SABSA Advanced A3 Architecture Design & Development

SABSA Chartered Architect Practitioner Level (SCP)

v1.9.1

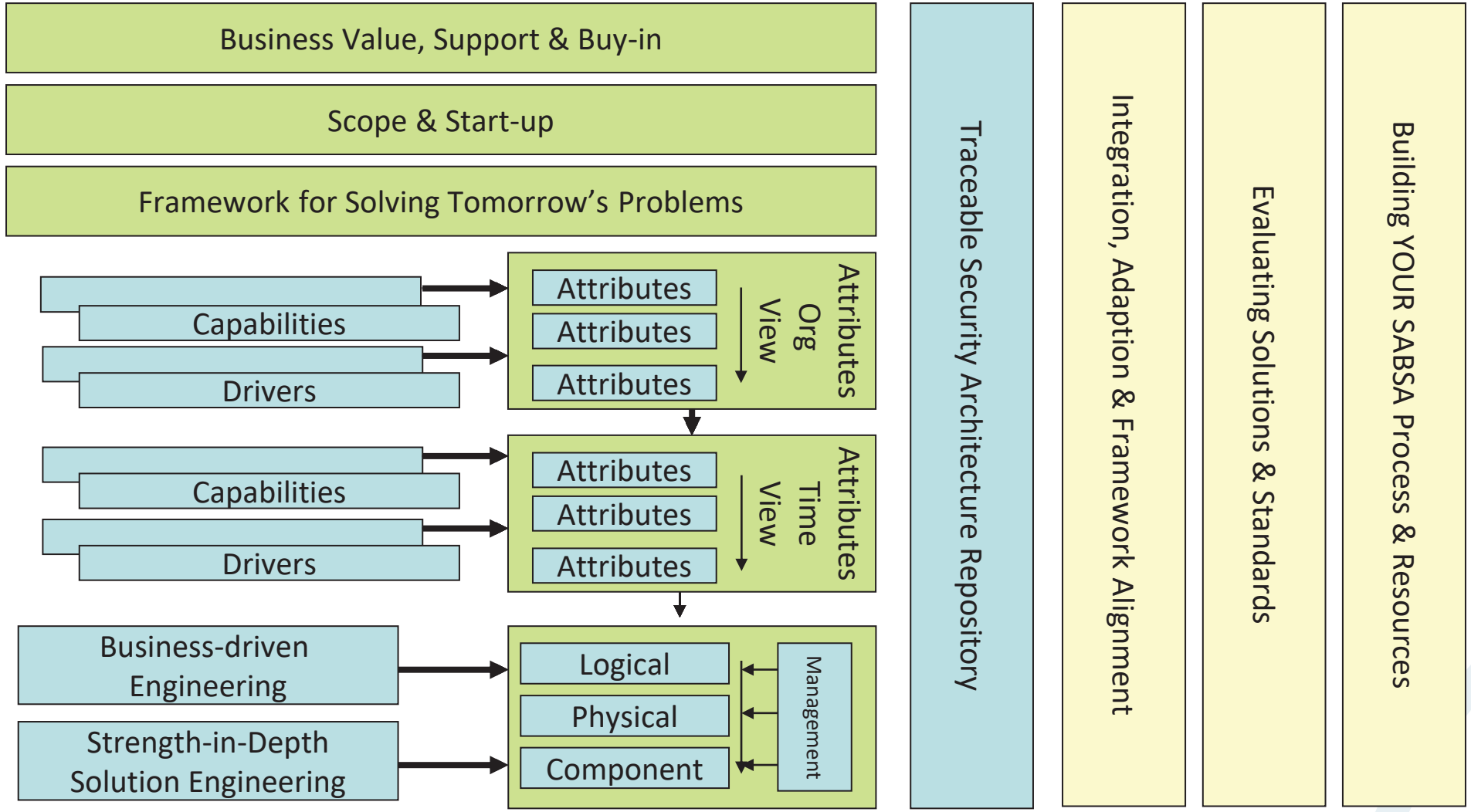
SABSA Updates

- Initiatives & Working Groups
- Alignments & Integrations
- Resources
- Events

Module A3– Course Outline

- Section 1 – Competency Development Objectives & Foundation Level Review
- Section 2 – SABSA as a Problem-solving Framework for Today's Burning Issues
- Section 3 – Stakeholder Value Propositions & Framework Alignment
- Section 4 – Advanced Attributes Profiling (1) – Multi-tier Organisations
- Section 5 – Advanced Attributes Profiling (2) – Programmes & Projects
- Section 6 – Traceability Concept: Architecture Layer-Map / Repository
- Section 7 – Logical Layer Engineering – Business-driven Requirements & Design
- Section 8 – Physical Layer Engineering – Business-driven Solution Design
- Section 9 – Engineering the Multi-Tier Control Strategy
- Section 10 – Adapting the SABSA Process – Fit-for-Purpose Process Design
- Section 11 – Full Requirements-to-Solutions Traceability
- Section 12 – SABSA for Evaluating Standards & Solutions

Module A3 Scope



Competency Development Objectives & Foundation Level Review

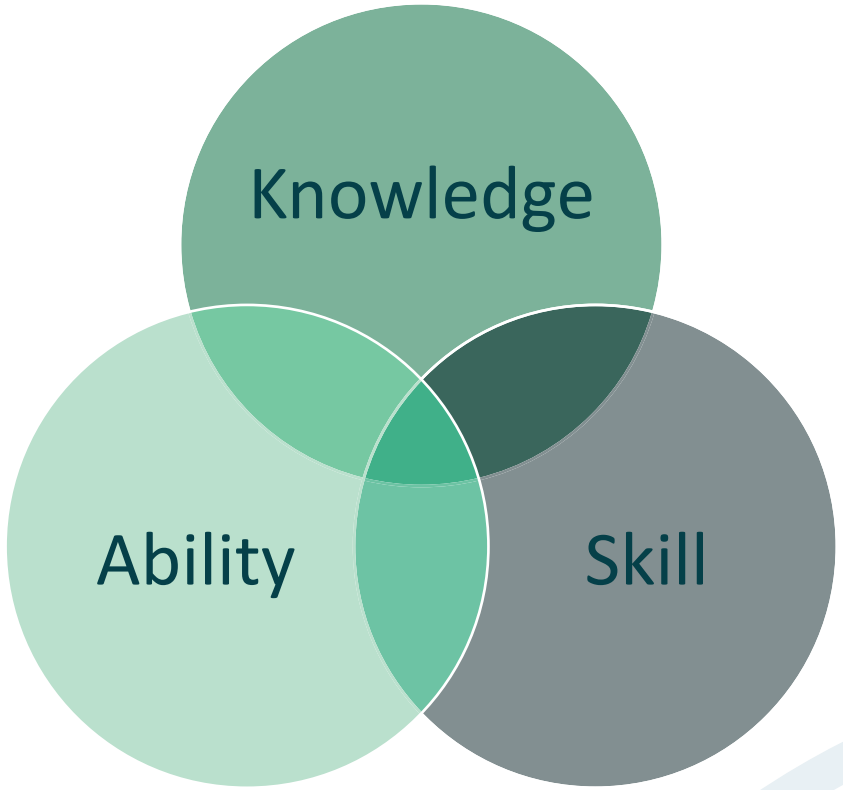
Section 1

Competency Based Certification

- TSI is a professional Institute, not a commercial vendor
- True professionals, particularly safety-critical professionals such as Doctors and Pilots, must demonstrate competence in order to obtain a license issued by their respective Institutes
- Institute status:
  - “SABSA’s community can obtain true competency-based professional certifications that provide trust and confidence to peers and employers of an architect’s capabilities”
- TSI certifies Architects’ competence to ***“do”*** SABSA to a range of levels

What is SABSA Competence?

Knowledge	Awareness of, and familiarity with, facts and information about SABSA
Skill	Learned activities to conduct specific SABSA tasks involving ideas (cognitive skills), things (technical skills), and people (inter-personal skills)
Ability	The talent and power to conduct specific SABSA tasks



SABSA Architecture Competence

A broad collection of skills, abilities, and knowledge that enable an Architect to successfully perform the SABSA Architect's role

For Advanced Module A3, the objective is to develop the broad collection of skills, abilities, and knowledge that enable an Architect to successfully perform the SABSA Architect's role in the context of Architecture Design & Development

Levels of SABSA Competence

- Based on ***Blooms Taxonomy of Cognitive Levels*** which defines six levels of competence

1	Know	Observe, research and recall SABSA subject matter
2	Understand	Understand, explain and interpret SABSA subject matter
3	Apply	Use and apply SABSA subject matter in context
4	Analyse	Break down SABSA subject matter into organised parts and explore the relationships between the parts
5	Evaluate	Critically examine and judge the value of SABSA subject matter in context
6	Create	Adapt and customise SABSA subject matter to create original Architecture in a new context

Competency Development

Foundation

- Data entry to predefined tables
- Follow set procedures
- Mandatory process rules
- Populate the reference artefacts
- Ask “What information should be entered into this field?”

Advanced

- Use the process, modelling techniques, and graphical communications style that works best for you
- Organise your work-product in the way that best suits the culture and approach used by your own team or organisation
- Use SABSA concepts & models in the way that makes them implementable, operational, meaningful & valuable to you in your business context

SCP certification requires an Architect to apply SABSA in-context

Advanced Module Course Approach

- Presentation of concepts
- Individual and group research
- Q&A and Open Forum discussions
- Coaching & mentoring
- Sounding board
- Validation & constructive criticism
- Workshops to apply techniques & develop work-product
- Peer groups & individual analysis
- Group presentations
- Collaboration & resource sharing
- In some cases, requires evening catch-up

Advanced Module Examination Format

- At the end of this course module you will receive a document containing 5 questions
- Choose any 2 questions
- Question paper does not expire
- Expectations are high – refer to and focus on competency verbs
- Competencies are defined in the exam paper
  - If you are asked to use SABSA to “solve” do not merely “discuss” how the problem could, in theory, be solved
  - If you are asked to produce a “model” do not merely “copy” a pre-existing reference or sample artefact provided by SABSA but demonstrate the structure and workings of your model

Recommended Approach to The SCP Examination

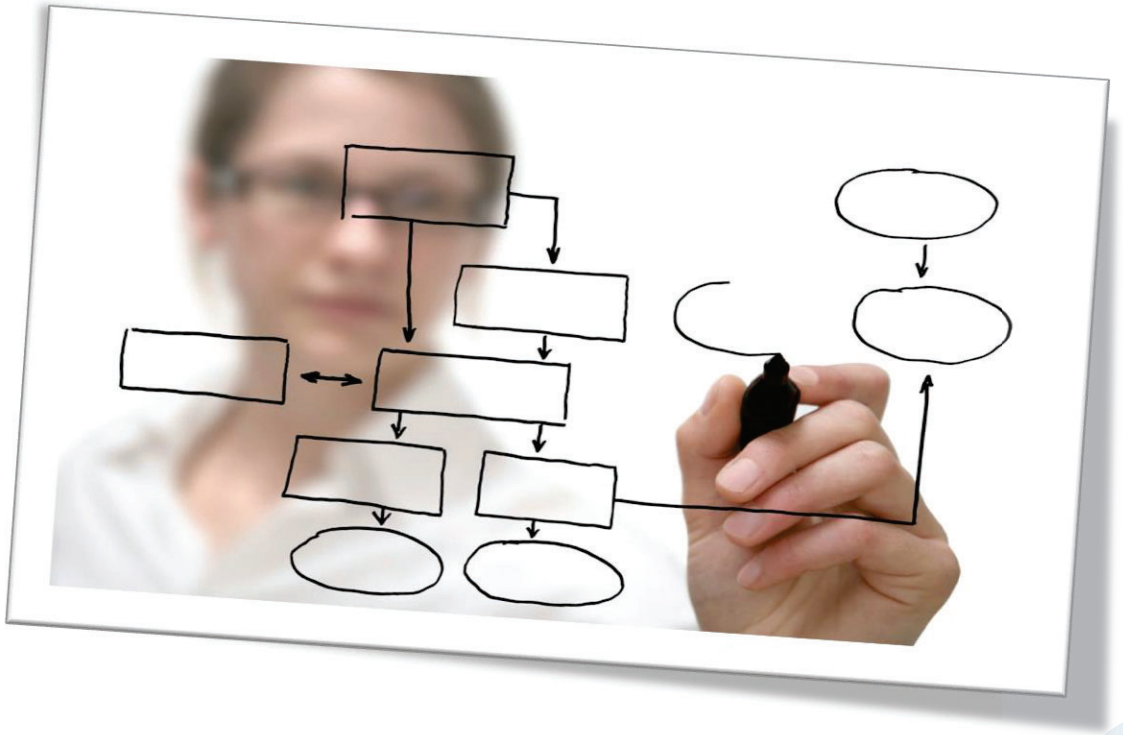
- SABSA certification exists to provide assurance and confidence about a practitioner's skill and competency to use the SABSA method
- You will not pass an Advanced Module examination by simply replicating materials from the course book
- It is challenging to build from scratch the work product required to demonstrate advanced competency without reference work
- We strongly recommend that you store the reference work product, ideas and techniques developed during course workshops and exercises as templates, guides and frameworks that may be re-used or populated when submitting your examination answers
- You may exchange and store other people's work products, but if you use them in an examination answer you must reference and credit the original source in the usual way

Advanced Module Examination Format, Marking & Re-sit

Format	Marking	Re-sit
Answer any TWO questions	Papers are dual-marked by SABSA Masters	In the event that a candidate fails to achieve the pass mark of 75%, the re-sit process is to resubmit their work having met the necessary improvements and enhancements noted in the Examiner Report
Each question is marked out of a maximum of 50 marks	Each examiner assesses the answers and compiles their examiner's report independently	
Each question requires multiple deliverables and will show the maximum marks available for each e.g. 2 parts worth 10 marks each and 2 parts worth 15 marks each	If the examiners recommended scores misalign by greater than a certain percentage (quite rare) they are required to hold a meeting to resolve their differences of opinion	
Accreditation as an SCP requires a candidate to score 75% overall	In the extremely rare event that the examiners still disagree, a third SABSA Master will arbitrate to a final recommended score	

Workshop A3-1

Foundation Level Competency Review

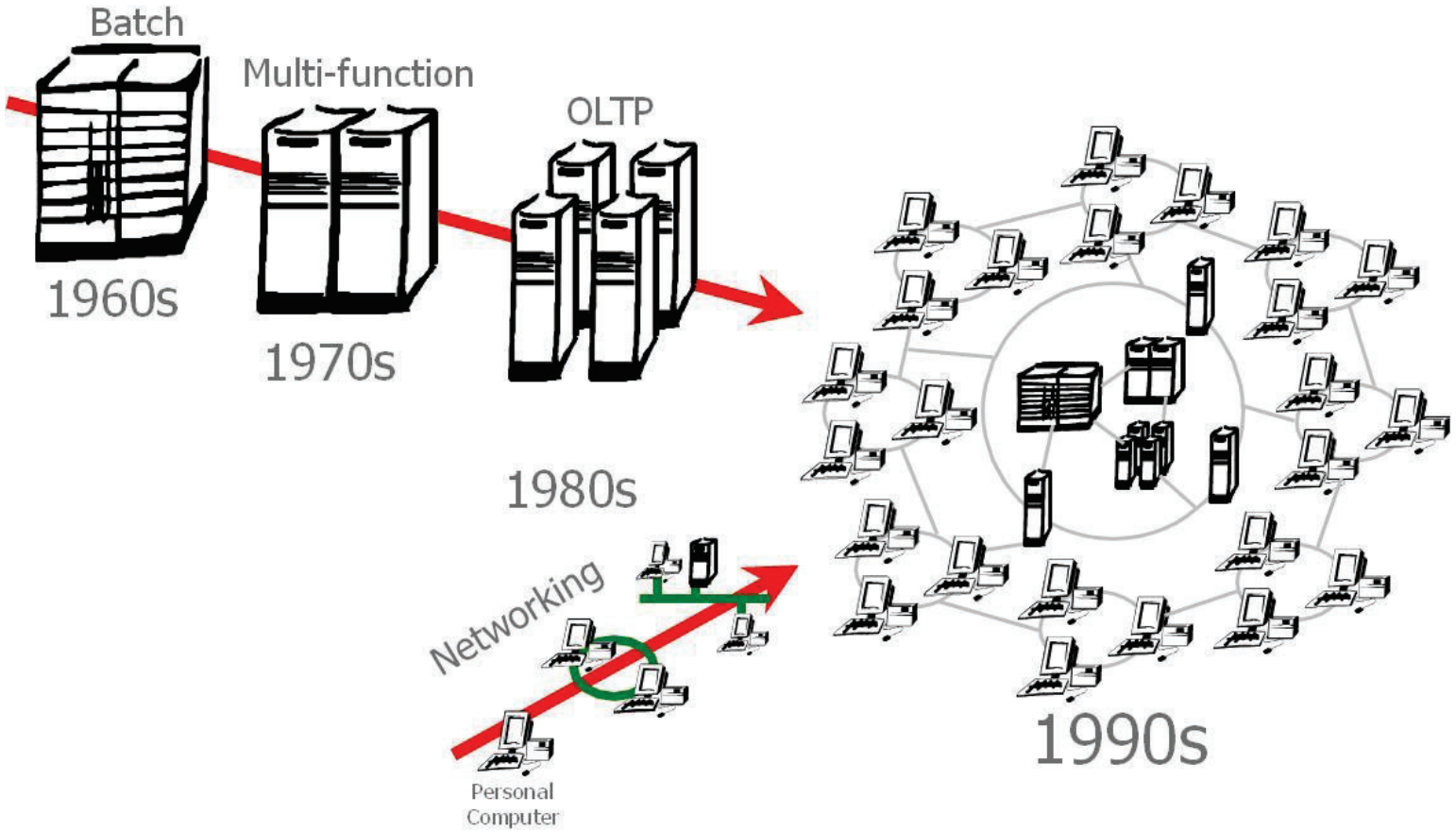


SABSA as a Problem Solving Framework

Section 2

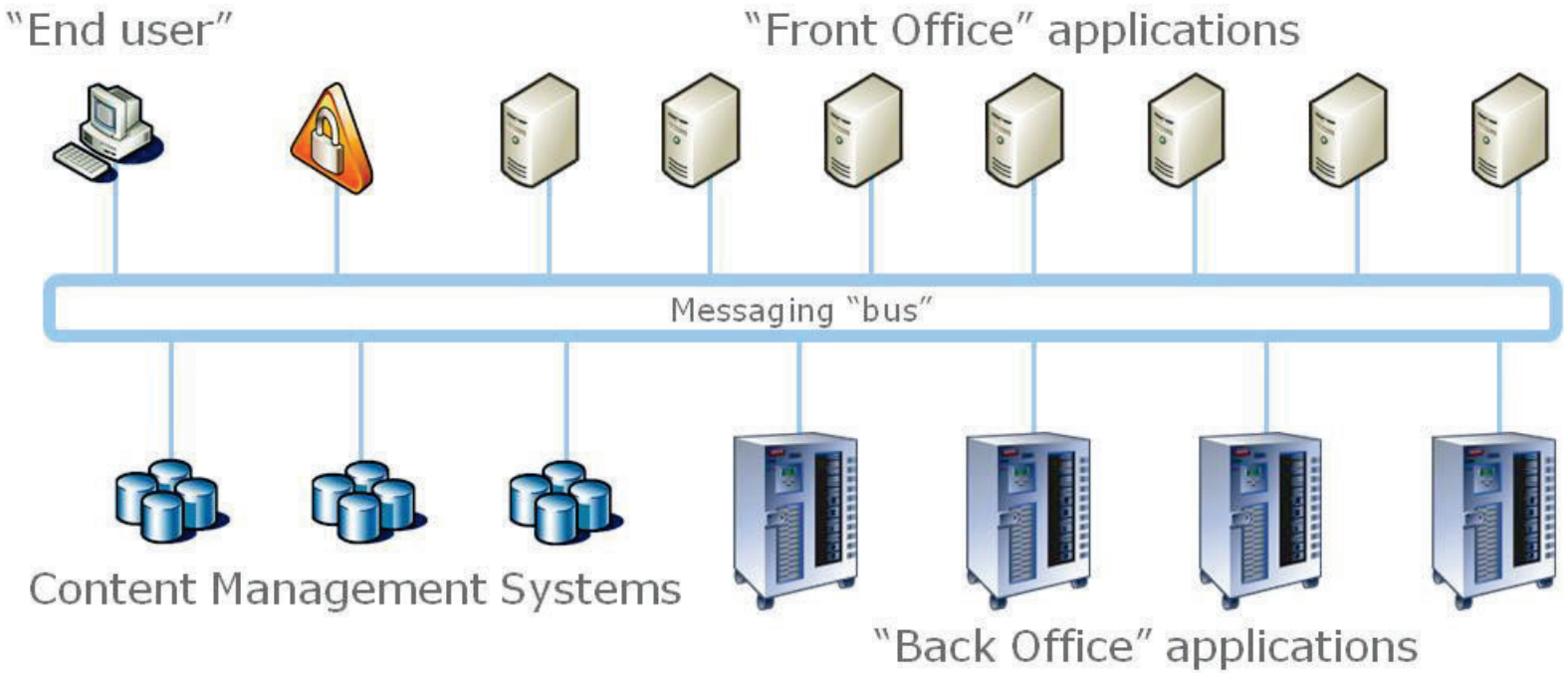
Architecture & Strategy: 20th Century

Power & complexity evolving together



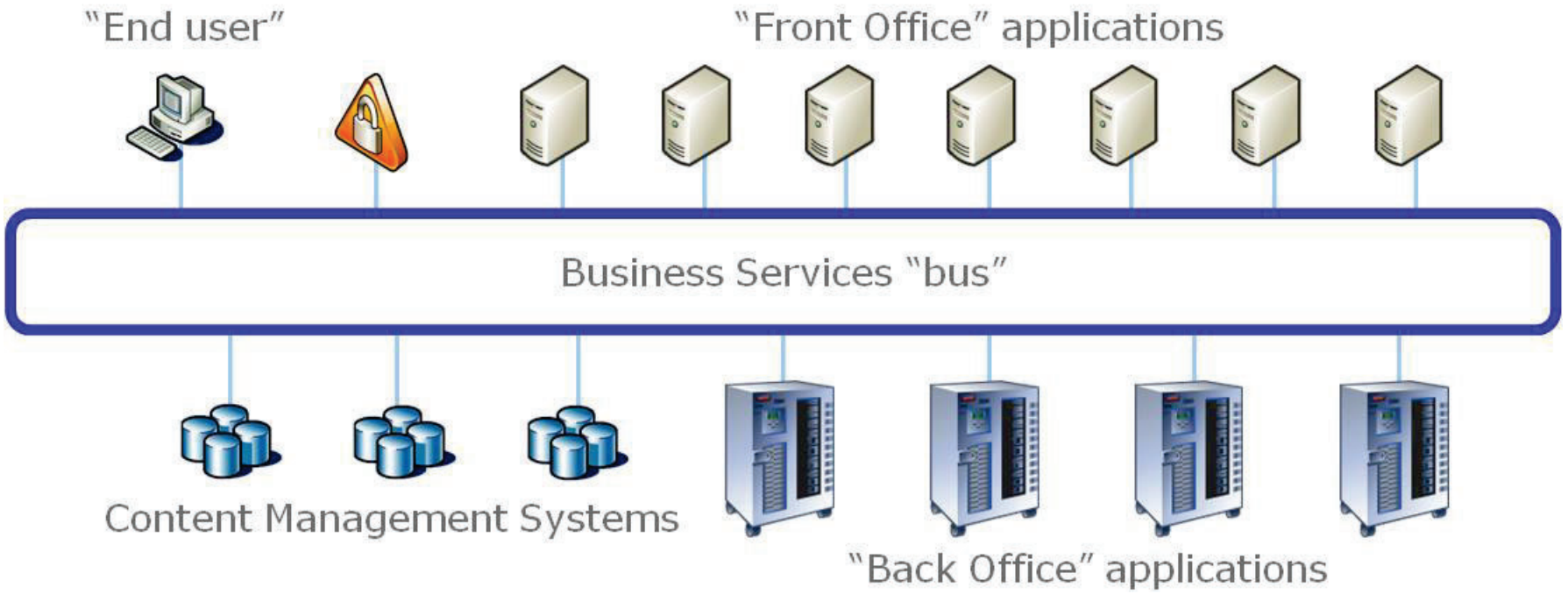
Architecture & Strategy: 21st Century

Looking simpler, but power and complexity still evolving



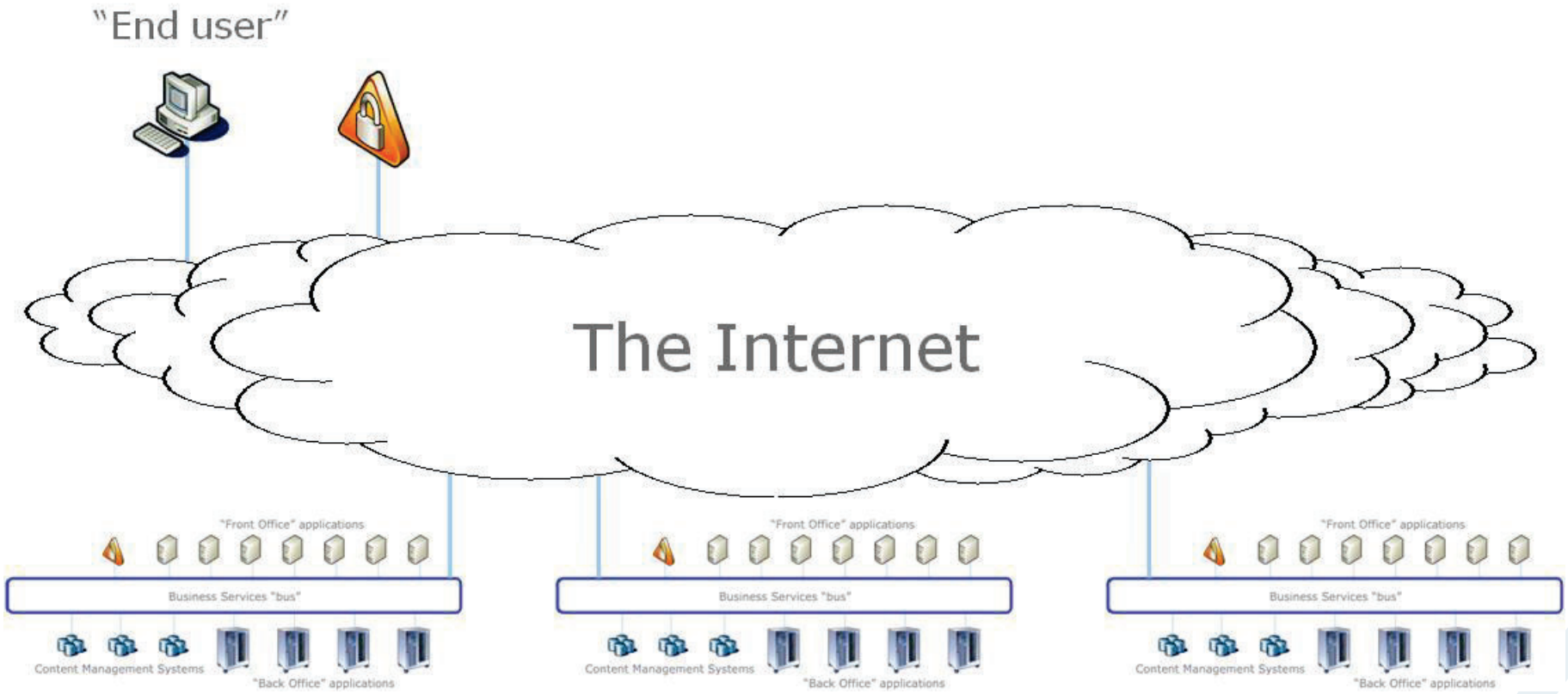
Architecture & Strategy: 21st Century

The emergence of SOA



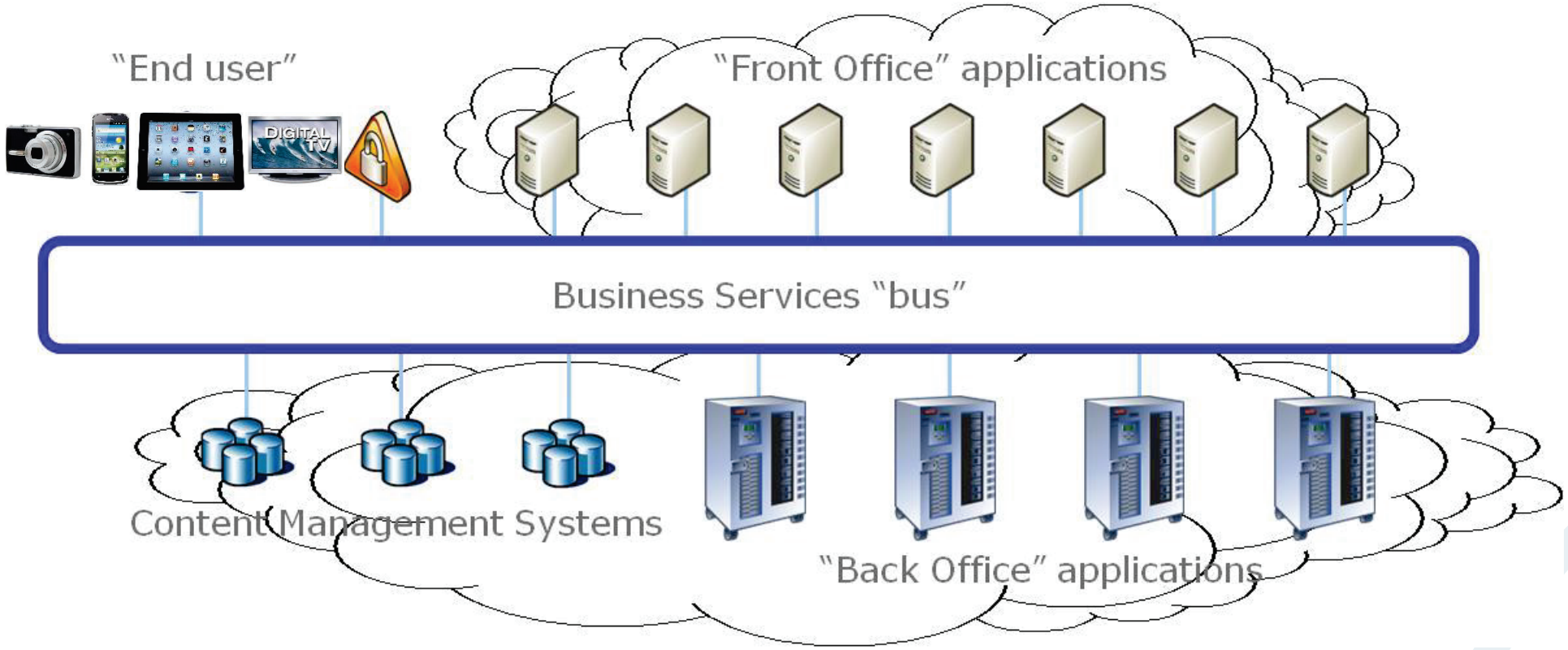
Architecture & Strategy: 21st Century

The emergence of federation



Architecture & Strategy: 21st Century

The Development of mobile interfaces & cloud computing



SABSA Architecture Guiding Principles

Dealing with change

- Architecture must not presuppose any particular:
  - Cultures or operating regimes
  - Management style
  - Set of management processes
  - Management standards
  - Technical standards
  - Technology platforms
- Because all of these things will change over time

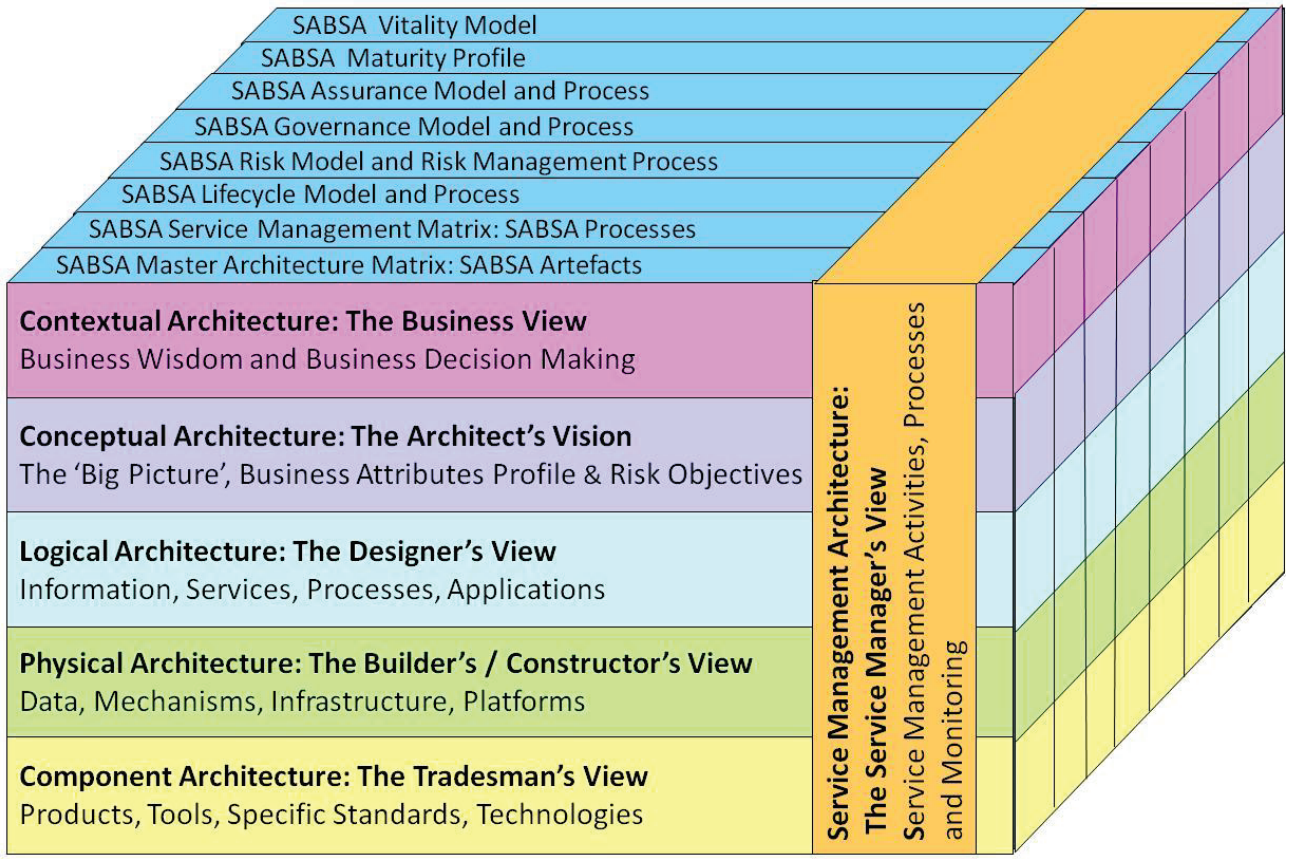
SABSA Architecture Guiding Principles

Future proof

- Architecture must meet YOUR unique set of business requirements
- Architecture must provide sufficient flexibility to incorporate choice and change of policy, standards, practices, legislation or technology
- When a question is asked starting with “Is this Architecture compatible / compliant with….?” a good Architecture framework with automatically have the answer “Yes”
- A good architecture provides the roadmap for joining together all of your requirements, whatever they might be, or become

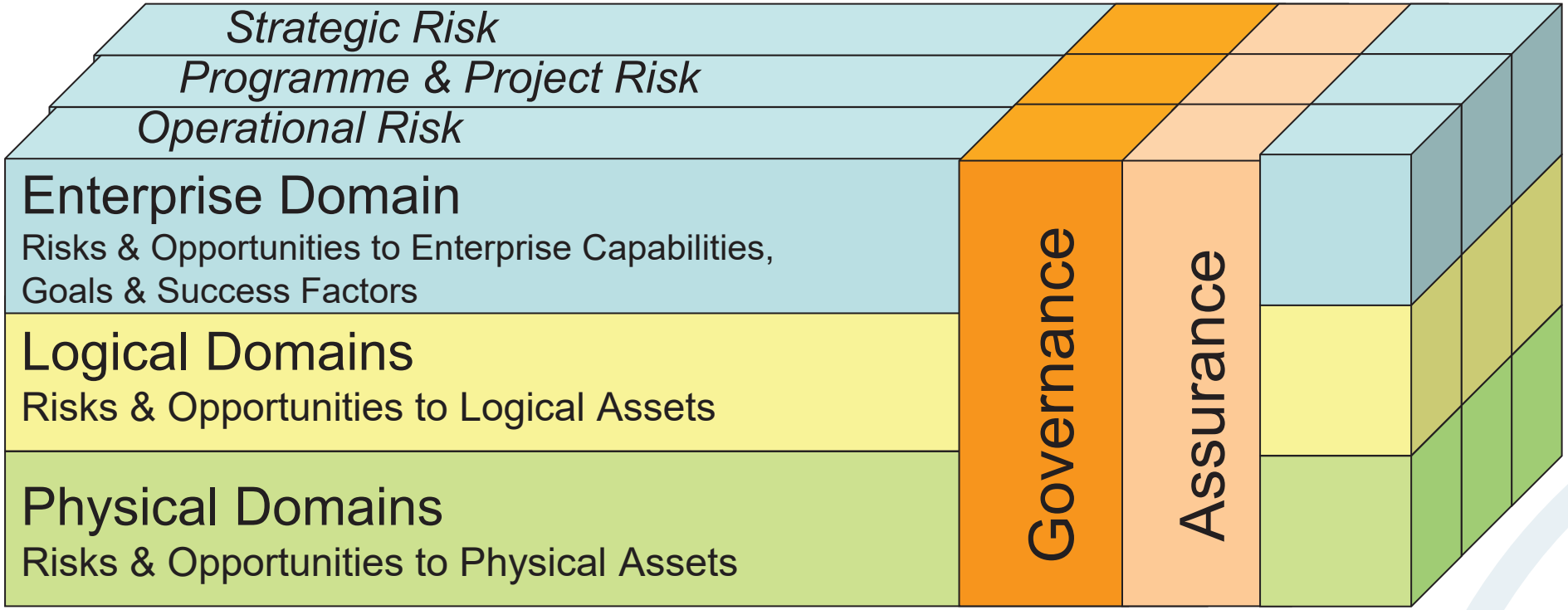
A Framework for Solving Any Problem

Structured thought process & layered abstraction



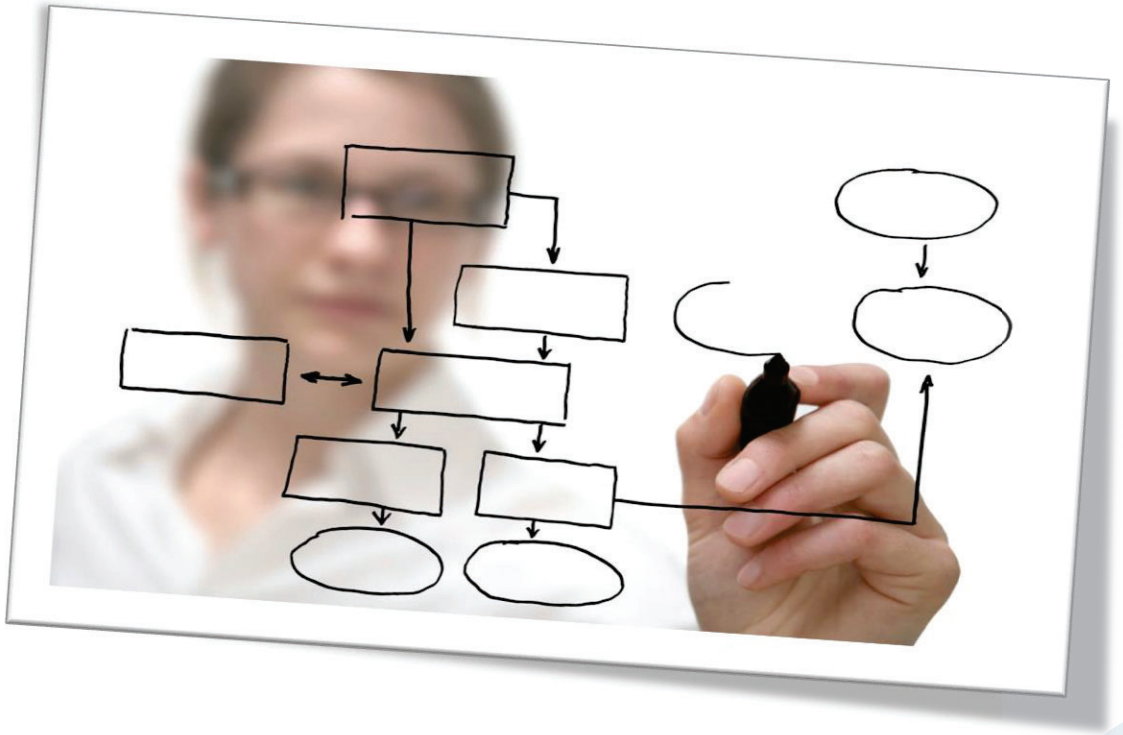
A Framework for Solving Any Problem

Through-life Risk, Governance & Assurance



Workshop A3-2

Problem-solving Framework for Today's Hot Topics & Burning Issues



Stakeholder Value Propositions & Framework Alignment

Section 3

Evaluating Enterprise Security Architecture

Open forum discussion

- How would you evaluate an Enterprise Security Architecture? Imagine you are a newly appointed CIO who comes in from outside the enterprise. You realise that ESA is a complex concept, comprising a blend of three fundamental concepts: ‘enterprise’; ‘security’ and ‘architecture’.
  - What do you understand by each of the these component concepts?
  - What are the essential characteristics of the ESA that you expect to see?
  - What evaluation criteria will you use to make your evaluation?
  - In making the evaluation, which criteria would carry the highest weight?

