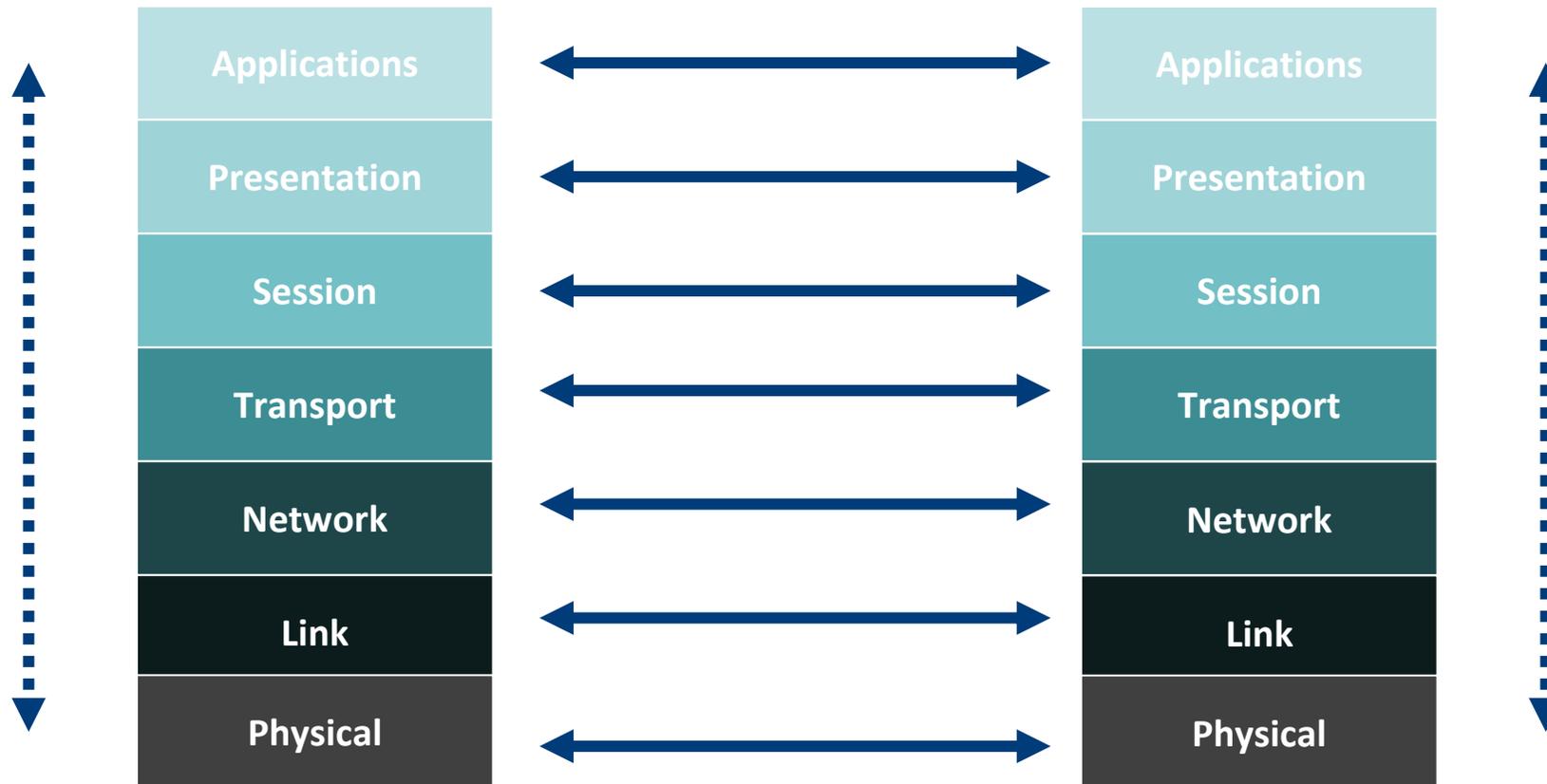
- A characteristic of transistors (the lowest layer) compromised each layer above, ultimately compromising the whole system and the business objectives
- Insecurity appears as complexity increases
- Our ability to understand elements of a system creates a false impression that we understand the system



# OSI Cryptographic Services Case Study

- Placement of cryptographic services within the Open Systems Communications Model
- OSI layering principles
- Security association principles
- Cryptography in OSI layers – the reality

# Open Systems Communications Model (OSI)



# Security Architectures in ISO

- OSI security architecture (ISO 7498-2)
  - applies only to OSI communications stack
  - provides a general description of security services and related mechanisms
  - defines the positions within the 7-layer OSI reference model for the location of services and mechanisms
  - describes pervasive security mechanisms
  - describes security management for OSI

# Security Services Defined

- Authentication
- Peer entity authentication
- Data origin authentication
- Access control
- Data confidentiality
- Data Integrity
- Non-repudiation

# Placement of Security in OSI Layers

OSI LAYER	SERVICES	MECHANISMS
7. Application	See next slide	See next slide
6. Presentation	Connection confidentiality Connectionless confidentiality Selective field confidentiality	Encipherment of appropriate data fields in protocol Encipherment of appropriate data fields in protocol Encipherment of appropriate data fields in protocol
5. Session (no services)		
4. Transport	Peer entity authentication Data origin authentication Access control Connection confidentiality Connectionless confidentiality Connection integrity (with recovery) Connection integrity (w/o recovery) Connectionless integrity	Cryptographically derived authentication exchanges Encipherment or signatures Specific access control mechanisms Encipherment Encipherment- Data integrity (and encipherment) Data integrity (and encipherment) Data integrity (and encipherment)
3. Network	Peer entity authentication Data origin authentication Access control Connection confidentiality Connectionless confidentiality Traffic flow confidentiality Connection integrity (w/o recovery) Connectionless integrity	Protected authentication exchanges Encipherment or signatures Specific access control mechanisms Encipherment and/or routing control - Traffic padding and routing control Data integrity (and encipherment) Data integrity (and encipherment)
2. Link	Connection confidentiality Connectionless confidentiality	Encipherment (sensitive to link layer protocol) -
1. Physical	Connection confidentiality Traffic flow confidentiality	Total encipherment of data stream Transmission security e.g. spread spectrum data transmission

