DLCBRUA1250512

SABSA Advanced A1 Risk, Assurance & Governance

SABSA Chartered Architect Practitioner Level (SCP)

v2.1

SABSA Updates

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

Module A1– Course Outline

- Unit 1 – Fundamentals
    - Section 1 – Fundamentals of Risk in SABSA
    - Section 2 – The Role of Architecture in Enterprise Risk, Governance & Assurance
    - Section 3 – Fundamentals of Governance in SABSA
    - Section 4 – Fundamentals of Assurance in SABSA

Module A1– Course Outline

- Unit 2 – Risk Context
    - Section 5 - Risk Context
    - Section 6 - Stakeholder Identification & Engagement

Module A1– Course Outline

- Unit 3 – Risk Assessment
    - Section 7 - Identify Risk
    - Section 8 - Analyse Risk
    - Section 9 - Evaluate Risk

Module A1– Course Outline

- Unit 4 – Risk Treatment
    - Section 10 – Risk Treatment Strategy
    - Section 11 – Risk Treatment

Module A1– Course Outline

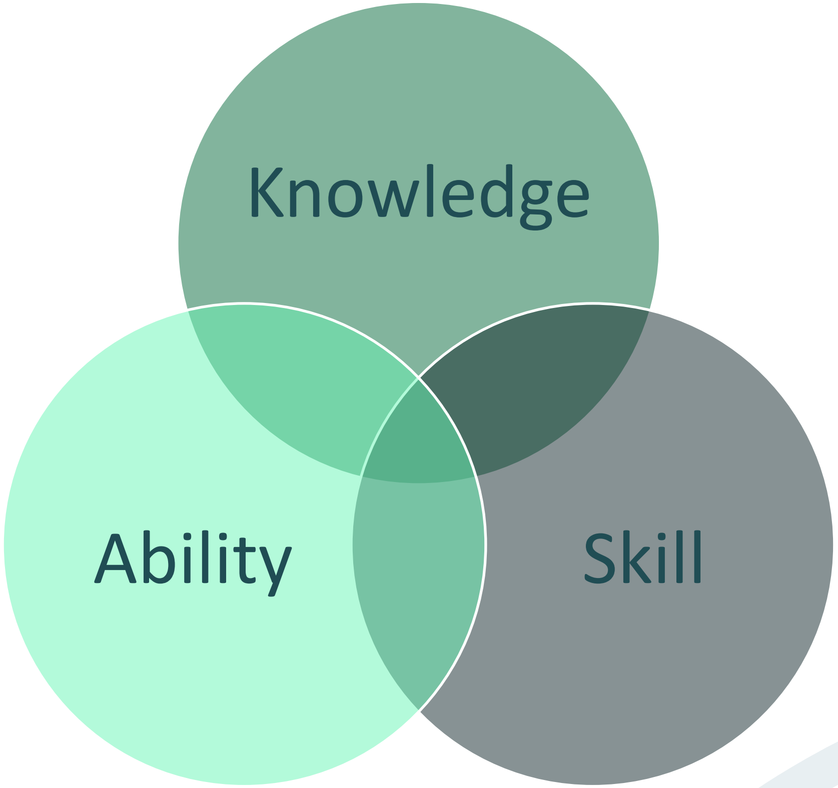
- Unit 5 – Risk Management
    - Section 12 – Risk Management
    - Section 13 – Risk Assurance

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 A1, 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 Risk, Assurance & Governance

SABSA®

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

SCP Certification requires an Architect to develop and demonstrate competency levels 3 and 4

How is SABSA Competence Measured?

Certification Level	Competence Level	Example Competence Required	Testing Method
Foundation (SCF)	1. Know	Define, identify, list, tell, locate, label	Multiple choice test
Foundation (SCF)	2. Understand	Interpret, summarise, describe, explain, infer, discuss	Multiple choice test
Practitioner (SCP)	3. Apply	Use, solve, model, execute, implement, demonstrate	Written test
Practitioner (SCP)	4. Analyse	Categorise, organise, compare, contrast, sequence, relate	Written test
Master (SCM)	5. Evaluate	Assess, evaluate, judge, value, modify, integrate	Written test & thesis
Master (SCM)	6. Create	Design, develop, create, invent, devise, prove	Written test & thesis

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	

Advanced Module Examiner Report

SABSA® INSTITUTE	**SABSA Practitioner Examiner Report**	**A1**

Candidate Number:	**DLCAMSA1190222-01**		
Question Numbers:	**Q1 & Q5**		
Total Score:	**78%**	**Result:**	**PASS**