Evaluating Enterprise Security Architecture

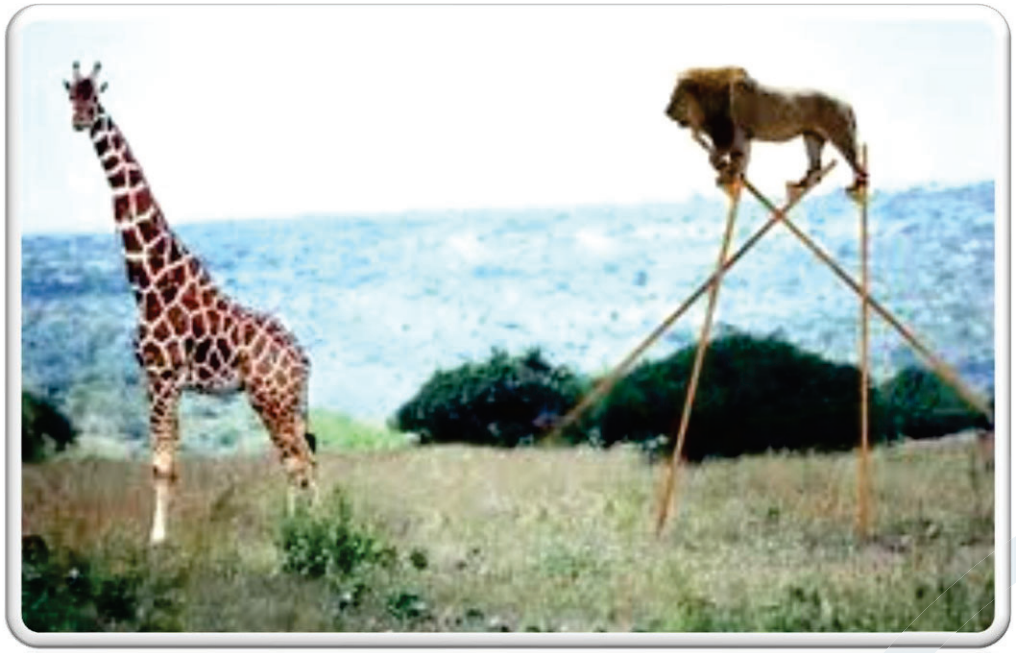
Open forum discussion

- Again in your new position as CIO you are required to make a presentation to the Board on your recent decision to adopt SABSA as the methodology and framework for use in future ESA developments.
- You must limit your presentation to three key messages, because you judge that Board members will be overwhelmed by more detail.
- What should be your three key messages?

The Architect's Real-world Dilemmas

In theory, theory & practice are the same: In practice they aren't

- Buy-in & Support
- Strategy versus Operations
- Greenfield site versus alignment & integration with existing investments



What are Principles

Principle a fundamental law, doctrine or assumption ***Merriam Webster***

Principle a fundamental truth, or proposition that serves as the foundation for a system of belief or behaviour or for a chain of reasoning ***OED***

SABSA Principles

The SABSA Architect's fundamental propositions to benefit business and inform solutions

Challenges of Principles

- Principles can be perceived as academic
- Seemingly not relevant to those at the operational ‘coalface’ who deal with the ‘now’
- Can be misunderstood by those with no direct visibility of business requirements
- Can be seen as impractical in the urgent need to deliver detailed tactical solutions
- New principles are subject to cultural resistance as adoption may render current or legacy policies, processes and systems to be instantly non-compliant

Benefits of Having Architectural Principles

Benefit	Rationale
Consensus	Drive organisational consensus on what we are to achieve
Socialisation	Breakdown barriers, establish alignment and communicate common purpose
Stability	Enduring values protect from unfocused ‘hot topic’ fluctuations
Informative	Decisions motivated by clarity not social dynamics or individual whims
Governed	Evaluating alignment to principles is more meaningful than anarchy
Advocacy	Clarity of direction enhances stakeholder buy-in
Decisiveness	Defined direction improves decision making
Traceability	Provides targets for evaluation and informs measurement

Rationale for SABSA Principles

Legacy of security as a constraint

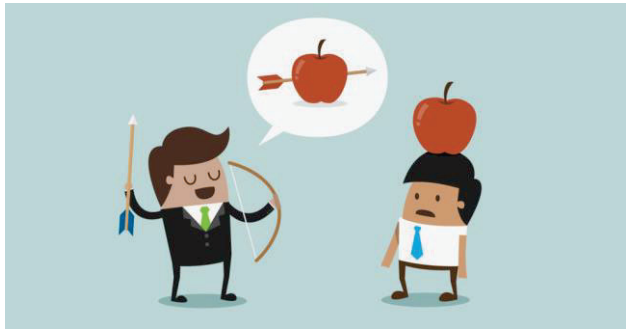
- ‘Badge, gun & guard-dog’ attitude
- Inflexible rules and restrictions
- Barriers to access and shareability
- Arrive ‘late to the party’ and spoil all the ‘fun

Security exists to serve the enterprise mission: It should be an enabler not a constraint

Rationale for SABSA Principles

Being “secure” doesn’t mean being “trusted”

- Something can be:
  - Brilliantly designed
  - Well constructed
  - Rigorously security tested
  - Demonstrably resilient
  - Cheaper than the competition
  - Proven to have unbeatable performance
- And still not be trusted



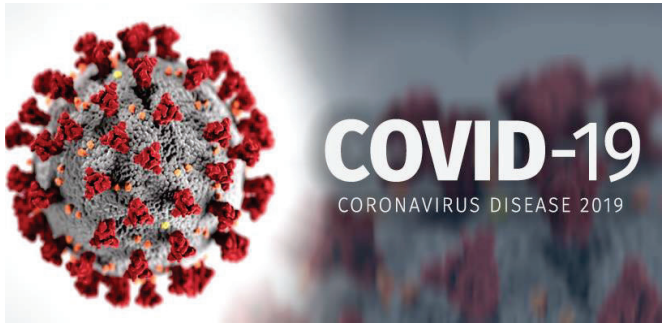
Transparency & assurance of transparency inspire trust

The singlemost important ingredient in the recipe for success is transparency because transparency creates Trust”***Denise Morrison – CEO, Campbells Soup***

Rationale for SABSA Principles

Disruption is inevitable

- Increasing complexity of inter-connectedness
  - Ability to understand critical dependency
- Increasing complexity of threat
- Complexity brings uncertainty
  - Unintended, unexpected consequences
  - Known & unknown unknowns



Resilience to withstand disruption is a critical success factor

Rationale for SABSA Principles

An obsession with negatives by people who like to say “no”

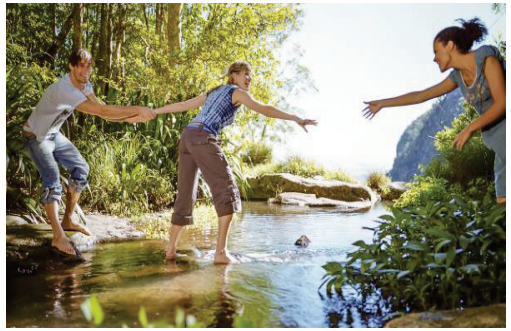
- A tradition of fear, uncertainty & doubt
- Selling negatives to stakeholders who desire enablement, excellence and value
- An enterprise must take risk in order to succeed
- Security should not determine enterprise risk appetite, it should be the centre of expertise to manage security within a defined risk appetite

Risk is a balance between enablement and control

Rationale for SABSA Principles

Risk ownership confusion

- Confusion when technical risk ownership is allocated to a business entity
- Avoidance of accountability
- Conflict between accountability and ownership



Practitioner's note – Ownership without accountability fosters tyrannical leadership, while accountability without ownership breeds fear and disengagement.
ITSMTransition.com

Clarity improves accountability, responsibility and action

Rationale for SABSA Principles

Control decisions lack direction and justification

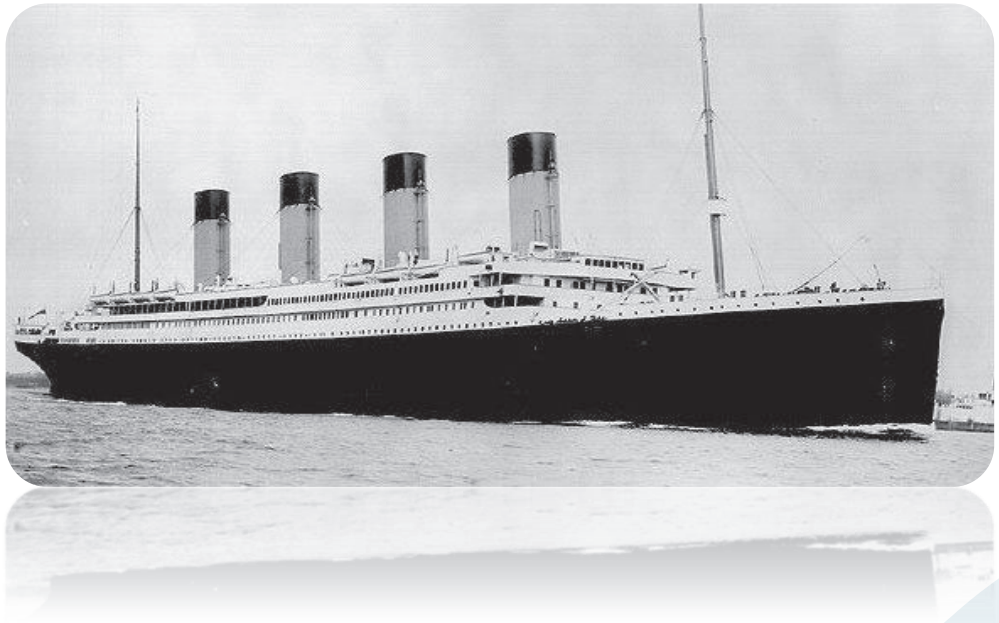
- Controls are deployed not because the business demonstrably benefits from them but because:
  - Everyone does it
  - Vendor called it “best practice”
  - The standard says so
  - The project is fun

Traceability improves decision-making and optimises resources

Rationale for SABSA Principles

Rigid culture & technical legacy

- Need to change and adapt is not foreseen
- Need to change and adapt is not supported by an ability to change and adapt
  - Cultural resistance
  - Inhibited by pre-existing static solutions
- There will always be another “new normal”



The enterprise needs the capability to change and adapt, quickly

Rationale for SABSA Principles

A gulf in language and understanding

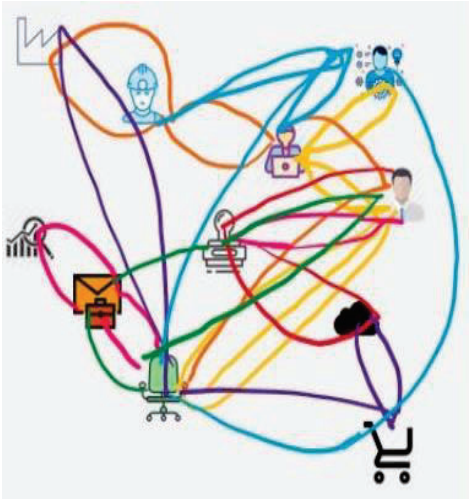
- Specialist (and conflicted) nomenclature
- Silo-ed thinking
- Territorialism and protectionism
- “My way is the only way”
- Start from differences as a points of weakness rather than commonality as points of strength

A common language aids collaboration and adoption

Rationale for SABSA Principles

Marketing is deemed superior to science

- Marketeers leverage human “Complexity Bias”
  - Undue credence to complex concepts
  - Complexity looks impressive and smart
  - Spaghetti diagrams are satisfying
  - Incessant jargon where simpler synonyms exist
- Scientists use “Occam’s Razor”
  - Everything should be made as simple as possible, but not simpler
  - Exploit unrecognised simplicities
  - Simple propositions are easier to test (proven or falsified)
  - A complex question is best answered by breaking it down into simpler component questions

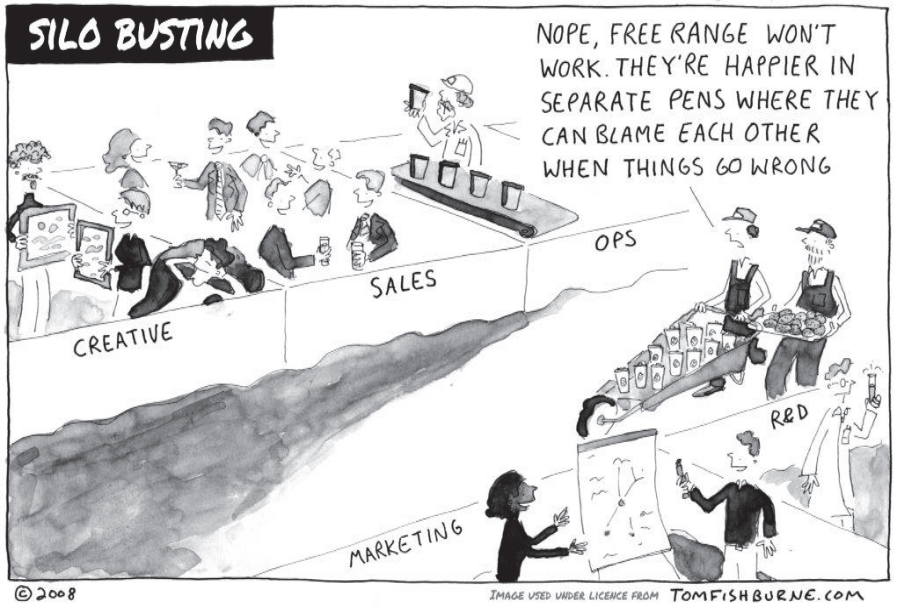


Scientific top-down engineering approaches resolve complexity

Rationale for SABSA Principles

Silo-ed tactical decisions

- Point solutions for tactical problems
  - Isolated, technology-led, IT-based, security projects
- Failure to cater for complex interactions
  - If there is a risk of taking an action, there is a risk of not taking an action
  - An action in one part of the enterprise has a positive or negative effect on many other parts

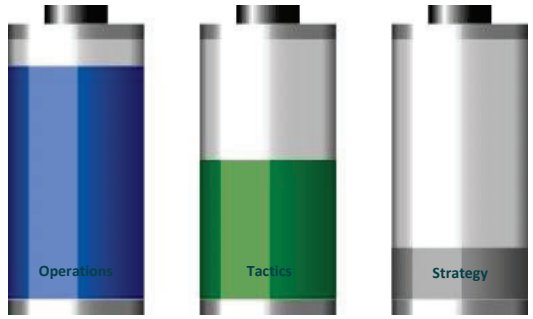


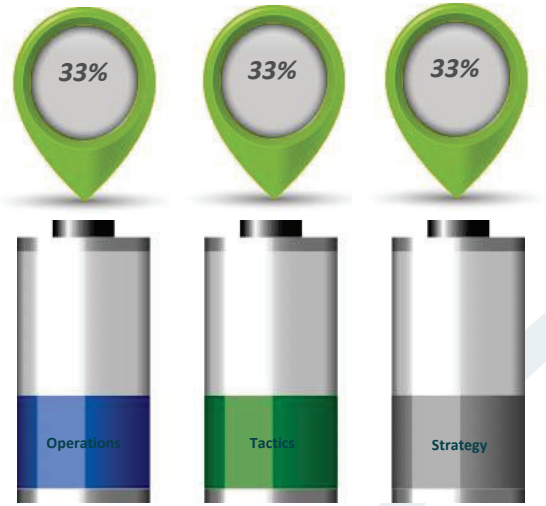
Complex systems require an holistic 'joined-up' approach

Rationale for SABSA Principles

Lifecycle imbalance

- Operational imbalance
  - Typical security function is ‘operations heavy’
  - Inability to adapt
- Lifecycle imbalance
  - Typical architecture function is ‘strategy heavy’
  - Inability to transition strategy into reality





Practices and solutions should cater for through-life requirements

Rationale for SABSA Principles

Point in time focus

- Assumed stability of requirements over time
  - Too slow
  - Unresponsive
  - Of no lasting value
- Tail wags the dog
- Solution is redundant on delivery

Solutions must be adaptable to stand the test of time

Rationale for SABSA Principles

No practical means to achieve the big picture

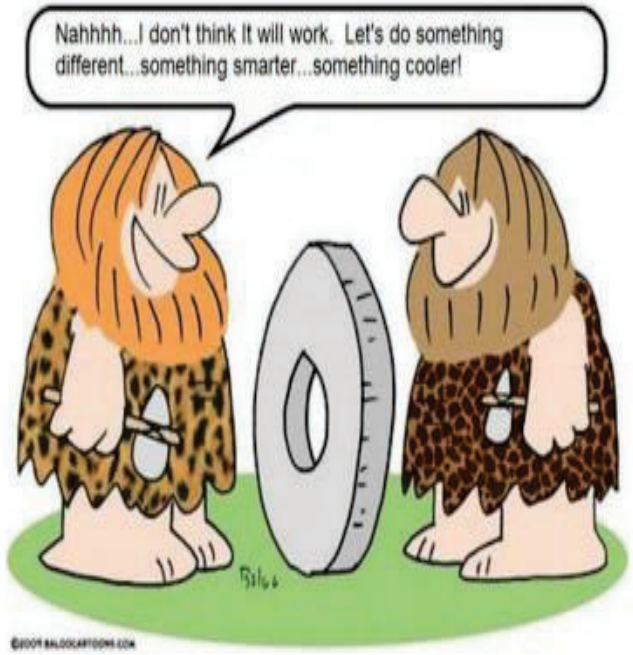
- The ‘big picture’
  - The goalposts are always moving
  - Hard to find the place to start
  - Cannot go live with strategy, it requires transformation & migration
- The ‘small picture’
  - Bottom-up engineering
  - Disjointed and disconnected
  - No real business alignment
  - No long-term strategy
  - No real standardisation
  - No framework within which to design solutions for new problems

Enterprise methods must be scalable

Rationale for SABSA Principles

Continuous re-invention of the wheel

- Lack of Architectural Commonality
  - The same ‘solution’ is defined multiple times, differently
  - Existing working solutions are not re-used
  - Lack of flexibility
  - Integration difficulties with diverse systems
- Inconsistent security approach
  - Security is not consulted
  - Security is consulted too late
  - Every project repeats the same question: “What are the security requirements?”



Consistency creates repeatability

SABSA Principles

Principle	Definition
Enable Business	Enable business to achieve goals and optimise value
Inspire Trust	Provide assurance that services, products, systems, processes, and culture will be trustworthy, and behave in ways that provide trust
Enact Resilience	Overcome inevitable disruption through resilience and continuity
Balance Risk	Balance enablement of benefit and control against loss
Create Certainty & Clarity	Create and sustain clarity of policy, governance, and risk ownership
Establish Traceability	Empower stakeholders at all levels to make justified and fit-for-purpose decisions
Capitalise Change & Agility	Support business ambition to transform, transition and change
Establish Common Culture & Language	Establish a common culture and language, enabling the enterprise to collaborate, integrate, adopt, consume & implement
Simplify Complexity	Leverage the proven benefits of a top-down engineering approach to resolve complexity into consumable simplicity
Solve Holistically	Achieve systemic understanding of how each part effects the whole
Deliver End-to-End & Through-life	Deliver capability end-to-end and through-life
Ensure Sustainability	Ensure vitality to stand the test of time
Realise Scalability	Apply methods, approaches and models at any scale from enterprise to detailed solution
Enable Consistency	Enable repeatability for design integrity and consistent application

SABSA Approach: Actionable Principles

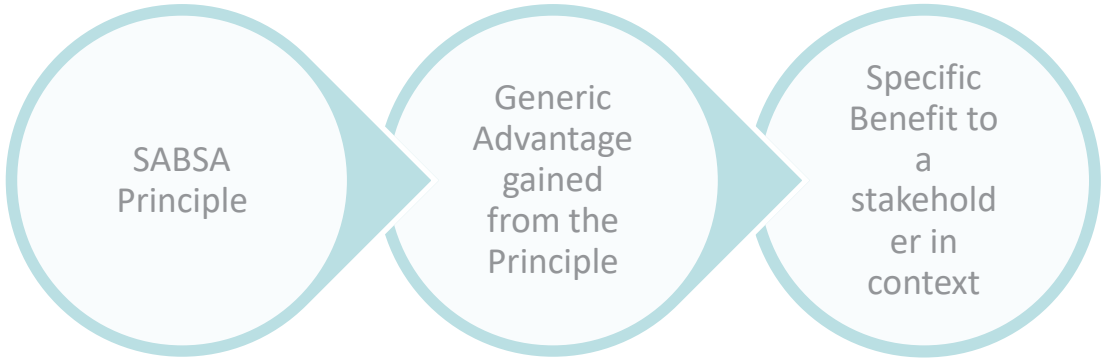
Perceived Challenge of Principles	SABSA Approach to Resolve the Challenge
Academic	Embed principles in SABSA frameworks, models and techniques to enable real-world application
Not relevant	Provide the technique to interpret principles into direct meaningful relevance for individuals
Misunderstood	Provide the technique to interpret principles into direct meaningful context for individuals
Impractical	Provide the technique to transpose principles into meaningful practical applications of frameworks and models
Resisted	Articulate the benefits that result from application of the principles

- The SABSA approach is to interpret generic SABSA principles as defined actionable improvements and successes for individuals in a model called the SABSA Principles, Advantages & Benefits model (SABSA PAB)

Using Principles to Define Benefit

SABSA Principles, Advantages & Benefits Model

- The SABSA PAB transposes principles into specific adoptable benefits in a stakeholder context



SABSA Principle:
The SABSA Architect's fundamental propositions to benefit business and serve solutions

SABSA Advantage:
The generic improvement or success gained from the principle

SABSA Benefit:
The specific improvement or success, to a particular stakeholder, in a particular context

SABSA PAB Model

Principle	Advantage
Enable Business	Value-assured
Inspire Trust	Assures stakeholder confidence
Enact Resilience	Continuity through disruption
Balance Risk	Prioritised & proportional response
Create Certainty & Clarity	Effective governance & risk ownership
Establish Traceability	Demonstrates transparency of decisions and actions
Capitalise Change & Agility	Enable transformation & adaptability
Establish Common Culture & Language	Enables collaboration, integration & adoption
Simplify Complexity	Consumed easily
Solve Holistically	Systemic understanding
Deliver End-to-End & Through-life	Better lifecycle management
Ensure Sustainability	Return-on-investment
Realise Scalability	Applicability at any scale, to any scope
Enable Consistency	Design integrity & repeatability

SABSA PAB Model

Generating benefits statements for stakeholder context

Advantage
Value-assured
Assures stakeholder confidence
Continuity through disruption
Prioritised & proportional response
Effective governance & risk ownership
Demonstrates transparency of decisions and actions
Enable transformation & adaptability
Enables collaboration, integration & adoption
Consumed easily
Systemic understanding
Better lifecycle management
Return-on-investment
Applicability at any scale, to any scope
Design integrity & repeatability

Ask the right questions to define the context

What does value mean to this stakeholder?

About what does this stakeholder need to have confidence & trust?

What kind of disruption could this stakeholder face and what would be the impact of that disruption?

What is the stakeholder's approach to risk appetite?

SABSA PAB Model – Interpreted Benefit Examples

Principle	Advantage	Benefit to	Benefit
Enable Business	Value-assured	CIO	Enables value from digital transformation
Inspire Trust	Assures stakeholder confidence	Head of Product Development	Provides assurance to our customers that our engineering processes are trustworthy and that our products can be trusted
Balance Risk	Prioritised & proportional response	CTO	Technology risk is understood in the overall context of business risks & opportunities
Create Certainty & Clarity	Effective governance & risk ownership	CRO	Ownership, accountability, and responsibility for security-related risk is clearly defined and assigned
Establish Common Culture & Language	Enables collaboration, integration & adoption	CTO	The SABSA Architecture supports the goals and objectives of our Agile team, and integrates and aligns with our Agile method
Solve Holistically	Systemic understanding	COO	The positive and negative effects of changes to be introduced by any plan of action are understood enterprise-wide

The Framework Alignment Issue

- Security does not exist in isolation – it is a property of something else
- 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 usually already defined, organised and architected in a number of different ways according to other architectural frameworks, approaches and standards
- It is 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

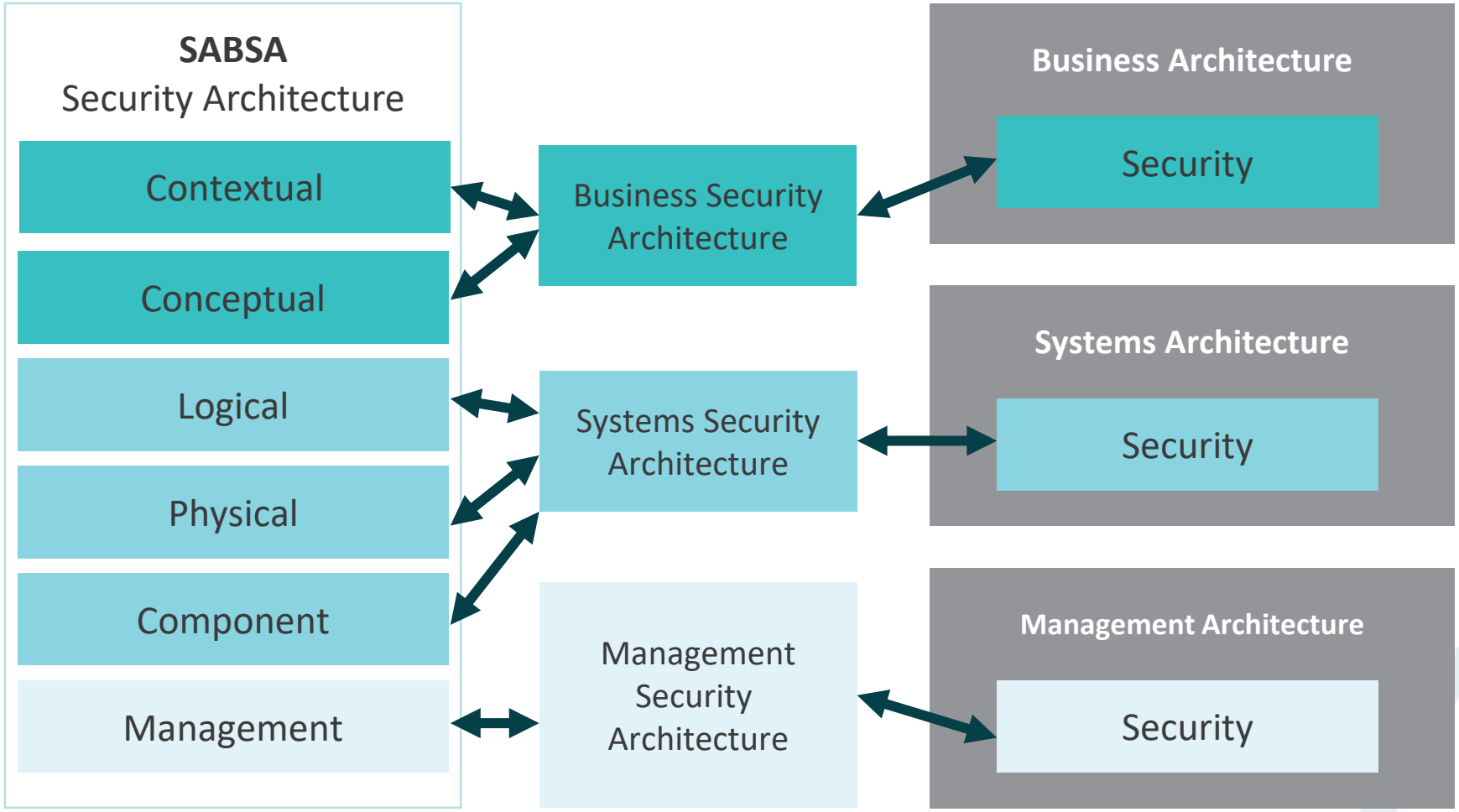
The Framework Alignment Issue

Built 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

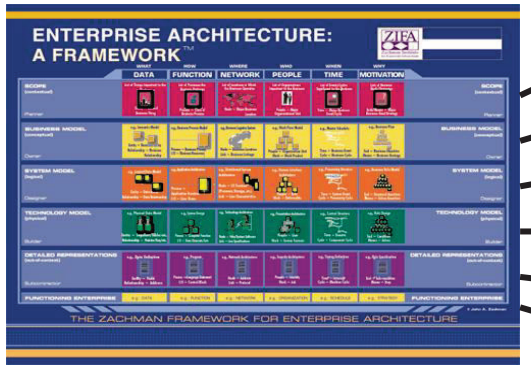
The Framework Alignment Issue

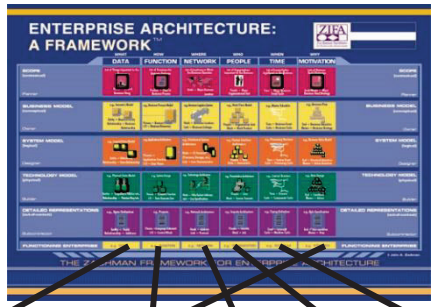
Align & enhance, don't replace



The Framework Alignment Issue

Zachman architecture alignment

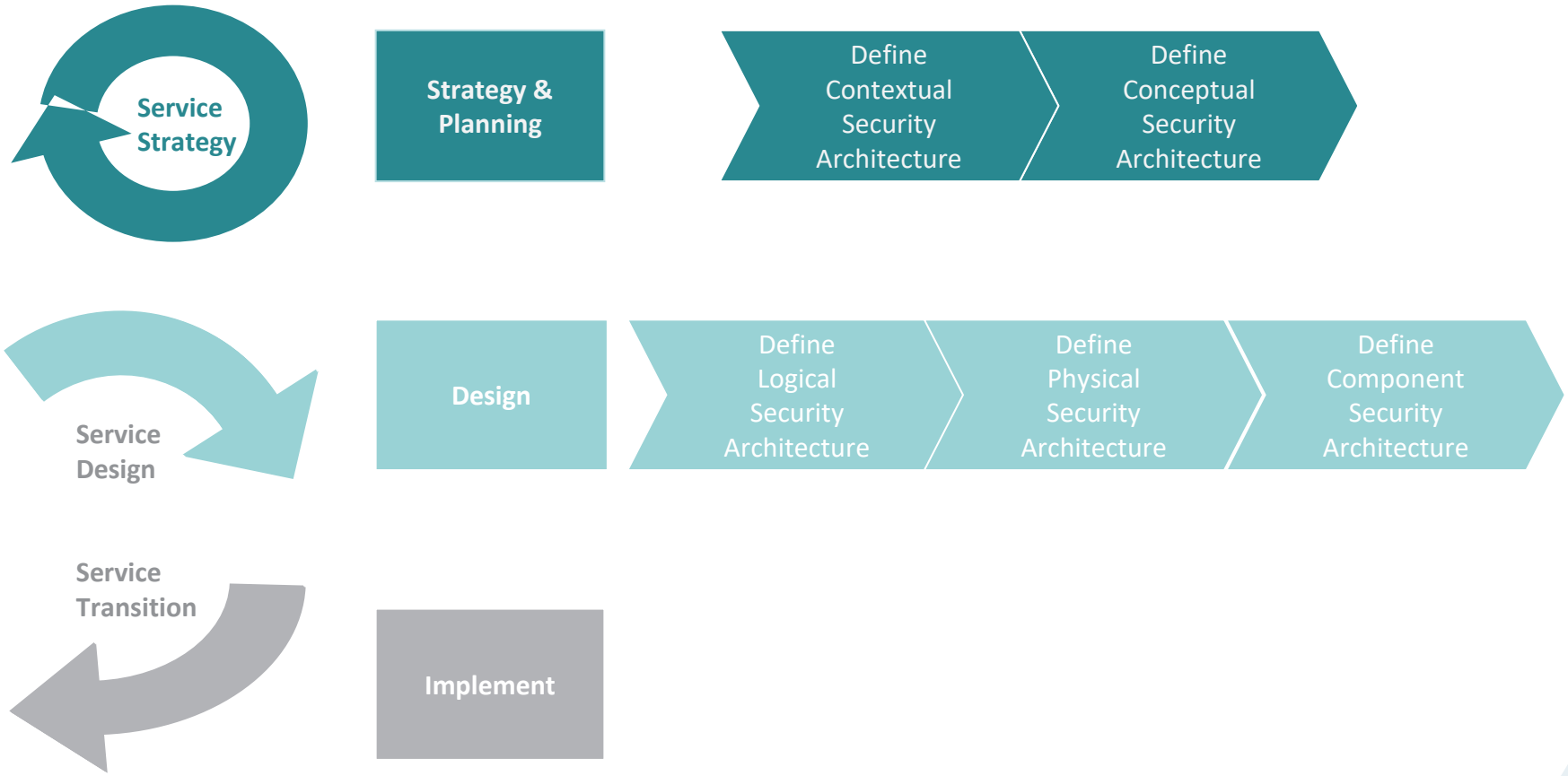




	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
Conceptual	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
Logical	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
Physical	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
Component	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
Operational	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management

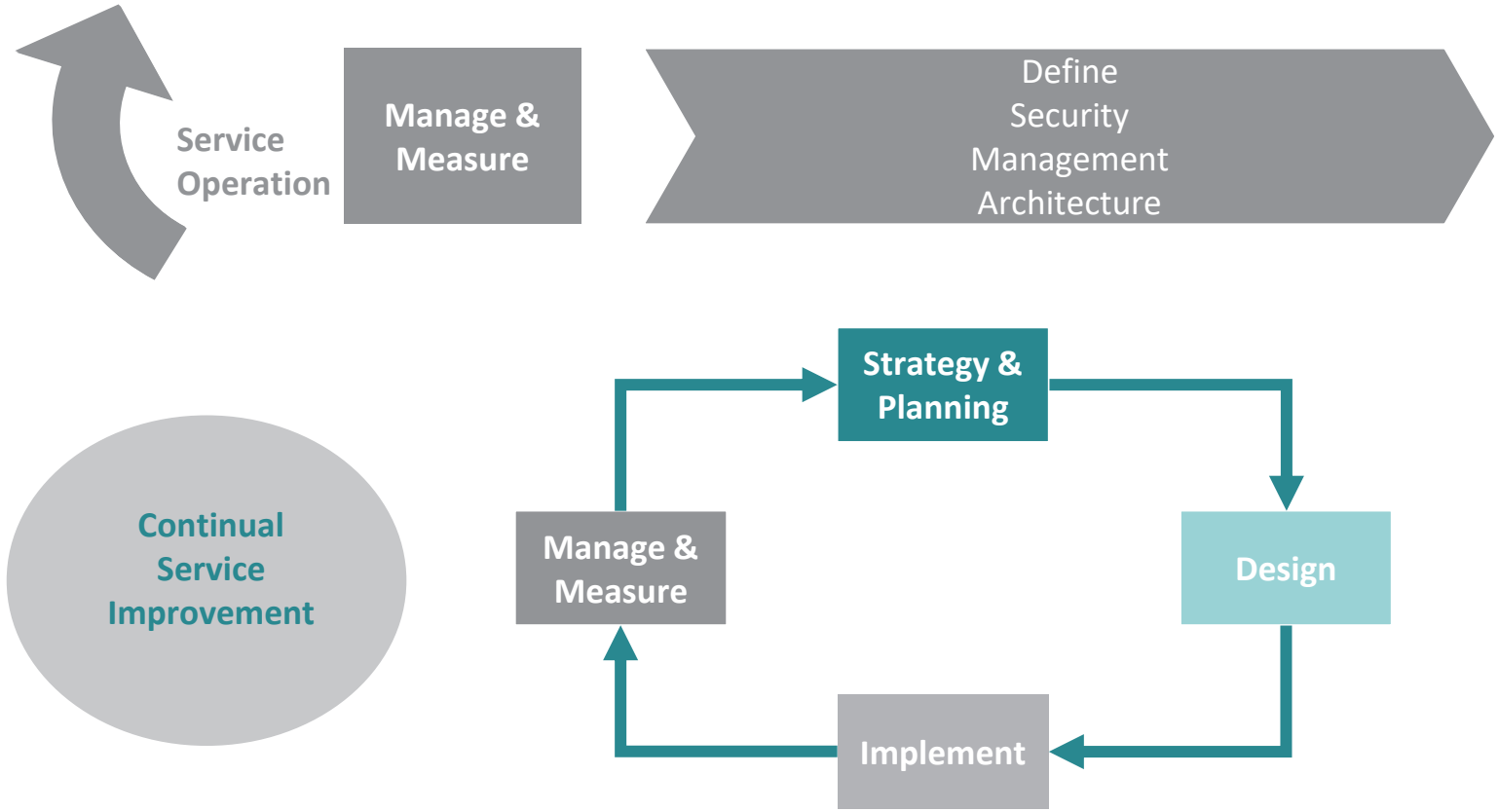
The Framework Alignment Issue

SABSA & the ITIL Service Lifecycle



The Framework Alignment Issue

SABSA & the ITIL Service Lifecycle



The Framework Alignment Issue

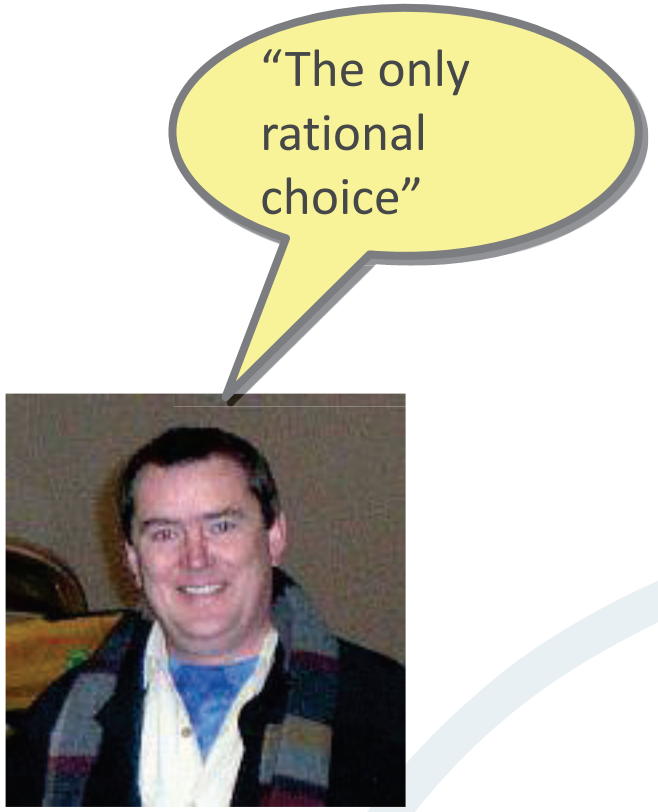
SABSA Management Matrix

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Management	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	The row above is a repeat of Layer 6 of the main SABSA Matrix. The five rows below are an exploded overlay of how this Layer 6 relates to each of these other Layers					
Contextual	Business Driver Development	Business Risk Assessment	Capability Management	Relationship Management	Point-of-supply Management	Performance Management
Conceptual	Proxy Asset Definitions	Developing Risk Objectives	Delivery Planning	Role Management	Business Portfolio Management	Service Level Definition
Logical	Logical Asset Management	Policy Management	Delivery Management	Enterprise-wide User Management	Service Catalogue Management	Evaluation Management
Physical	Physical Asset Management	Risk Data Management	Operations Management	User Support	Resources Management	Performance Data Collection
Component	Component Management	Risk Management Components	Component Deployment	Personnel Component Management	Component Environment Management	Monitoring Components

The Framework Alignment Issue

Why SABSA for TOGAF?