# Placement of Security in Layer 7

OSI LAYER	SERVICES	MECHANISMS
7. Application	<ul style="list-style-type: none"> <li>Peer entity authentication</li> <li>Data origin authentication</li> <li>Access control (to system or remote app)</li> <li>Connection confidentiality</li> <li>Connectionless confidentiality</li> <li>Selective field confidentiality</li> <li>Traffic flow confidentiality</li> <li>Connection integrity (with recovery)</li> <li>Connection integrity (w/o recovery)</li> <li>Connectionless integrity</li> <li>Selective field connection integrity</li> <li>Non-repudiation with proof of origin</li> <li>Non-repudiation with proof of delivery</li> </ul>	<ul style="list-style-type: none"> <li>Authentication info xferred between app entities &amp; protected by presentation (or lower) encipherment</li> <li>Signatures or lower layer encipherment</li> <li>Access control in App and lower layers</li> <li>Lower layer encipherment</li> <li>Lower layer encipherment</li> <li>Presentation layer encipherment</li> <li>Traffic padding at App and confidentiality at lower layer*</li> <li>Lower layer integrity (and encipherment)</li> <li>Lower layer integrity (and encipherment)</li> <li>Lower layer integrity (and encipherment)</li> <li>Presentation layer integrity</li> <li>Presentation layer integrity</li> <li>Presentation layer integrity</li> <li>Signature &amp; lower layer integrity (possibly 3<sup>rd</sup> party notary)</li> <li>Signature &amp; lower layer integrity (possibly 3<sup>rd</sup> party notary)</li> </ul>

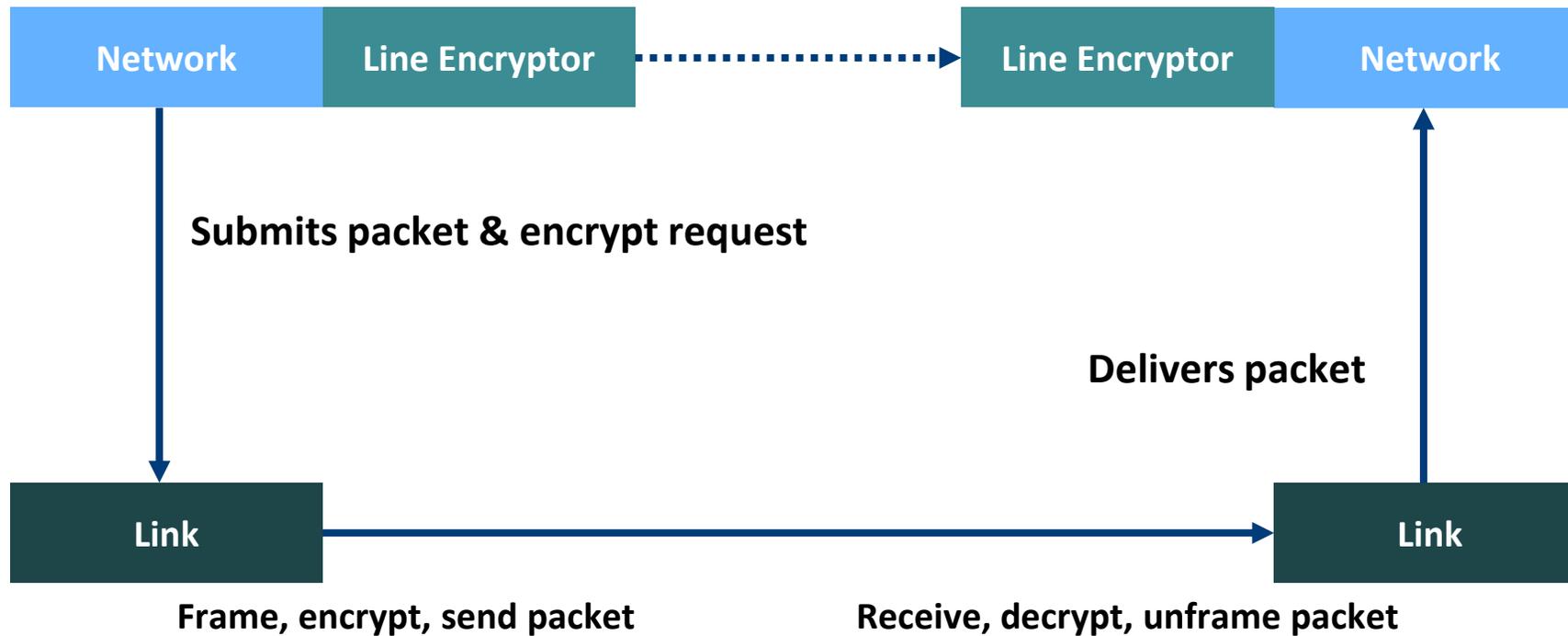
# OSI Layers in Practice (1)

- OSI layers are independent by design
  - “Violation of layer independence should be avoided”
- We know that in reality only Layer 1 is physically connected to Layer 1
- To create a logical connection through the stack each layer performs some function with the data sent by the layer below to make it seem that there is a physical connection of appropriate type at each layer

# OSI Layers in Practice (2)

- Layer n on system 1 knows that if it wants to send data to layer n on system 2 it must actually send it to its own layer n-1
- A logical layer n to layer n connection is achieved
- Layer independence means that layer n does not know or care how the connection is actually achieved by layer n-1 and it does not speak the language of layer n-1

# OSI Layers in Practice (3)



# OSI Layers in Practice (4)

- Confidentiality assured by the line encryptors?
- Consider what the layer 3 code actually knows in practice:
  - nothing except that it sent a request at one end and received a response at the other
  - The network engineers know (or think they do)
    - “It is all working fine today”
    - “What about yesterday?”
    - “We had a problem yesterday when a line encryptor failed so we took them both out. You know what? The system kept on working fine!”
  - Should the layer 3 code have known?
    - Often there is no means to test the fact – its an independent layer and does not talk the language