Question 1	**Question Marks: 50**	
Measurable Behaviour	**Available**	**Awarded**
demonstrate the **relationship between it and the risk appetite of stakeholders at a variety of domain levels** and	15	**12**
Assurance was demonstrated showing relevance across several different stakeholders, however it was difficult to follow the traceability through multiple artefacts. Fig. 12 was helpful for demonstrating at a high-level, but it wasn't clear where those inputs came from.		
throughout the scope of Strategic, Programme/Project, and Operational Risk.	10	**7**
Assurance was shown through several domain levels, and across all lifecycle phases. The candidate did not explicitly address this through the scope of strategic, project/programme and operational risk. Some key elements were demonstrated through the response.		
	Question Score:	**36**

A1 – Unit 1

Fundamentals

Fundamentals of Risk in SABSA

Section 1

Open Discussion – What is Risk?

What is Risk? – Traditional Sectoral Definitions

Risk The possibility of damage or harm and the likelihood that damage or harm will be realised ***ISC²***

Risk The combination of the probability of an event and its impact ***ISACA***

Risk The level of impact on organisational operations (including mission, functions, image, or reputation), organisational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring ***NIST***

The Need for Risk Balance

Historical Focus on Negatives

- Selling fear, uncertainty & doubt
  - "But it will never happen to me" response
- Y2K syndrome
  - "It didn't happen so the investment must have been wasted" response
- Difficult to credibly measure events that do not happen
  - "It didn't happen, so it wouldn't have happened anyway" response
- The insurance approach
  - "Not of benefit to me: I'm already dead" response

DLCBRUA1250512

Risk Represents Both Positive & Negative Perspectives

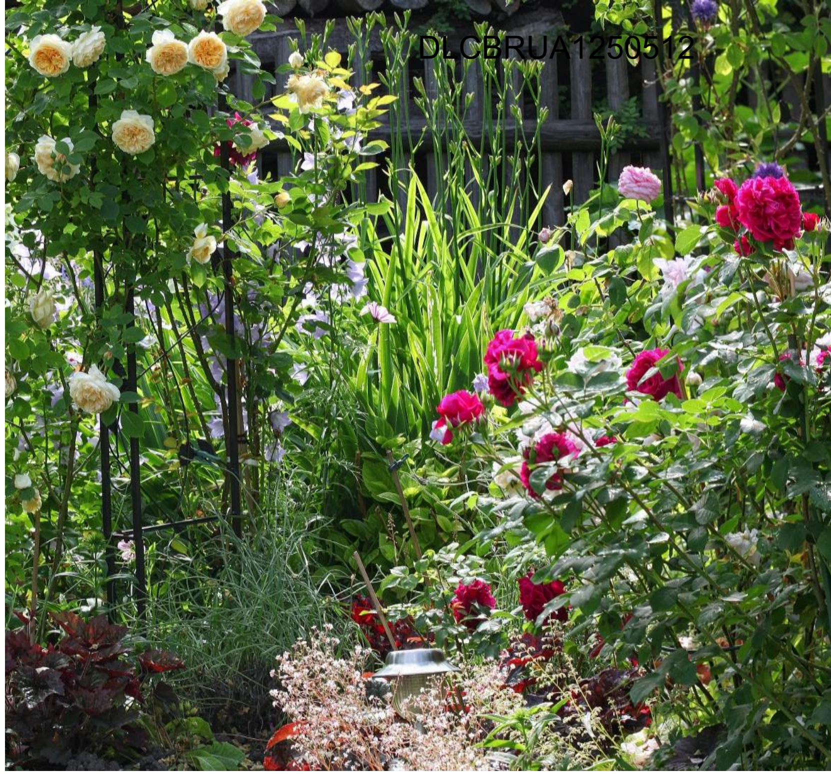
The Need for Risk Balance

Negative Focus Not Business-aligned

- Consider the Enterprise context
  - How much is focused on stopping things from happening?
  - How much is focused on making things happen?
- Risk is necessary for:
  - Growth & benefit
  - Development and change
- Negatively focused risk practices prevent damage to the business but do not actively assist or enable
  - Ability to meet objectives
  - Stakeholder bonuses
  - Annual appraisals
  - Performance targets

Treat the problem

Prevent the problem



Or generate a benefit?

The Need for Risk Balance

Risk Treatments Perceived as Lacking Ambition

What is Risk? – Balanced Risk Definitions

Risk An uncertain event or set of events which, should it occur, will have an effect on the achievement of objectives. A risk consists of the combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives. Within this definition 'threat' is used to describe an uncertain event that could have a negative impact on objectives or benefits; and 'opportunity' is used to describe an uncertain event that could have a favourable impact on objectives or benefits ***UK OGC MoR***

Risk The effect of uncertainty on objectives.