- There are no viable competitors
- Philosophical alignment with TOGAF is already explicit
- Business-driven (as opposed to deliverables-driven)
- TOGAF is a community seeking to enhance ADM around security architecture and around requirements management
- SABSA has achieved global acceptance by organic uptake in the marketplace
- De facto standard
- TOGAF and SABSA can see each other in the marketplace

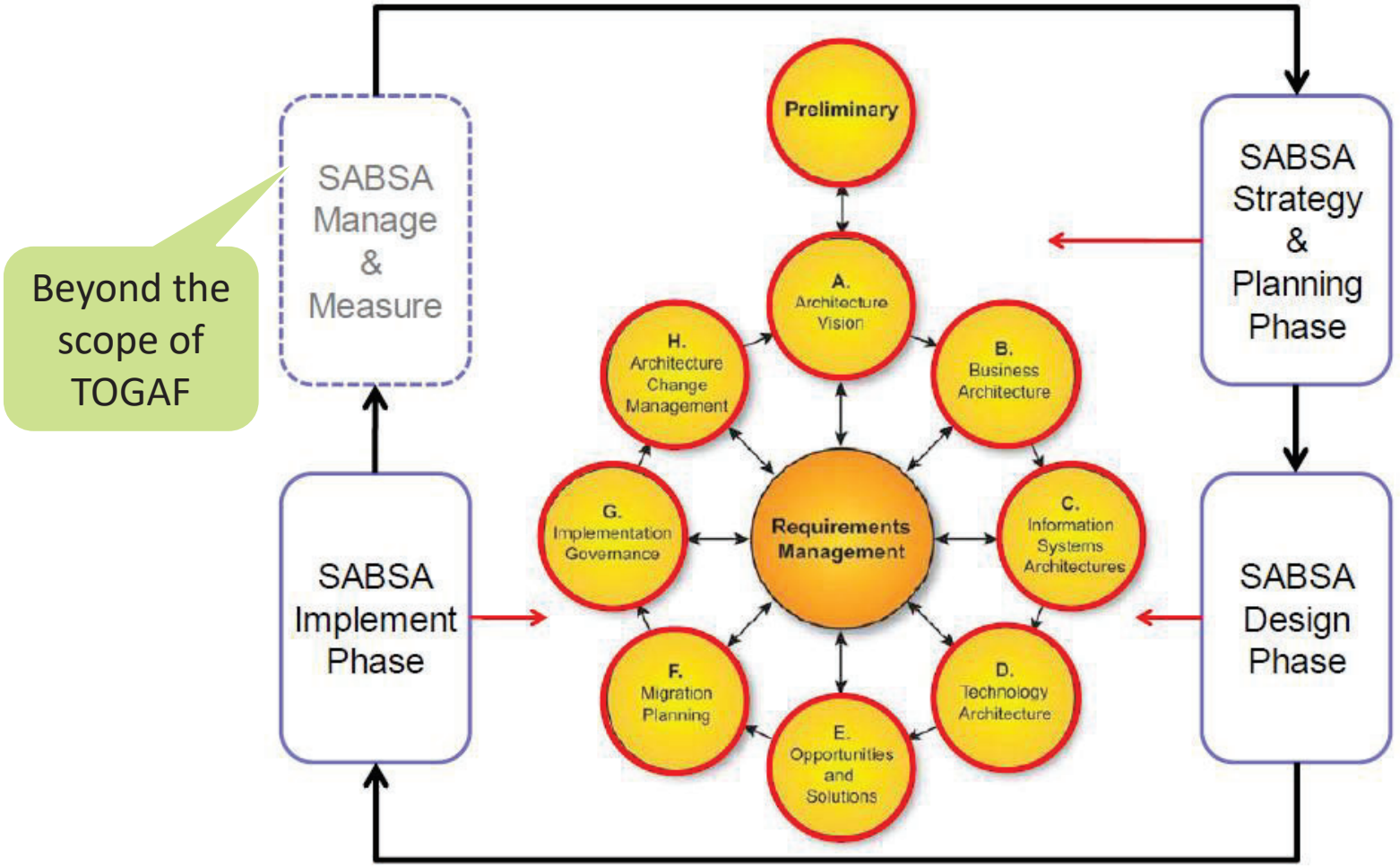


Dave Hornford

Chair of The Open Group ‘Architecture Forum’

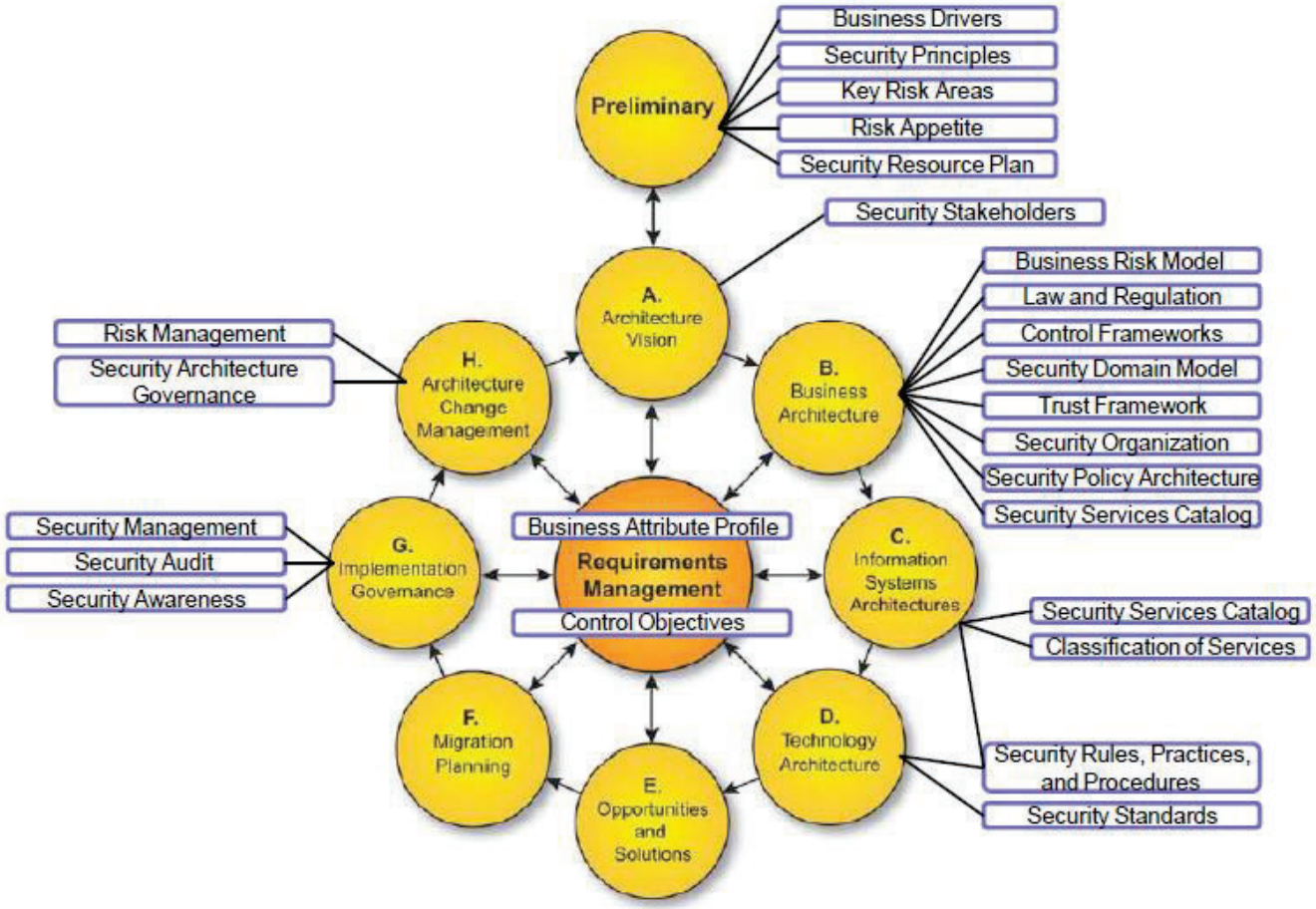
The Framework Alignment Issue

TOGAF SABSA Lifecycle Alignment



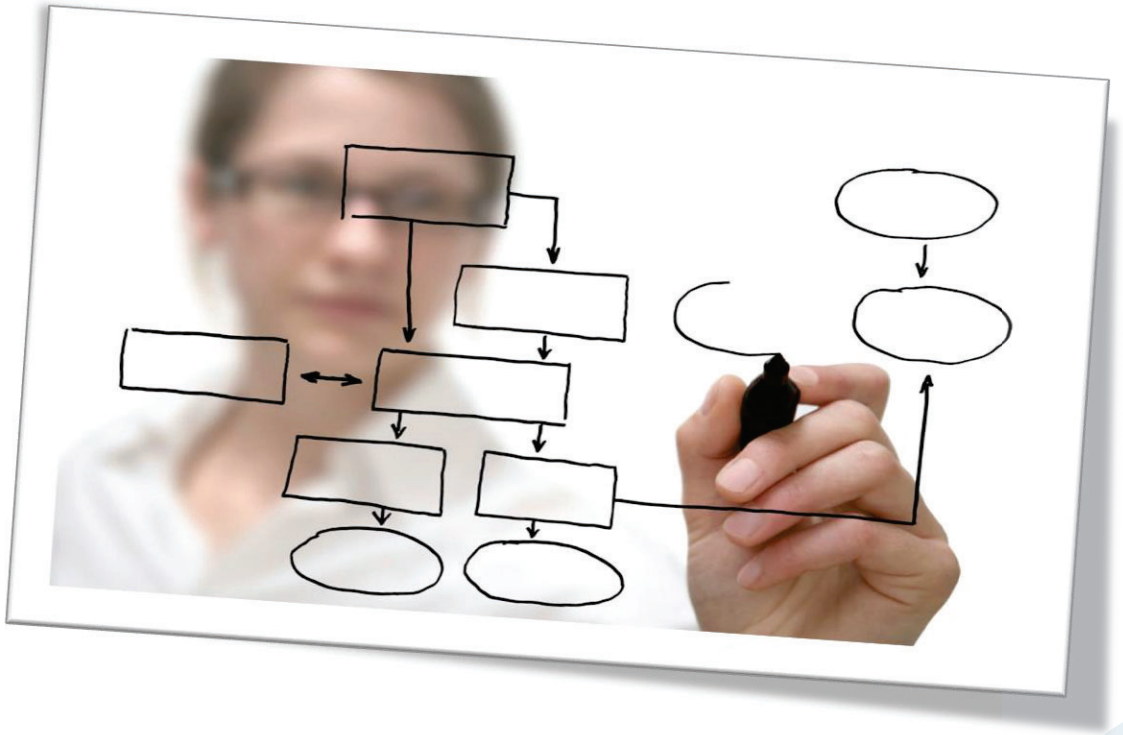
The Framework Alignment Issue

TOGAF SABSA Artefact Mapping



Workshop A3-3

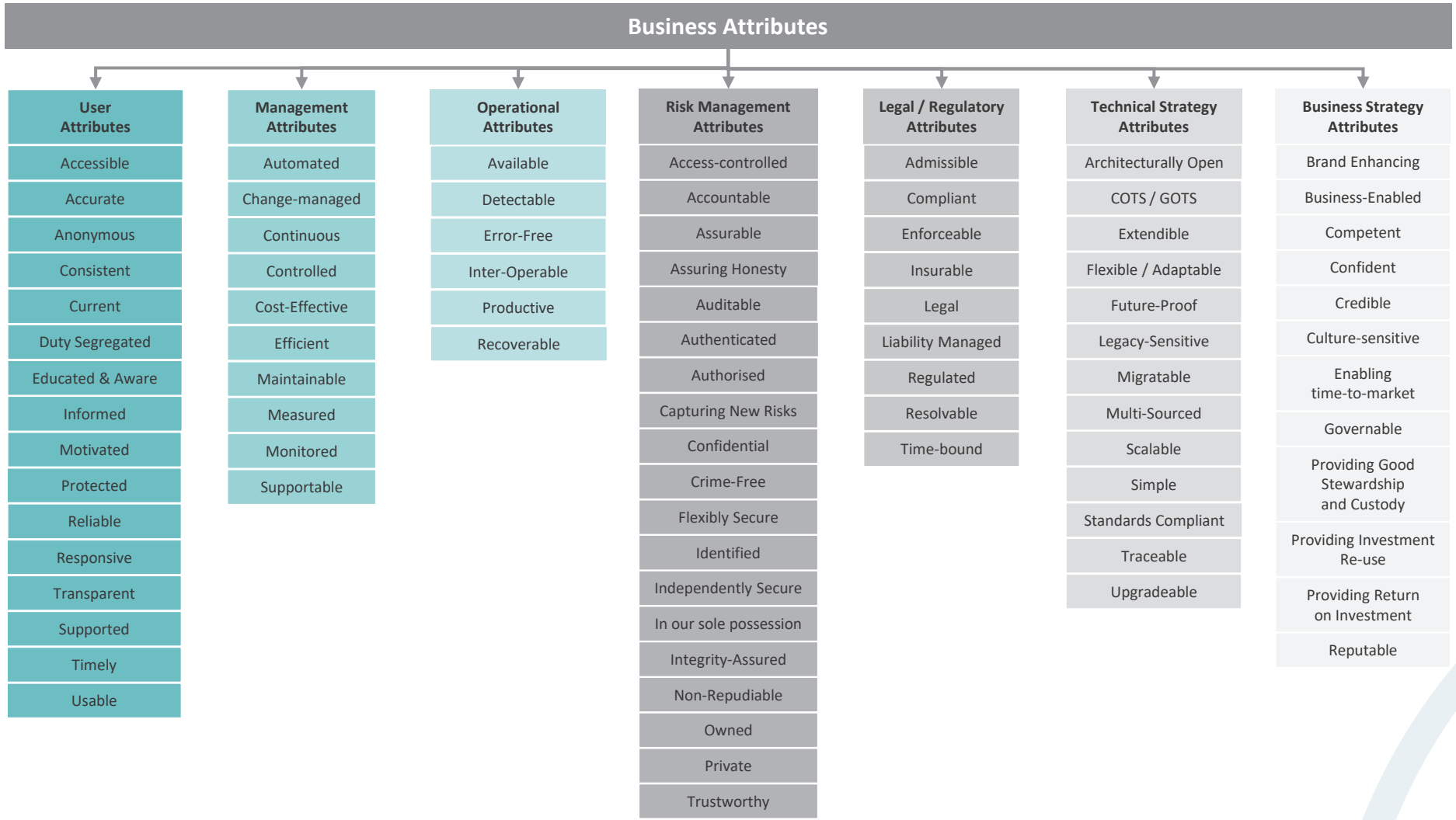
Stakeholder Value & Framework Alignment



Advanced Attributes Profiling (1): Multi-tiered Organisations

Section 4

Original Sample Taxonomy of Attributes



Attribute Performance Thresholds

Performance thresholds are flipside risk appetite thresholds

- The Attribute Performance Target represents the risk appetite
  - A 95% target for “Available” represents a risk appetite of 5% downtime
  - Greater than 5% downtime is unacceptable performance
  - Events leading to greater than 5% present unacceptable risks
  - The appetite threshold provides a first degree of objectivity in assessment
- Negative impact is expressed as
  - Reduction in Attribute performance below target
  - Failure to meet Attribute performance target
- Positive impact expressed as
  - Increase in Attribute performance above target
  - Increase in Attribute performance threshold to higher target

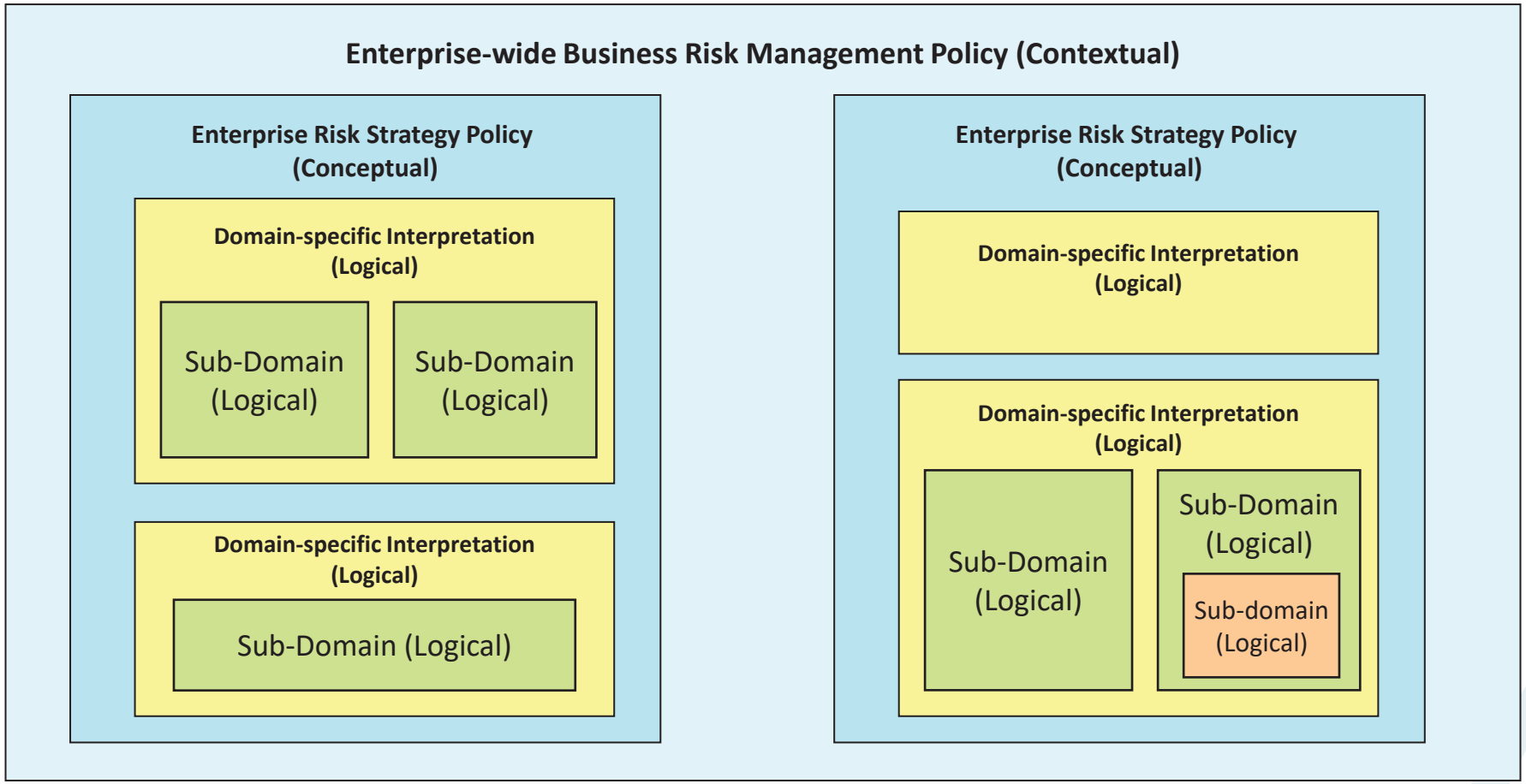
Risk Appetite & Responsibility Delegation

SABSA Domain Model used to embody risk appetite & responsibility delegation

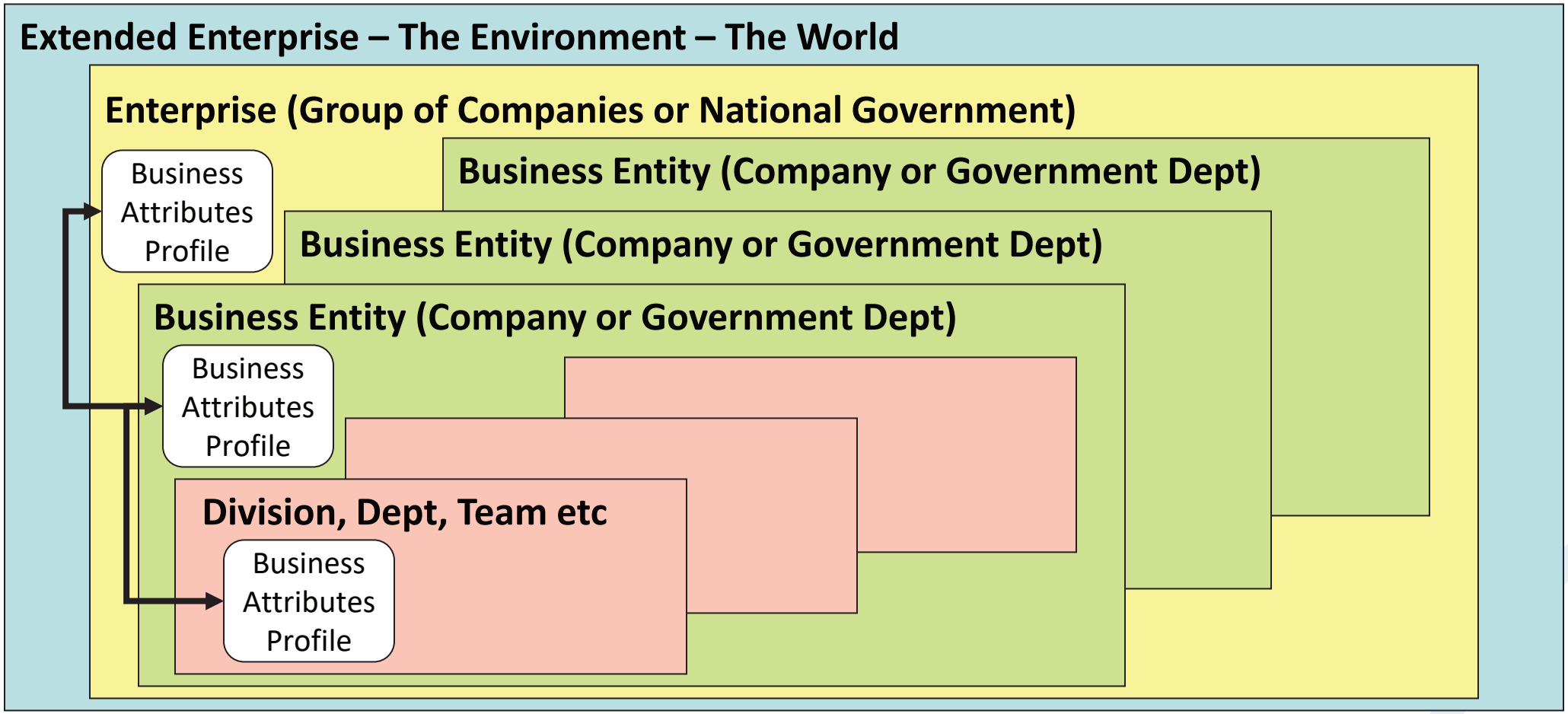
- Business risks & opportunities exist traceably through every layer of the architecture
- Responsibility for managing enterprise risks & opportunities is delegated to Domains
- Each Domain Policy Authority:
  - Operates within the risk appetite parameters of the super domain
  - Is compliant with the 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

Risk Appetite & Responsibility Delegation

SABSA Domain Model used to embody risk appetite & responsibility delegation



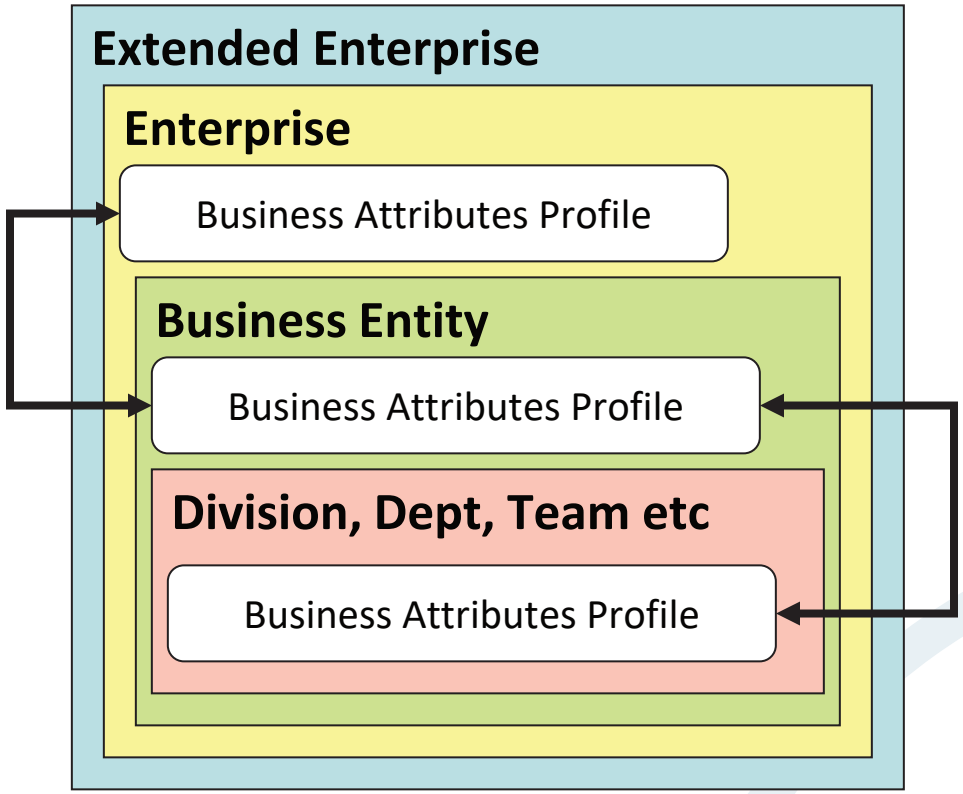
Multi-tiered Attributes – Organisation Domains



Multi-tiered Attributes – Organisation Domains

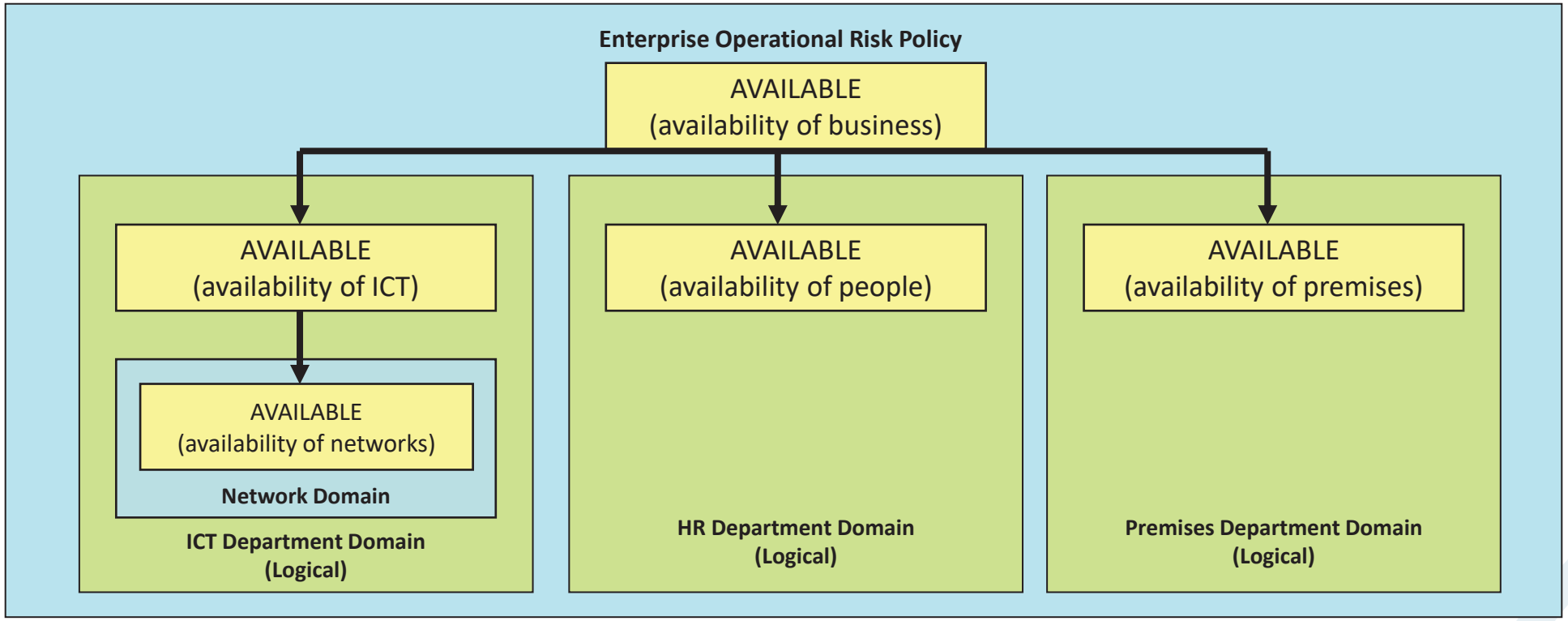
Domain view of Attribute inheritance & aggregation

- Attributes are inherited from domains to sub-domains so that Attributes-based risk appetite is distributed top-down
- Performance against Attribute targets is aggregated bottom-up
- Business Attributes can also feed upwards to contribute to the super-domain level profiles



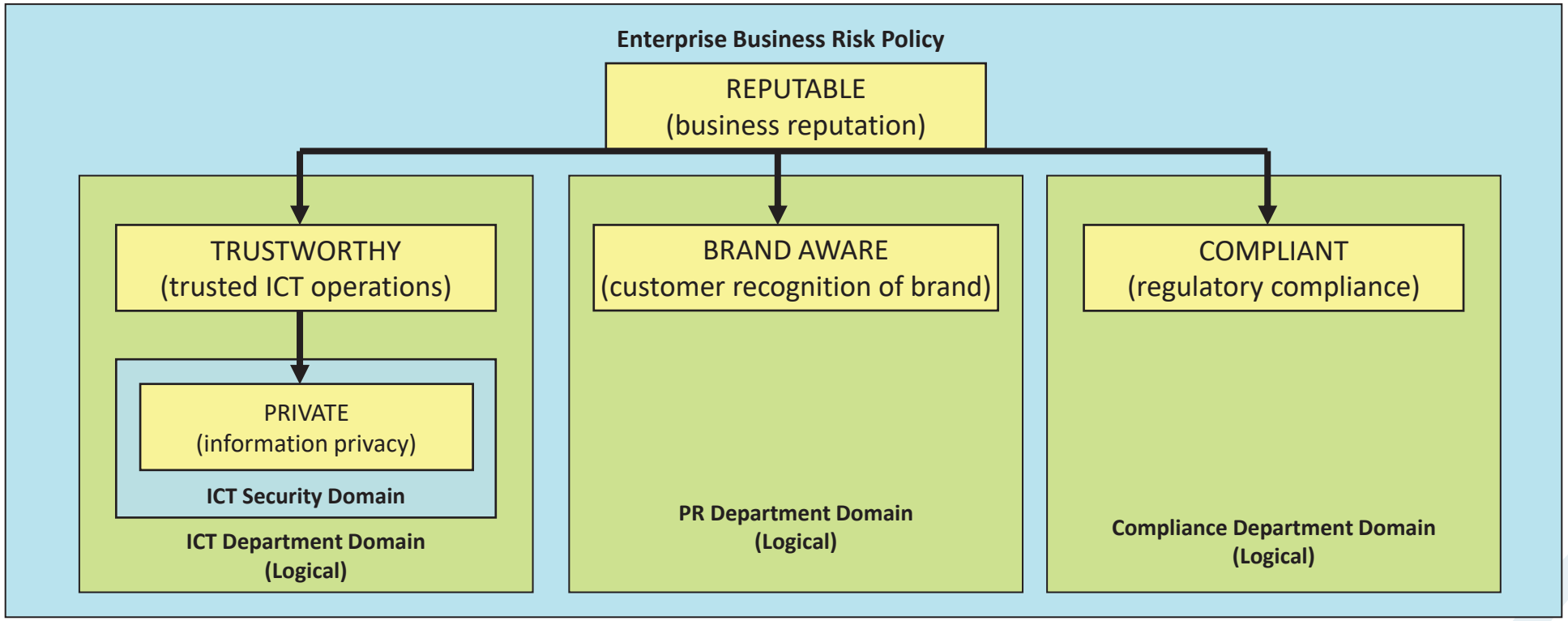
Risk Appetite & Responsibility Delegation

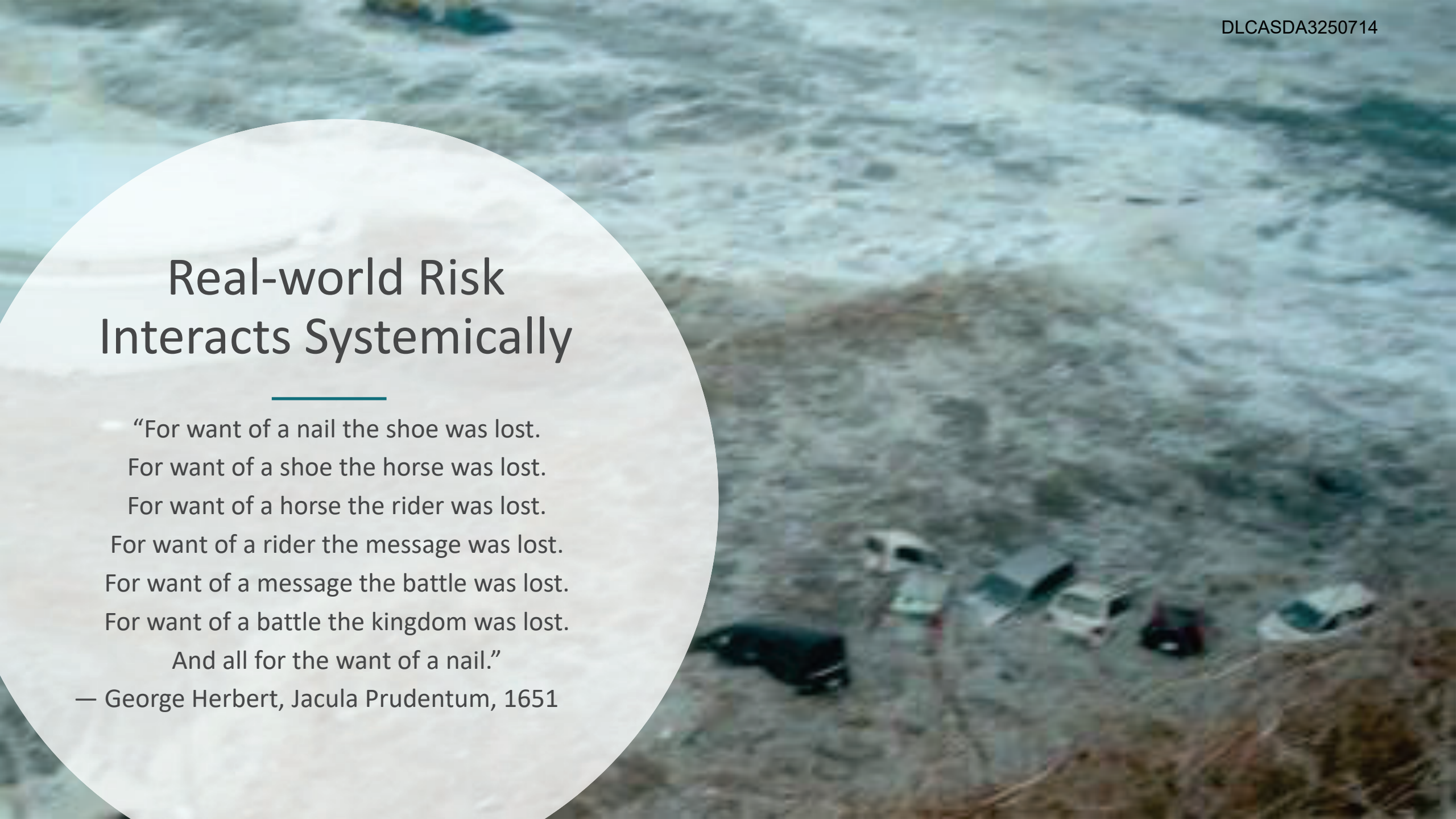
Example – Multi-tier delegation of common attribute



Risk Appetite & Responsibility Delegation

Example – Multi-tier delegation of contributing attribute



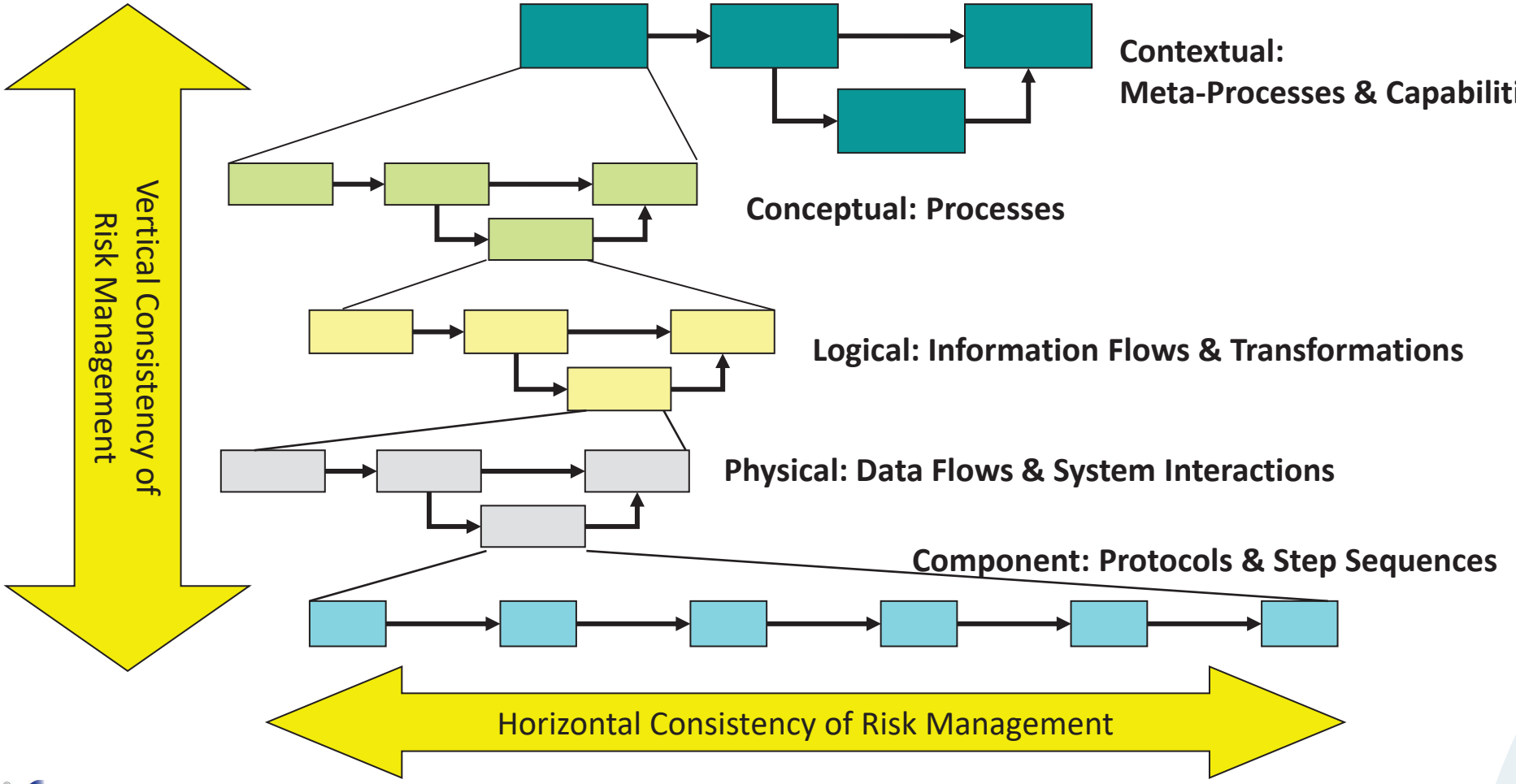


Real-world Risk Interacts Systemically

"For want of a nail the shoe was lost.
For want of a shoe the horse was lost.
For want of a horse the rider was lost.
For want of a rider the message was lost.
For want of a message the battle was lost.
For want of a battle the kingdom was lost.
And all for the want of a nail."
— George Herbert, Jacula Prudentum, 1651

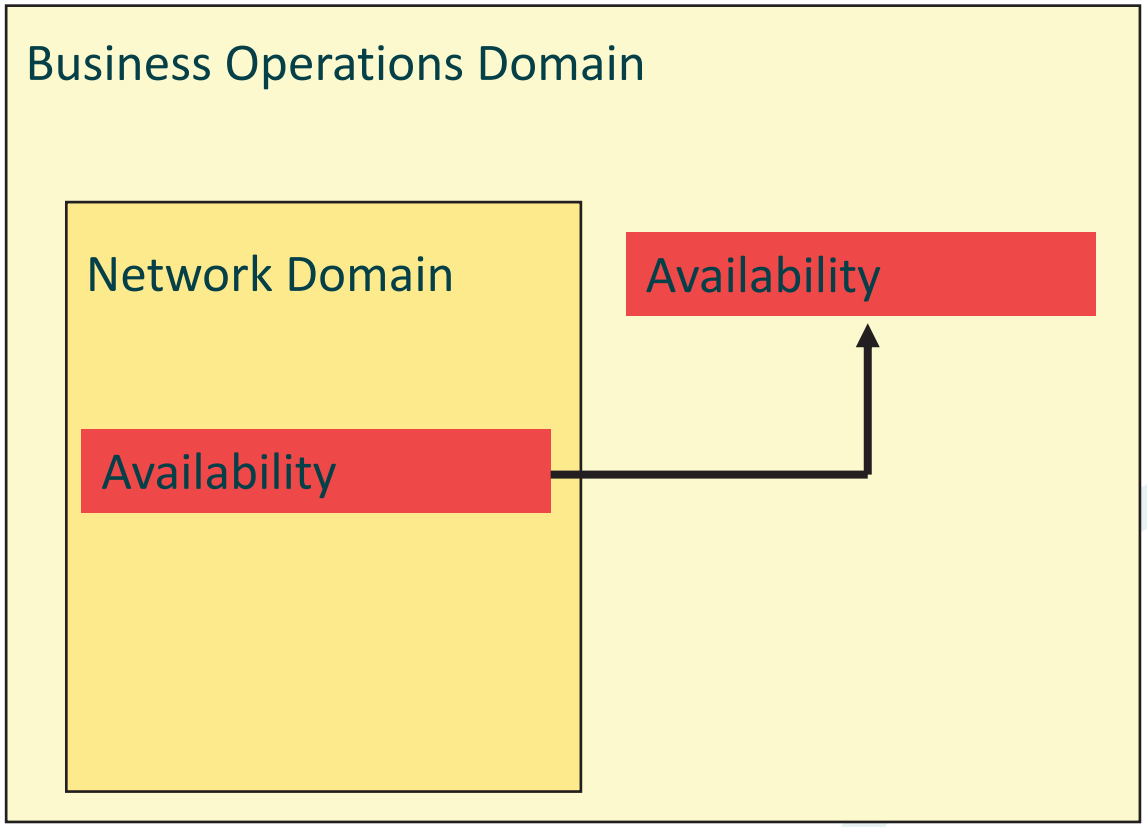
Vertical Risk - Process Engineering

How does the King check the horseshoe nails?