# OSI Layers in Practice (5)

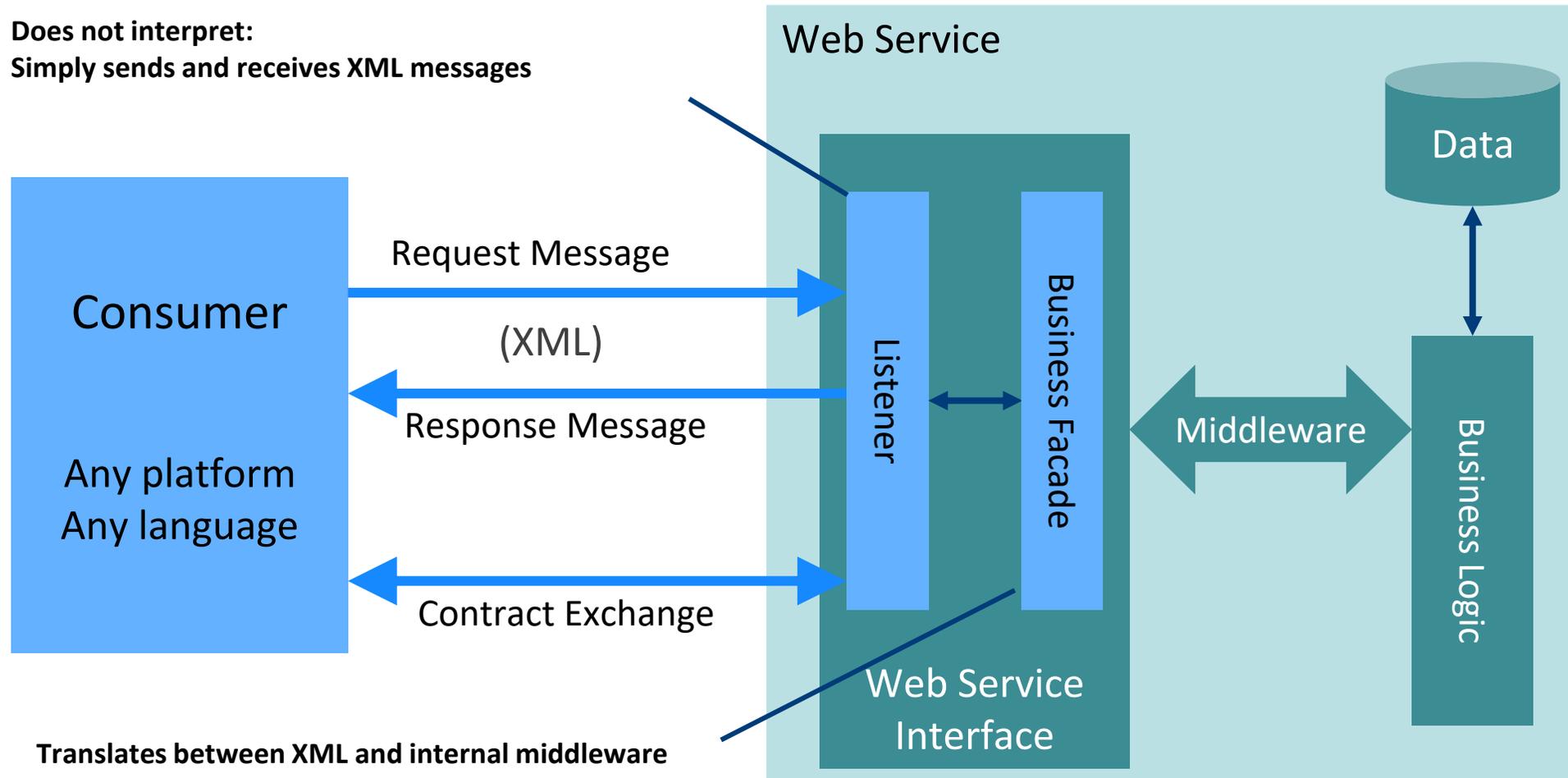
- This issue continues up to layer 7 where all the real data, real money, and real secrets are located
- How does it know that an authorisation response it receives is authentic or that the data it sends is treated correctly?
  - If crypto services are provided by a lower layer the application simply sends or receives data and trusts that the lower layers look after it
  - It could be coded to ask but what reliance can it place on the answer – it has no way to check for itself

# OSI Layers in Practice (6)

- Potentially an application could make use of cryptographic subsystems to provide its own crypto service before information is sent to lower layers
- It could also apply an authentication value on releasing the data and check it on receipt at the other end
- But to achieve that requires code
  - Ever tried applying that level of security coding as an afterthought?
  - How many ITTs have you seen than detail security properly?
  - Crypto servers are specialised and expensive
  - How many developers do you know who have the right knowledge and experience to code an application in this way?

# Web Services Architecture

Does not interpret:  
Simply sends and receives XML messages



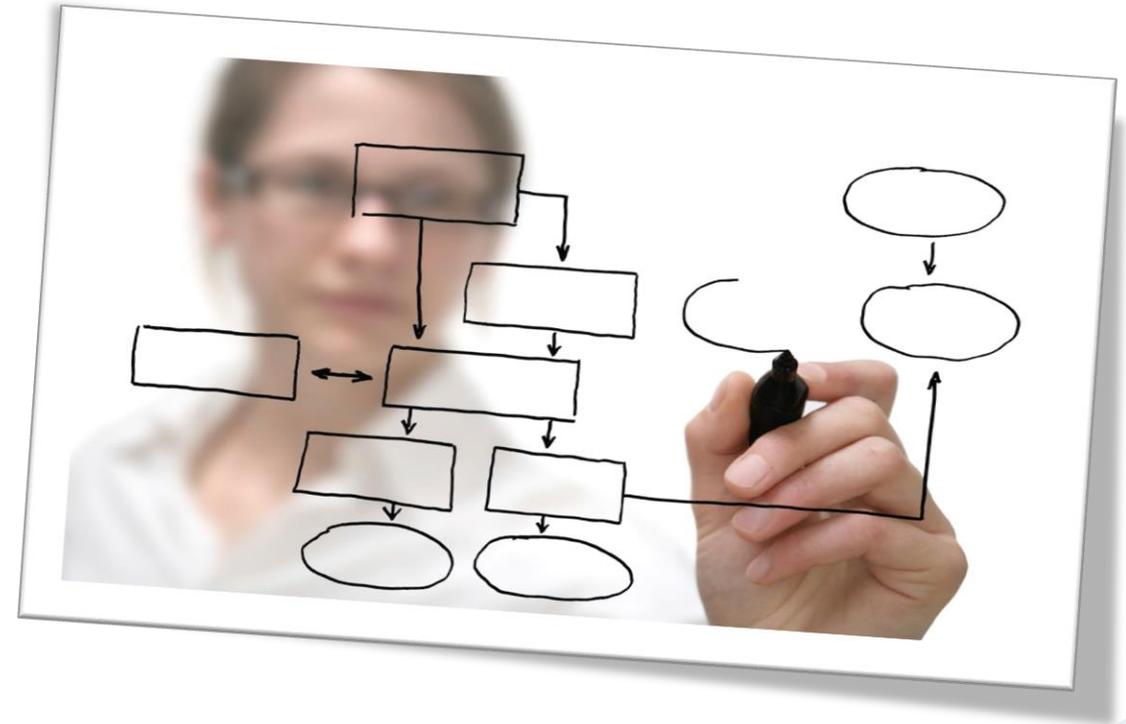
# Case Study Lessons

- The Architect must be able to model inter-domain associations
- They may not be built due to:
  - Expense
  - Risk justification
  - Technical feasibility
- But knowledge of the vulnerability is retained in the architect
  - It is part of the risk profile
  - The environment may change
  - The technical feasibility may change
  - The cost may change