The purpose of risk management is to achieve an appropriate balance between realising opportunities for gains while minimising losses ***ISO 31000***

The Need for a Normalised Language

A Confusion of Requirements

- Varied interpretation of objectives, goals, targets, drivers, & requirements
- Confusion between what we want to achieve, how we will achieve it & in what way
- Diverse organisational levels and layers of abstraction
- Different viewpoints and perspectives
- Mixed nomenclature, culturally specific terminology & jargon
- ’Grapevine’ interpretations & degrees of validation
- Conflicts in priority
- Focused on strategic, tactical or operational outcomes
- Bottom-up engineering enforcing solution on the requirement
- Ambiguous or specific
- Intangible or measurable

The Need for a Normalised Language

A Gulf in Language and Understanding

- We talk the wrong language
    - "What do you think about zero day exploits?"
- We ask the wrong question
    - "What are your security requirements?"
- Requirements are lost in translation
    - "Security must mean confidentiality because that is what my textbook says"
- We offer a non-business solution to a business problem
    - "If you want to improve your reputation, buy a firewall"

The Need for a Normalised Language

Inability to Identify and Agree Upon What Matters Most

- Requirements for risk and security are often focused on protecting "assets"
- Asset registers often omit critically important elements of great value:
  - Brand & reputation
  - Safety
  - Strategic objectives
  - Capabilities

Seraph to Neo – The Matrix Reloaded

"I protect that which matters most"

SABSA Approach to Normalisation

Attributes: Solving the Normalisation Challenge

- Clarity on what matters most
- A common language:
  - To define the requirements for what matters most
  - To measure the requirements
  - That serves the diverse sources of requirements
  - To traceably connect requirement to solution
- The structure within which the common language:
  - Can be applied
  - Can be made useful
  - Creates systemic understanding, distribution and aggregation between requirements

SABSA Attributes - Purpose

- Engineering technique for modelling Enterprise Requirements into normalised, measureable, demonstrable, re-usable, reportable form
- Embody all "Things that matter most" and present them to stakeholders at all levels in the most instinctive way possible
- A stakeholder engagement and communications technique to:
  - Bridge the language gap between requirements and solutions
  - Reach agreed, validated understanding
- Create an ability to clearly define and delegate targets and risk appetite, and measure performance against those targets

What are SABSA Attributes?

Attribute A quality or feature ***OED***

Attribute A quality, character, characteristic, or property ***Dictionary.com***

Attribute A quality or feature of a person or thing, especially one that is an important part of its nature ***Cambridge***

Attribute An inherent property or characteristic of an entity that can be distinguished quantitatively or qualitatively by human or automated means ***ISO/IEC/IEEE 15939 : 2017 Systems & Software Engineering Measurement Process***

SABSA Attribute

A normalised, measurable, in-context definition of what is important

What is the SABSA Attributes Framework?

SABSA Attributes Framework

The structured SABSA concepts that support our work, simplify complexity, and enable us to make informed decisions regarding requirements by creating a normalised language for those requirements

The application of the SABSA Attributes Framework results in a specific models (Attributes Profile and Attributes Taxonomies) that define, organise, engineer and present the normalised requirements of an Enterprise, or its constituent parts, in the unique context of that Enterprise

The SABSA Attributes Framework

Context
Analysed, Published or interpreted

Attribute Definition

Name:
Definition:

Attribute Taxonomy

Classification:

Attribute Definition

Measurement Approach:
Metric:
Performance Target:

SABSA Attributes Taxonomy

The classification and visual presentation of the SABSA Attributes, or a subset of Attributes, catalogued to represent particular Enterprise aspects or stakeholder requirements

SABSA Attributes Profile

Attribute Definition + Attribute Measurement

The SABSA Attributes in full measurable form comprised of Name, Definition, Measurement Approach, Metric, and Performance Target

What is Risk? – SABSA Definition

Attributes
(what we value)

Threat (event with negative impact)	**Vulnerability** (weakness exploited by the threat)	**Impact** (negative consequences to Attributes)
Opportunity (event with positive benefit)	**Strength** (capability to grasp the opportunity)	**Benefit** (positive consequences to Attributes)

SABSA Risk

The positive or negative effect of uncertain events on Attributes

The Need for Domains

A Need to Resolve Enterprise Policy, Governance & Risk Ownership Complexity

- Policy, governance & risk ownership relate to:
  - Multiple different levels of Enterprise
    - Multi-national, national, jurisdiction, Enterprise, departments, teams, etc…
  - Multiple different aspects of Enterprise
    - People, process, technology, etc…
  - Multiple different properties of Enterprise
    - Quality, security, etc…
  - Multiple different layers of abstraction
    - Function, classification, infrastructure, information, systems, containers, data, etc…
  - Both the internal Enterprise and its external interactions
    - Regulators, providers, partners, customers, etc.