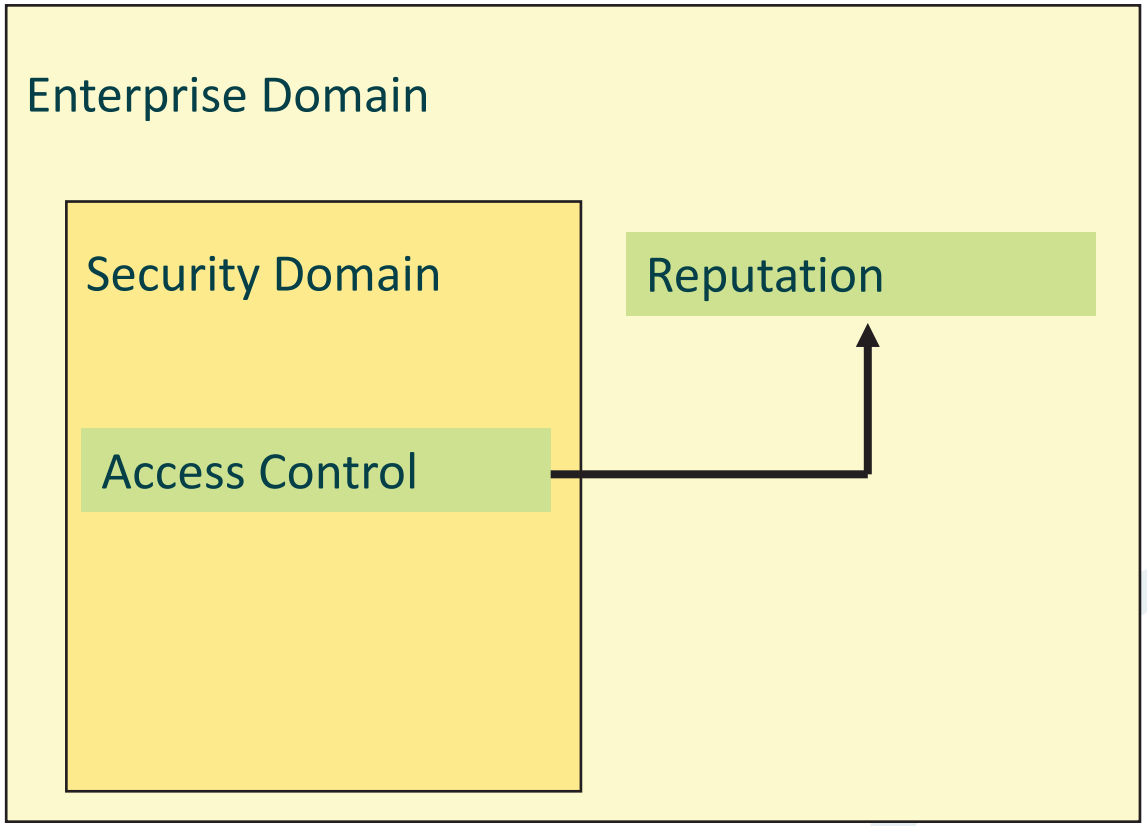
Vertical Systemic Impact

- Negative impact in subdomain has a negative impact in superdomain



Vertical Systemic Benefit

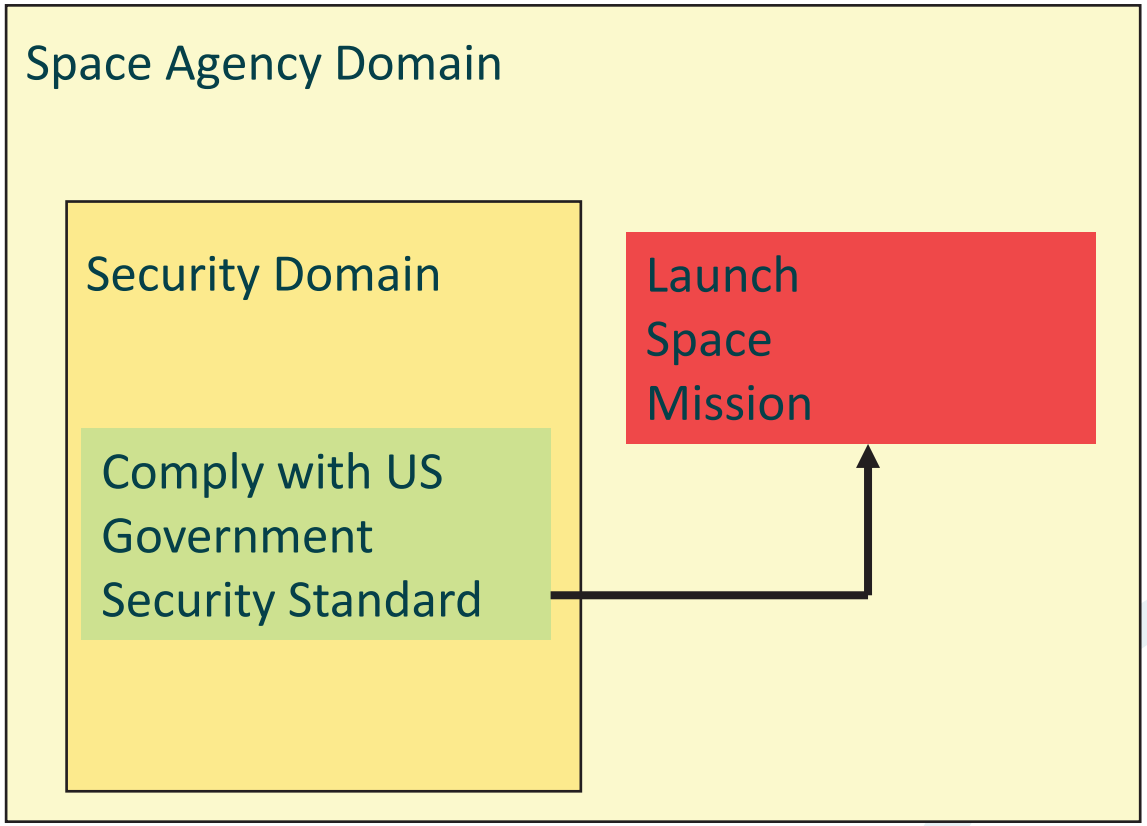
- Positive benefit in subdomain has a positive benefit in superdomain



Vertical Systemic Conflict

Risk treatment causes impact

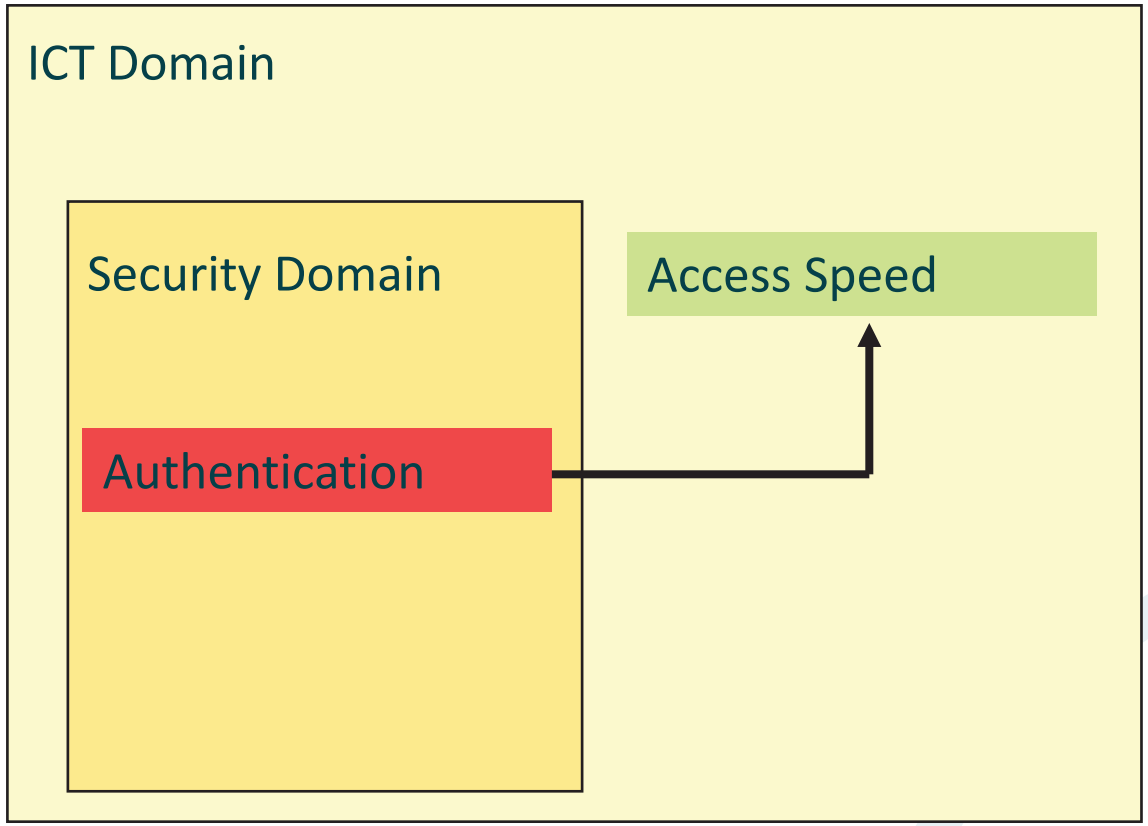
- Risk treatment in subdomain has a negative impact on superdomain



Vertical Systemic Conflict

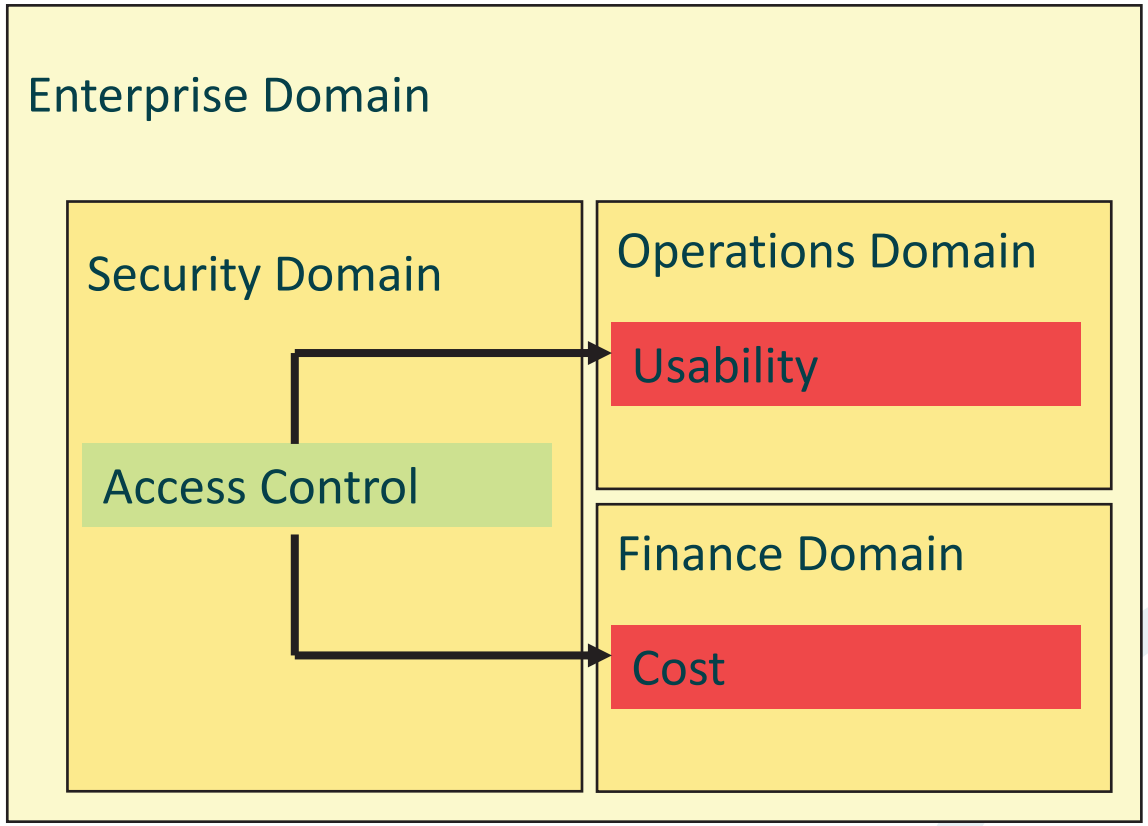
Risk failure causes benefit

- Risk failure in subdomain has a positive benefit in superdomain



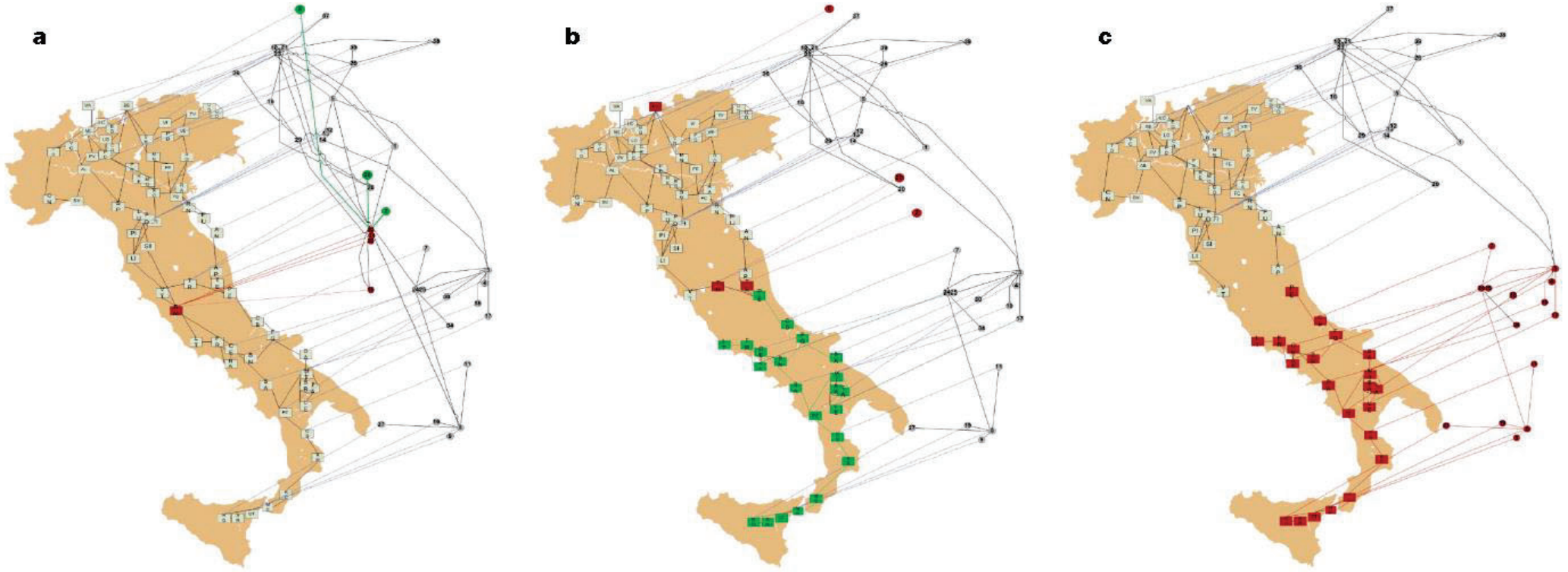
Horizontal Systemic Interaction

- Risk treatment in a domain has a negative impact in peer domains



Compound Interaction in Hyper-connected World

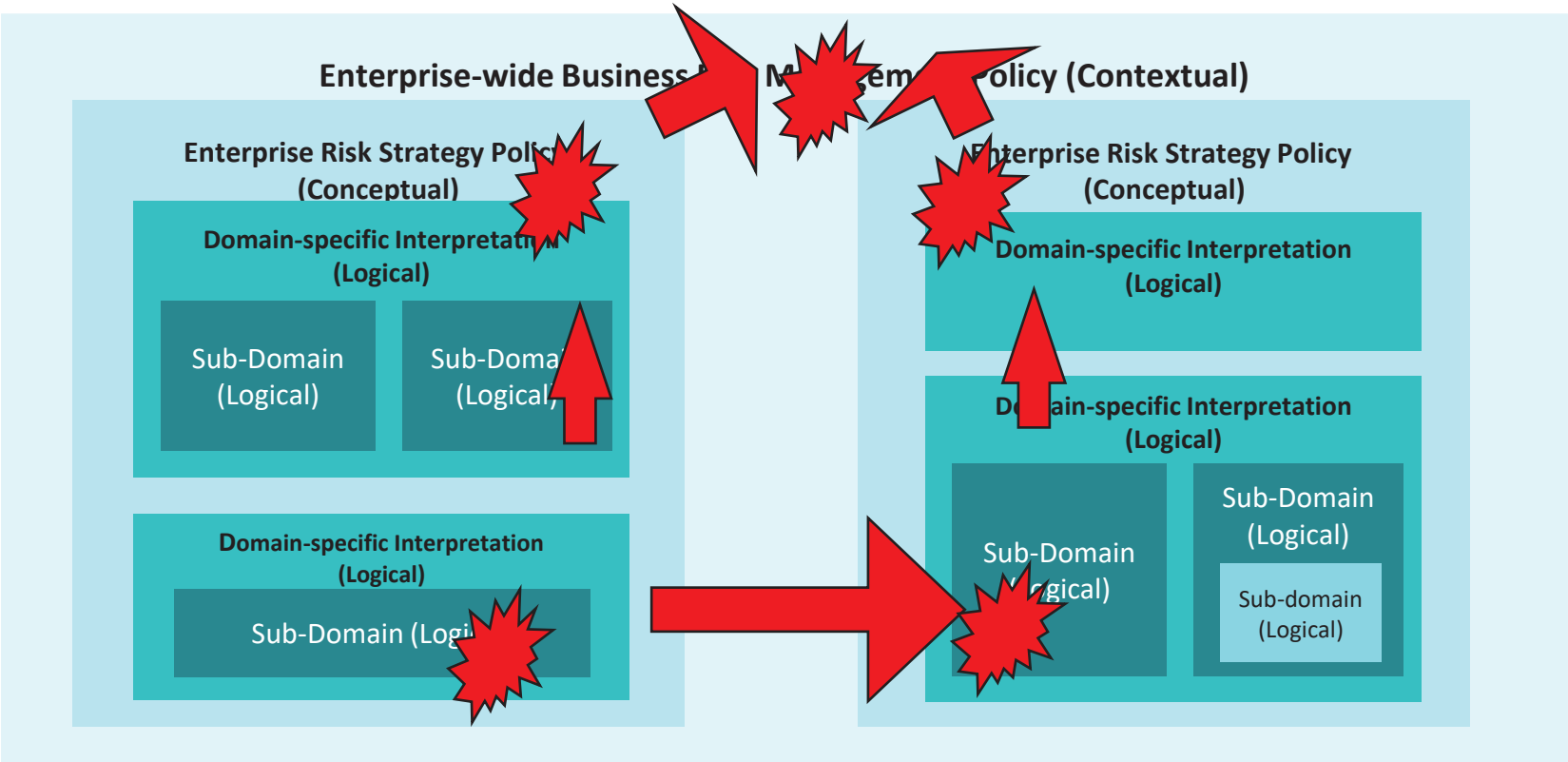
- The SmartGrid Era - Coupling two resilient networks can result in a fragile ‘network of networks’ that is prone to catastrophic fragmentation



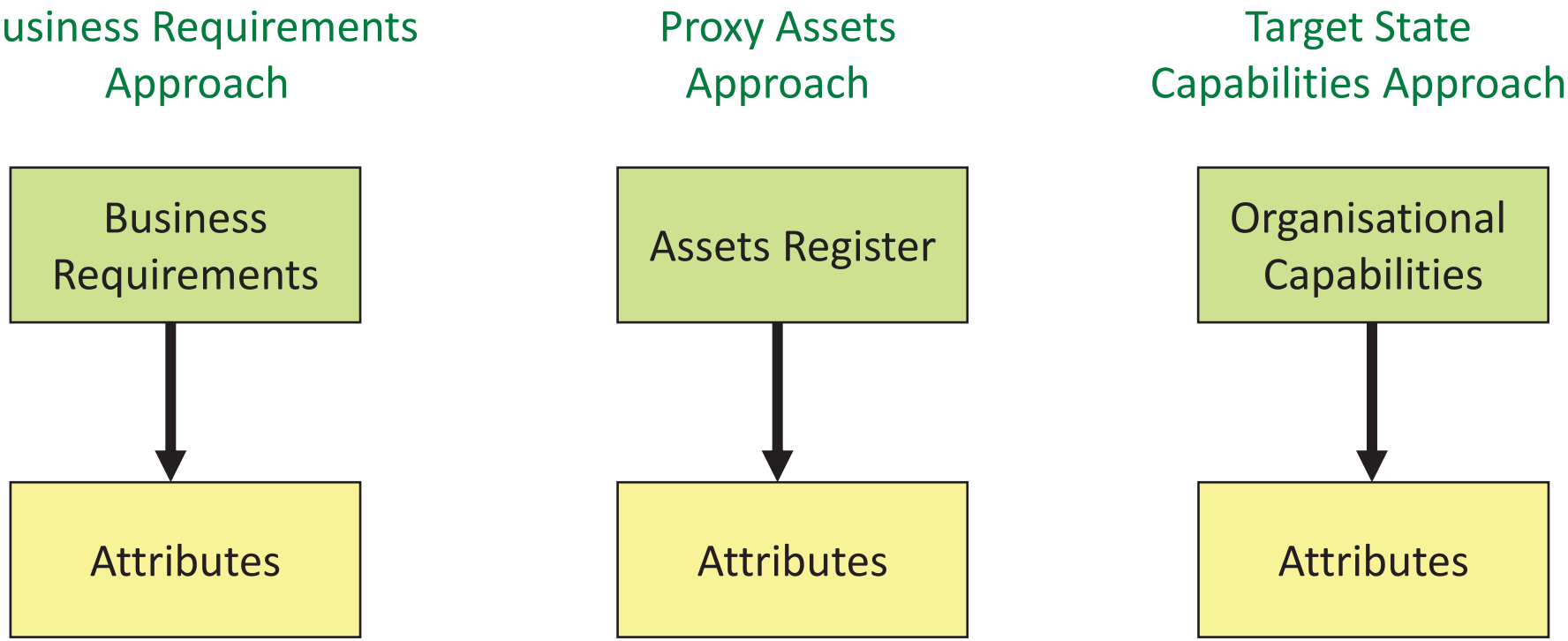
Power station down **Internet nodes down** **Everything down**

Attributes in Multi-tier Systemic Risk

Identify a risk in any Domain with consequences for any other Domain

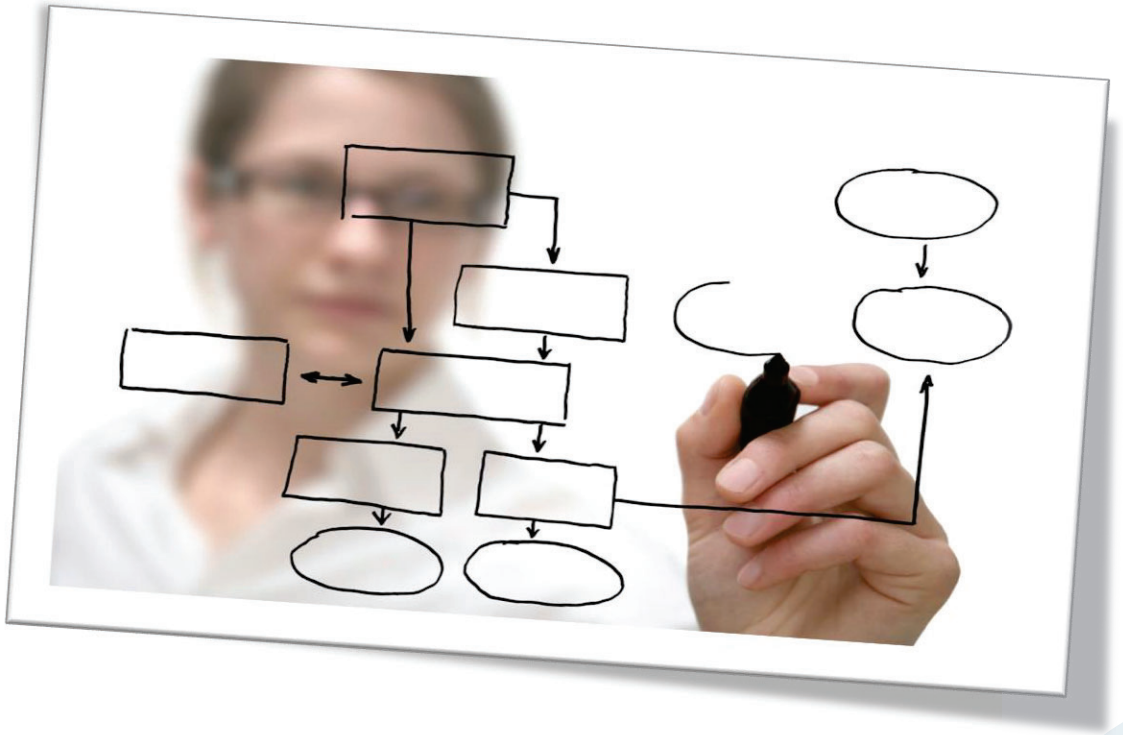


Conceptualising Requirements as Attributes



Workshop A3-4

Advanced Attributes Profiling – Multi-tier Organisations

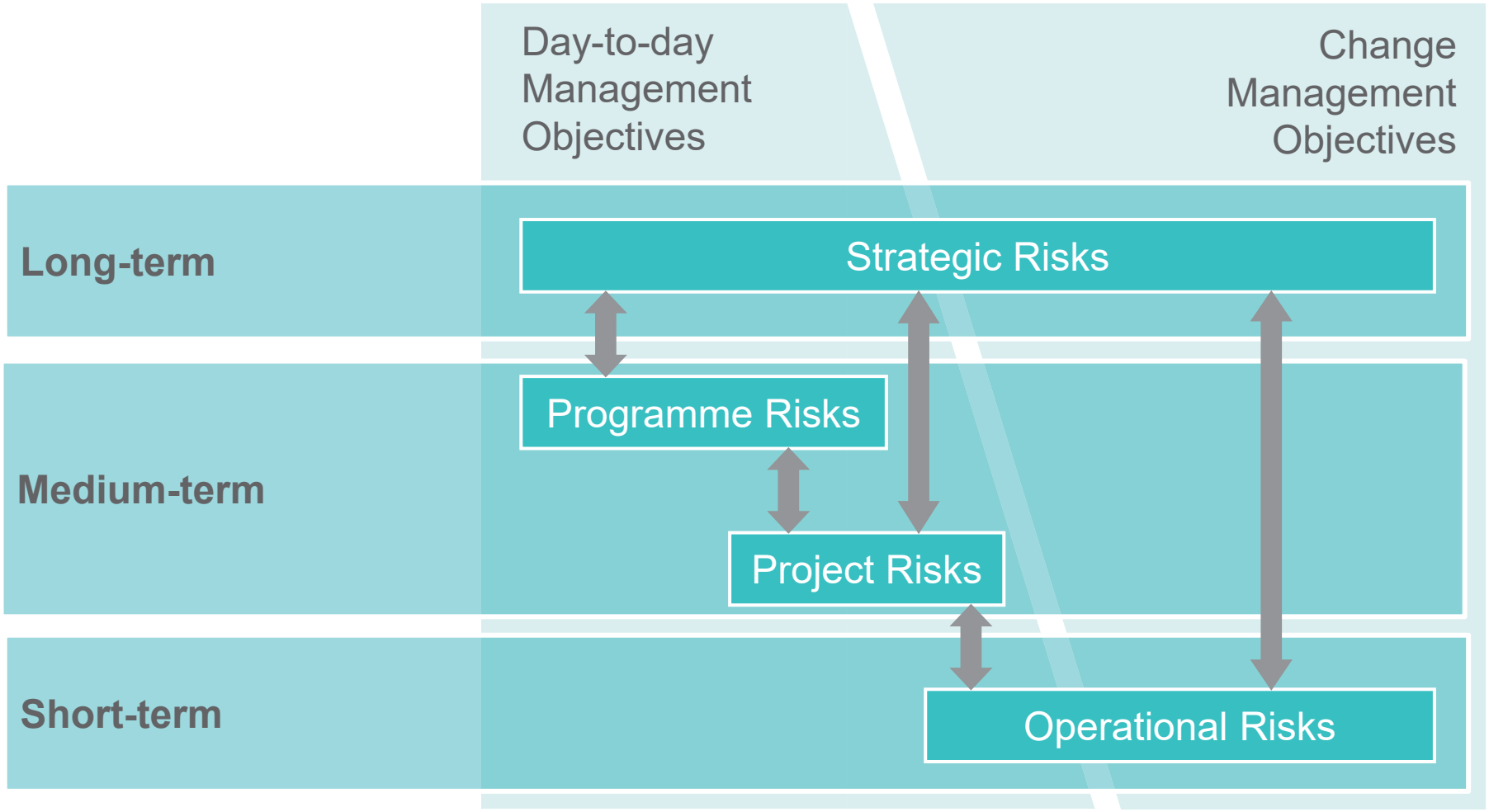


Advanced Attributes Profiling (2): Programmes & Projects

Section 5

Enterprise Lifecycle Risk Perspectives

Source: OGC M_o_R 2007

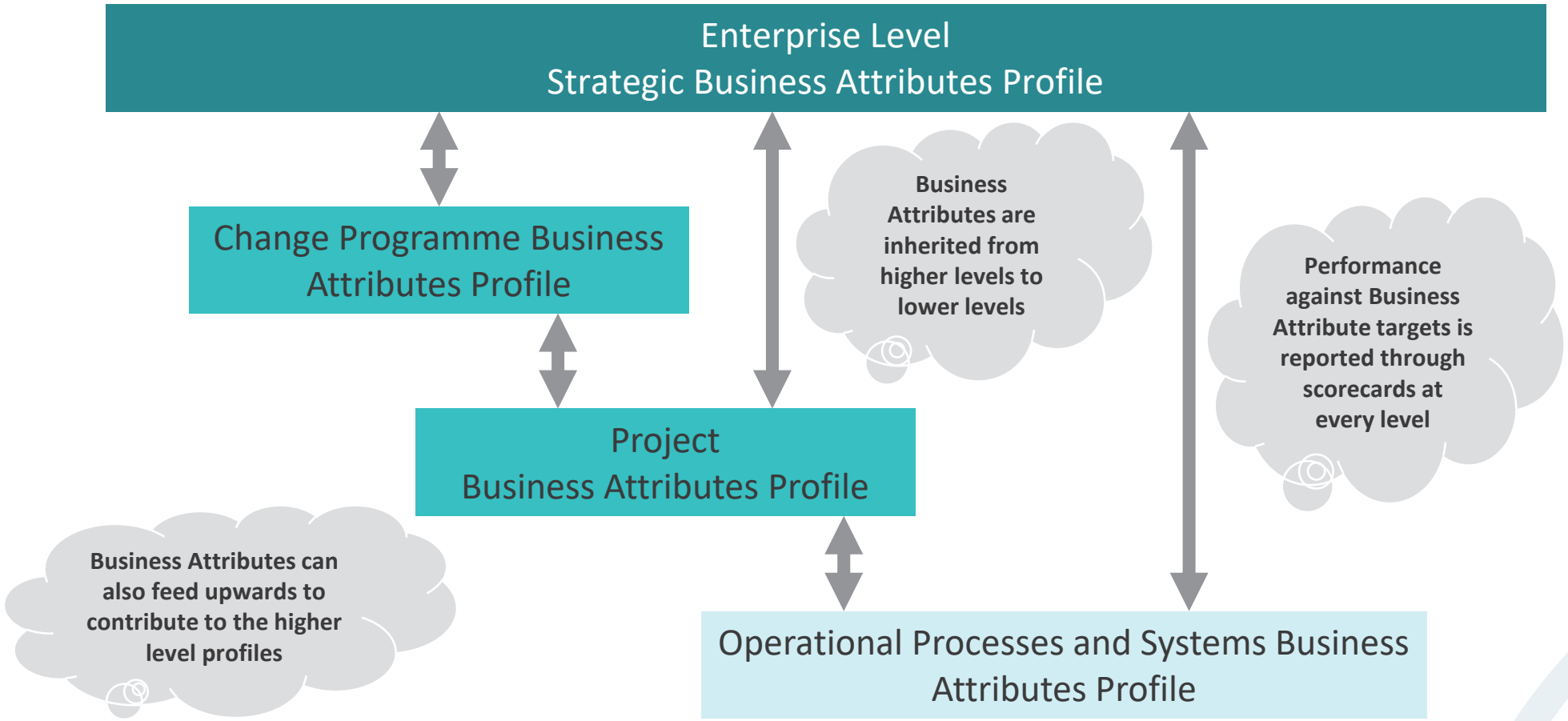


Lifecycle Domains

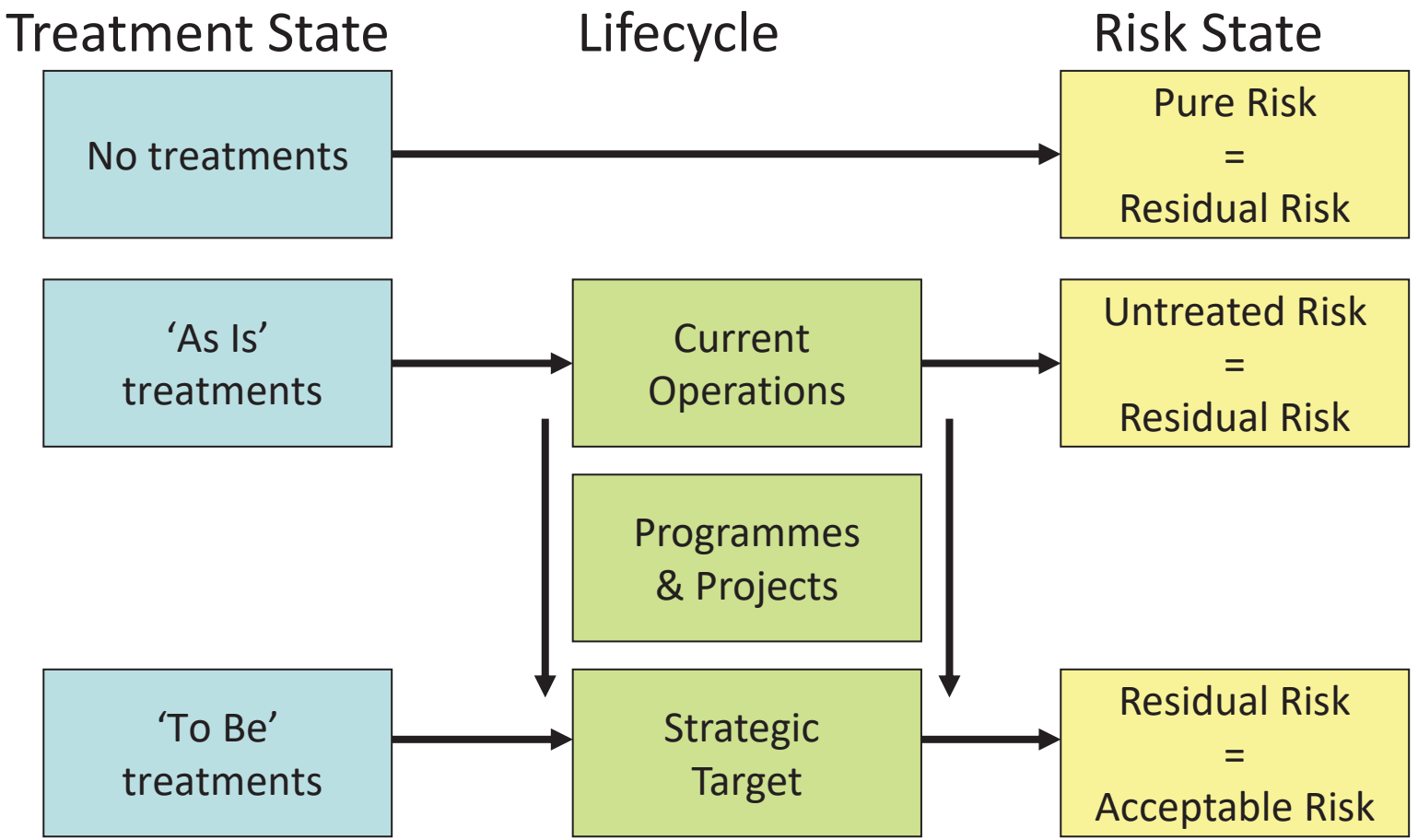
Applied for SABSA Attributes Inheritance

- Strategic domain
  - Sets overall business objectives
  - Sets security domain policy that applies across the entire enterprise
- Programme or project domain
  - Develops systems, processes and other ‘capabilities’ that are used to achieve specific business objectives (set at the strategic domain level)
  - Sets security domain policy for the use / application of the capability
- Operational domain
  - Uses systems, processes and other capabilities developed at the project level
  - Interprets, applies and implements policies set at higher levels
  - Makes ‘in the moment’ policy decisions (what do I do NOW!)

SABSA Lifecycle Domain Risk Perspectives

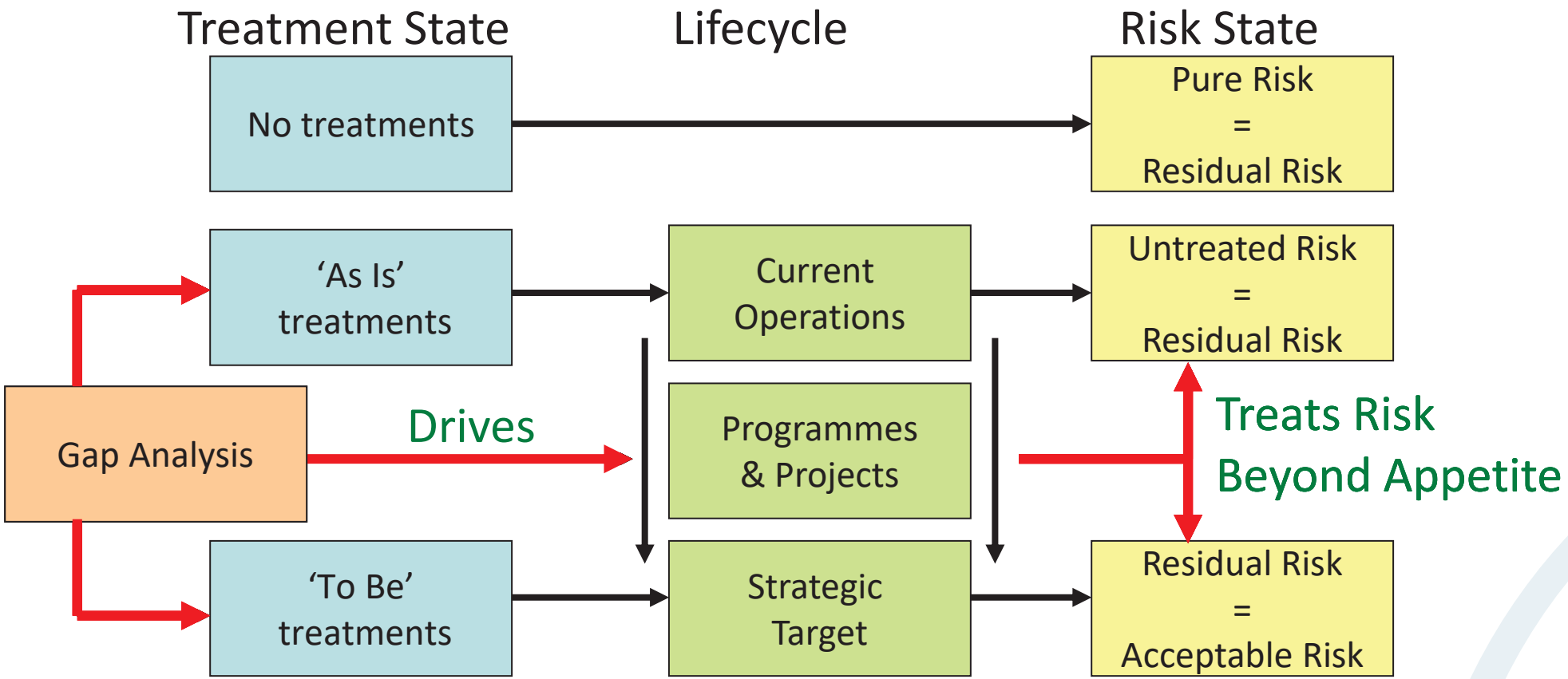


Project Perspective of the Risk Lifecycle



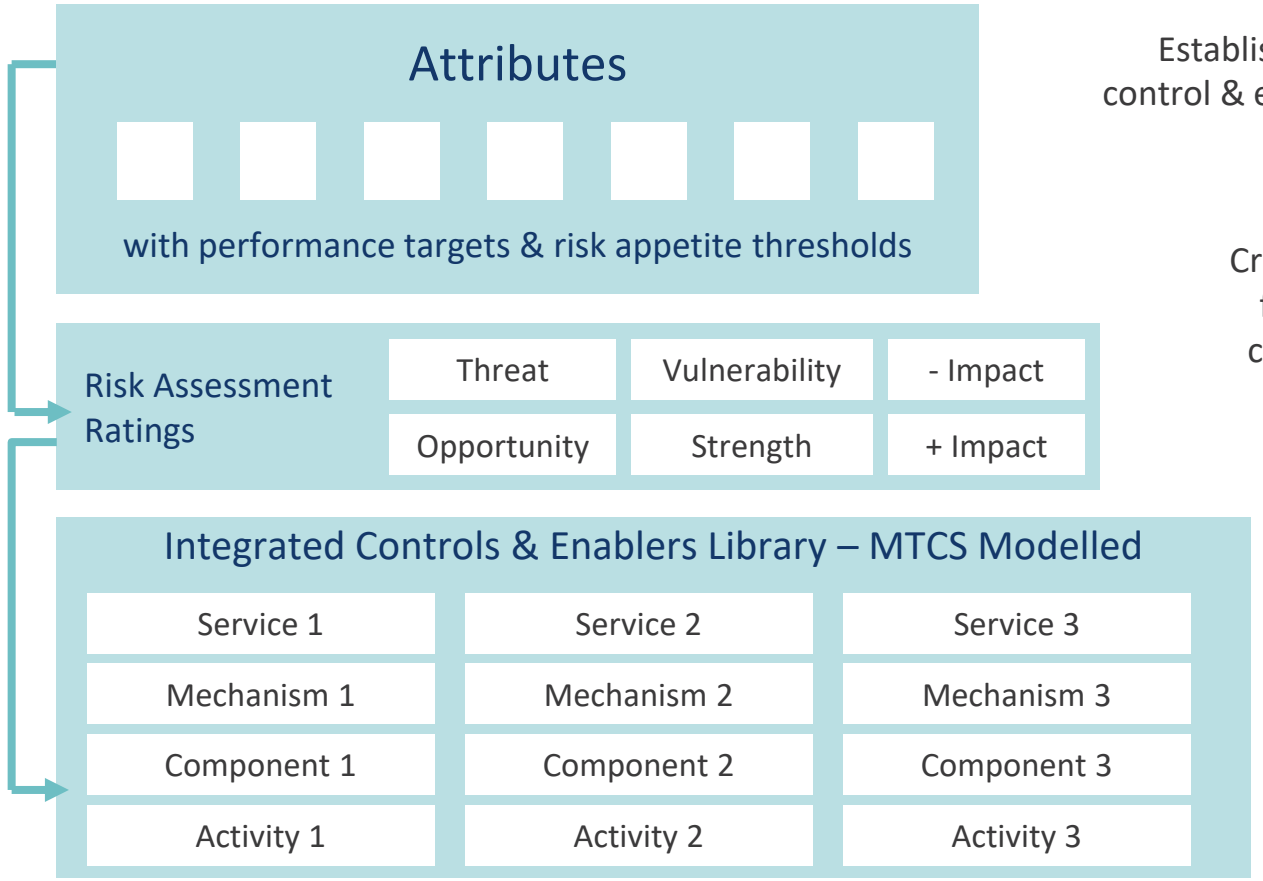
Gap Analysis

Develop the strategy for managing residual risk beyond appetite



ORM Architecture Inheritance & Re-use

SABSA Risk Assessment #1 / Pilot / Establishment Project



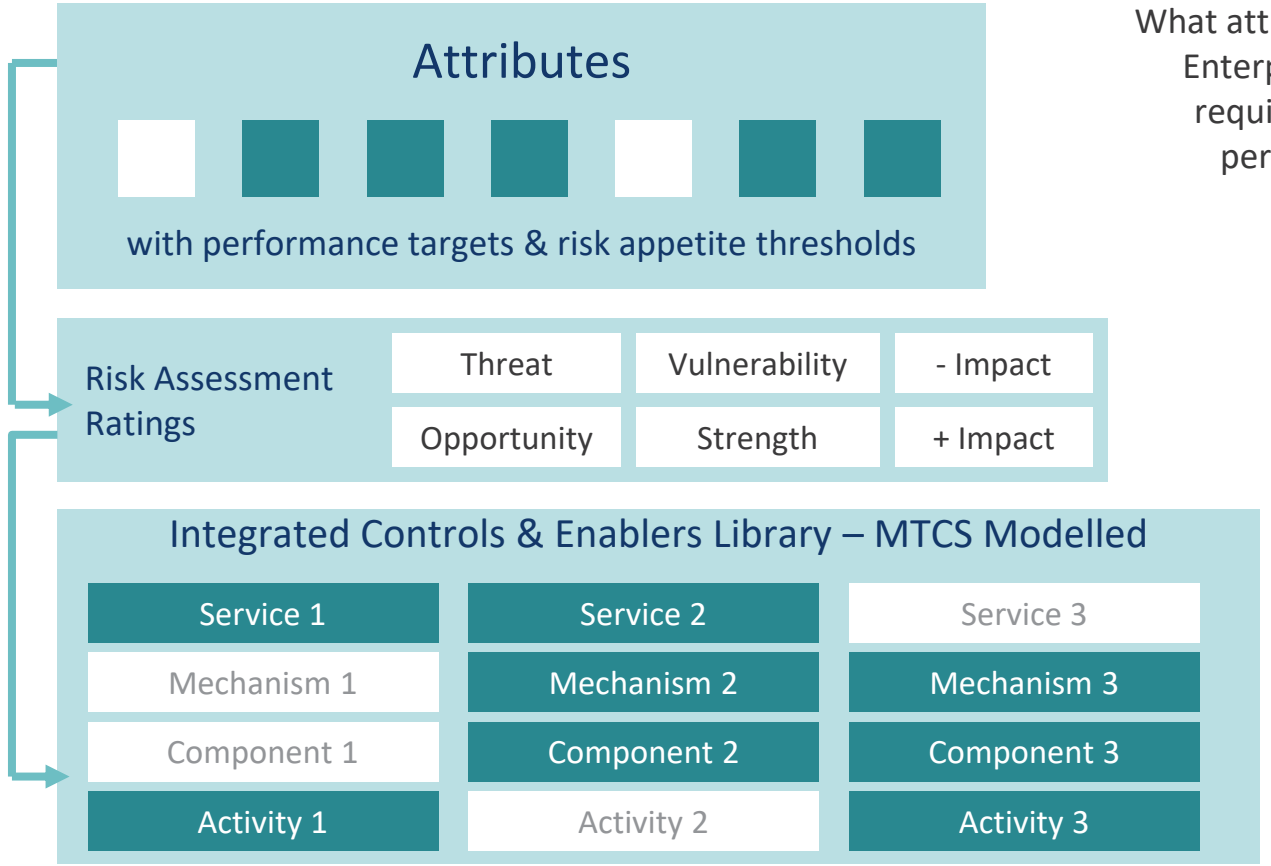
Establishes first enterprise attributes, control & enablement objectives and risk register for those attributes