# Workshop F2-4

## Inter-domain Security Associations



# Sample Questions

## Competency Domain 5

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



# Competency Domain 5

- Inter-domain associations are modelled in which column of which SABSA Matrix?
  - A. 'Where' column of the Management Matrix
  - B. 'Where' column of the SABSA Matrix
  - C. 'Why' column of the Management Matrix
  - D. 'Who' column of the SABSA Matrix

# Competency Domain 5

- Which ONE of the following statements about the use of Security Associations to model requirements at the SABSA logical layer is FALSE?
  - A. A security association describes the logical security relationship between two entities
  - B. A fully engineered set of security associations combines to deliver the required Attribute end-to-end of the business process, irrespective of which domain boundaries are crossed, or how many.
  - C. The scope of a single security association is intra-domain, inter-domain or end-to-end of a business process
  - D. Security associations provide a logical specification of attributes and trust requirements

# Service Sequencing

## Section 17

# Scope: Design Phase - Time

	Architecture Matrix	Management Matrix
Logical	<b>Calendar &amp; Timetable</b>	<b>Evaluation Management</b>
	Start Times, Lifetimes & Deadlines	Monitoring & Reporting Performance Against KPIs and KRIs
Physical	<b>Processing Schedule</b>	<b>Performance Data Collection</b>
	Timing & Sequencing of Processes & Sessions	Business Systems Monitoring Procedure Management
Component	<b>Step Timing &amp; Sequencing Components &amp; Standards</b>	<b>Monitoring Components</b>
	Time Schedules; Clocks; Timers & Interrupts	Analysis, Monitoring & Reporting Component and Standards Management

# Section 17 Competency Objectives

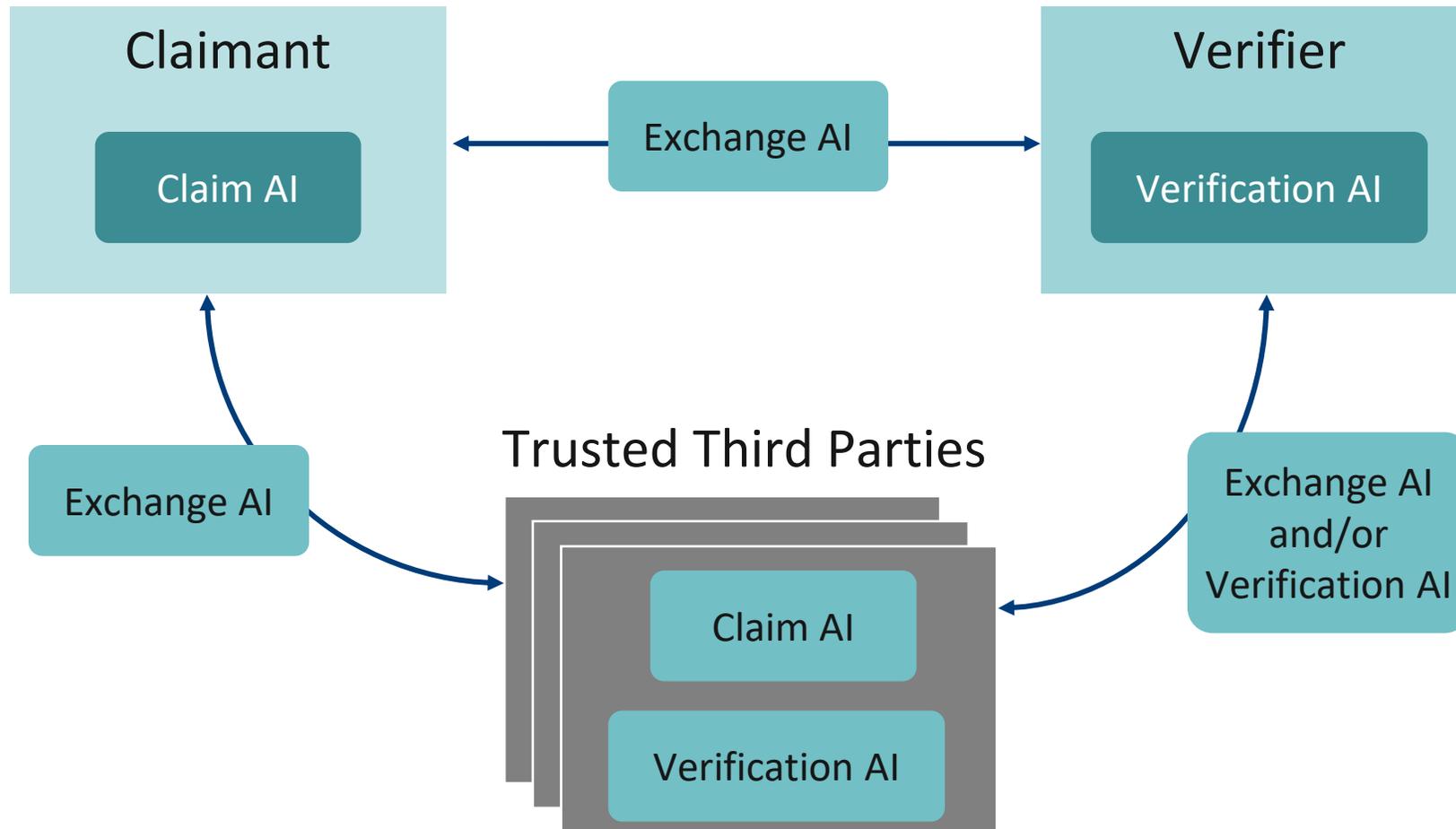
## Competency / Question Domain 6 – When (Time)

Knowledge Element	Knowledge Competency	Comprehension Competency
Timing & Sequencing	List temporal considerations for Security Architecture	Explain the application of temporal factors in Security Architecture
	Describe the sequencing of security services	Sequence security services according to business requirements
	Label logical relationships in authentication	Differentiate between parties in an Authentication schema & sequence their service interactions