The Need for Domains

A Need to Achieve Enterprise Policy, Governance & Risk Ownership Clarity

- Within a complex environment the levels, aspects, layers and properties co-exist with interactions and inter-dependencies between them

Scenario
Enterprise has goals & objectives and provides services to customers
Product Development Dept. defines the service but Business Process Engineering Dept. defines the process of creating and delivering the service
Sales Dept. sells the service but Customer Relations Team serves the customer
I.T. Dept. provides technology but Business Operations use the technology

Scenario
Cayman Islands Corporation manufactures in China
Belgian retailer sells product to an Australian customer via a website hosted in USA
Retailer’s information is digitally transformed into data by its I.T. Department based in Ireland
Data is transmitted across the public internet and stored by an Indian cloud storage provider

Who governs the scenario? Who owns the risk? Who determines policy?

The Need for Domains

A Need to Embrace Rather than Avoid Ownership

- Many different interested parties accountable and responsible for so many different inter-related elements
- Each uses diverse models, patterns, and nomenclature
- Focus on silo of interest
- Each avoids ‘ownership’ presented by unfamiliar models, patterns and nomenclature
  - “I don’t understand”
  - “That can’t be my problem”
  - “Too busy dealing with my own issues”

SABSA Domain Framework - Purpose

Architecting Risk Ownership, Governance & Policy

- A technique to resolve complexity in risk ownership, governance & policy
- Create certainty and clarity
- Establish a holistic common structure and language applicable at all levels that enables:
  - Ownership to be embraced rather than resisted
  - Accountability and responsibility to be assigned
  - Risk appetite and performance targets to be delegated
  - Performance against appetite and targets to aggregated
  - Systemic relationships to be identified, understood, and resolved
  - Traceability of risk treatments and solutions to requirements

What is the SABSA Domain Framework?

SABSA Domain Framework

The structured SABSA concepts and techniques that support our work, simplify complexity, and enable us to make informed decisions regarding risk ownership, governance and policy

The application of the SABSA Domain Framework results in specific Domain models that define and visualise the normalised risk ownership, governance and policy structures of an Enterprise, or its constituent parts, in the unique context of that Enterprise

What is a SABSA Domain?

Domain An area of interest or an area over which a person has control ***Cambridge***

Domain An area of knowledge or activity; especially one that somebody is responsible for ***OED***

Domain A territory over which dominion is exercised ***Merriam Webster***

Domain (legal) Complete and absolute ownership ***Merriam Webster***

SABSA Domain

A set of elements, area of knowledge or activity, subject to the common dominion of a single accountable authority

SABSA Security Domain

A set of elements, area of knowledge or activity, subject to the common security dominion of a single accountable authority

Domain Rules

- A Domain must have a single Domain Authority
- The Domain Authority is accountable for the risk to, and performance of, the Domain
- A Domain must have a definable boundary
- Elements within a Domain share common trust defined by their common policy and common risk appetite
- An accountable Domain Authority may delegate risk appetite or performance targets to a specialist Authority at a lower level of abstraction (a Subdomain)
- The Superdomain authorises Subdomains, and Subdomains are responsible to the Superdomain for compliance to delegated appetite and meeting delegated performance targets