Creates first traceable layer-map from business requirements to controls (services, mechanisms, components & management activities)

This layer-map becomes the current-state SABSA Enterprise Security Architecture

ORM Architecture Inheritance & Re-use

Subsequent SABSA Risk Assessments / Project – Re-use



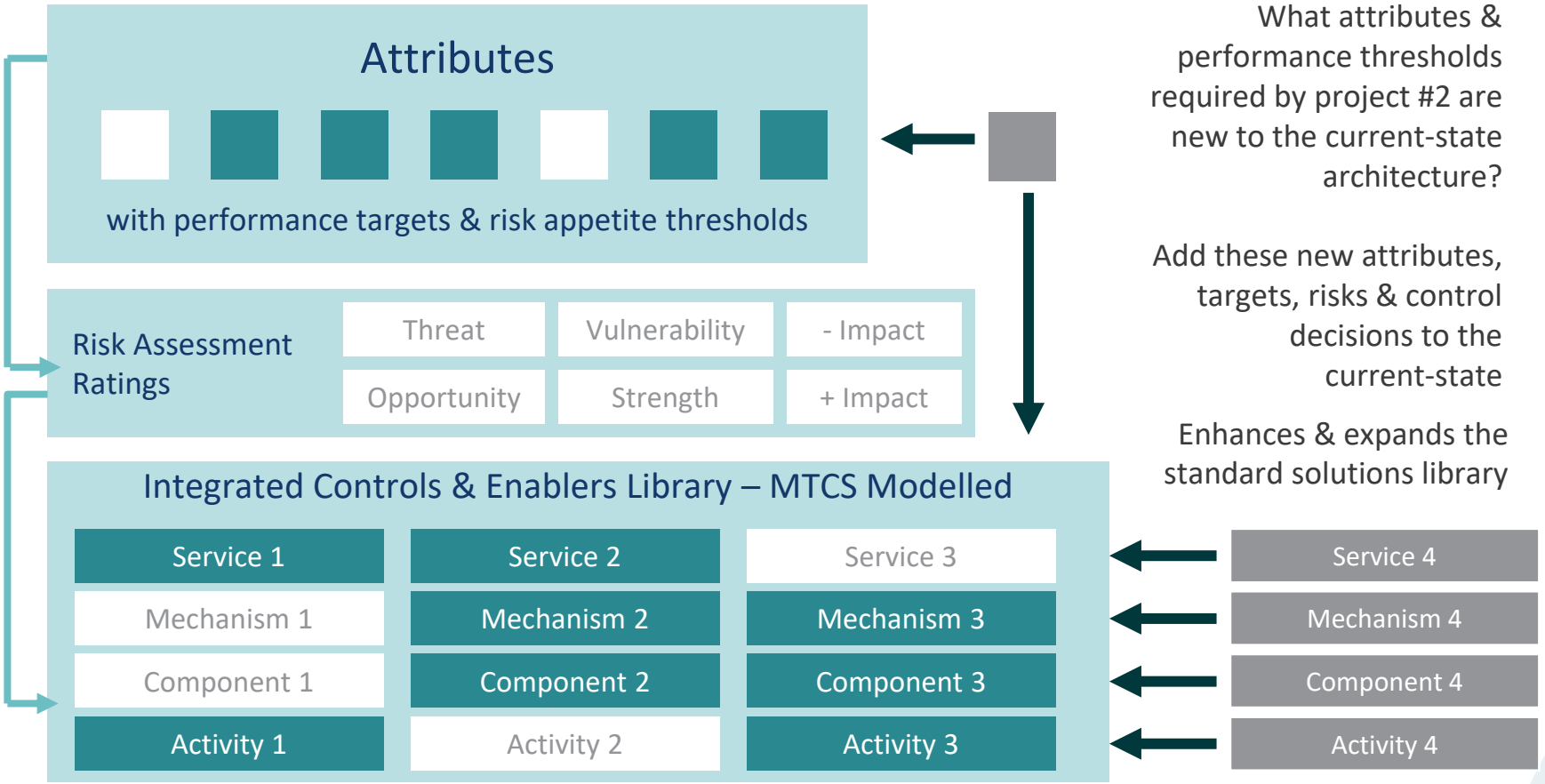
What attributes from the current-state Enterprise Security Architecture are required for project #2 with similar performance bands / thresholds?

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

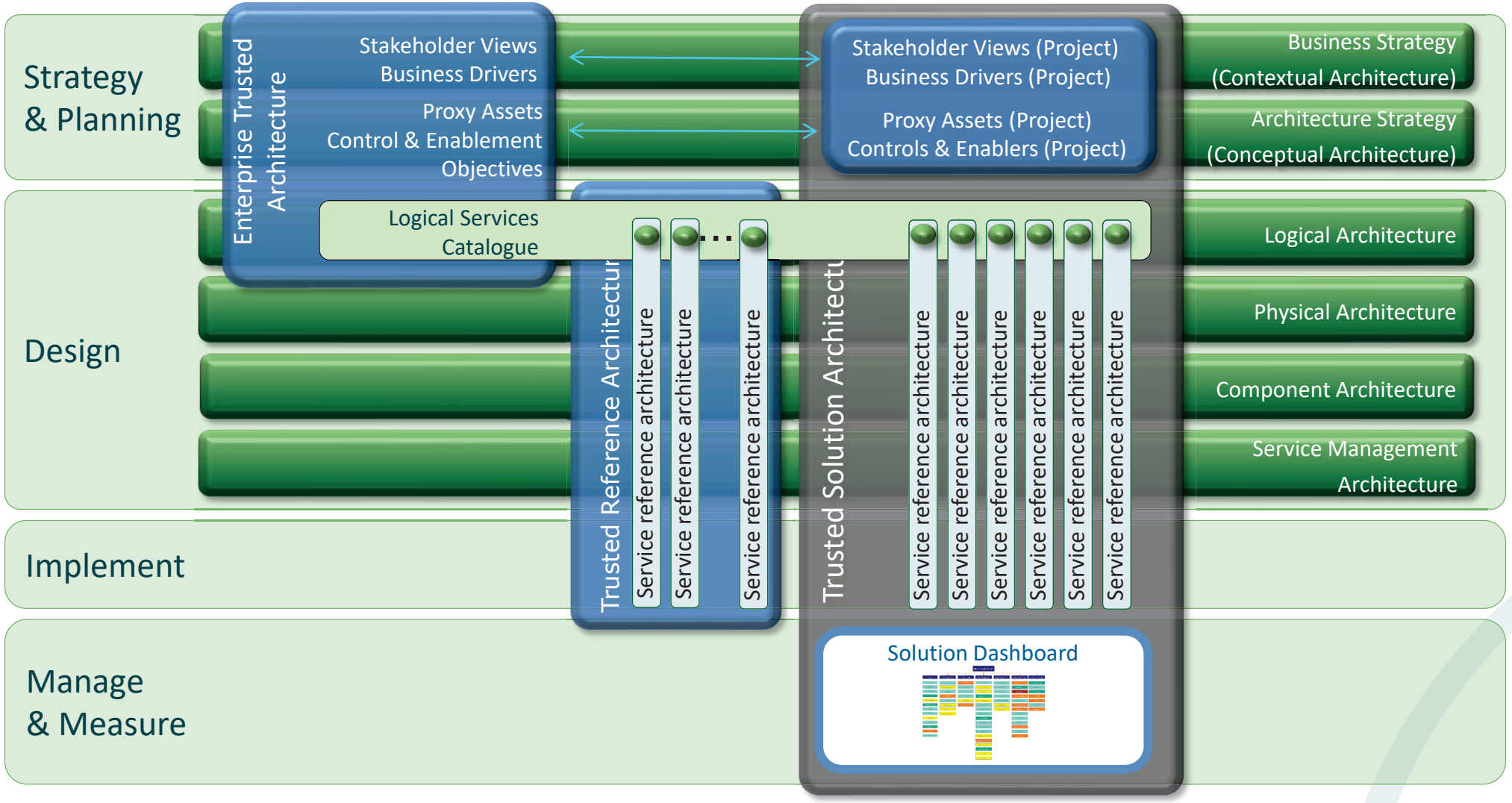
We have already solved this problem – inherit all entries in layer-map linked to the attributes:
re-use our now‘standard’ solutions

ORM Architecture Inheritance & Re-use

Subsequent SABSA Risk Assessments / Projects – Enhance

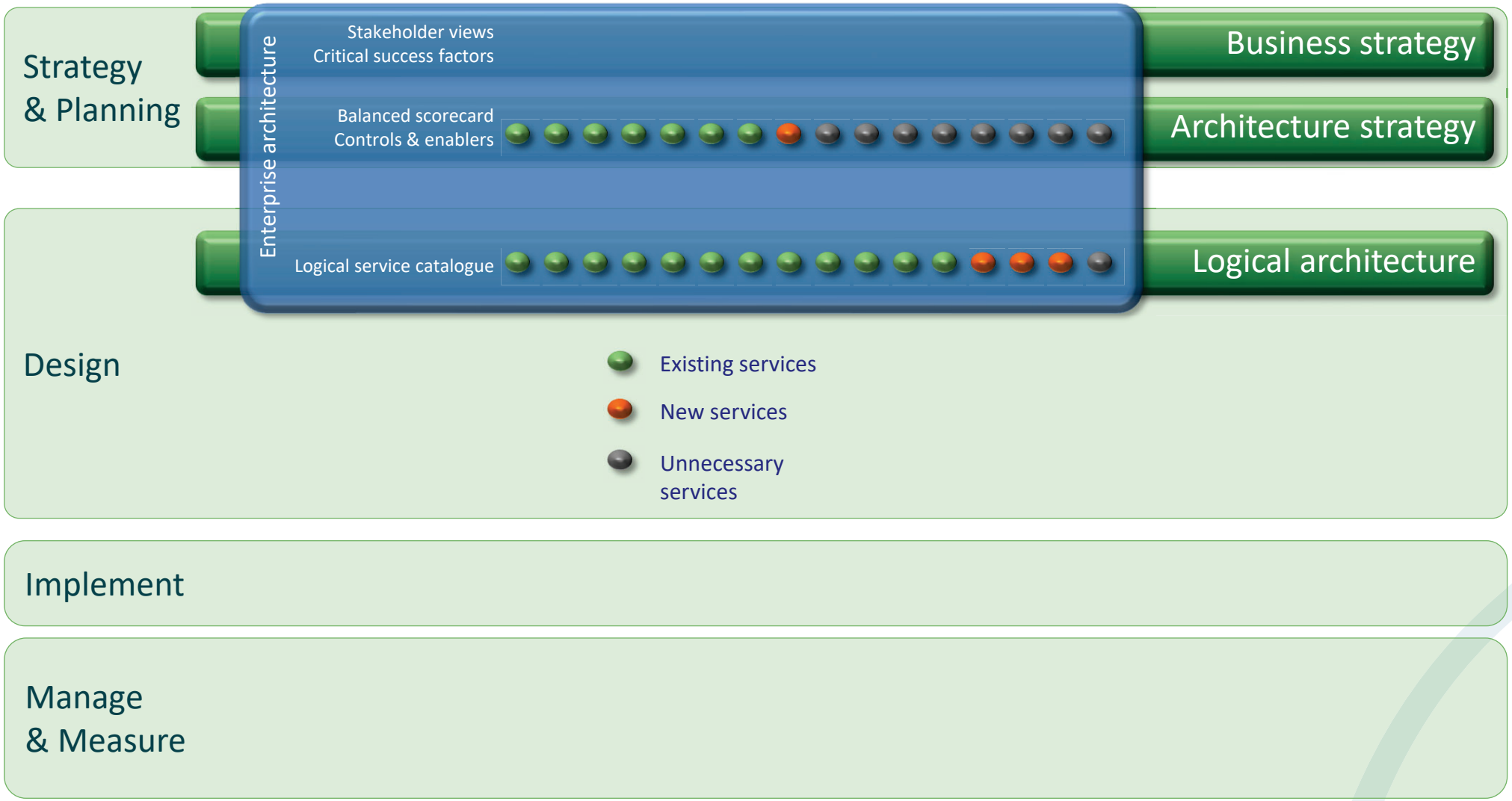


Executing a Programme or Project

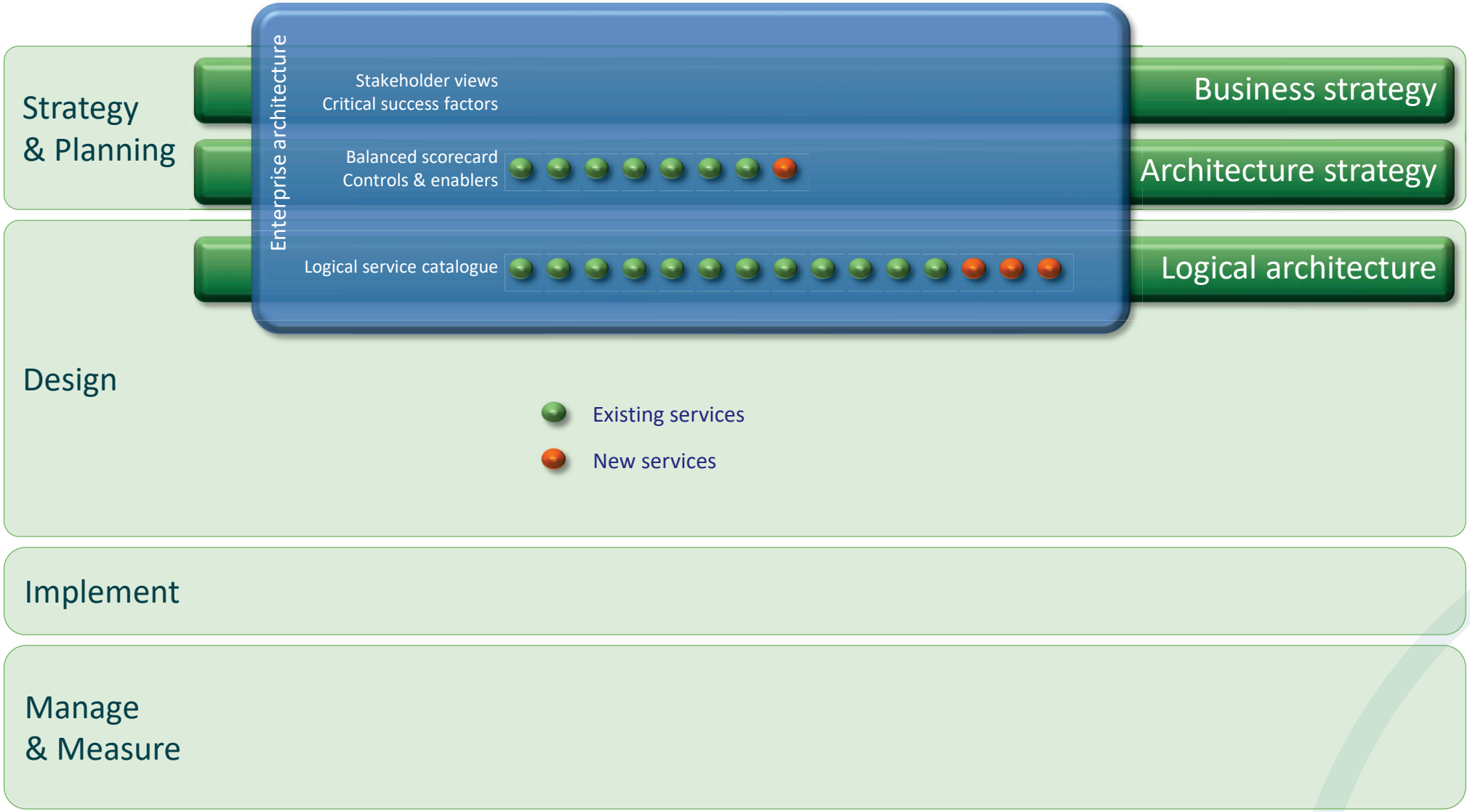


The Strategy and Planning Phase

The Strategy and Planning Phase…

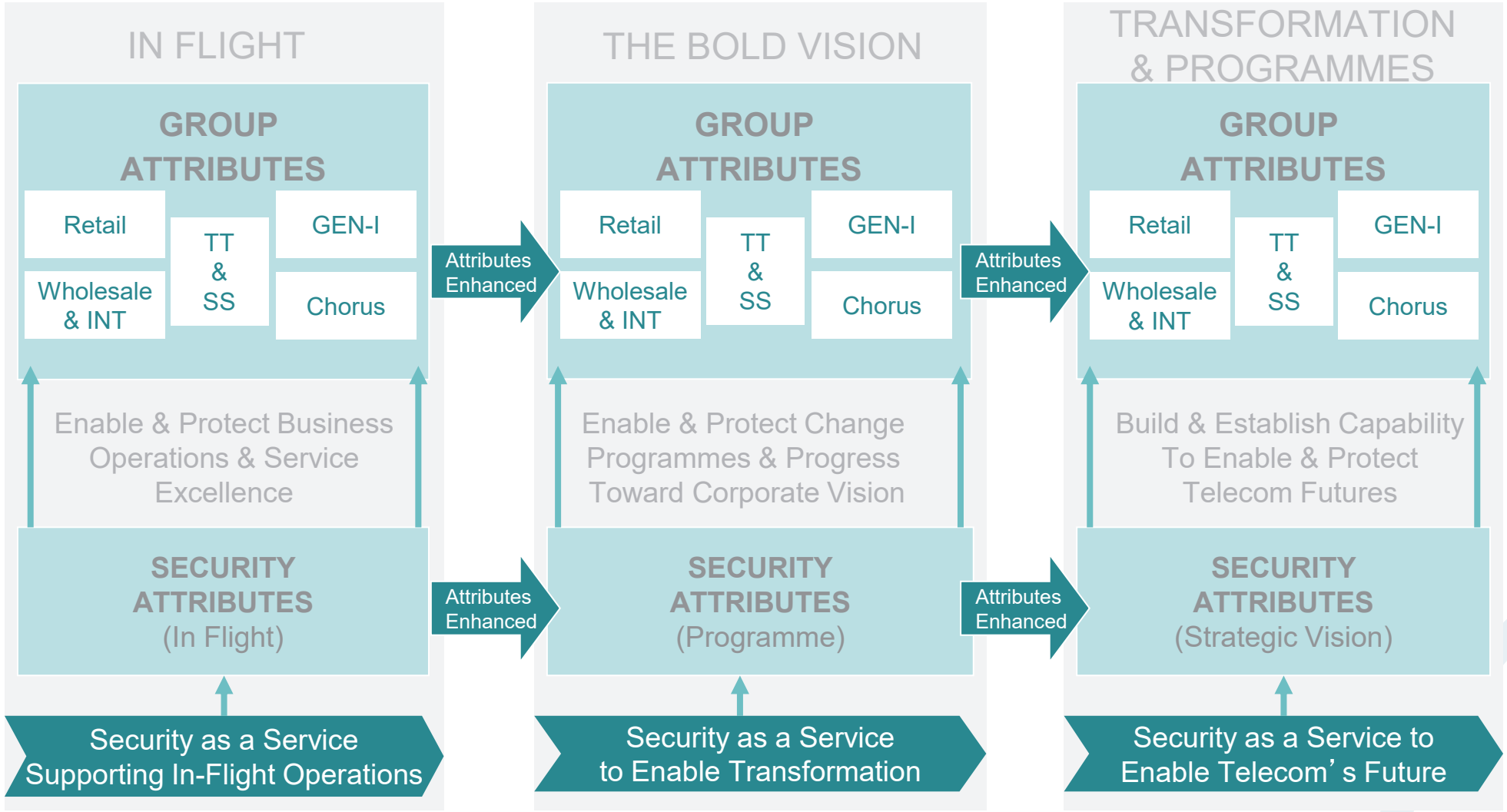


The Strategy and Planning Phase



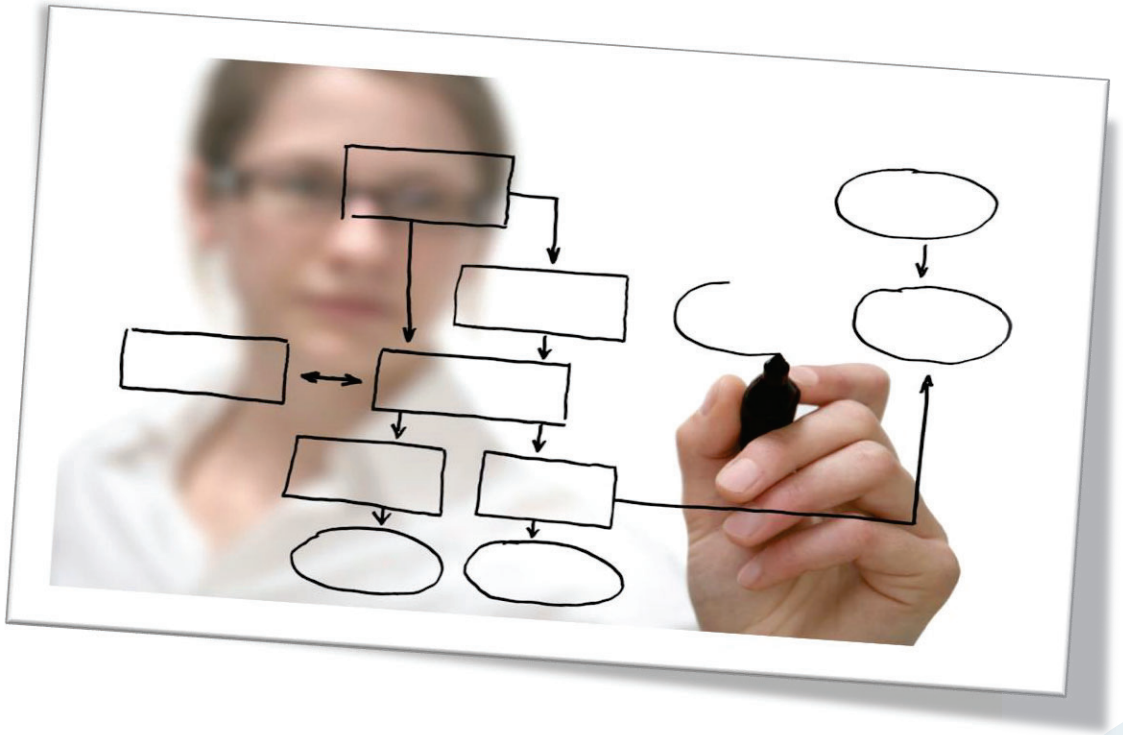
SABSA Risk Treatment Migration Strategy

Reproduced with permission from New Zealand Telecom



Workshop A3-5

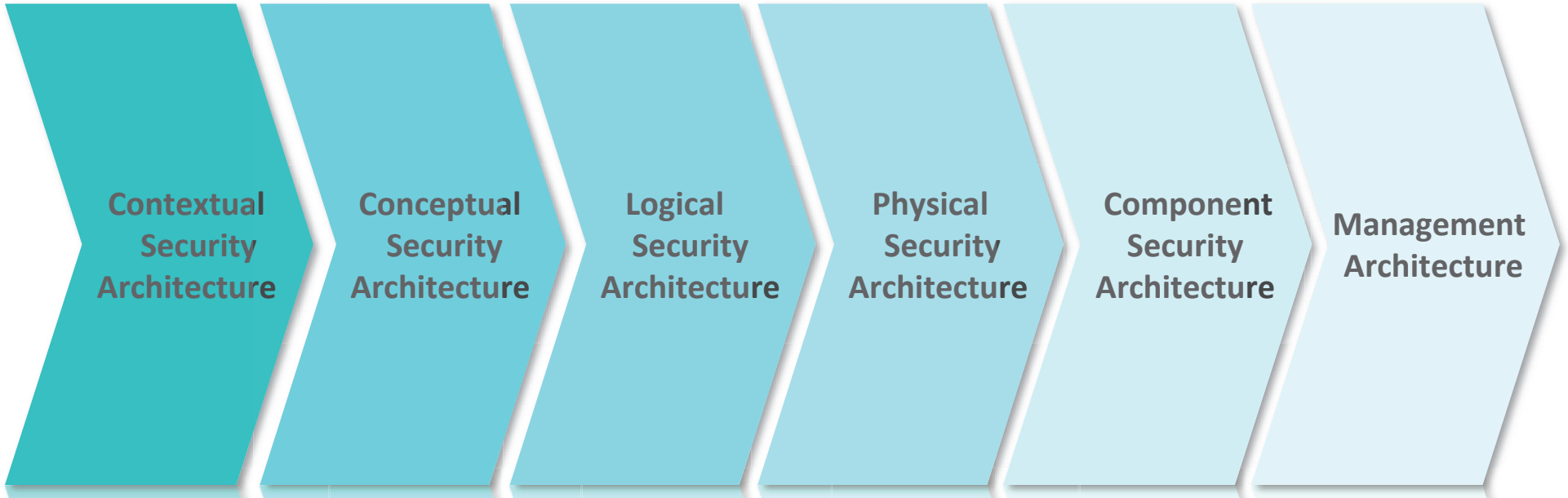
Advanced Attributes Profiling – Strategic Roadmap of Programmes & Projects



Traceability Concept: Architecture Layer-map / Repository

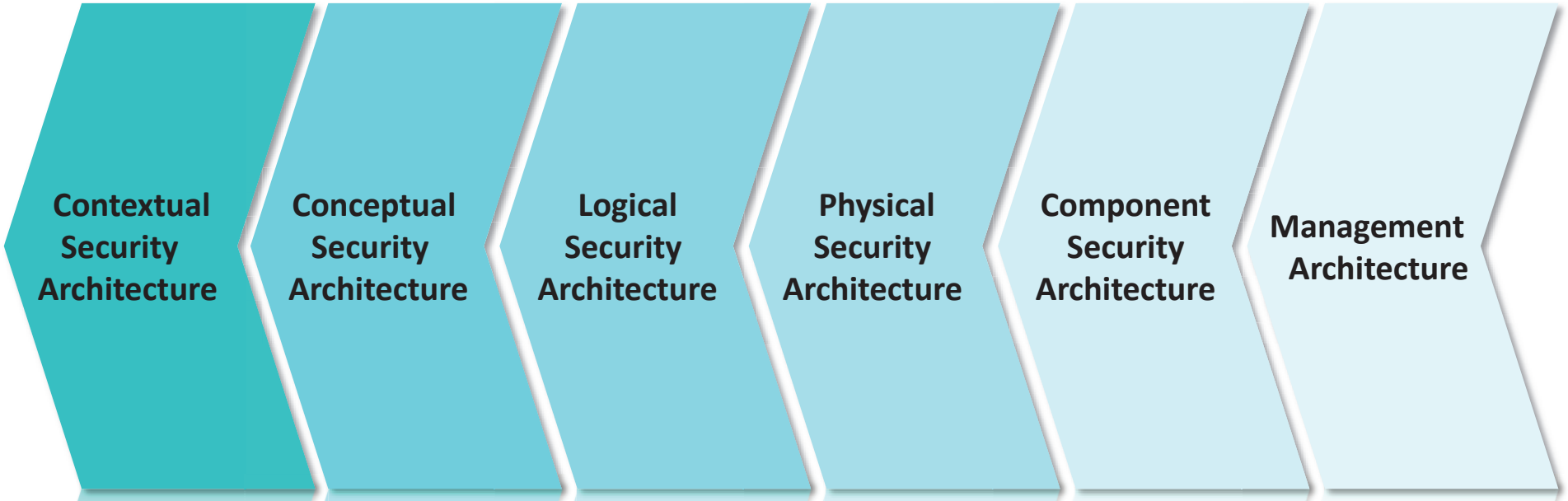
Section 6

Traceability for Completeness



- Every business requirement for security is met and the residual risk is acceptable to the business appetite

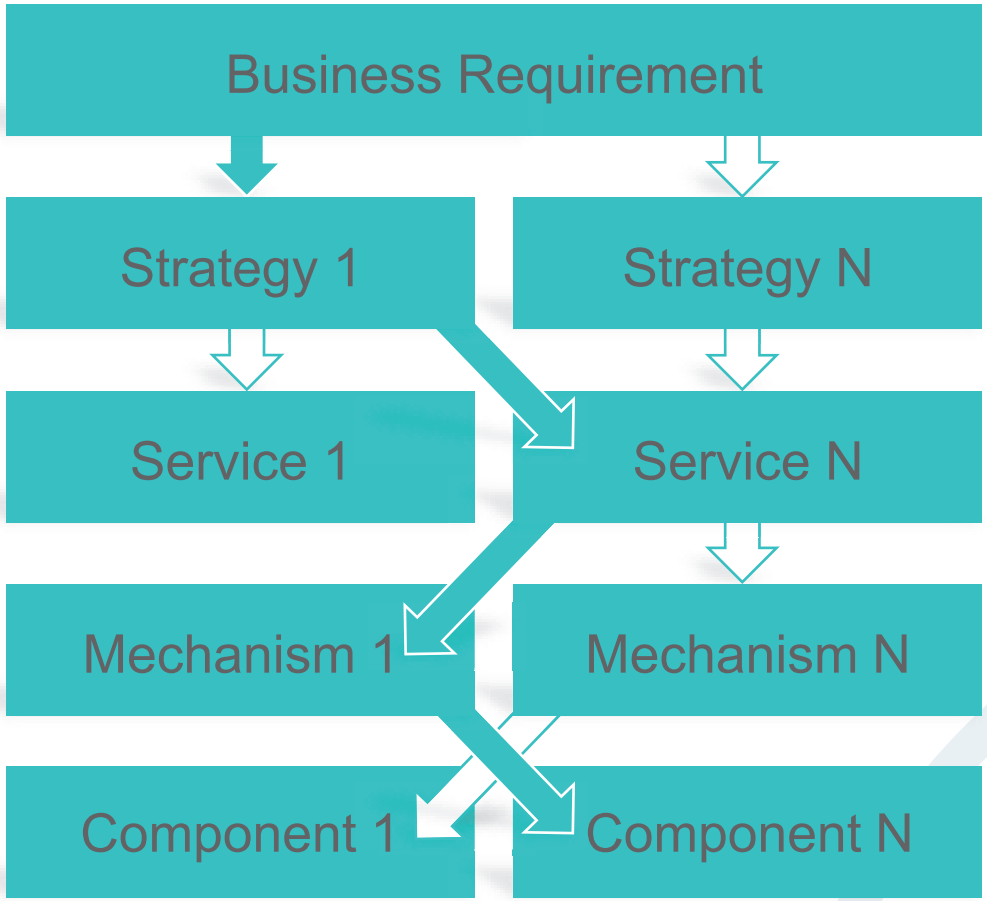
Traceability for Justification



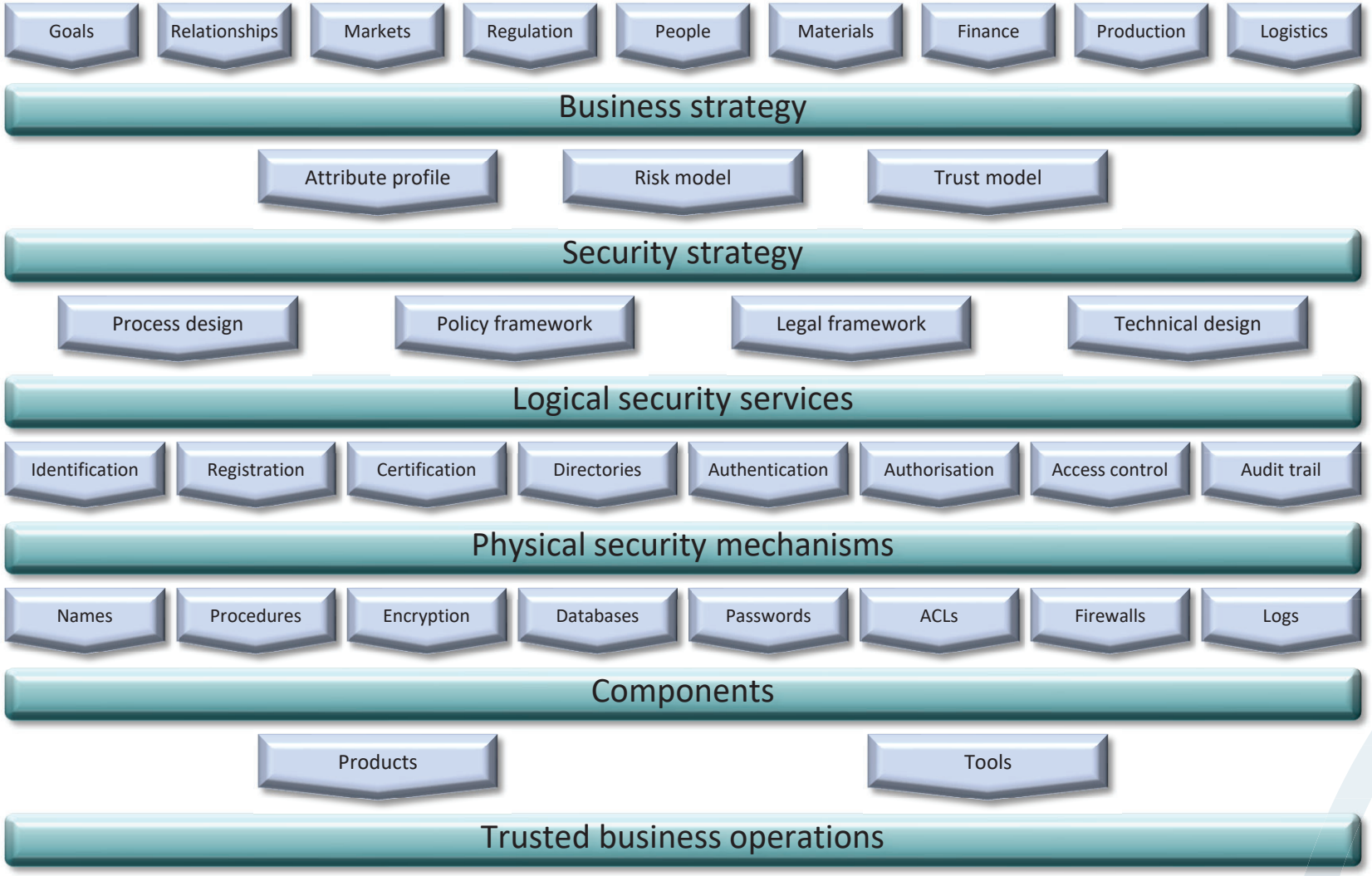
- Every operational or technological security element can be justified by reference to a risk-prioritised business requirement

Applications of the Traceability ‘Layer-map’

- Bi-directional
  - Completeness
  - Justification
- Actuarial Preservation
  - Controls
  - Enablers
- Manage Change
  - Confirm links not removed
  - Identify redundancy
- Knowledge Management
  - Re-use components
  - Predictability