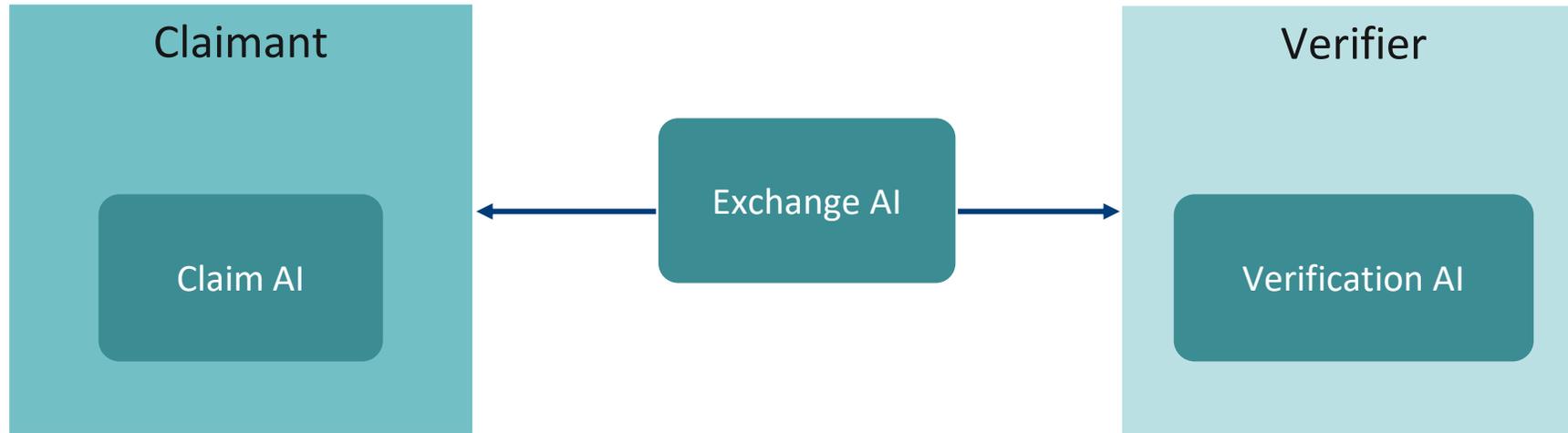
# Conceptual Lifetimes & Deadlines

- Registration
- Certification
- Cryptographic key lifetimes
- Policy lifetimes
- Password lifetimes
- Time-to-live
- User session lifetimes
- System session lifetimes
- Stored data lifetimes
- Data secrecy lifetimes
- Response time out
- Inactivity time out
- Context-based access control
- Replay protection
- Trusted time
- Time stamps
- Performance levels / SLA
- Disaster recovery targets

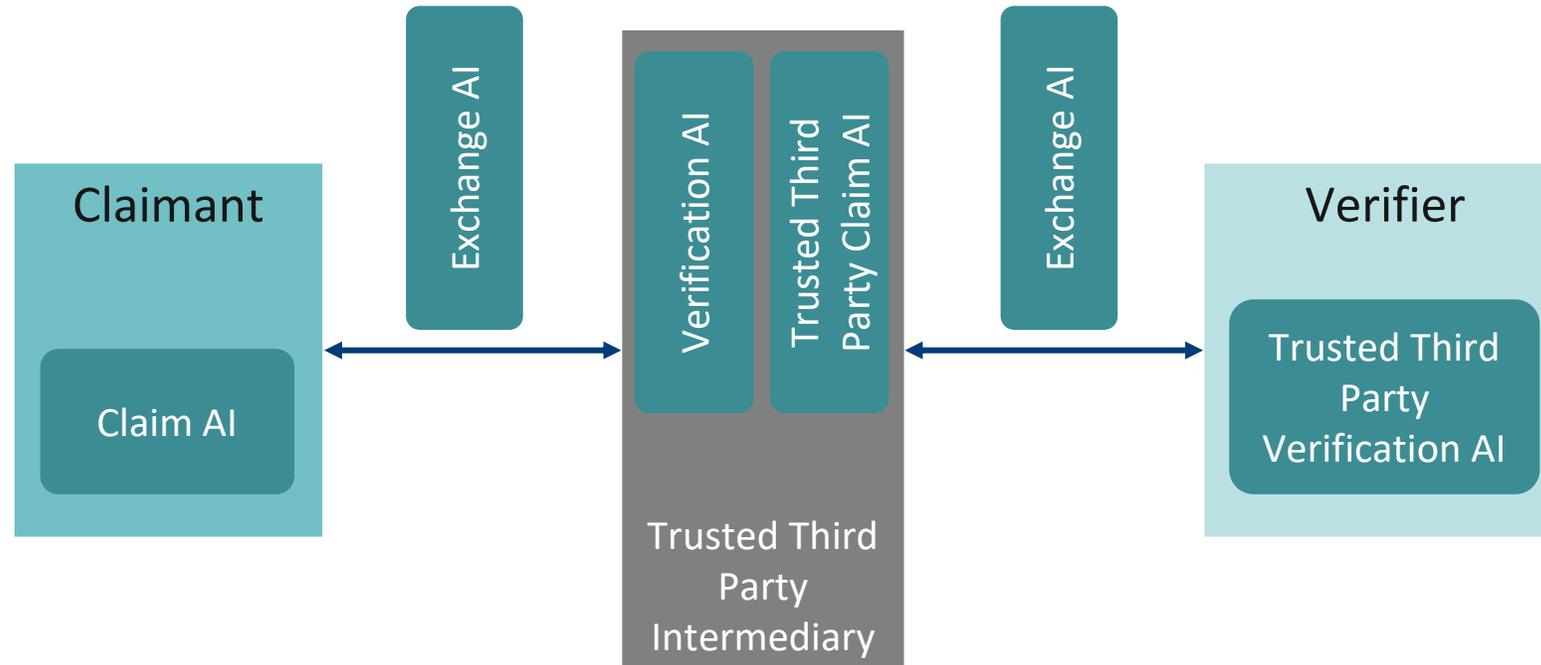
# Logical Relationships in Authentication