A Normalised Language with a Common Structure

Attribute

Attributes define what matters

Domain

Domains define authority for what matters

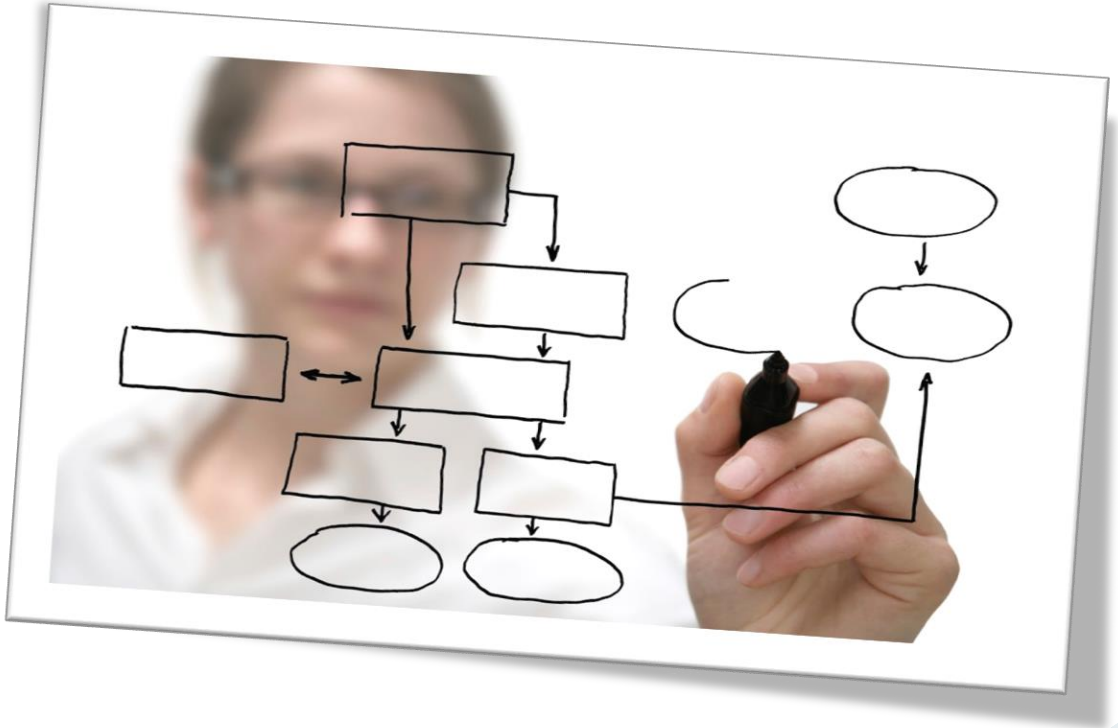
Domain

Attribute

Together, these two core SABSA concepts play a vital role in providing meaningful context for risk, governance & assurance

Workshop A1-1

Current-state Evaluation Part 1



The Role of Architecture in Enterprise Risk, Governance & Assurance

Section 2

SABSA®

The Need for an Architected Holistic Approach

The Enterprise as a Complex System

Ashby's Homeostat

- The parts of the Architecture interact and have inter-dependencies, conflicts and systemic relationships
- Complex interactions with the environment in which it exists
- May change organically as a result of the behaviours of its parts, each of which has its own objectives, success factors, methods and risks
- Emergent properties arise from interactions between its parts, and between the architecture, its parts and the environment
- Cannot be defined by reference to its constituent parts alone because no part is independent of the behaviour of the other parts
- An Enterprise ecosystem shares properties of complex systems including:
  - Organic & evolutionary
  - Non-deterministic & spontaneous
  - Continuous re-adaption
  - Nonlinearity & feedback loops

Challenges of Enterprise Complexity

- Complexity is an inherent characteristic of the modern Enterprise
- Future success may depend upon an Enterprise's ability to understand complexity, be resilient to complex disruption, and adapt to ever-changing complex requirements
- Complex properties are inherently difficult to model
- The complex climate presents challenges in building, integrating, and modifying solutions, particularly large-scale solutions, and very rarely starting with a 'green field'
- Risk, Governance & Assurance Architecture practice is often unsuited to complex characteristics
  - Unchanged underlying "mental model", philosophy, and processes
  - Define risk and risk treatment functionality assuming stability over time
  - Often imposed by the restrictions of tools and known current solutions
  - Customers view outcomes as "too late", "unresponsive," and "of no lasting value"

Complex dynamic environments are not well served by isolated static solutions

The SABSA Approach to Enterprise

- Treat the enterprise as a single entity with complex properties
- Offer an approach capable of describing enterprise complexity
- Provide a means to translate ever-changing complexity into requirements for workable solutions that can transform and adapt
- Inform the way the various professions (particularly Architecture, Security, Risk, Governance & Assurance) approach their work and help frame the questions they ask
- Deliver a structure to extend Systems Engineering concepts and methods to the enterprise as a complex system
- Embrace enterprise complexity to optimise and balance systemic risk with performance targets across all parts of the organisation in a coherent way

In-Context Thinking: Connecting to Business

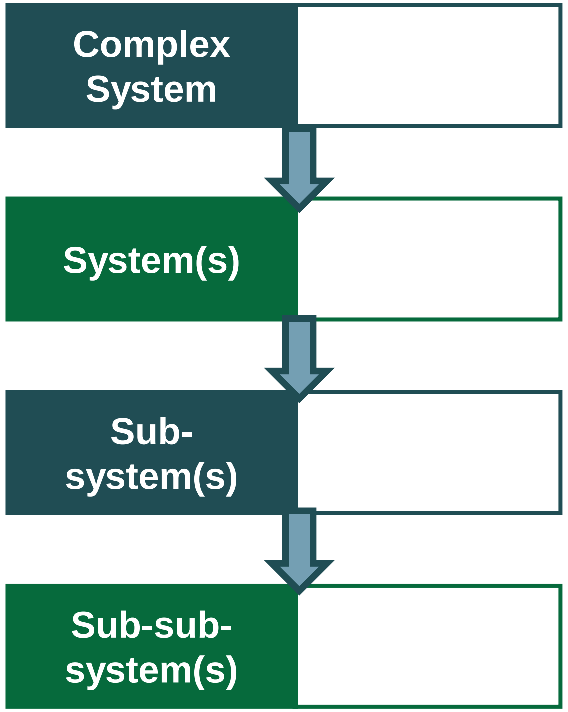
Traceability Requires Architectural Layering