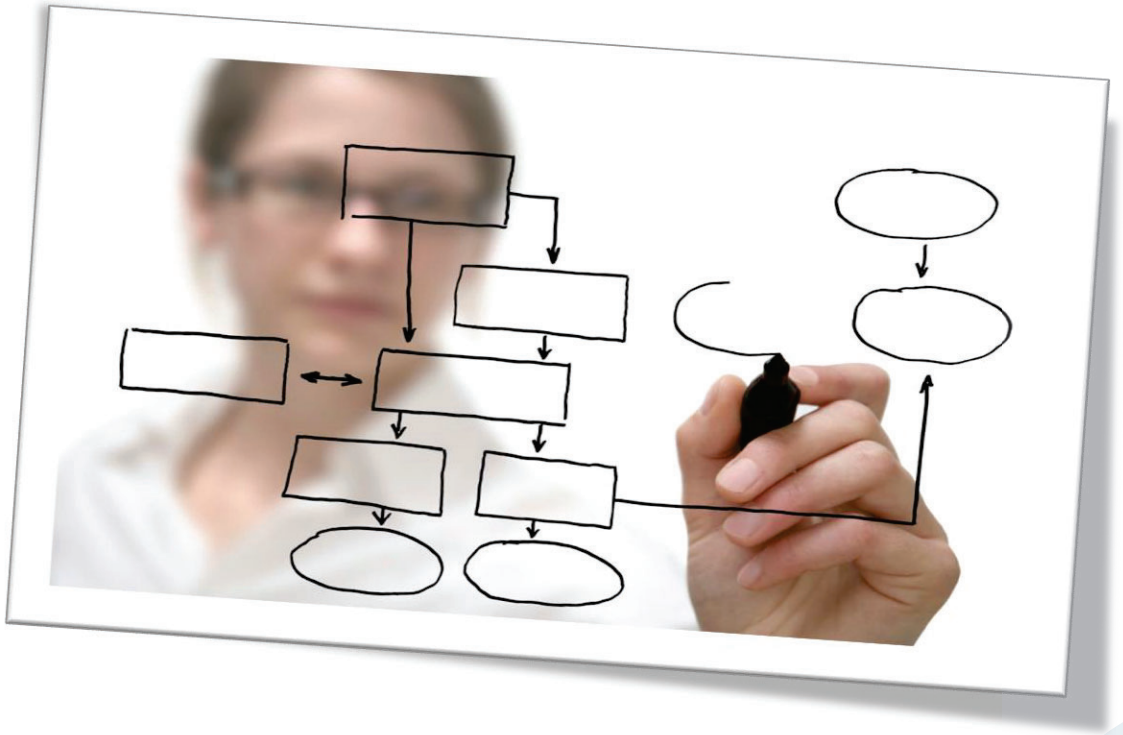


SABSA Traceable Capability for Providing Trusted Business Operations



Workshop A3-6

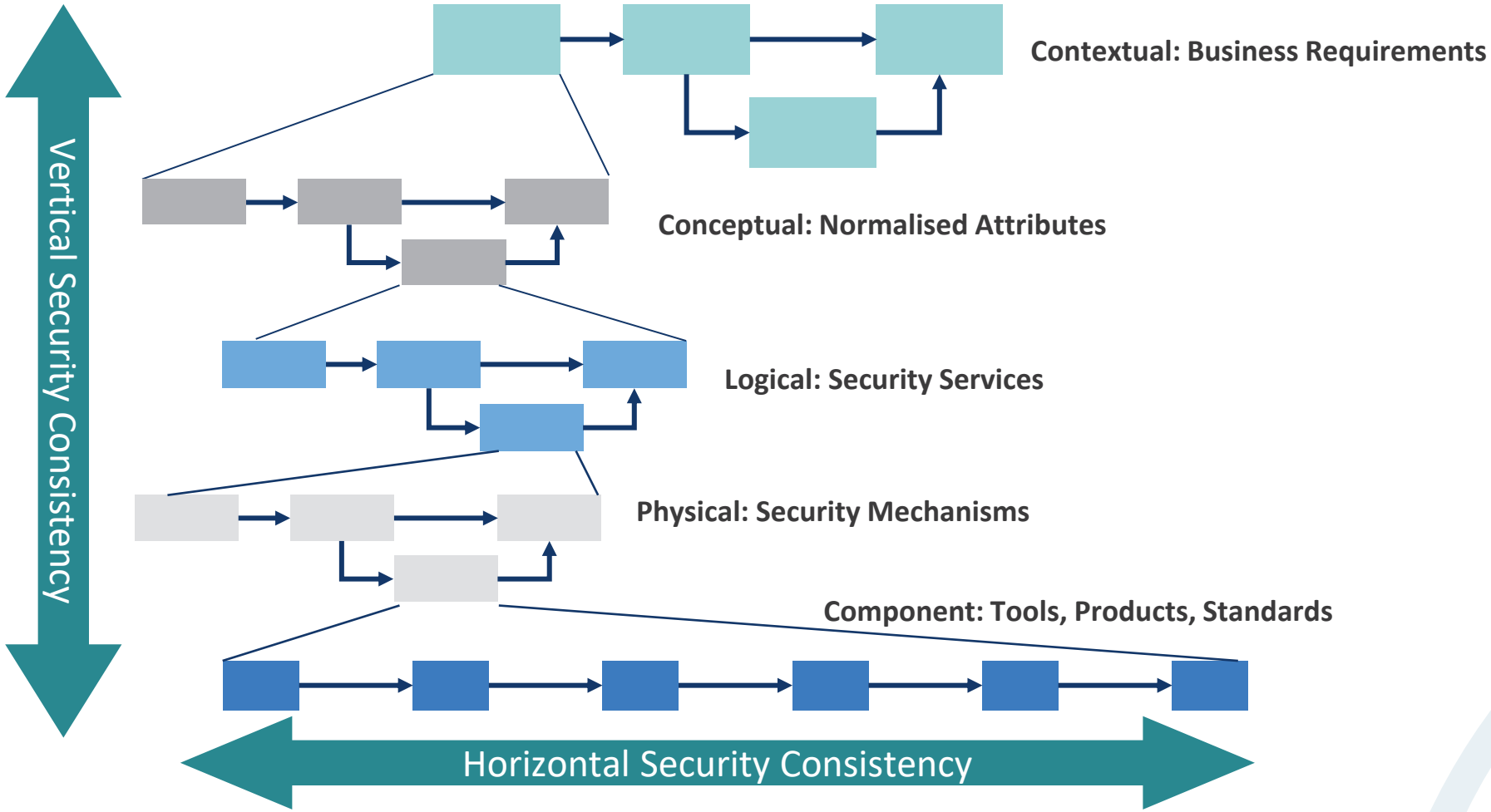
Traceability Strategy



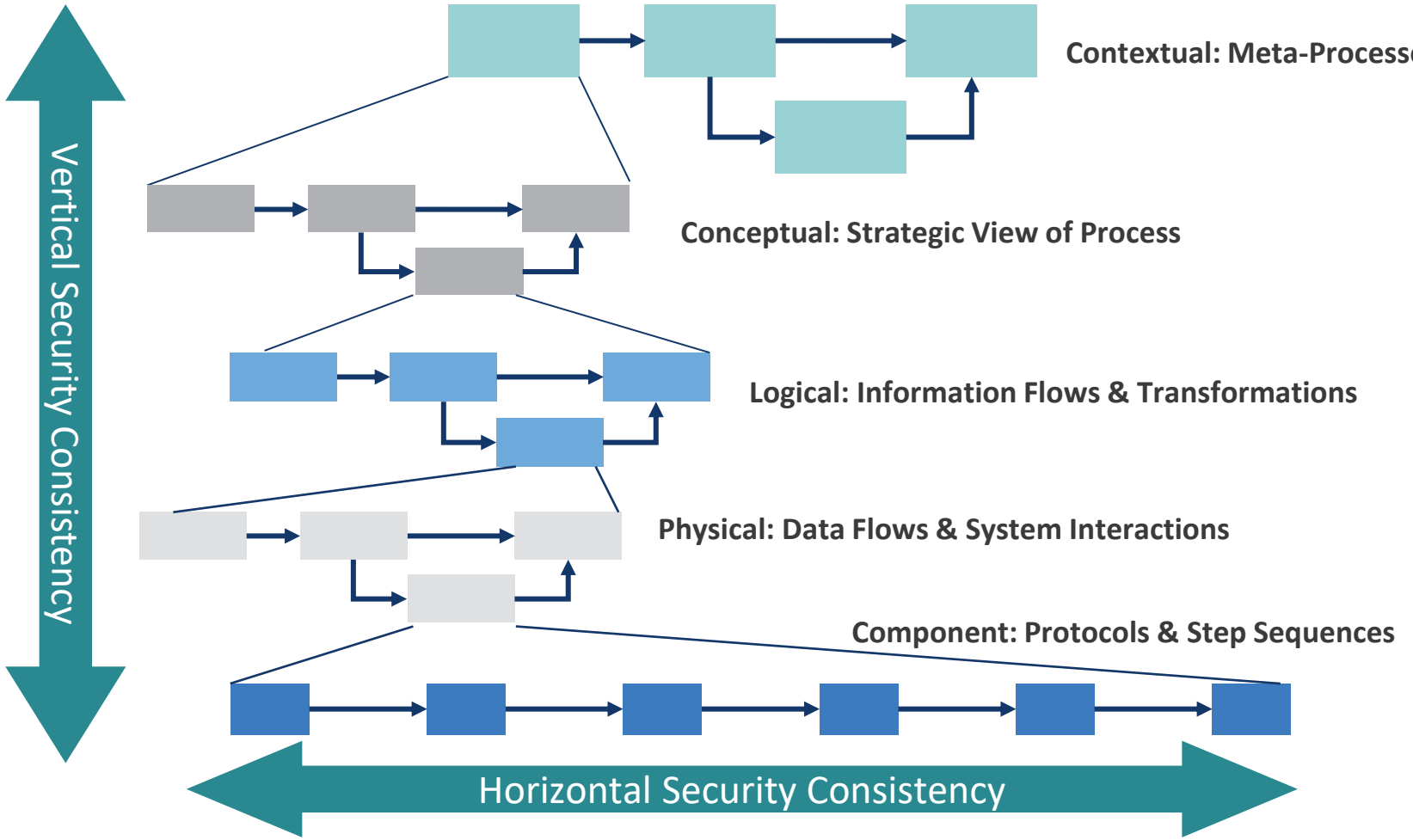
Logical Layer Engineering – Business-driven Design

Section 7

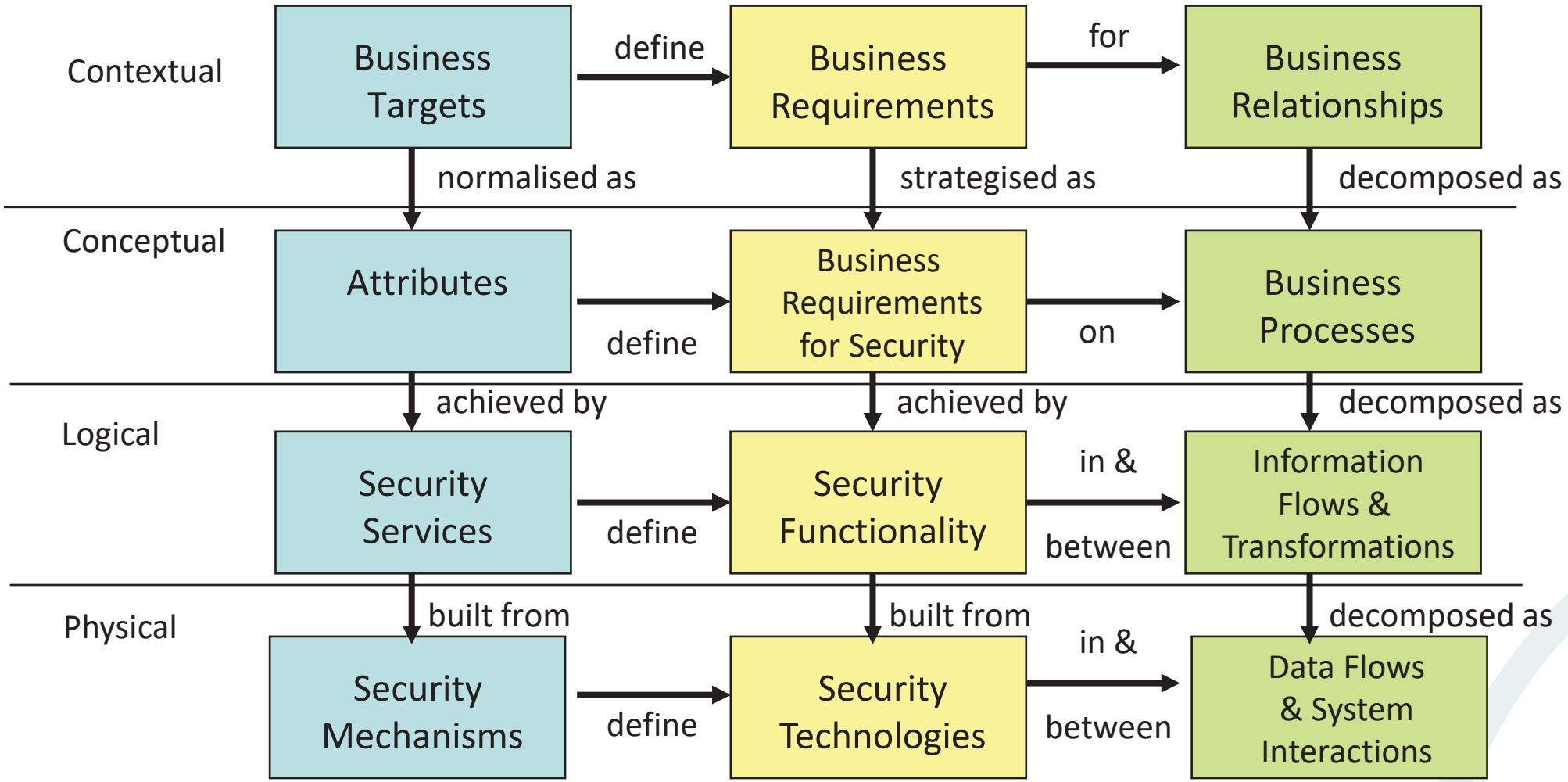
SABSA Top-down Systems Analysis



SABSA Top-down Process Analysis

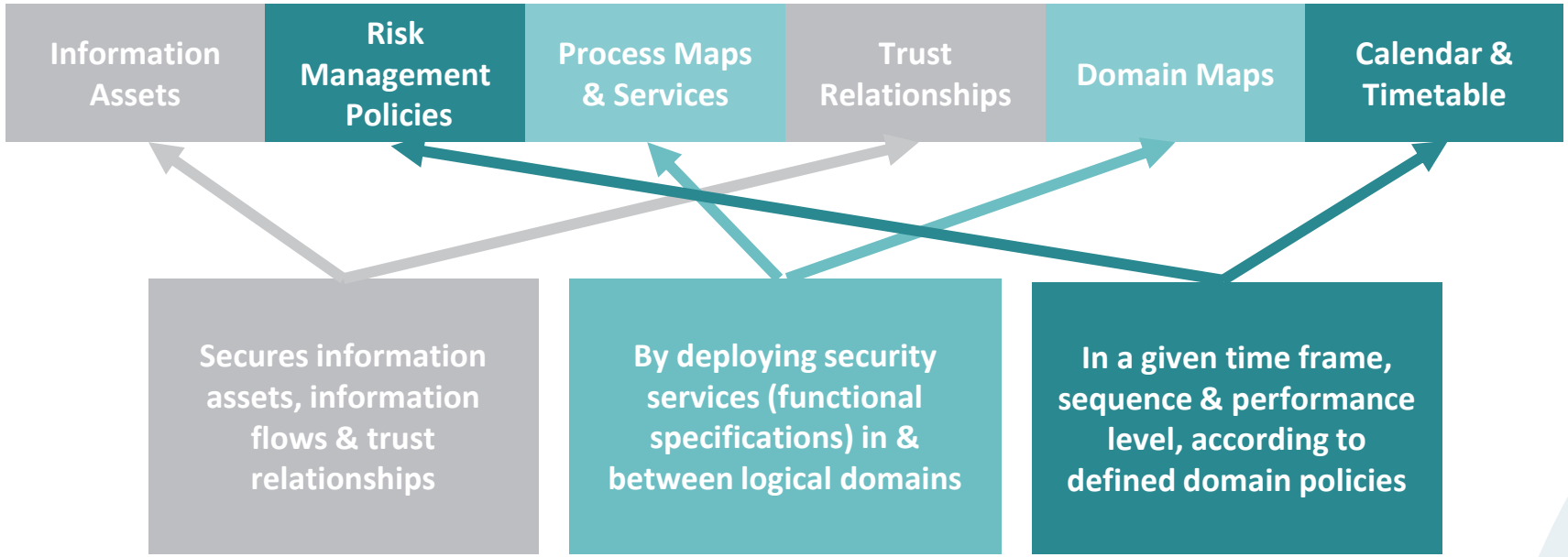


Security Relationships of Systems & Processes



Overview of the 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



Constructs & Characteristics of Assets

- Raw facts, figures & events (quantitative)
- Collected by observation & recording
- Stored in a specific location (physical)
- No context (little meaning until organised, arranged & developed)

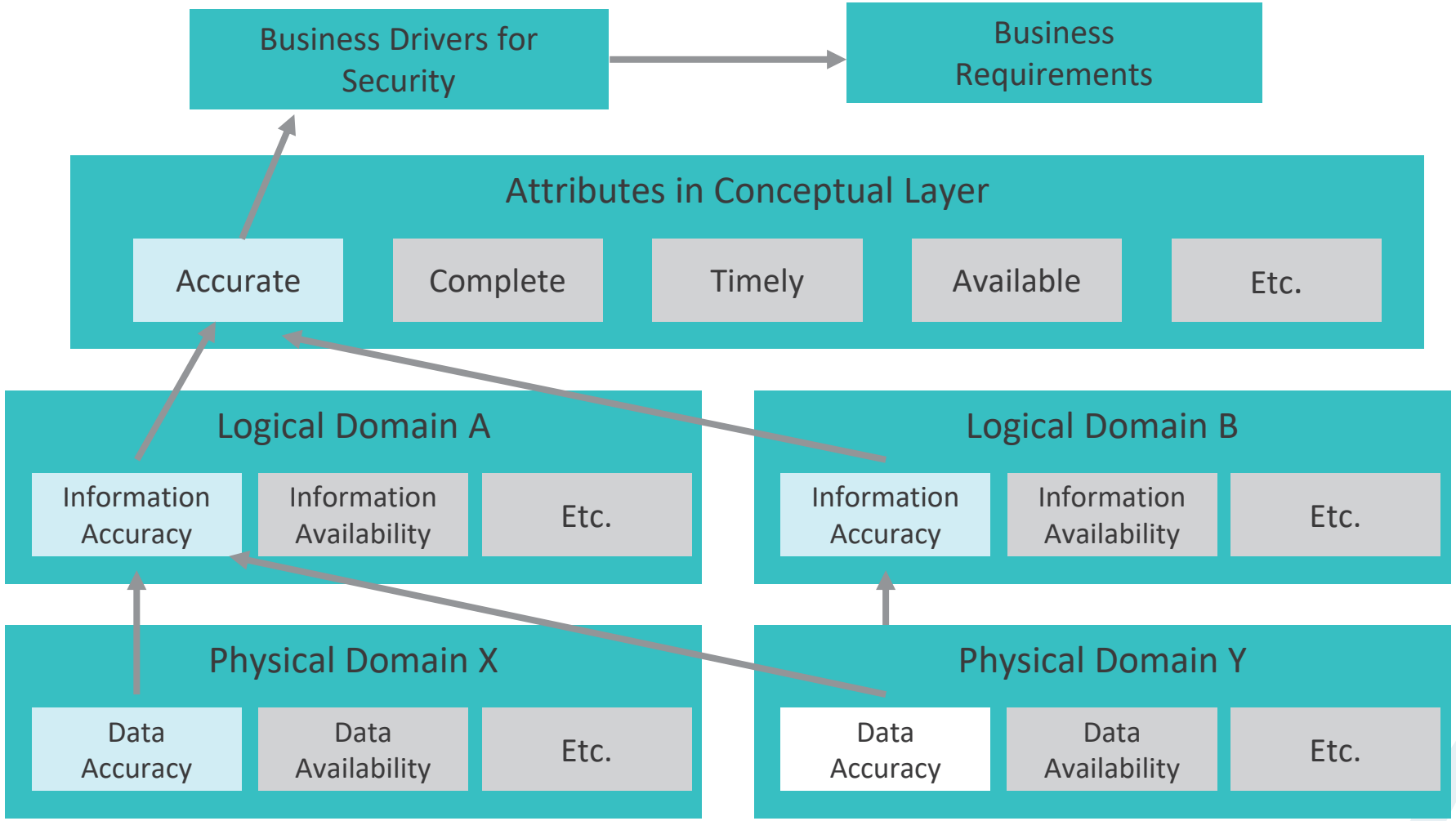
- Set of people, processes, services & resources that collects & transforms data into information and disseminates & presents this information
- The “information system” or “ICT system”

- Transformed data (qualitative)
- Created by analysis and structured presentation of data
- Virtual (logical) – not stored in a specific location
- Context (has meaning through organisation & presentation)

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

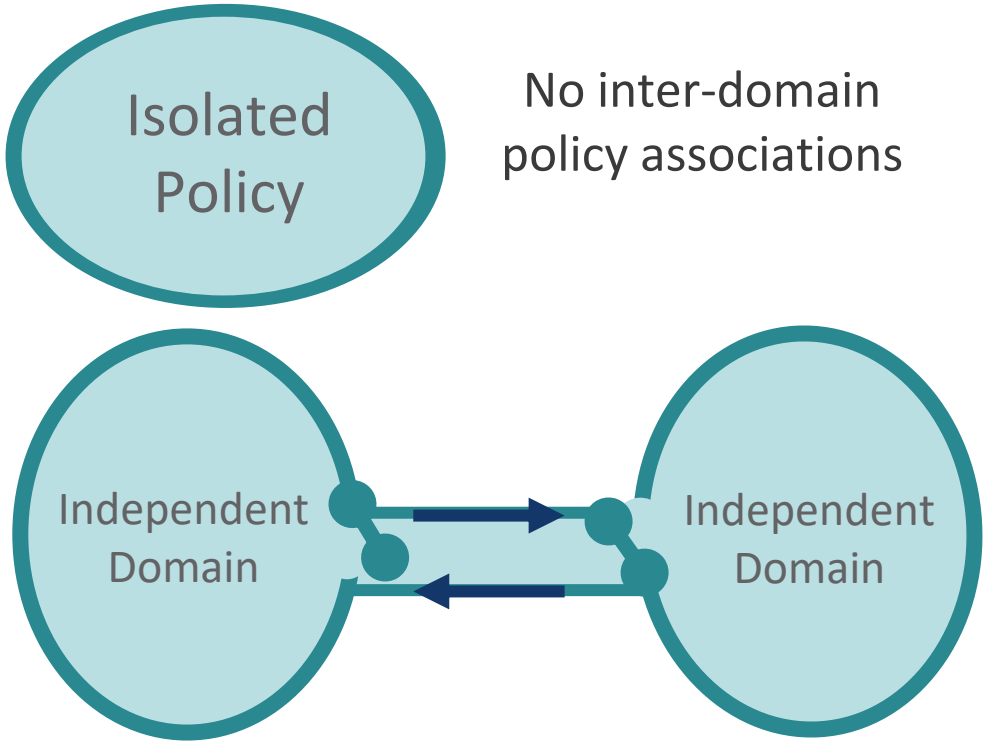
Relationship With Conceptual Assets



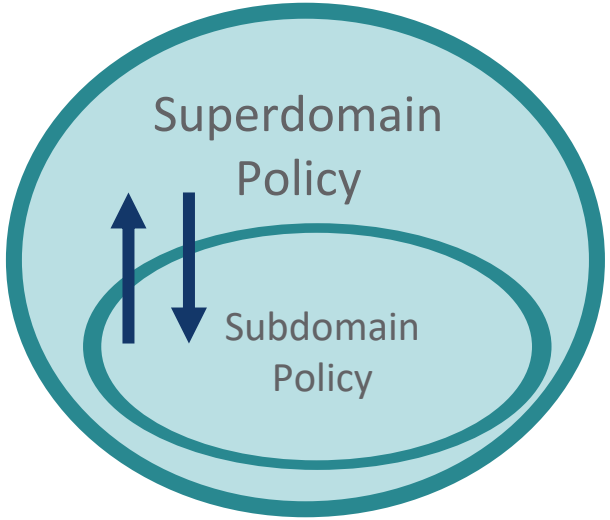
Logical Security Domains

- A logical domain is a set of logical elements (virtual or without specific physical location) subject to a common security policy defined and owned by a single security policy authority
  - Line of business, community of users, information classification, application, etc.
- Logical domains are segregated logically
  - Logical access control services

Simple Inter-domain Policy Associations

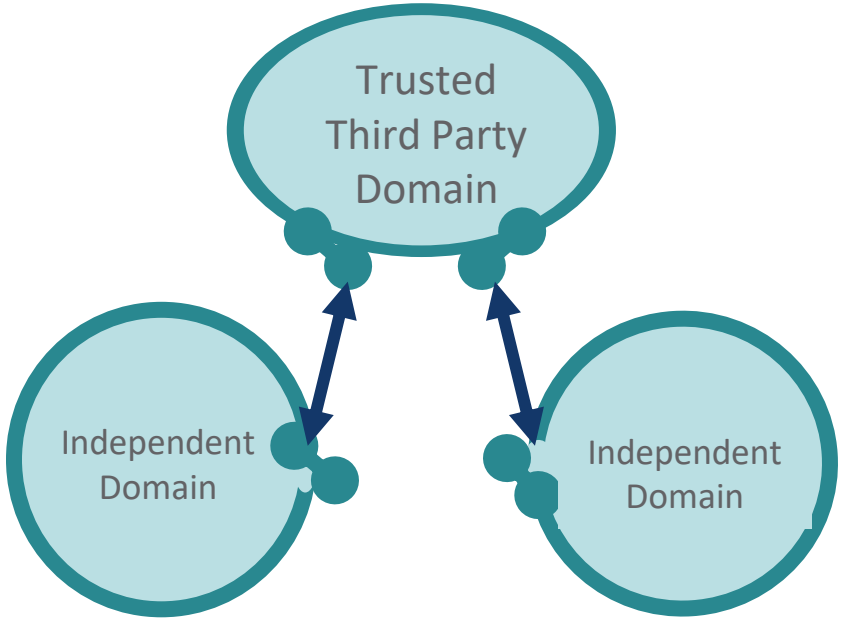


Each independent domain authority manages their own risk by enforcing their own policy (inbound & outbound) at the boundary / gateway

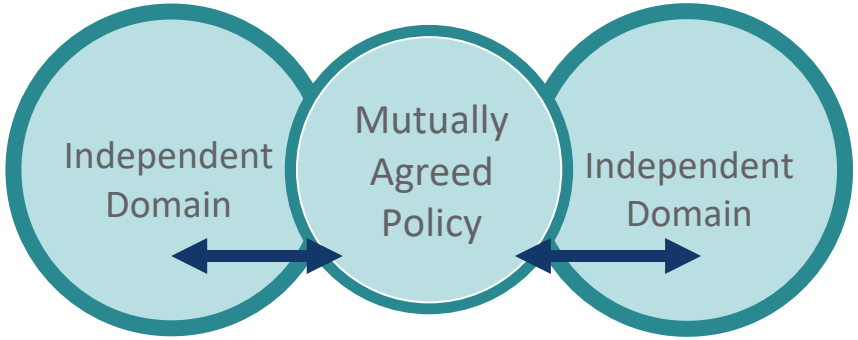


Subdomain policy is derived from, and compliant with, super domain but has specialised local interpretation authorised by super domain authority

Complex Inter-domain Policy Associations

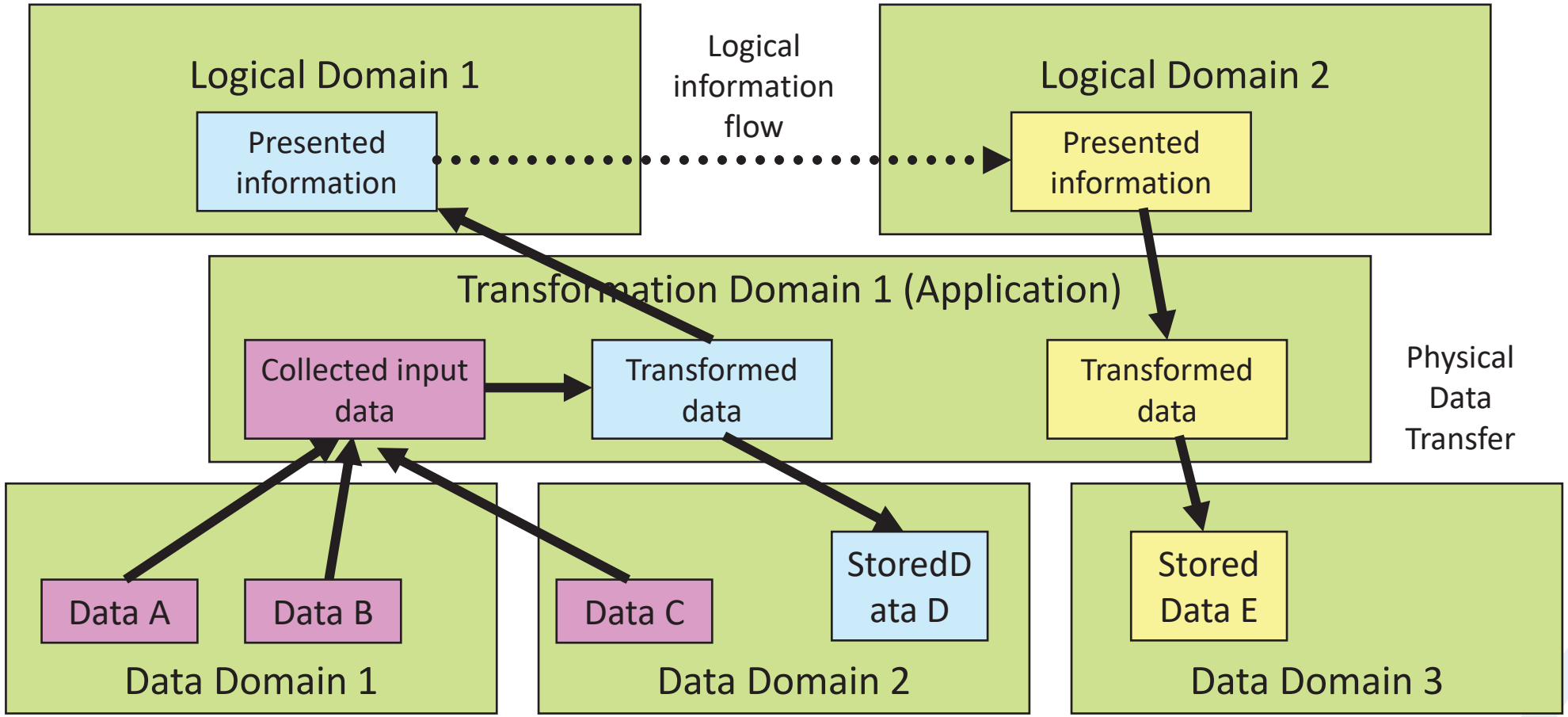


A special type of subdomain: the Trusted Third-Party mandates policy for all associations – no local interpretation is permitted

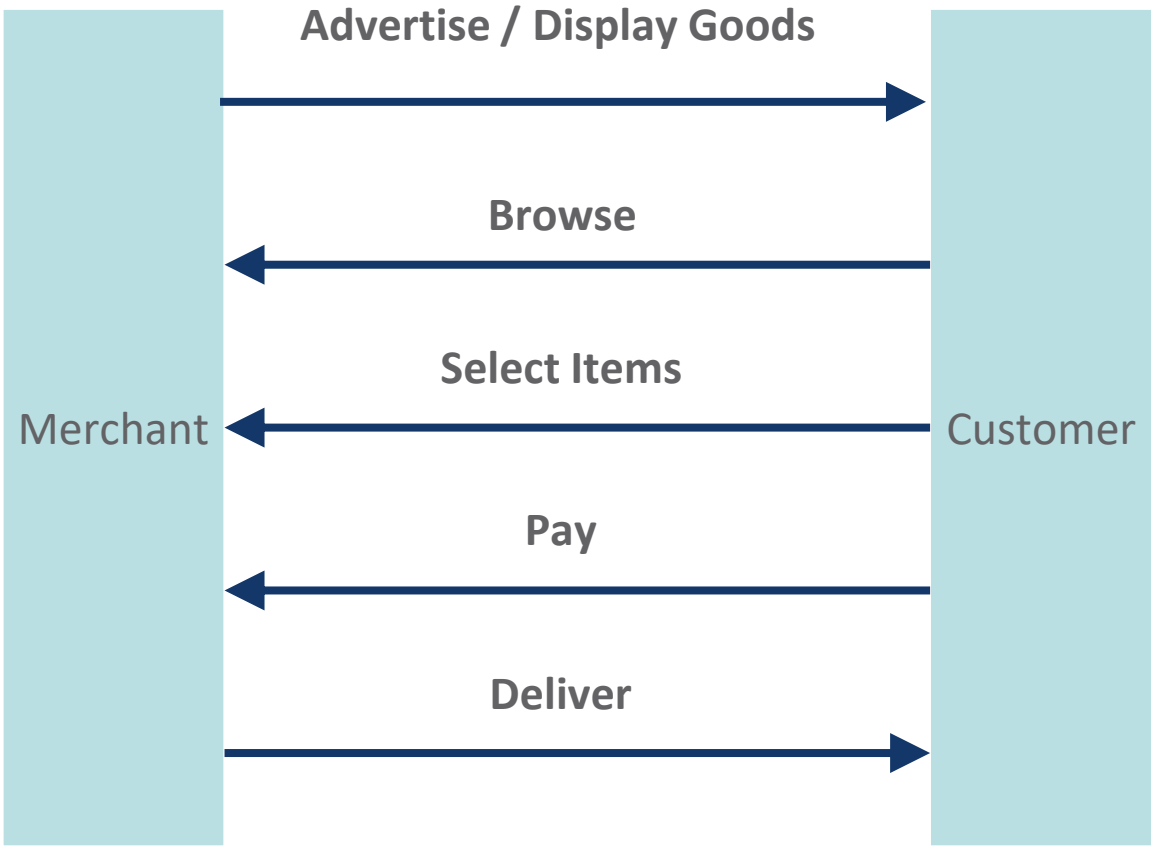


The two independent domain authorities act collectively to agree / negotiate a common policy for a shared domain. Challenging: the common policy must contain every possible circumstance and/or very specific risk conflict resolution processes & procedures

Information Flows & Transformations



Logical Process Flow Viewpoint

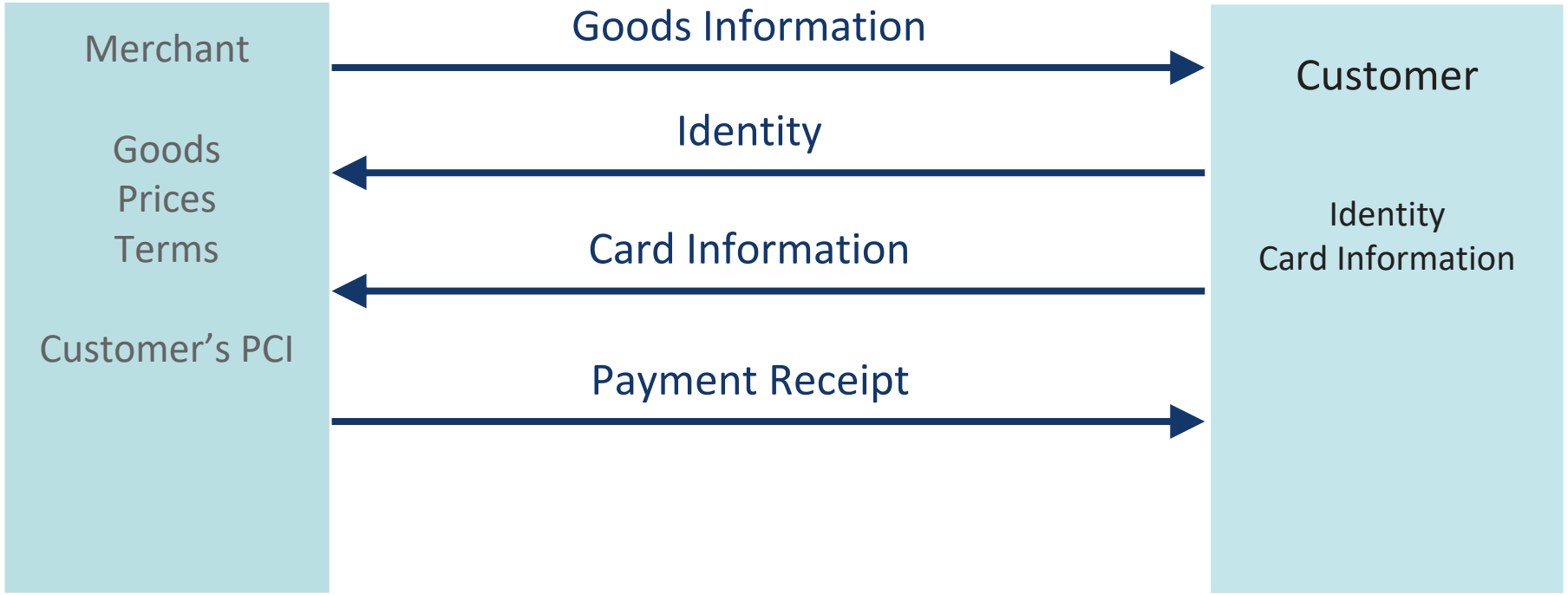


What needs to be protected here?
What is the 'security' that we require?
What function does it serve?

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?

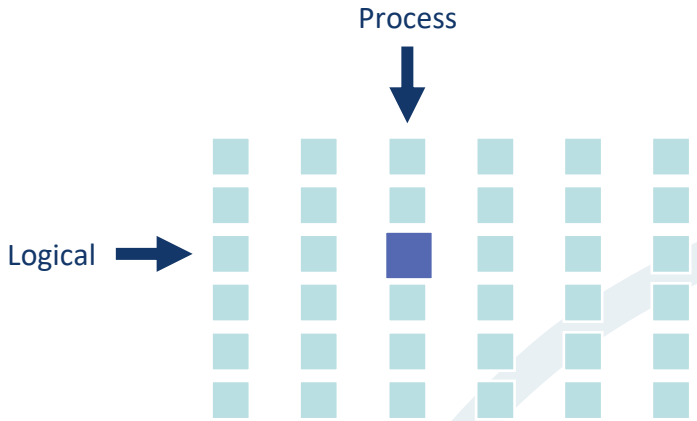
Logical Information Flow Viewpoint



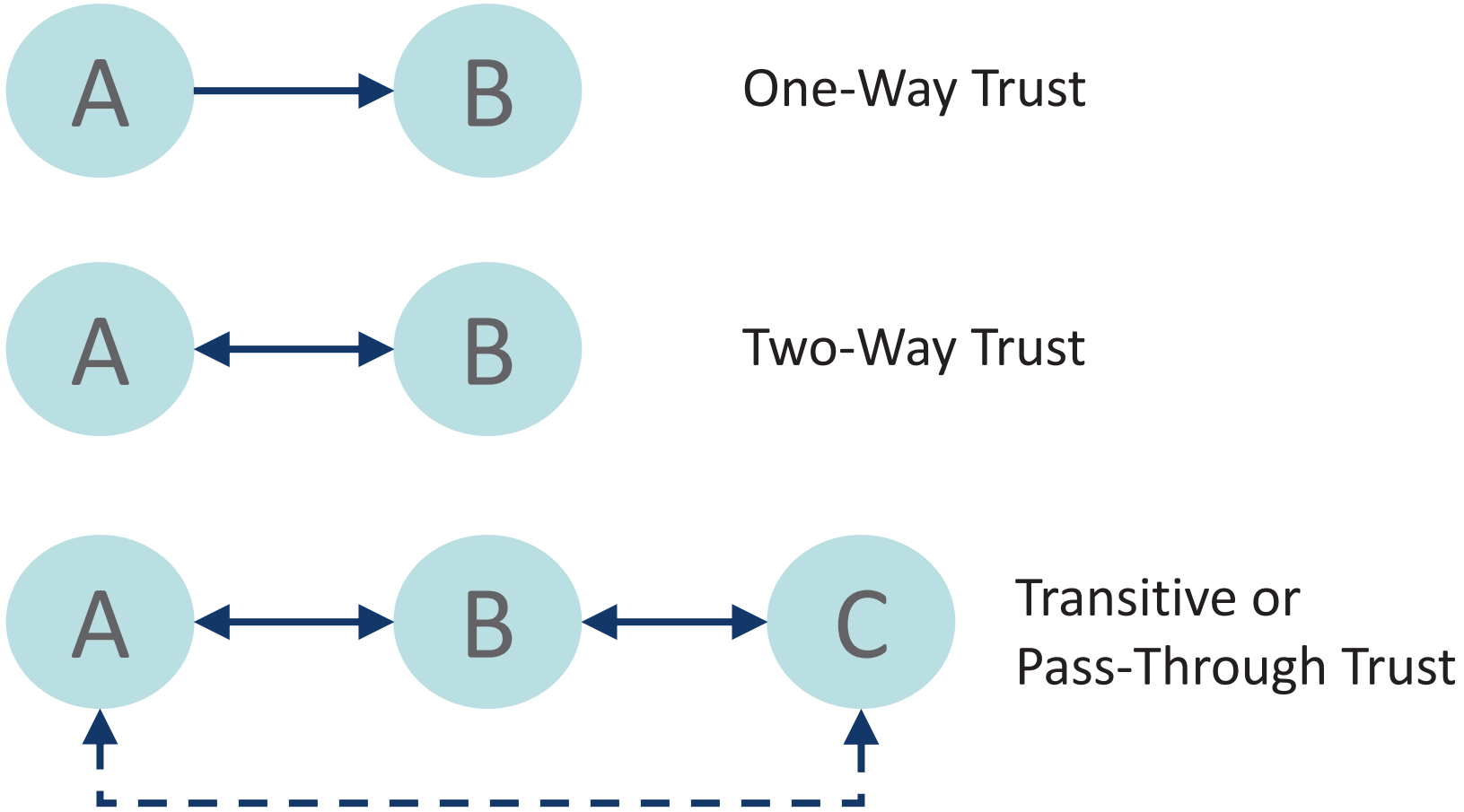
SABSA Concept of a Security Service

- 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)