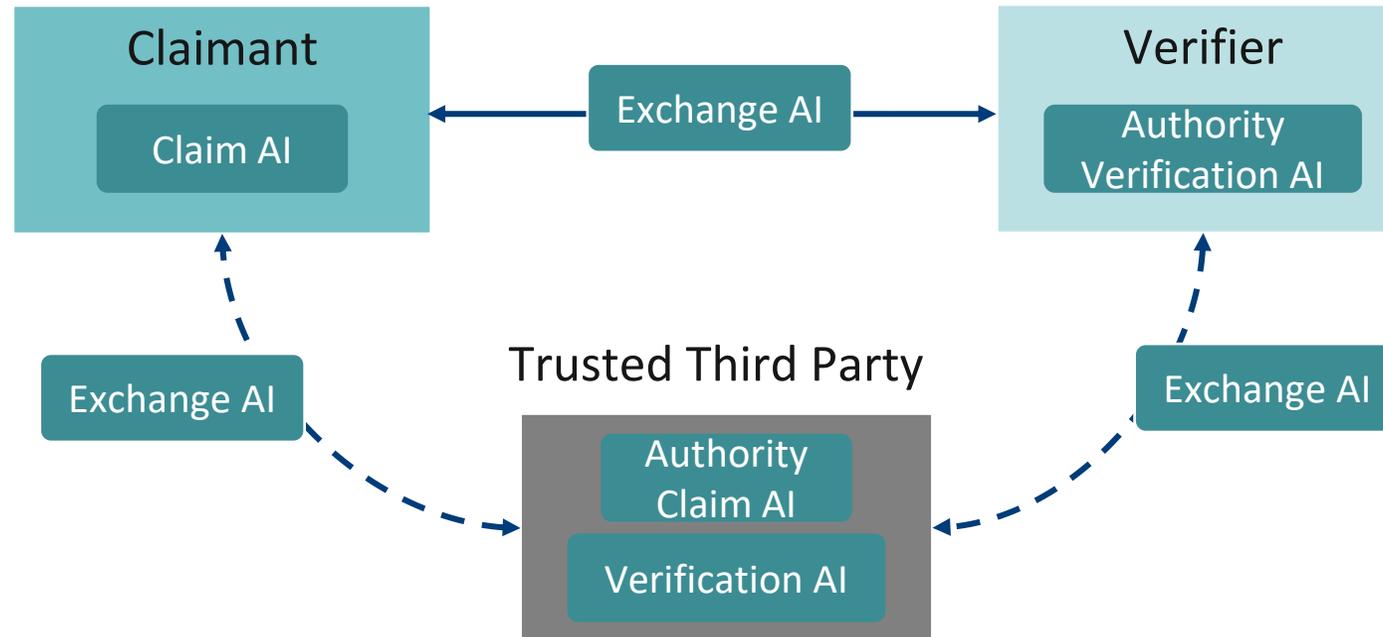
# Direct Authentication Relationship



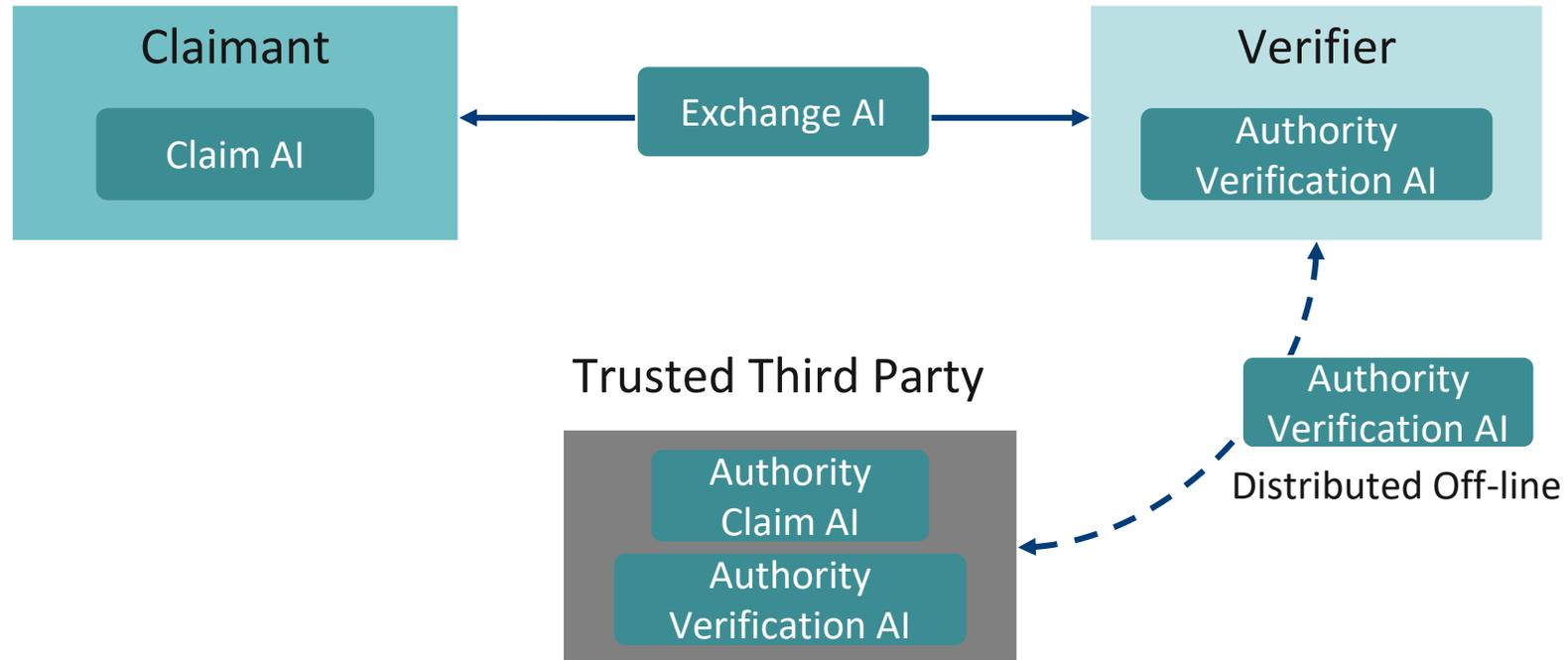
# Indirect In-Line Authentication



# On-Line Authentication



# Off-line Authentication



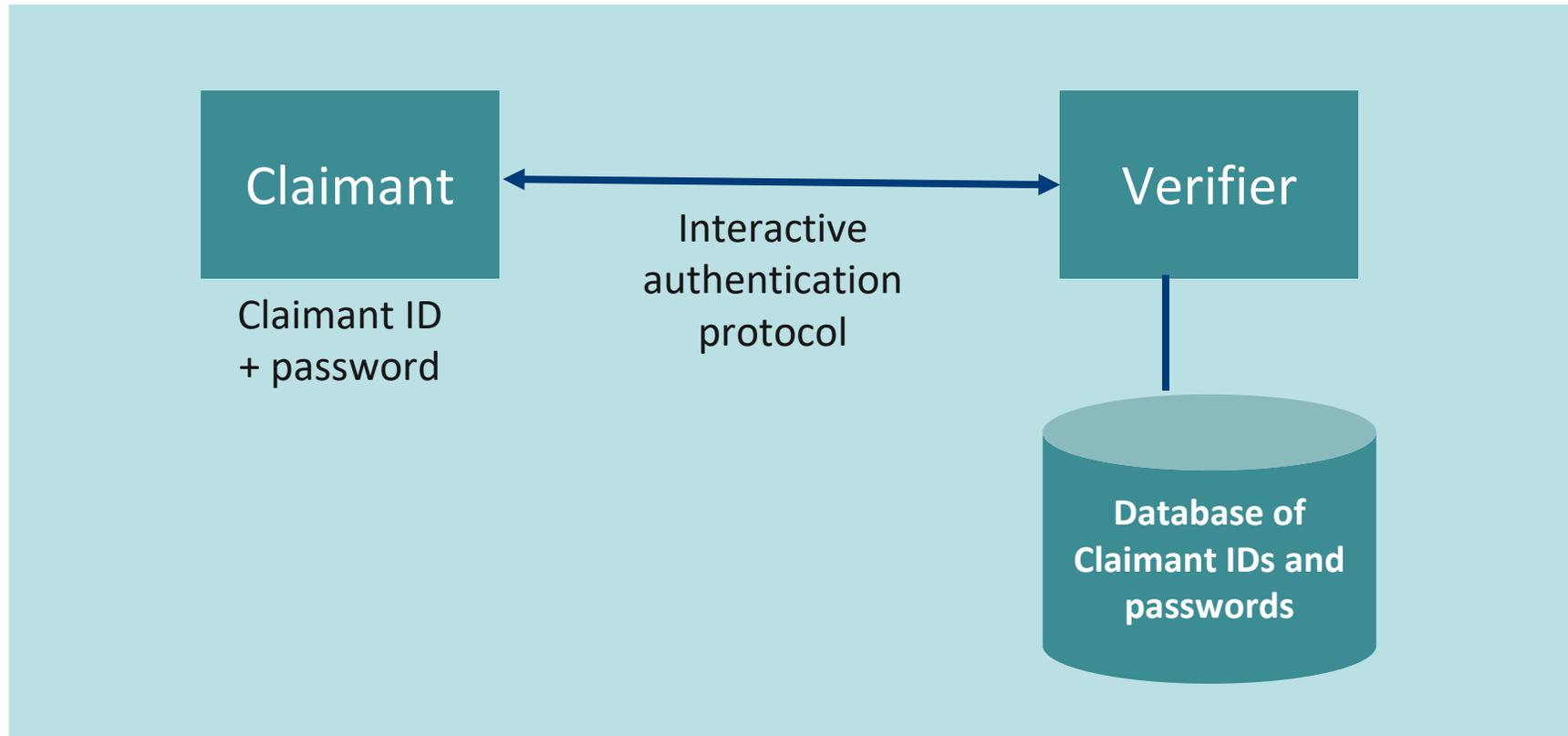
# Security Processing Cycle

- The security processing cycle involves a number of security management activities such as:
  - Introducing and registering new organisational entities.
  - Introducing and registering new users.
  - Setting up authorised privileges.
  - Registration renewal.
  - Certificate issue and renewal.
  - Provisioning and configuring equipment throughout the environment.