- Specification question is difficult to answer
- Disconnect between the Business view and the Specification view
- Not enough context to fully inform the solution decision
- The decision also affects (and is affected by) many other (unseen) elements
- But fit the wrong tyres and the business fails in its objective

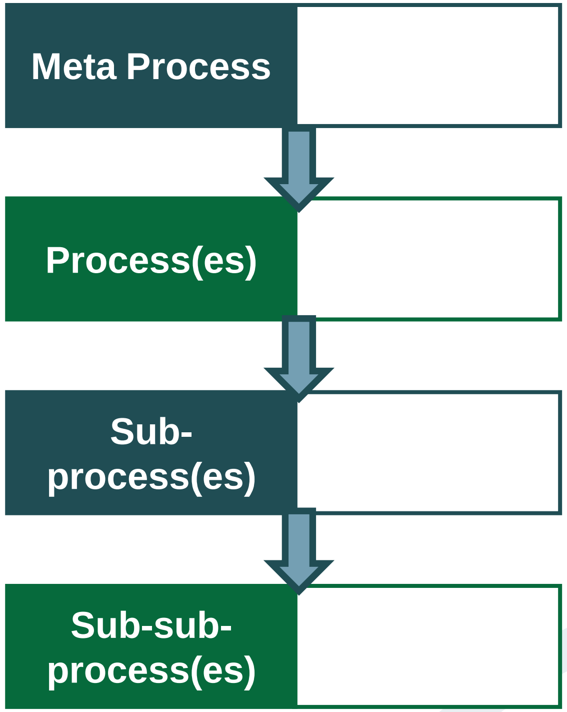
Business View
How do we win the world championship?

Technical View
Which rubber compound should I deploy?

Architecture Layers – Top-Down Engineering



- Top-down engineering deconstructs a complex challenge into progressively more specific layers of abstraction
- Requirements are driven by the layer above
- Each layer serves the requirements of the layer above
- Each layer is traceable and meaningful to the specialists who operate at that layer



Architecture Layers – Black Box Models

- An element viewed in terms of its inputs and outputs without any knowledge of the detailed internal workings
- In a top-down approach a view of the system is formulated, determining the requirements for any next-level subsystems, but not detailing the specification
- Each subsystem is then refined in greater detail, sometimes in many additional subsystem levels, until the entire specification is reduced to base elements