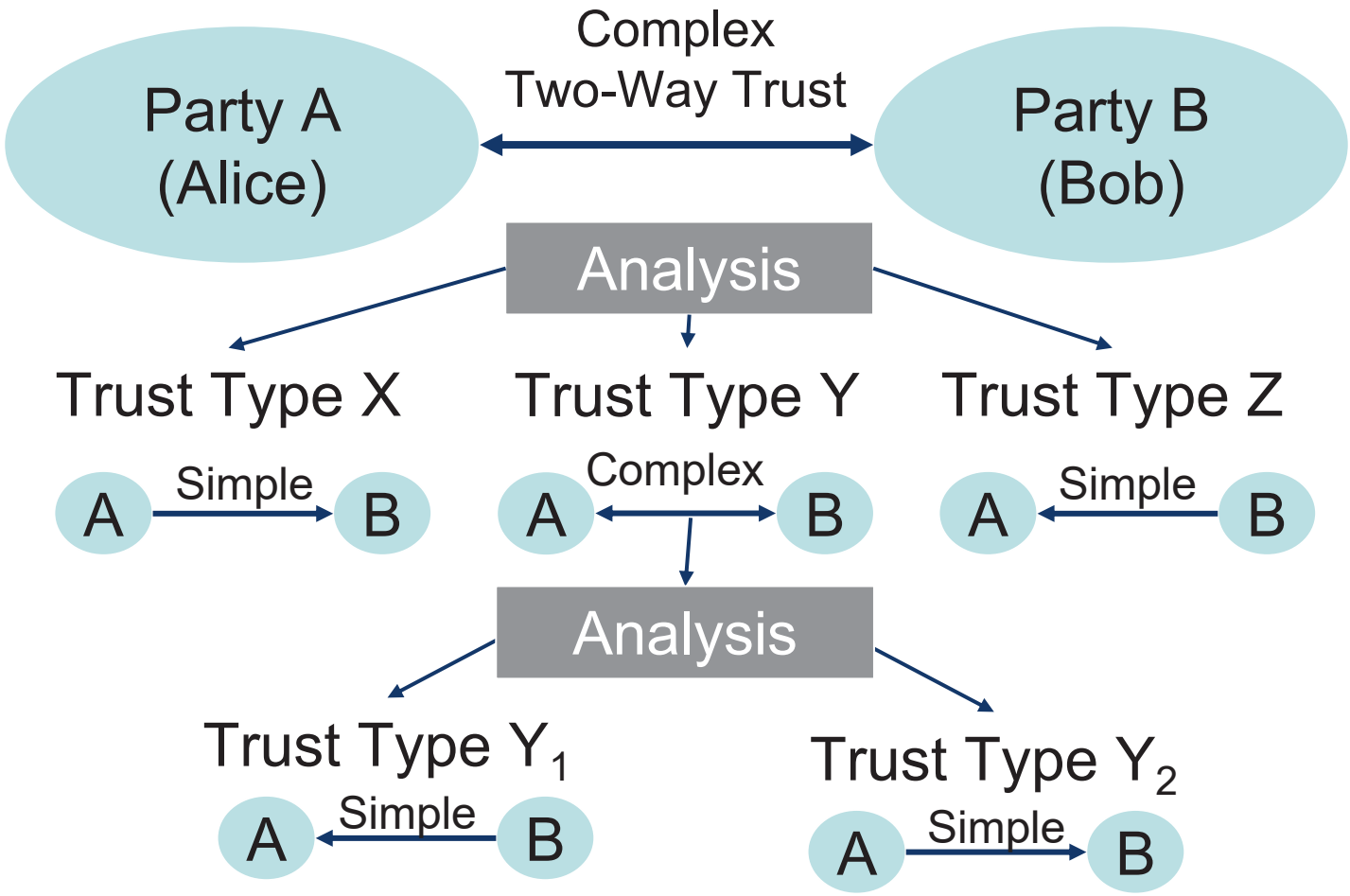
SABSA Matrix



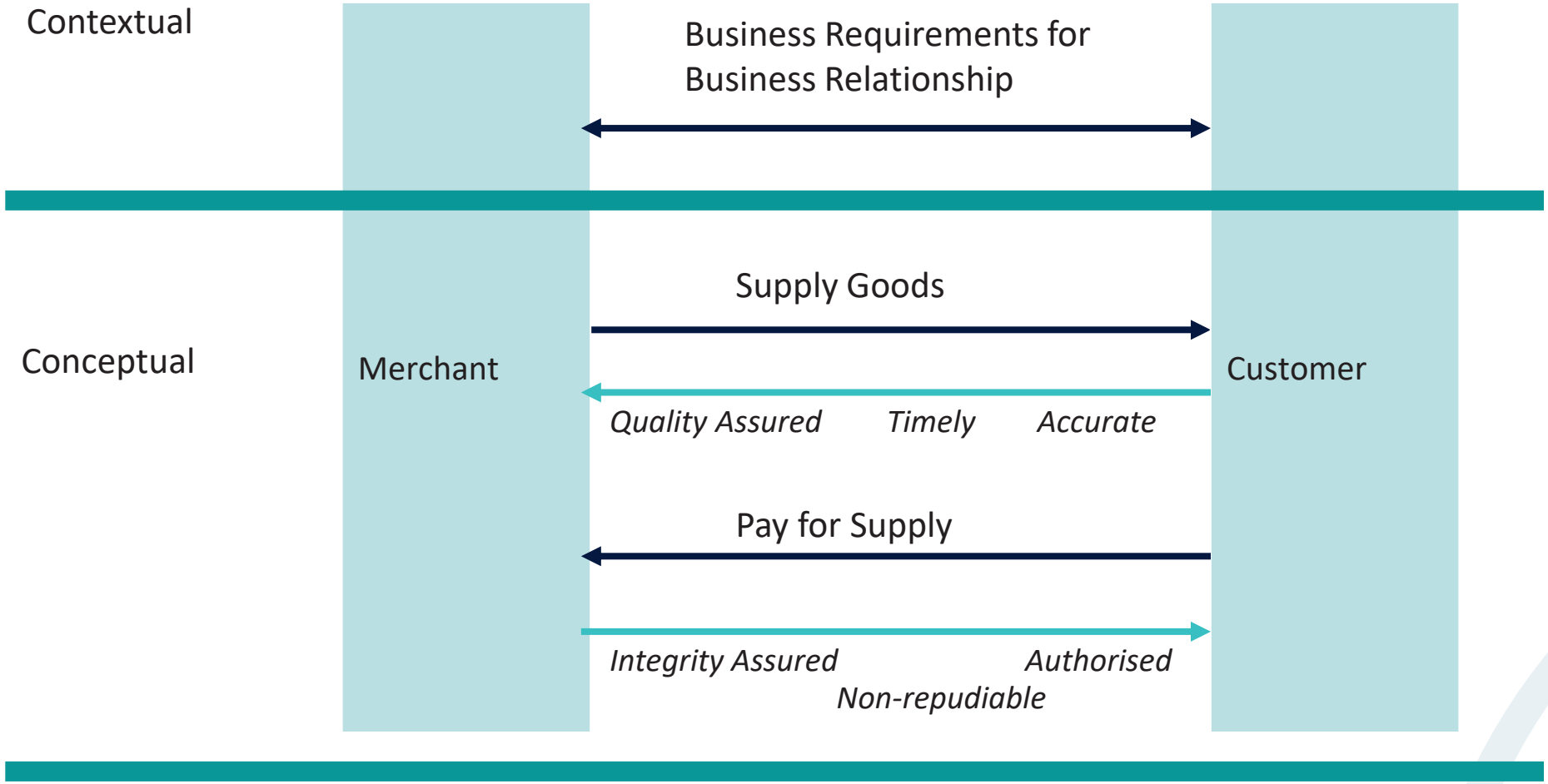
Trust Types


A
B
One-Way Trust
A
B
Two-Way Trust
A
B
C
Transitive or
Pass-Through Trust

Decomposition of Two-way Trust

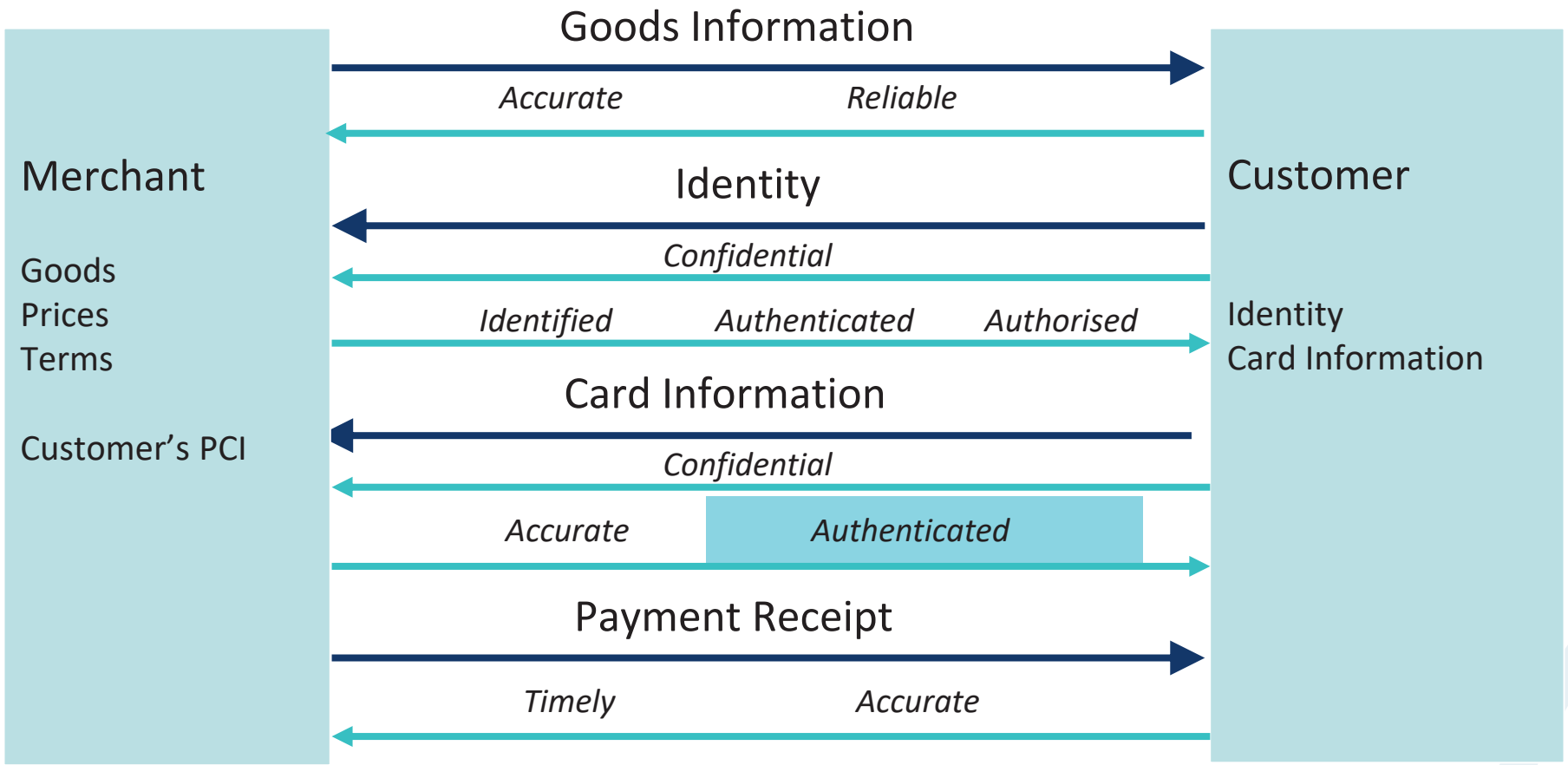


Trust Model Decomposition



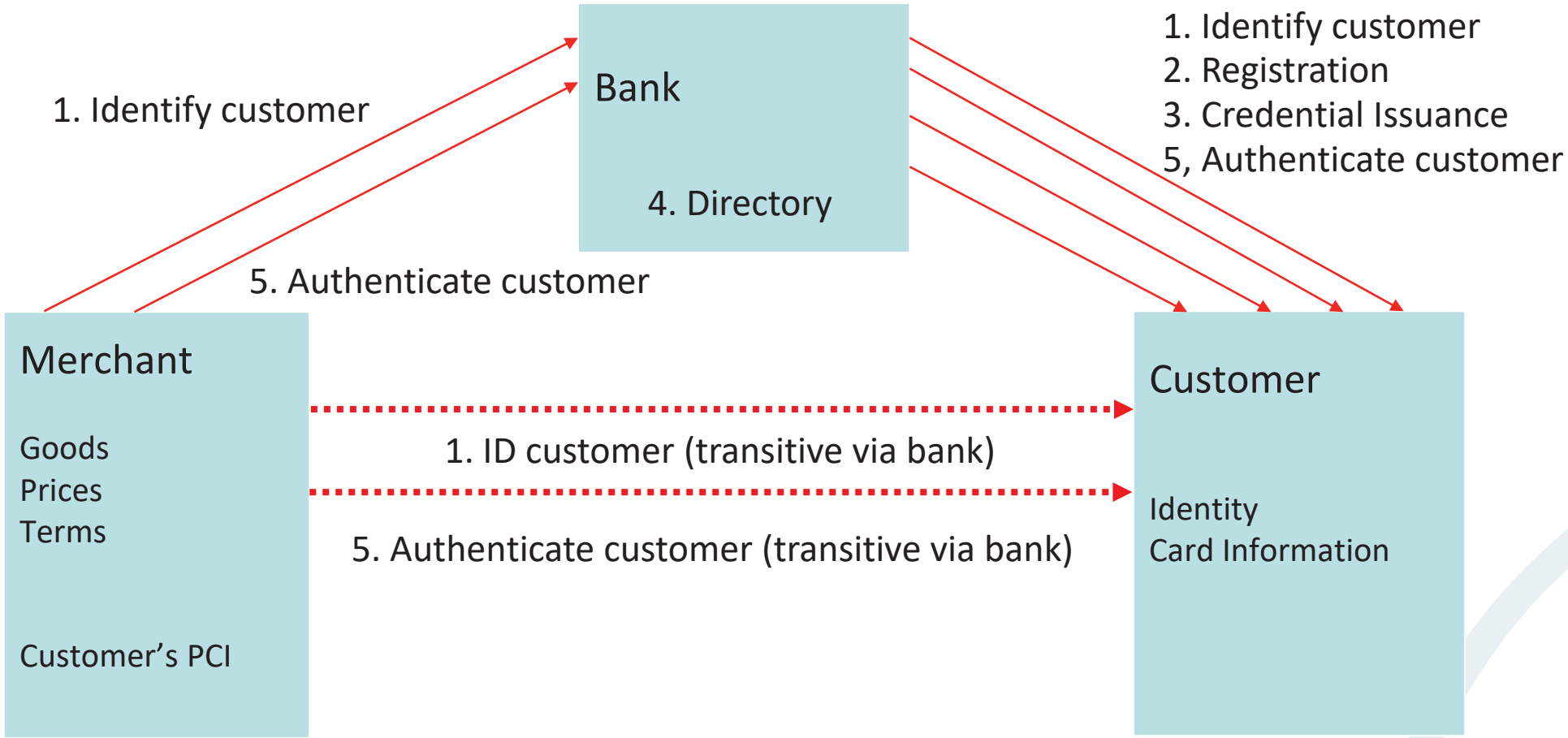
Trust Model Decomposition

Logical Decomposition – Attributes to Information Flows



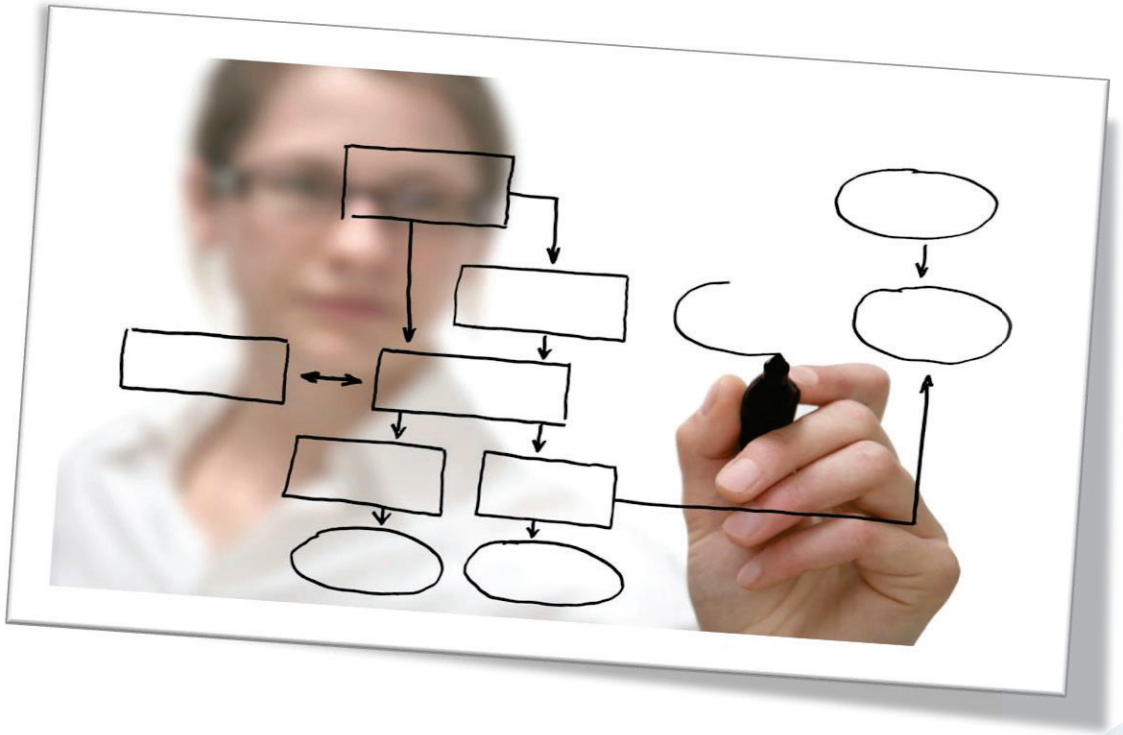
Trust Model Decomposition

Logical Decomposition – Attributes to Services



Workshop A3-7

Logical Layer Design



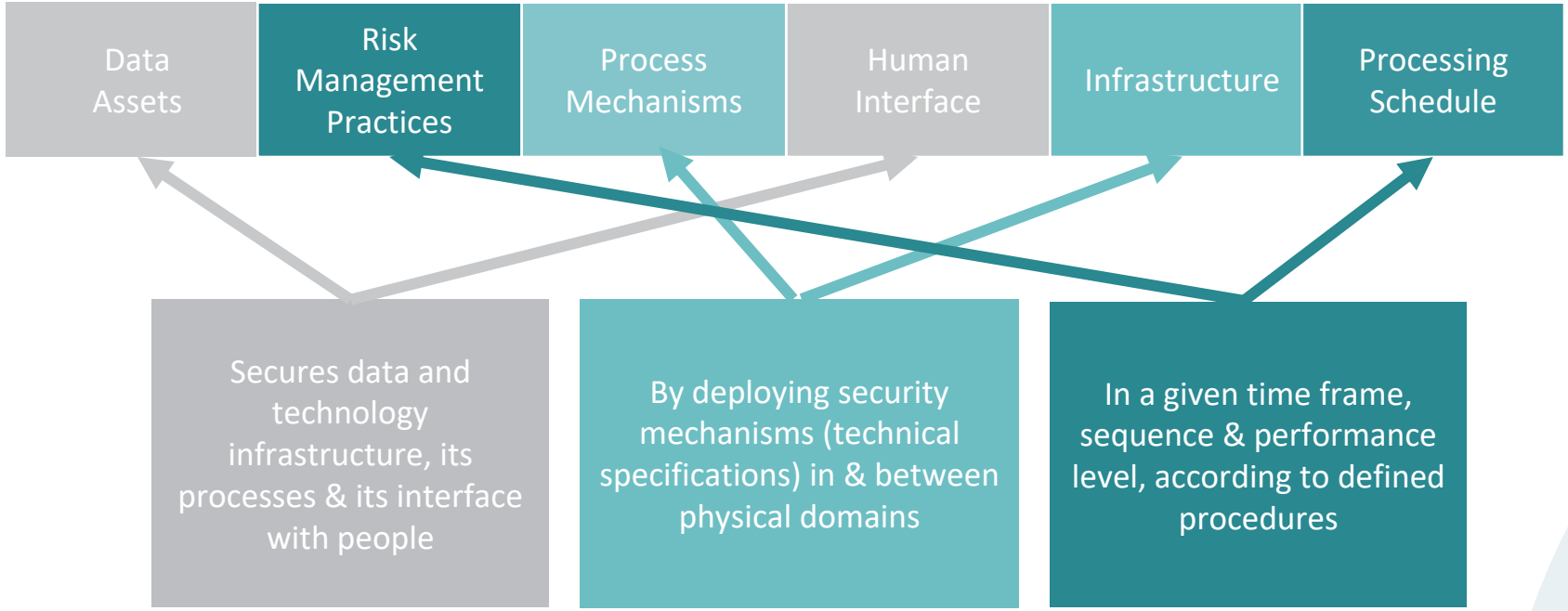
Physical Layer Engineering – Business-driven Solution Design

Section 8

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

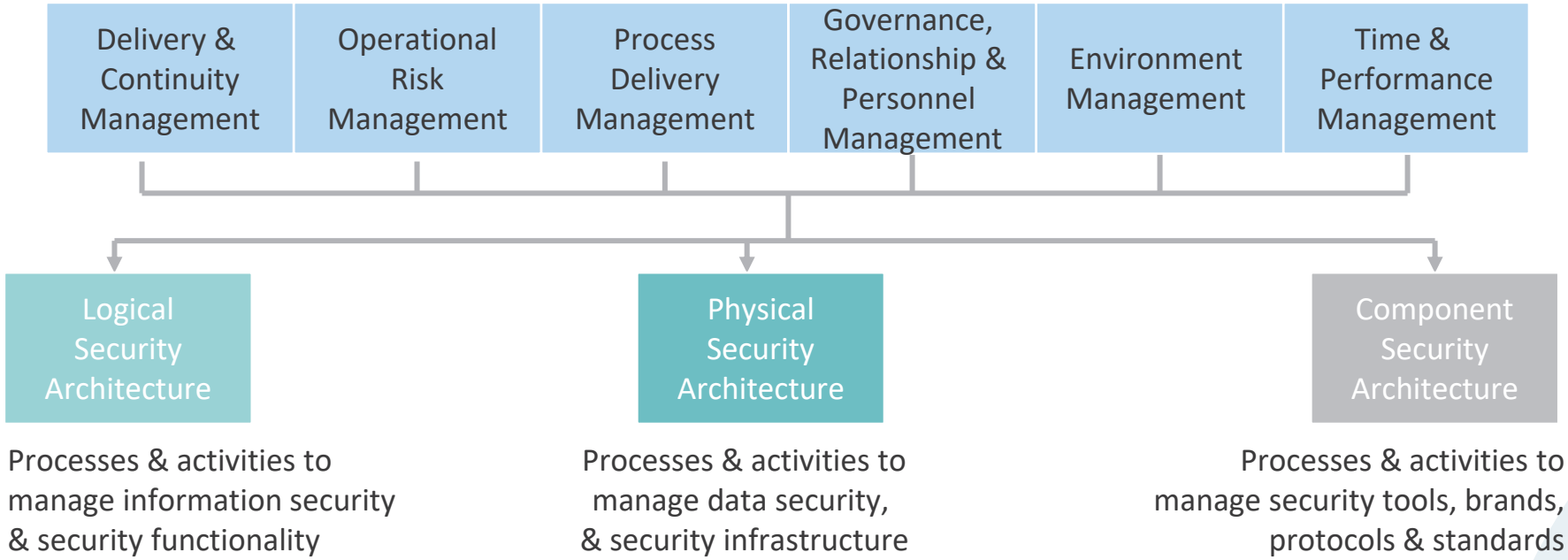
- Components are the Tradesman's View of ICT Systems
- Specialised
  - Tools
  - Brands
  - Specific granular technical specifications & standards
  - Protocols

Component Assets	Risk Management Components & Standards	Process Components & Standards	Human Entities: Components & Standards	Locator Components & Standards	Step Timing & Sequencing Components and Standards

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



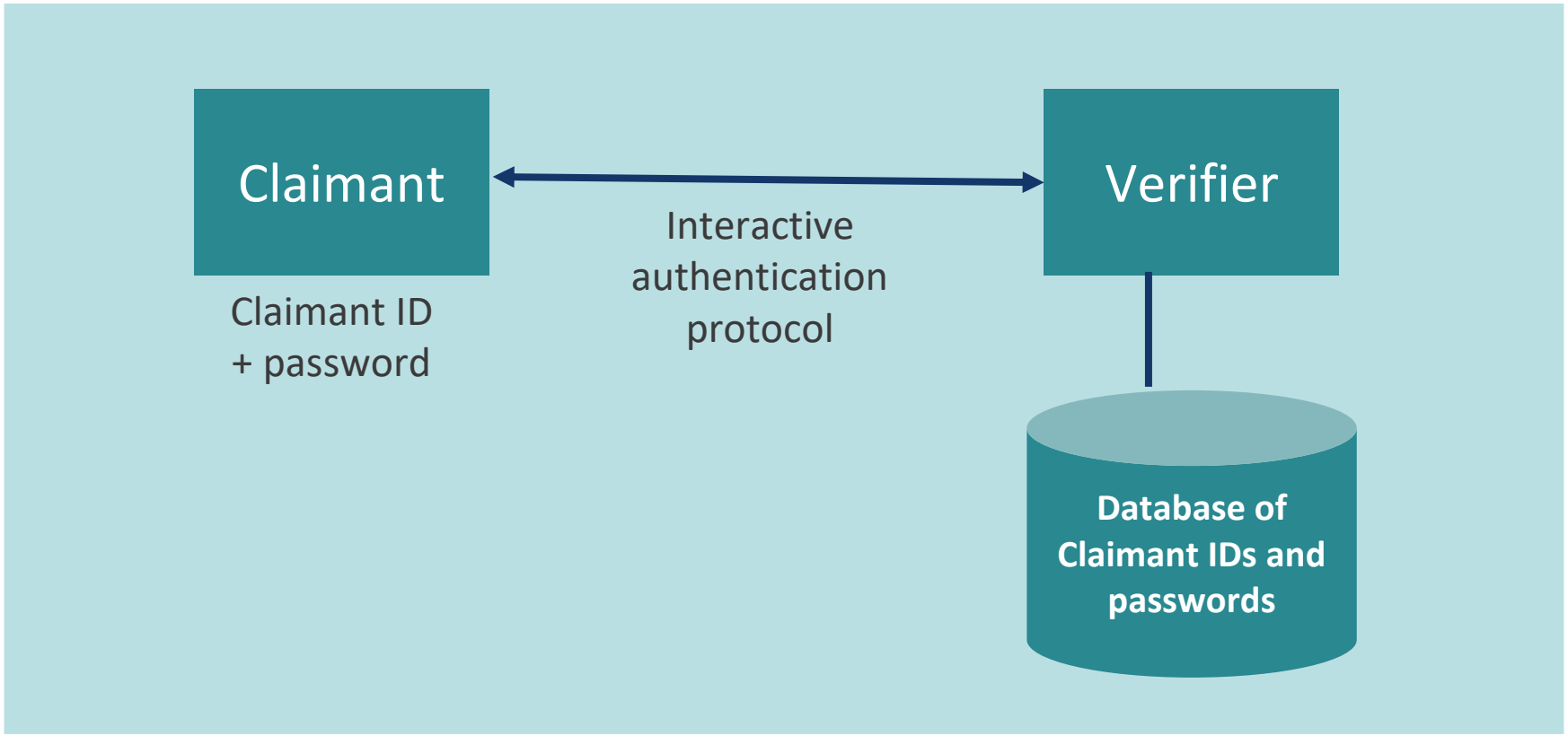
Physical Security Domains

- A physical domain is a set of physical elements (in a specific physical location or technology layer) subject to a common security policy defined and owned by a single security policy authority
  - Territory, site, building, platform, network, system classification, etc.
- Physical domains are segregated physically
  - Borders, fences, doors, firewalls, etc.

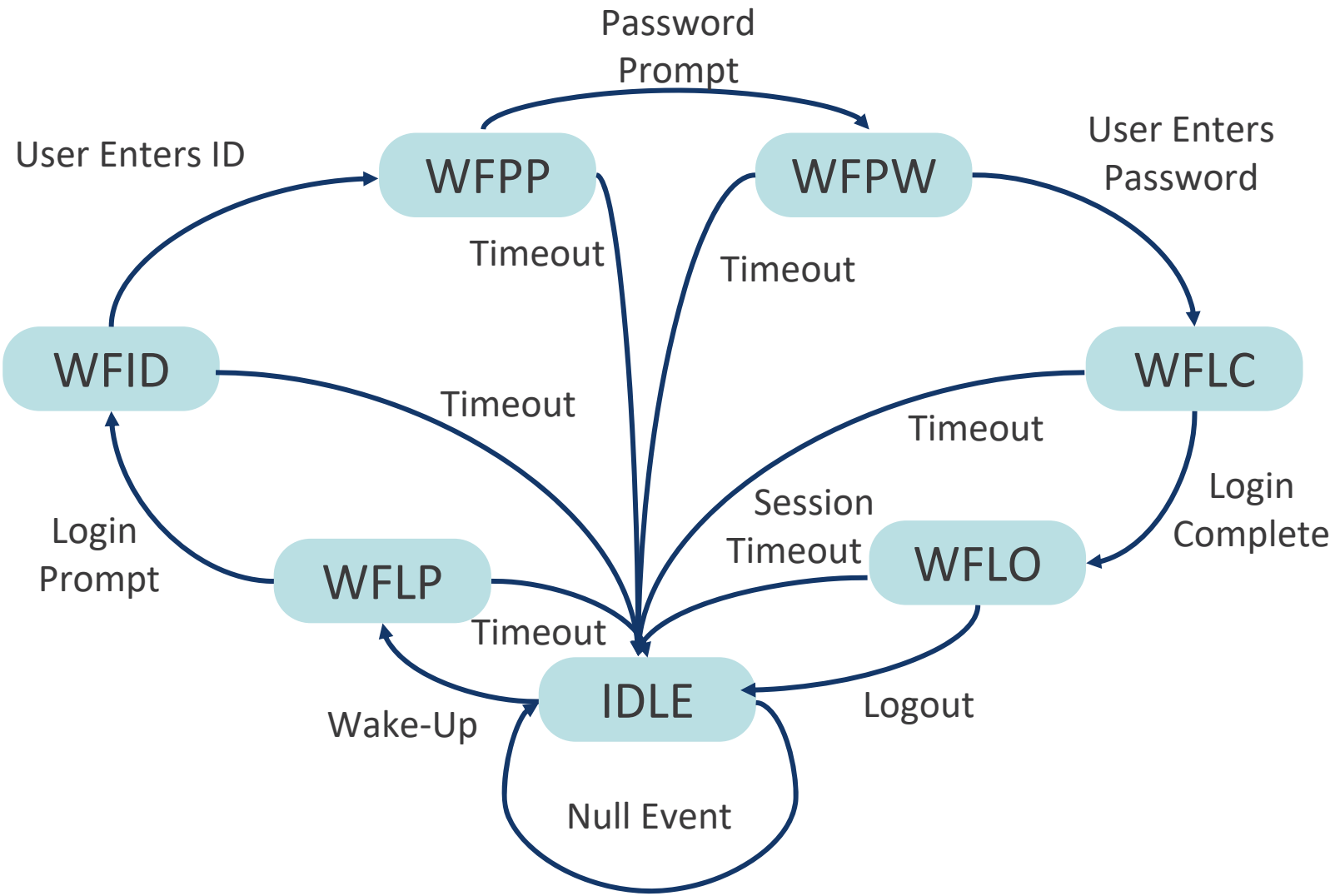
Security Processing Cycle

- 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

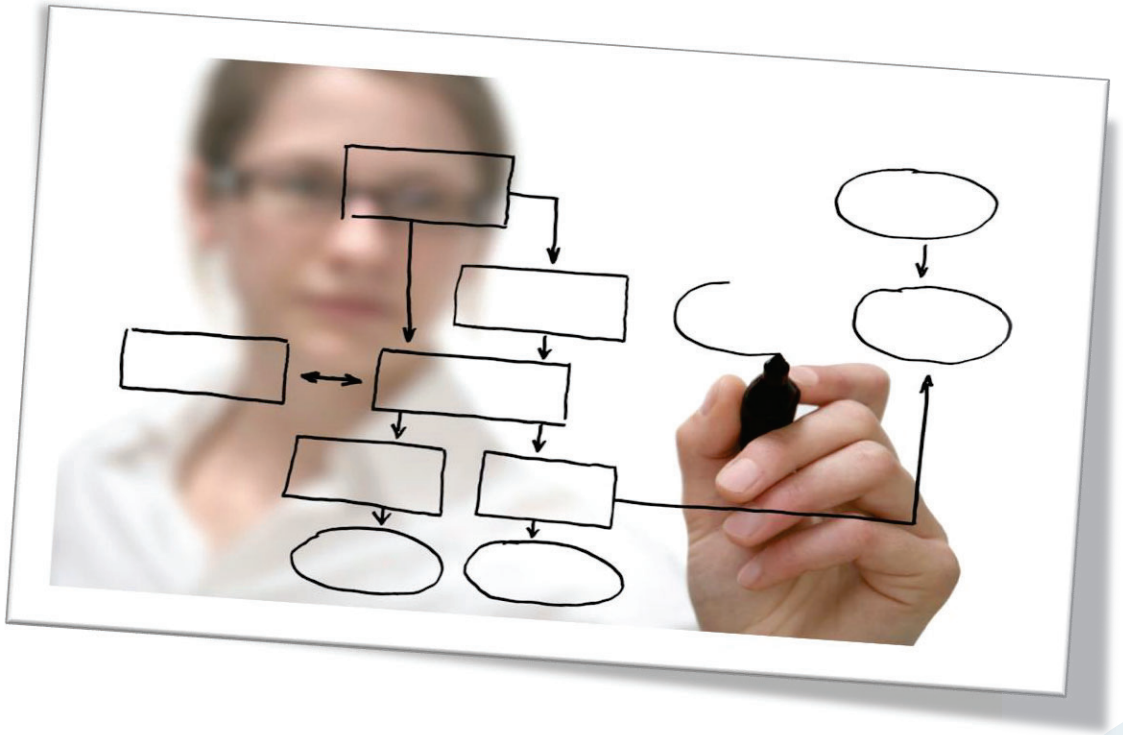


Finite State Machine Model



Workshop A3-8

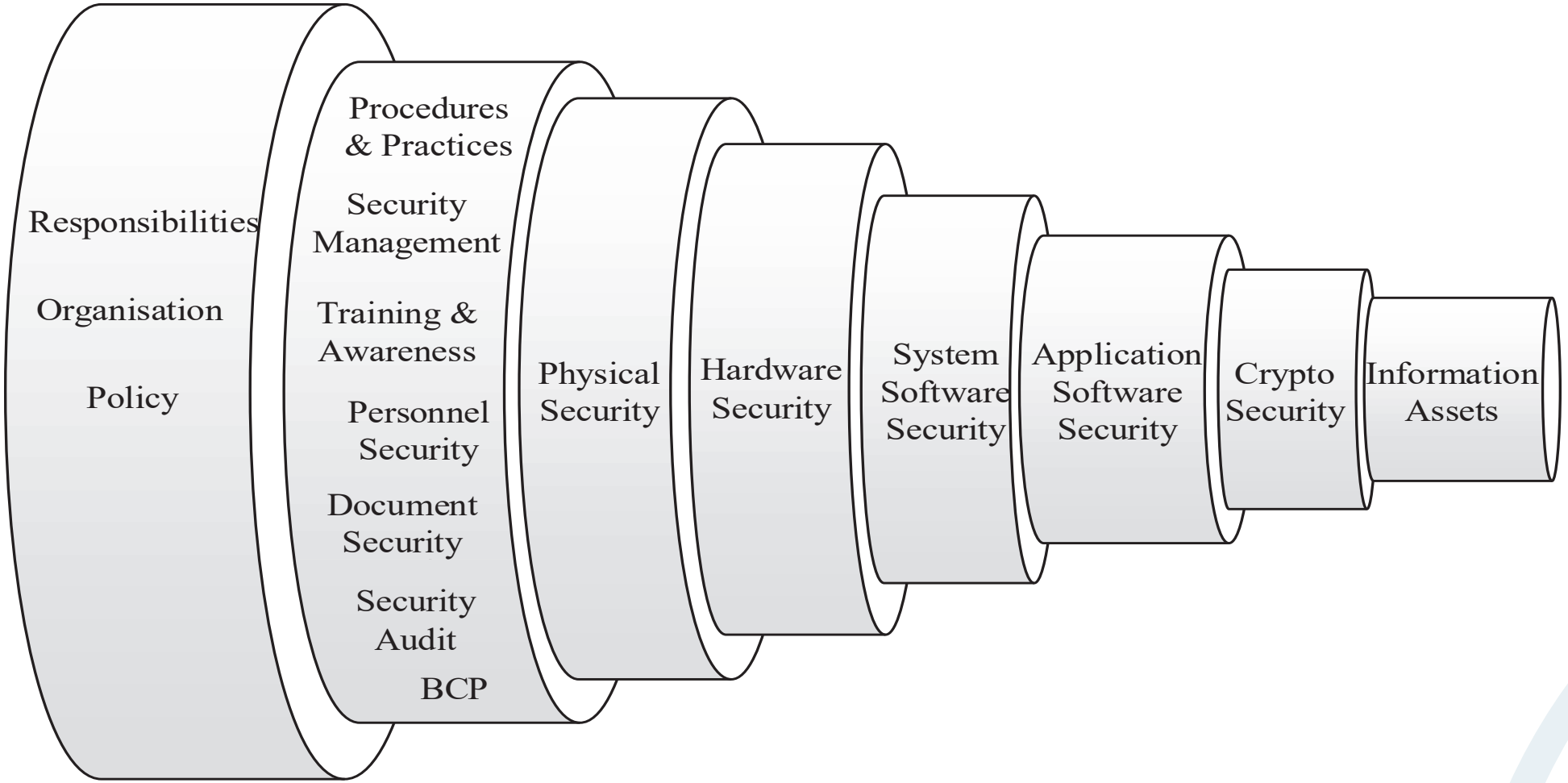
Physical Layer Solution Engineering



Engineering the Multi-tier Control Strategy

Section 9

Generic Defence in Depth Layering

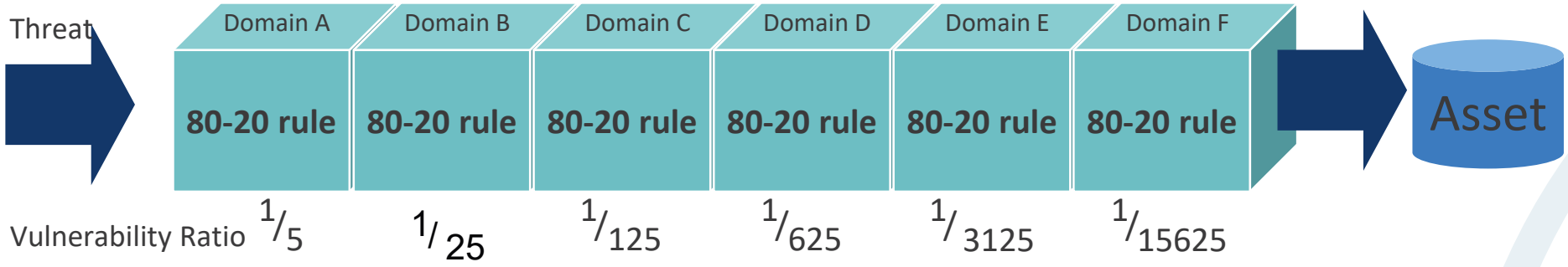


Strength-in-Depth Controls Models

- SABSA has no controls library (standard set of controls or control objectives) of its own
- However, controls are architected within the framework (slides 136 & 187)
- If desired, this controls architecture can fully utilise control sets from other standards
  - ISO 27001 has 11 domains of control objective
  - CobiT has 4 lifecycle-based domains of control objectives
  - NIST has 17 control domains
  - Sox, PCI, Etc.
- SABSA can incorporate and integrate any/all such defence-in-depth constructs in addition to the specific SABSA models on the following slides

SABSA Defence-in-Depth Principles

- No single point of failure
- The architectural structure of the controls set improves security
  - The value of the whole is greater than the sum of the individual parts
  - Combinations of sensible measures in a collection of well designed control domains can deliver reasonable security
    - Without ‘rocket science’
    - Without over-expenditure
  - The control domain structures themselves add value to overall security

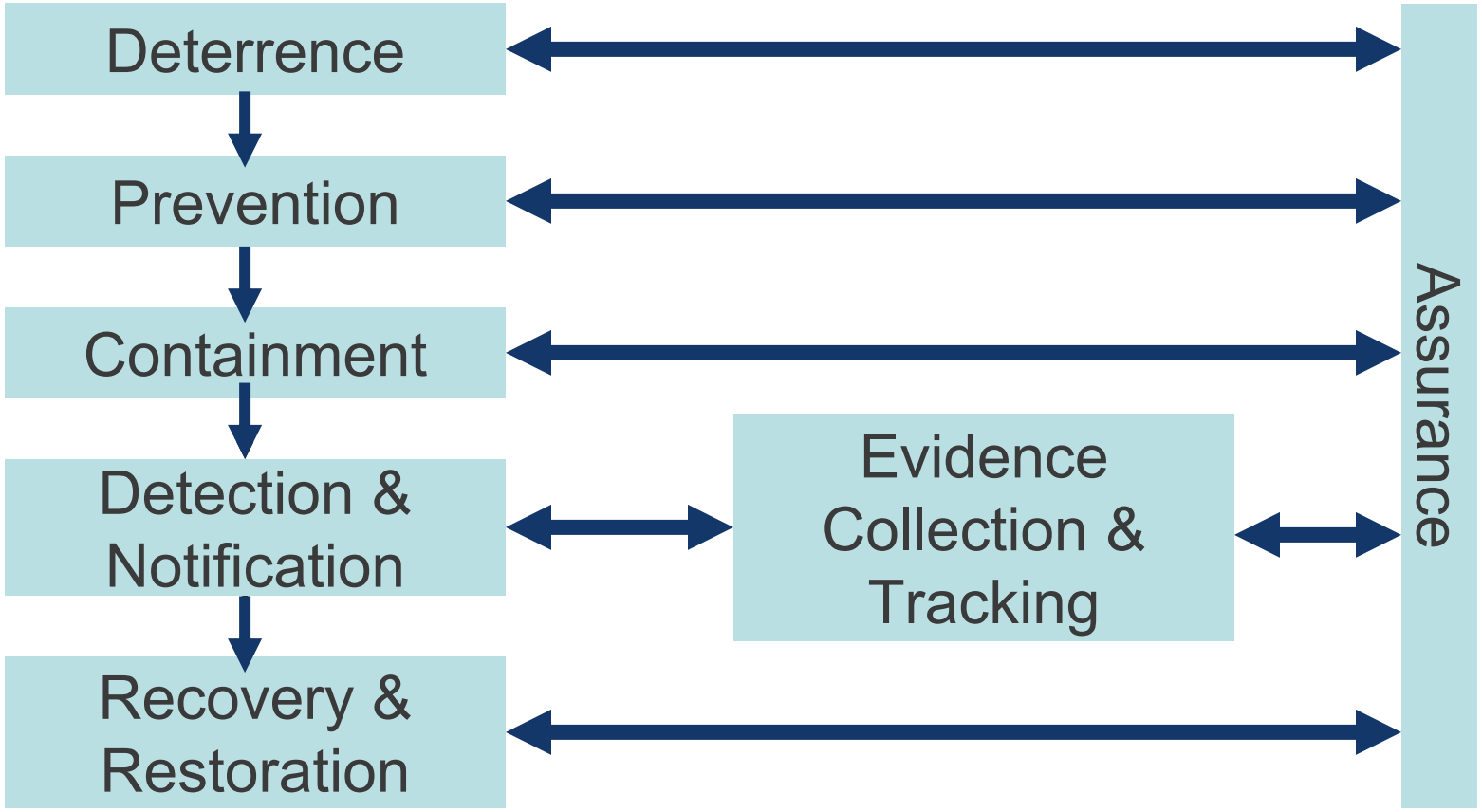


Multi-tiered Controls Strategy - Capabilities

Prioritised, Proportional & Balanced Investment

- Over-investment in preventative measures results in prevention of business and opportunity
- SABSA multi-tiered control strategy provides assurance of security capabilities (in design or in review/audit):
  - Risk-proportional capability to Deter
  - Risk-proportional capability to Prevent
  - Risk-proportional capability to Contain
  - Risk-proportional capability to Detect
    - Risk-proportional capability to Track
  - Risk-proportional capability to Recover
  - Risk-proportional capability to Assure the other capabilities