- There are also a number of automated processes, such as for setting up and closing down sessions, and for handling messages that have a defined 'time-to-live' so that they are discarded if they prove to be undeliverable.

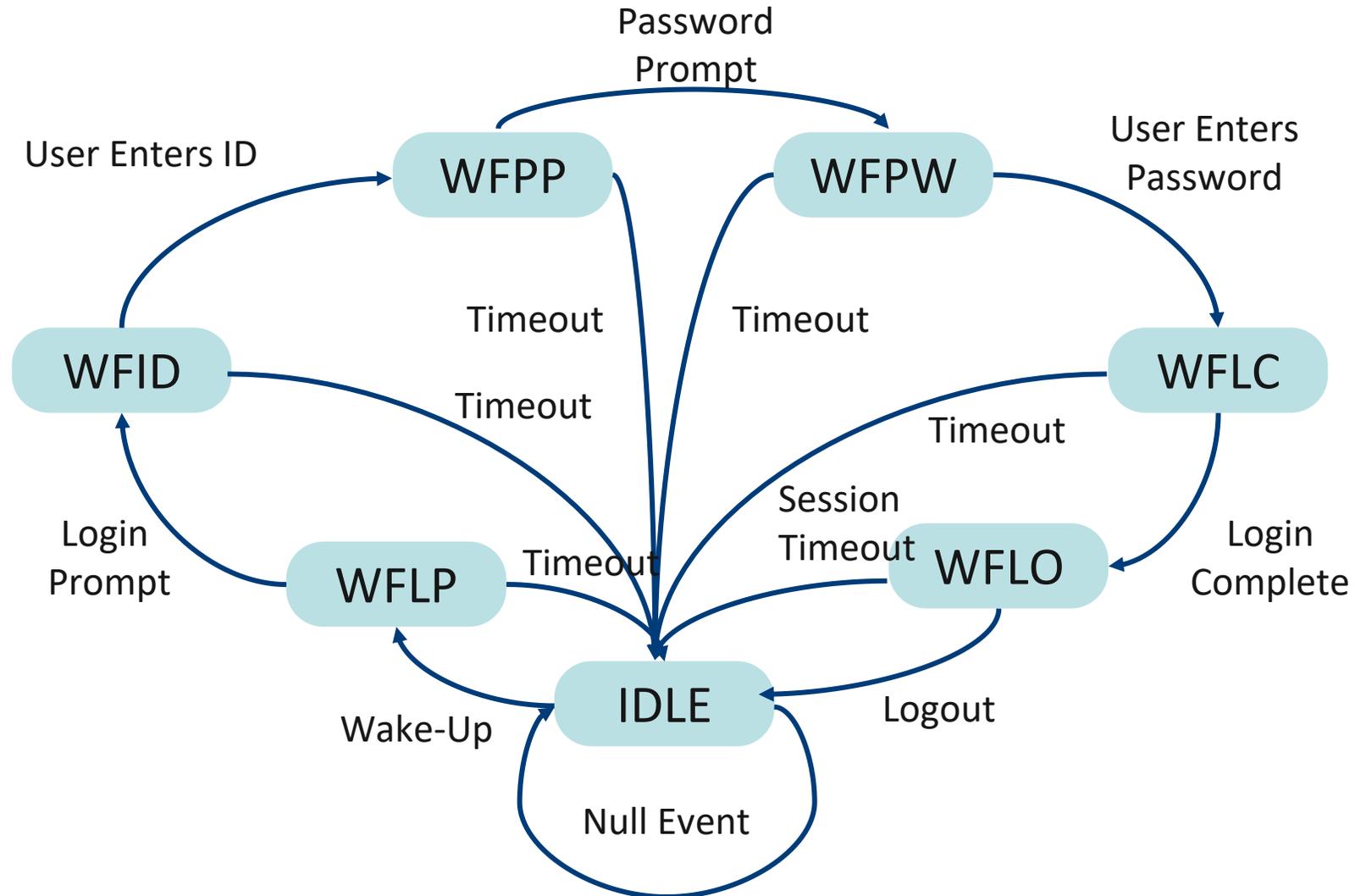
# Security Processing Cycle

- To define the logical flow of each of these processes you will need to adopt a systematic method (a loose version of ‘finite state machine modelling’)
- Here are some of the key considerations:
  - What is your complete list of security processes?
  - What event initiates each of these processes?
  - What event closes the process?
  - What intermediate stages are there in the process where it moves from one state to another?
  - What events trigger the transition of the process from one intermediate state to another?