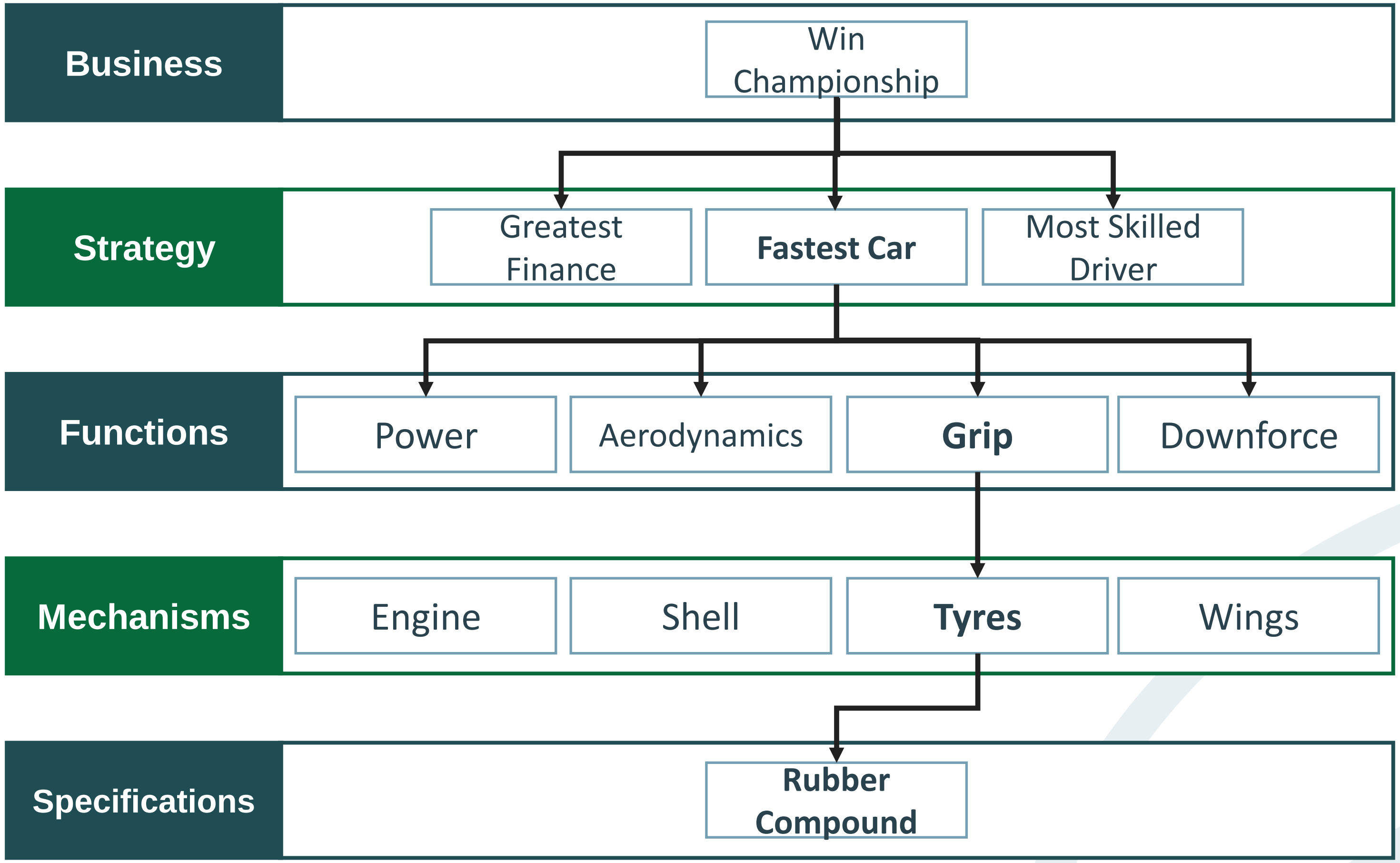
Architecture Layers - Purpose

Viewpoints of Understanding Through a Complex System

- To make sense of where an element might best fit in the overall complex system it must be viewed with perspective and context
- Within a complex system any element can be viewed in multiple ways through many different view filters or lenses, or with many different specialist overlays
- Complex system engineering requires structure to manage complexity by top-down decomposition
- The top-down structure consists of layers representing the different levels of abstraction (nomenclature, syntax, semantics, morphology, level of detail) required for each viewpoint
- Each layer states the requirements for the next until the entire system is reduced to the specification of the base elements
- Each layer serves the requirements of the layer above

Architecture Layers - Example

- Rubber compound may be the focus of the Tyre Engineer's world and expertise but that is a means to an end and not an end in itself
- The decision is based on the need to serve the performance requirements of Tyres in the layer above
- Tyre mechanisms provide the Grip function, and so on in a dependent relationship