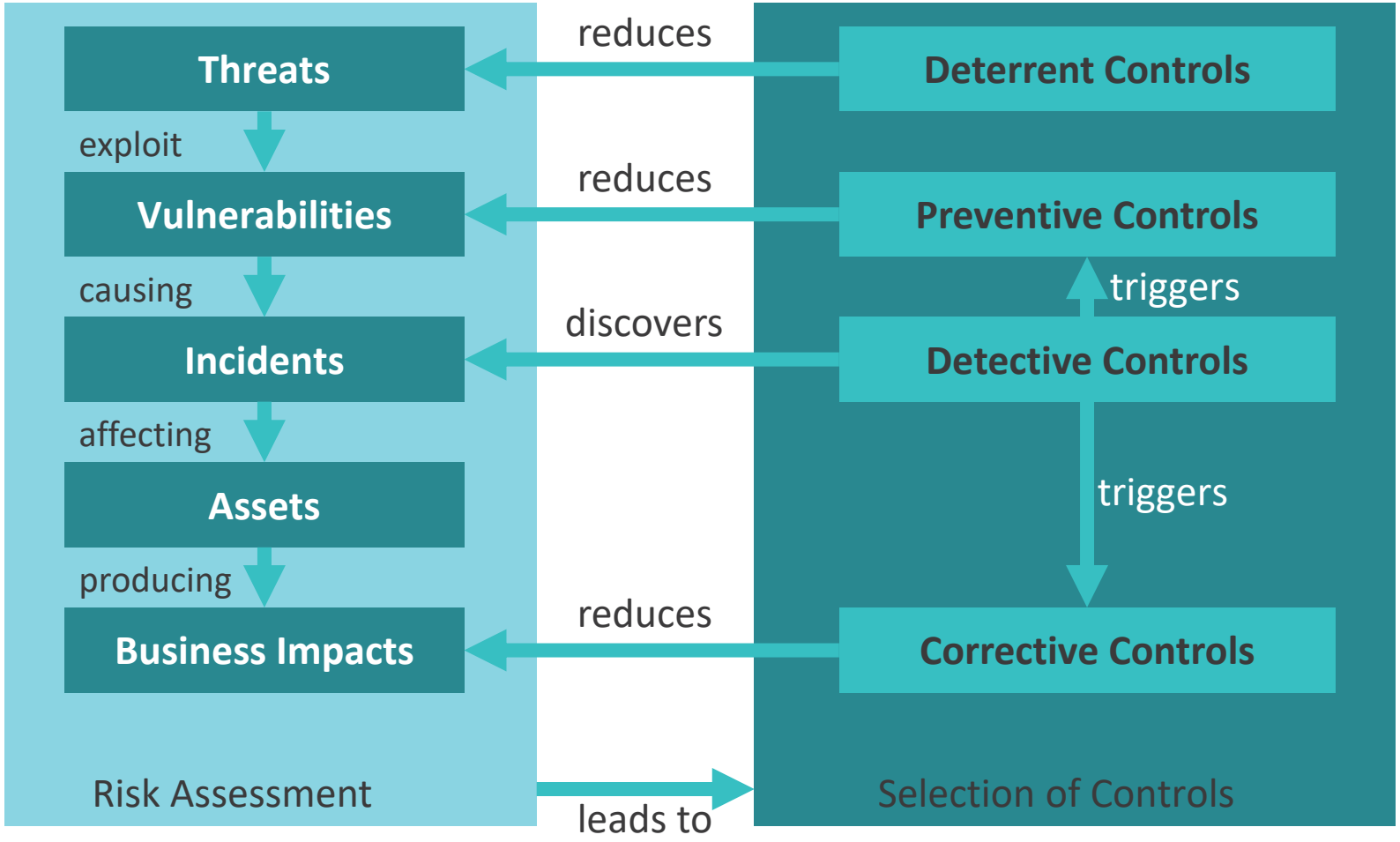
SABSA Multi-tiered Control Strategy



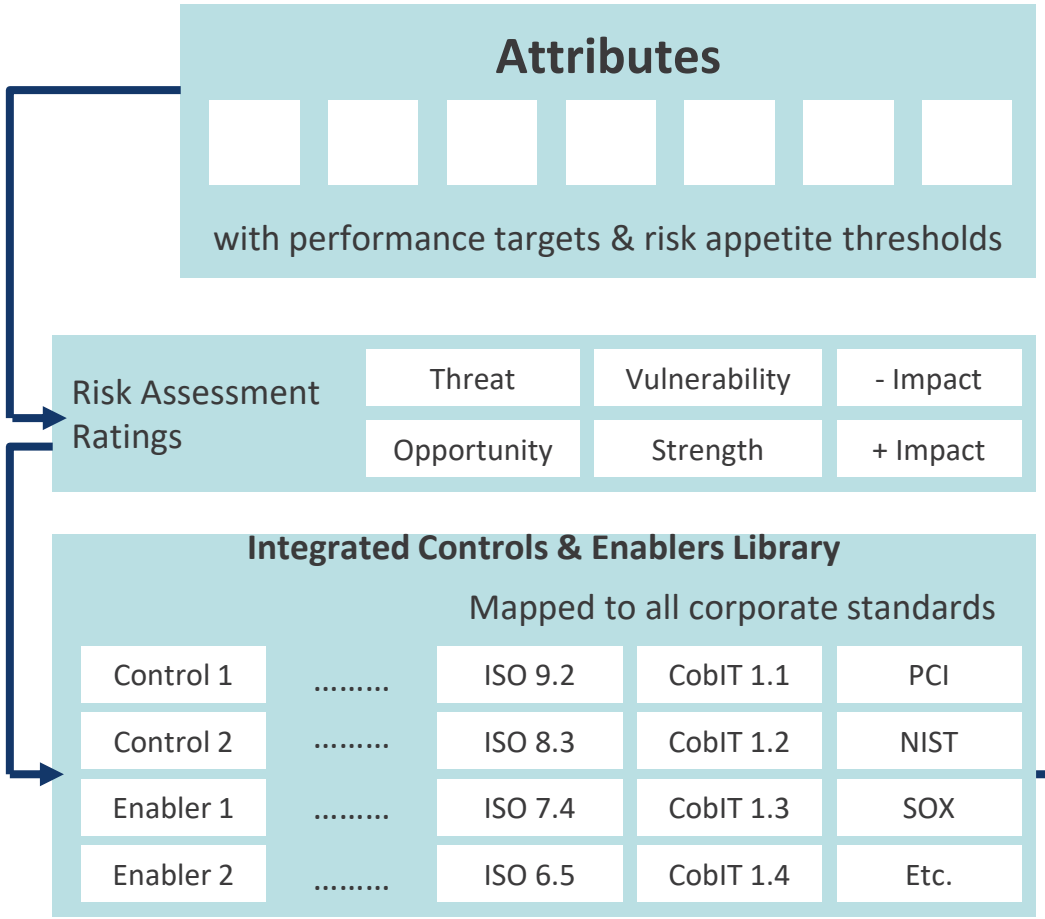
Application of Multi-tiered Controls in Risk

- The multi-tiered controls strategy is modeled against the risk assessment to determine proportional and appropriate response
- Contributes to selection of the right control in the right place at the right time
- Enables further removal of subjectivity in selection of Risk Treatments
- Facilitates construction of databases and risk management tools that respond to definitive risk scenarios with definitive control decisions
- Increases speed and ease of use of Risk Assessment

Application of Multi-tier Control



Application of Multi-tiered Control Strategy



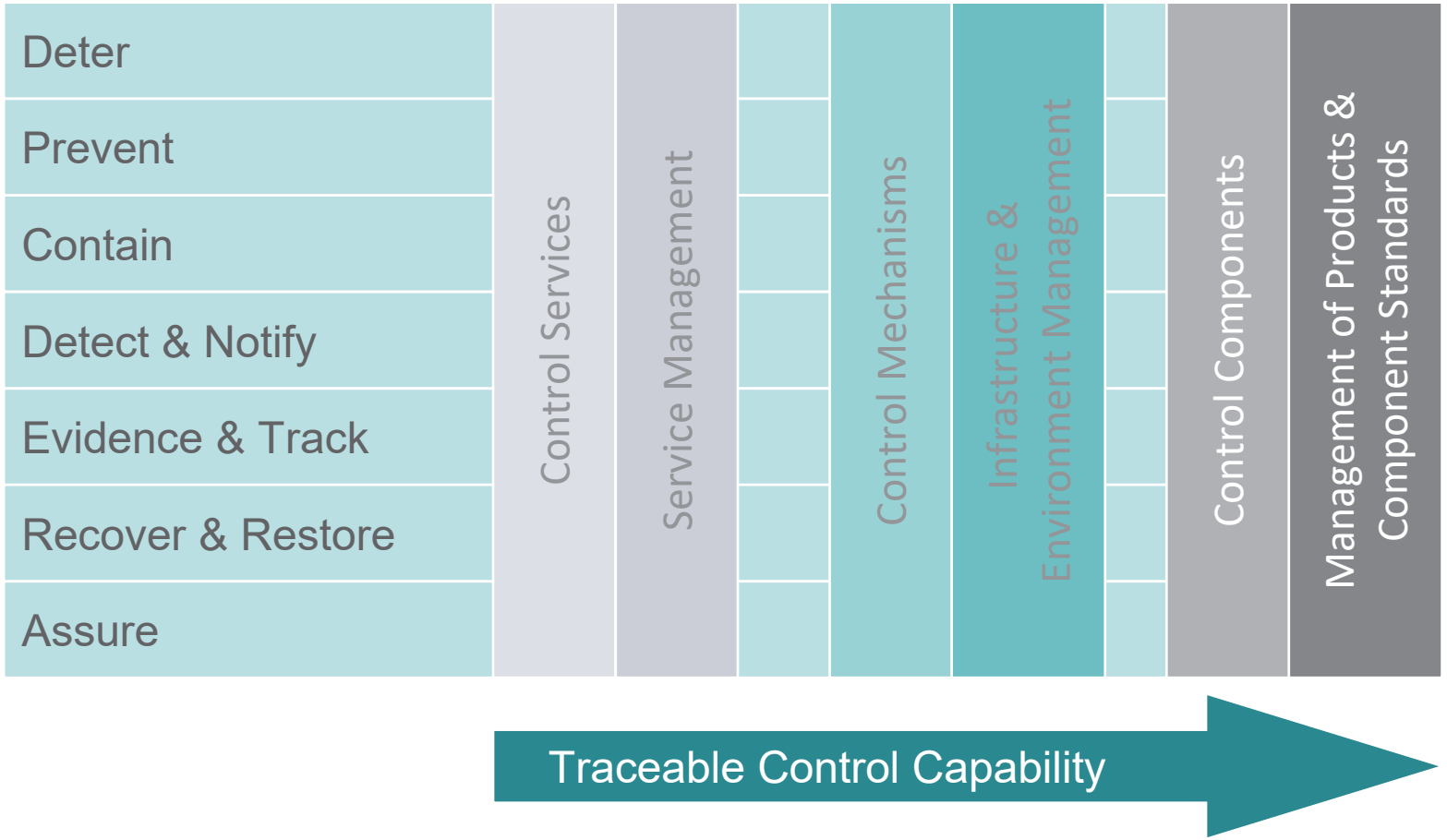
Assess risks to attributes

For risks beyond appetite, analyse risk factors:
If risk is high due to vulnerability on network use defence-in-depth indicators to select from library only vulnerability management controls (i.e. prevention capability) for the network

Keep actuarial data to validate control ratings
Next risk assessment on same Attribute inherits all actuarials and control effectiveness ratings
Exceptions reported to risk manager

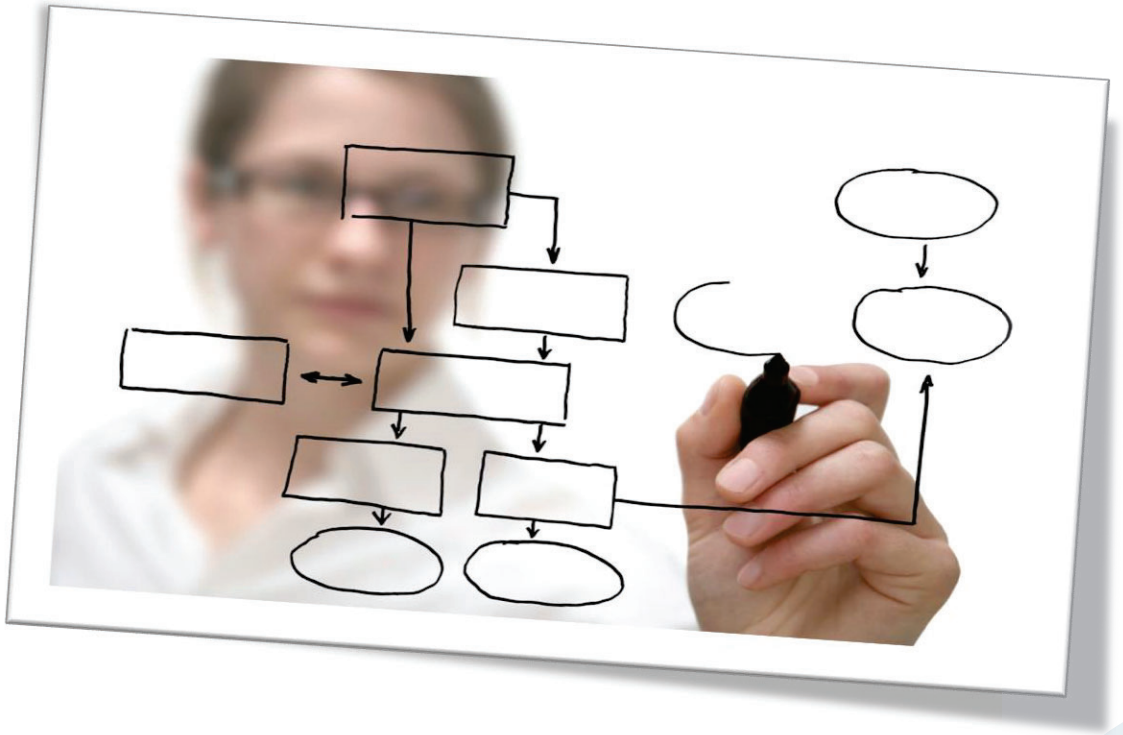
Strength-in-Depth Capability Engineering

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



Workshop A3-9

Engineering the Multi-tier Control Strategy



Adapting the SABSA Process – Fit-for-purpose Design

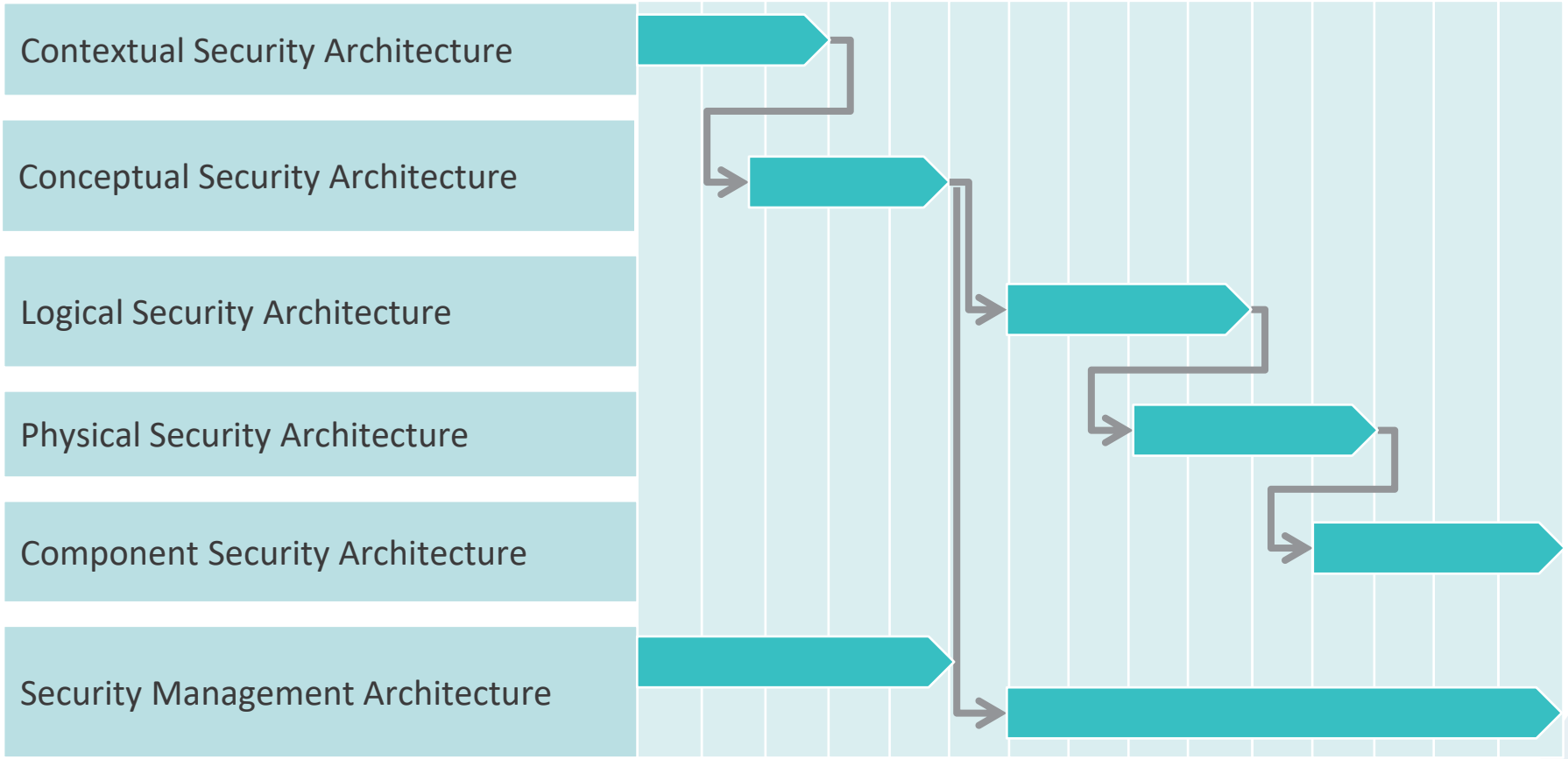
Section 10

Frameworks & Models Provide Dynamic Interpretation

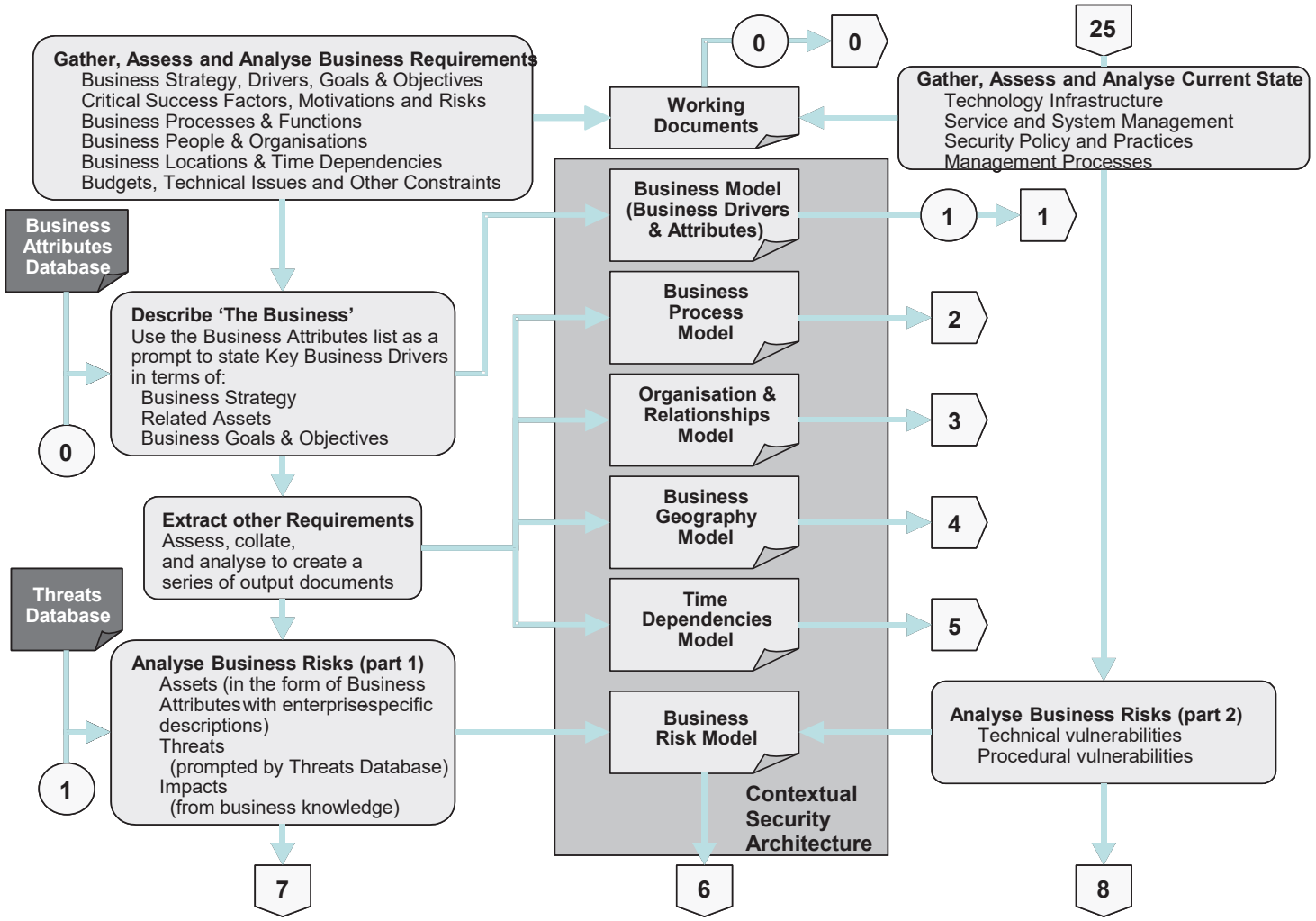
- Every organisation:
  - Starts from a different place
  - Heads toward a different destination
  - Via a different route
  - With different priorities
  - At different speeds
  - To cater for different risk appetite
  - With different levels of architectural maturity
  - And different alignment and integration challenges
  - Embody different cultures, styles & attitudes
  - And with very different budgets
- SABSA is never exactly the same twice

SABSA Development Process

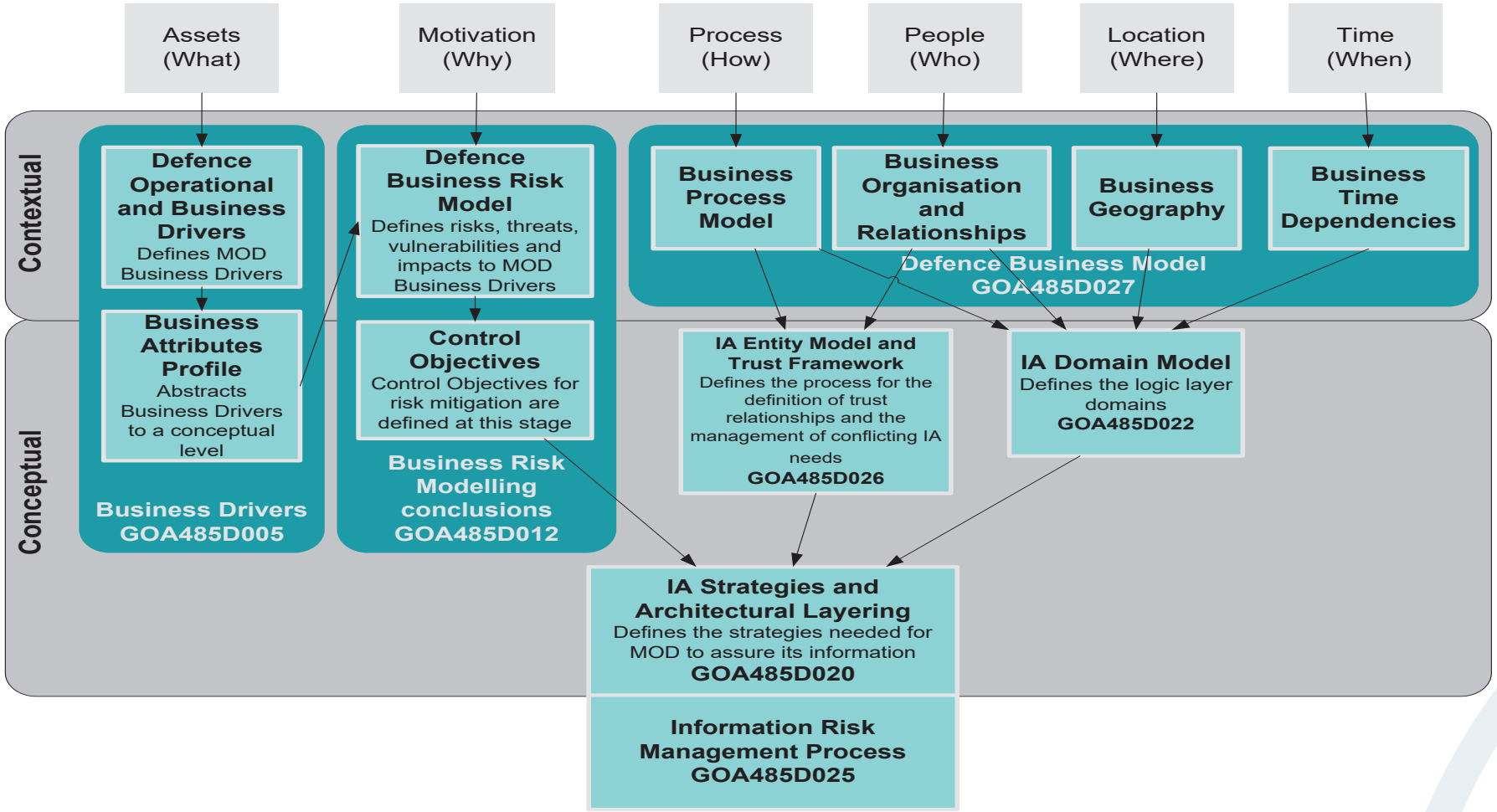
Variability in overlap of layers



Variability in Sequence of Inputs & Outputs

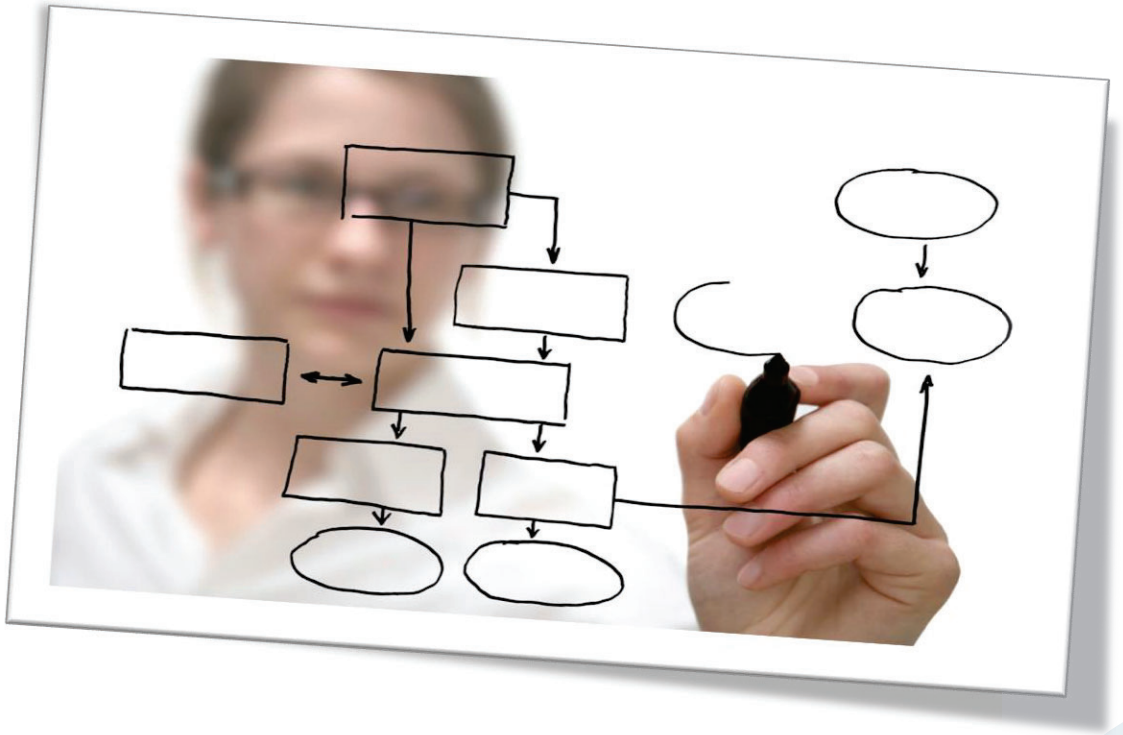


Variability in Scope



Workshop A3-10

Methodology Process Map

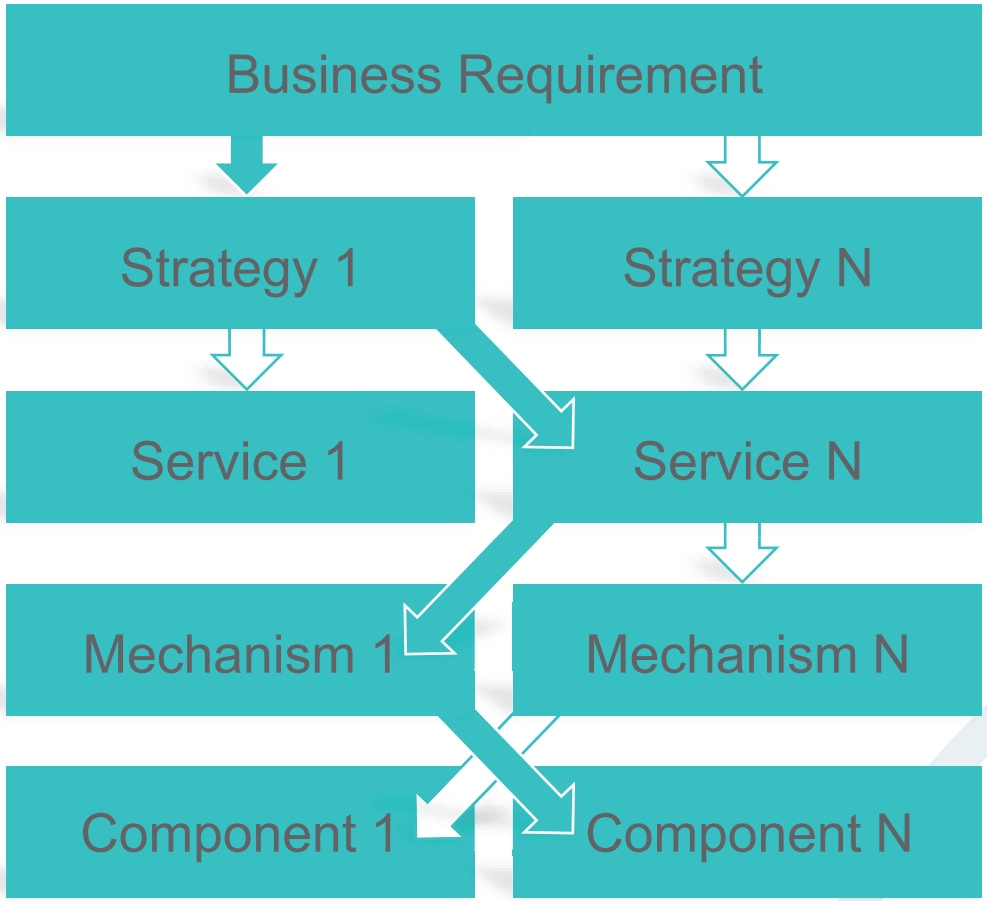


Full Requirements to Solutions Traceability

Section 11

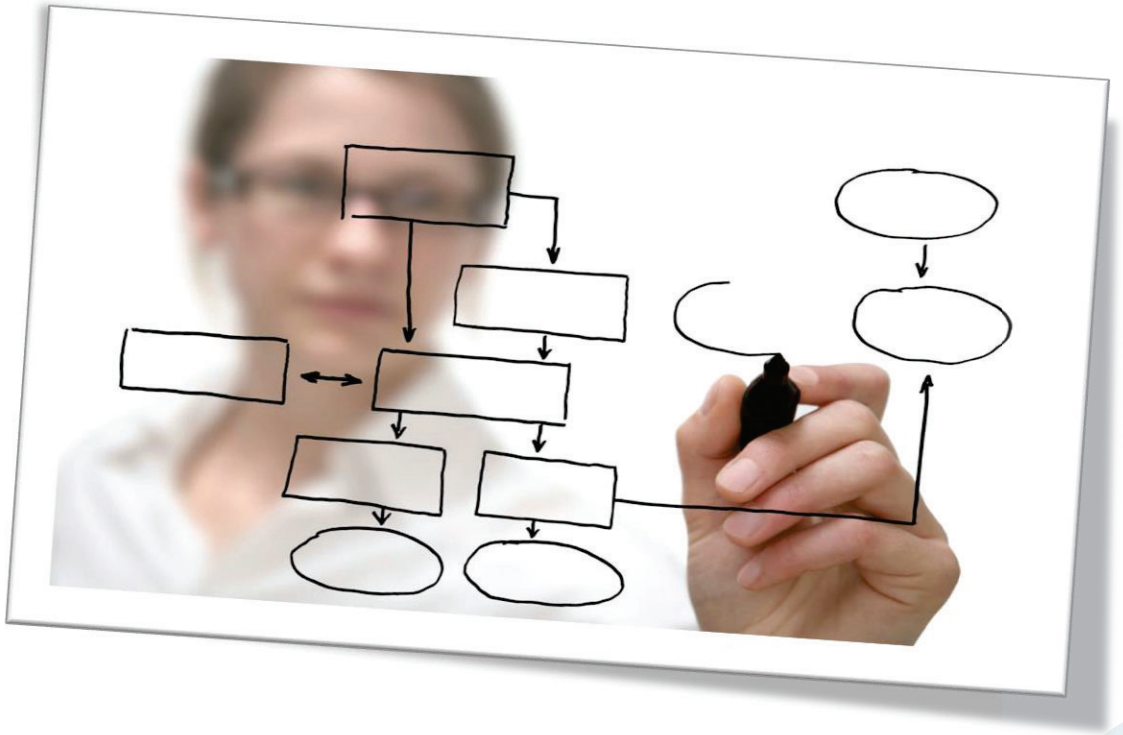
Applications of the Traceability Layer Map

- Bi-directional
  - Completeness
  - Justification
- Actuarial Preservation
  - Controls
  - Enablers
- Manage Change
  - Confirm links not removed
  - Identify redundancy
- Knowledge Management
  - Re-use components
  - Predictability



Workshop A3-11

Full Requirements to Solutions Traceability



SABSA for Evaluating Standards & Solutions

Section 12

Very Few Standards are Architected

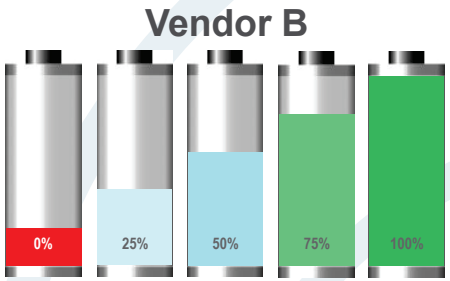
- Few controls standards are written from the Architect's holistic and structured point of view
- Example: ISO 27001 / ISO 27002 – 11.4 Network Access Control

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

Very Few Solutions Deliver Everything

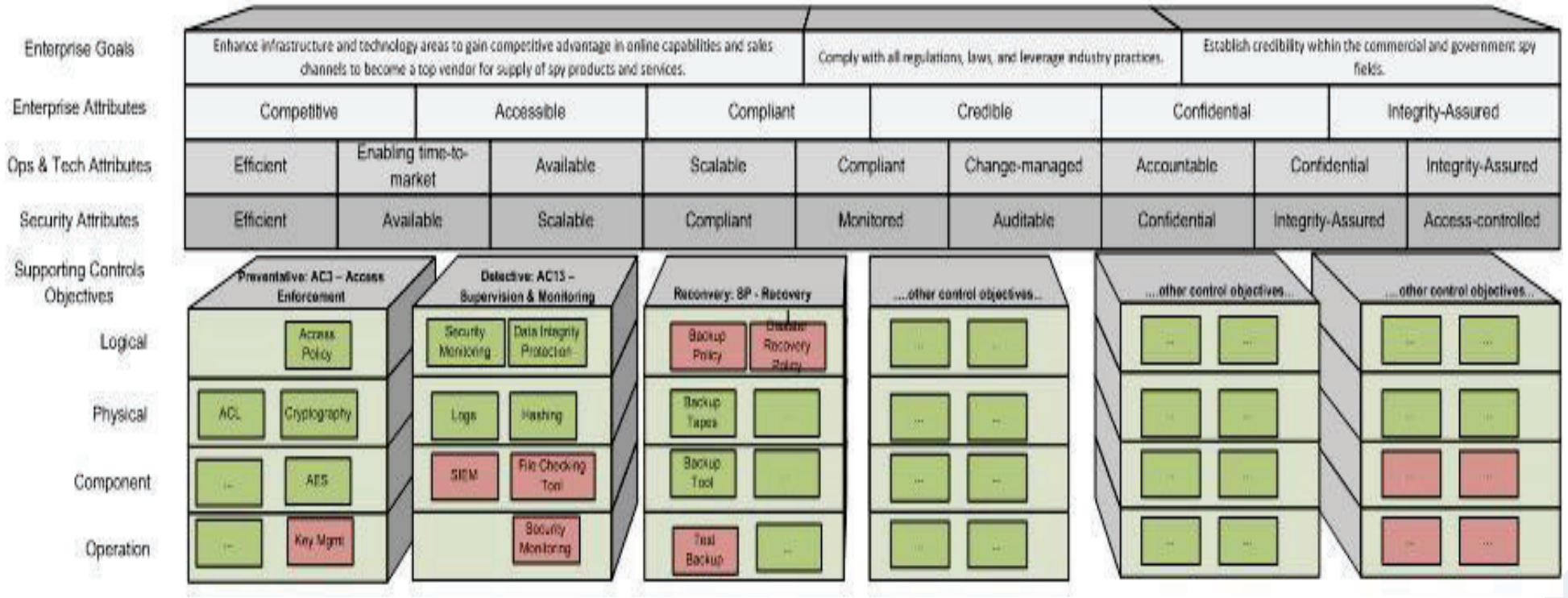
Business Attributes

User Attributes	Management Attributes	Operational Attributes	Risk Management Attributes	Legal / Regulatory Attributes	Technical Strategy Attributes	Business Strategy Attributes
Accessible	Automated	Available	Access-controlled	Admissible	Architecturally Open	Brand Enhancing
Accurate	Change-managed	Detectable	Accountable	Compliant	COTS / GOTS	Business-Enabled
Consistent	Controlled	Error-Free	Assurable	Enforceable	Extendible	Competent
Current	Cost-Effective	Inter-Operable	Assuring Honesty	Insurable	Flexible / Adaptable	Confident
Duty Segregated	Efficient	Productive	Auditable	Liability Managed	Future-Proof	Credible
Educated & Aware	Maintainable	Recoverable	Authenticated	Resolvable	Legacy-Sensitive	Governable
Informed	Measured		Authorised	Time-bound	Migratable	Providing Good Stewardship and Custody
Motivated	Supportable		Capturing New Risks		Multi-Sourced	Providing Investment Re-use
Protected			Confidential		Scalable	Reputable
Reliable			Crime-Free		Simple	
Supported			Flexibly Secure		Standards Compliant	
Timely			Identified		Traceable	
Usable			Independently Secure		Upgradeable	
			In our sole possession			
			Integrity-Assured			
			Non-Repudiable			
			Owned			
			Private			
			Trustworthy			



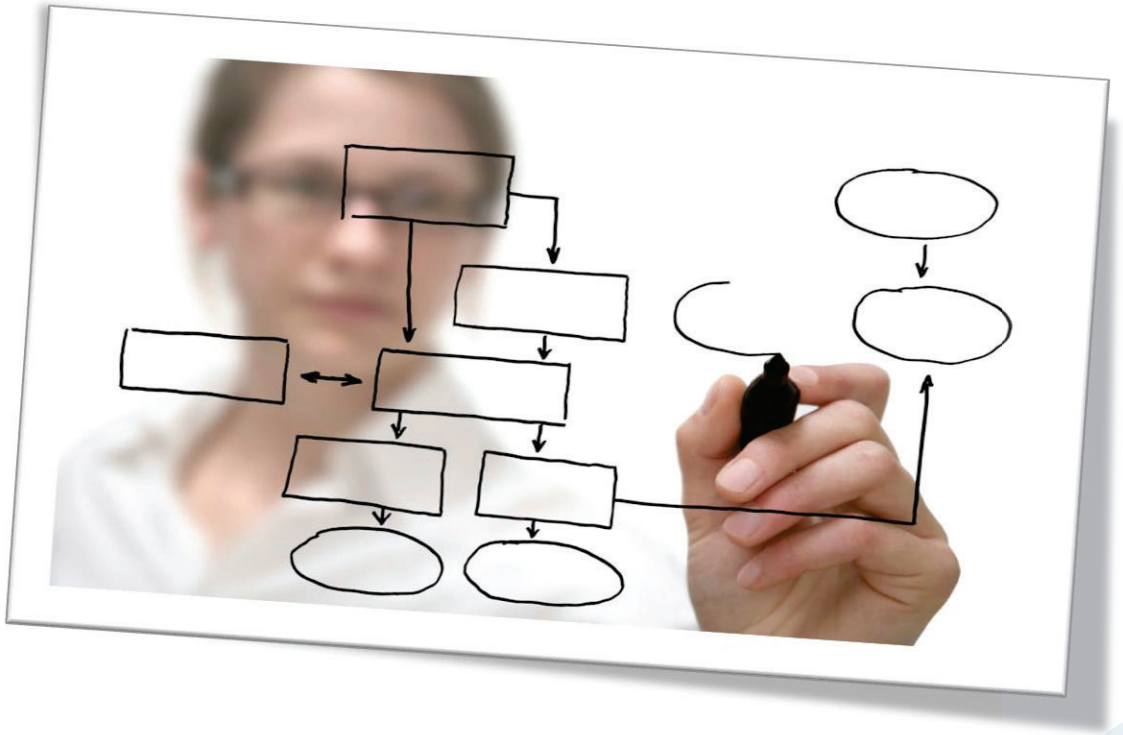
SABSA®

Very Few Environments are 100% Compliant



Workshop A3-12

Evaluating Standards & Solutions Packages



Exam Briefing:
SABSA Chartered Architect – Practitioner Level (SCP)

SABSA Advanced A3 – Architecture Design & Development

Thank You!

The SABSA Institute C.I.C