# Authentication Example

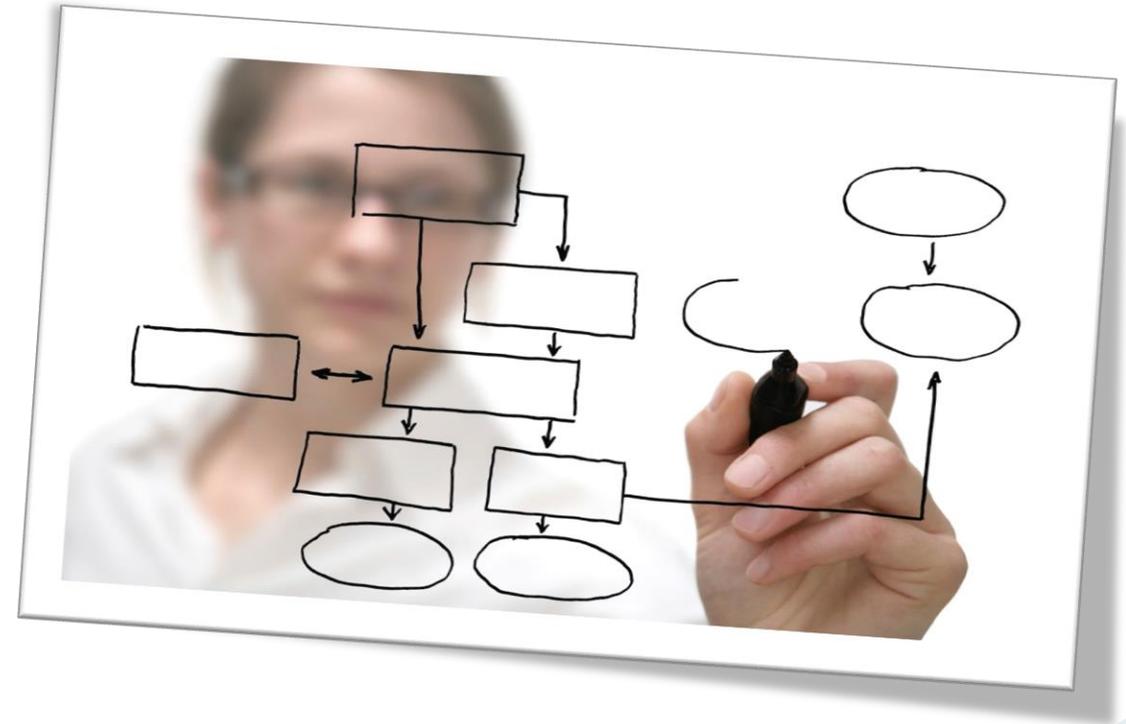


# Finite State Machine Model



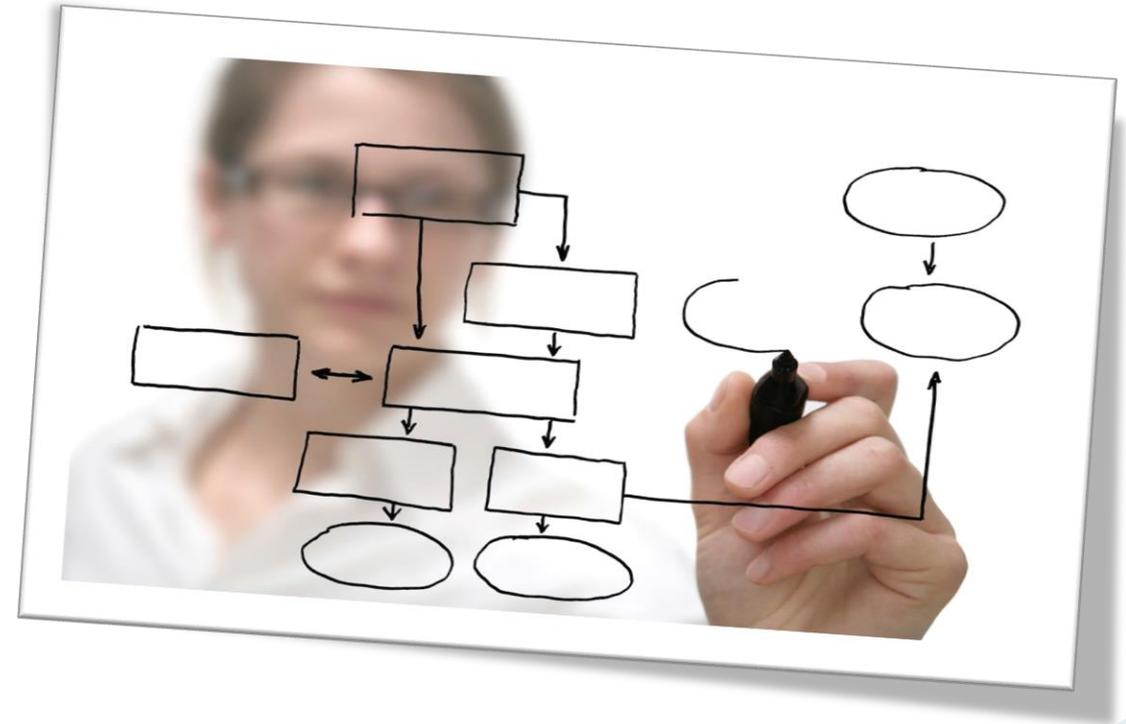
# Workshop F2-5

## Sequencing of Security Services



# Workshop F2-6

## Application of SABSA Foundation



# Sample Questions

## Competency Domain 6

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



# Competency Domain 6

- In an Authentication Relationship which ONE of the following represents the use of Authentication Information in the CORRECT SEQUENCE?
  - A. Claim AI, Exchange AI, Verification AI
  - B. Exchange AI, Claim AI, Verification AI
  - C. Verification AI, Claim AI, Exchange AI
  - D. Claim AI, Verification AI, Exchange AI

# Competency Domain 6

- Which ONE of the following is NOT a temporal consideration when architecting the Security Processing Cycle?
  - A. Time-to-live of messages
  - B. Close of session
  - C. Credentials renewal cycle
  - D. Public key certificate attribute extensions

# Thank you

The SABSA Institute C.I.C

<https://www.sabsa.org>

[info@sabsa.org](mailto:info@sabsa.org)