Architecture Layers - Conventions

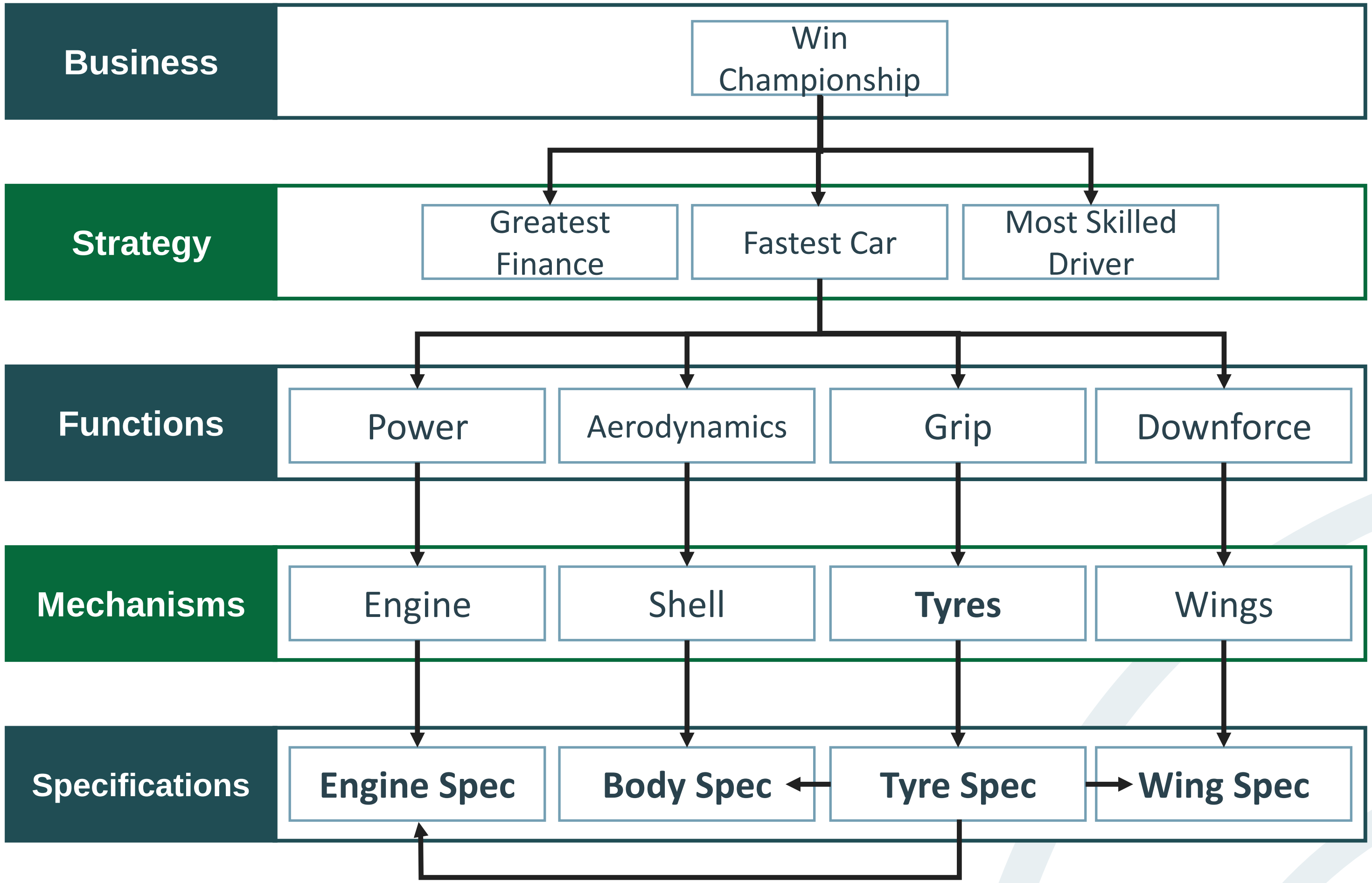
- The end goal is defined by the top layer
- The end goal and requirements to meet the goal are delegated top-down through each successive layer to a level of abstraction and detail that is meaningful at that level
- Each layer is a means to an end, serving the requirements of the layer above
- Layers are closed
  - The layer's requirements are delegated to the layer directly below which cannot be by-passed
  - Interfaces between layers are defined only for layers directly above and below
- Layers are independent
  - A layer is a black box to the layer above
  - A layer is specified independently of the layer below
- Changes of specification can be made in a layer to meet the requirements of the layer above without effecting the specification of other layers
  - The rubber compound can be changed when it starts to rain so that the performance of the tyres continues to provide the grip required

Architecture Layers - Benefits

- Provides the structure required to manage complexity by top-down decomposition
- The strategic goals and objectives of the top layer are delegated downwards
  - The constituent goals of the lower layers are traceable to the overall strategy
  - The constituent goals of the lower layers are aligned and integrated with each other
- Defines contained, non-overlapping partitions to separate the concerns of the whole into meaningful viewpoints
- Requirements are presented at the appropriate level of abstraction (models, patterns, nomenclature, level of detail) required for each viewpoint
- Layered viewpoints make it easier to architect effective risk ownership and governance

Architecture Layers - Example

- In a complex system there are many inter-relationships between elements
- Layering can also serve the requirement to understand systemic peer element relationships
- The tyre specification chosen must align and integrate with the other specifications at the same layer of abstraction



SABSA®

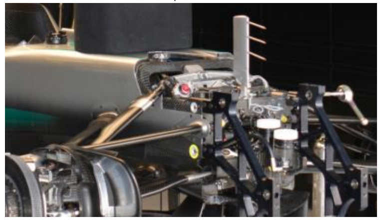
The Need for Systemic Understanding

- Complex System architecture demands that the systemic interactions, inter-relationships, and inter-dependencies, are holistically identified and understood

Vertical Context Traceability

The rubber compound ultimately serves the goal of winning the World Title

Each element must be risk-managed, governed & assured in its own specific and unique context defined by its inter-relationships and dependencies



Lateral Systemically Integrated Context

The rubber compound cannot achieve its contextual goals by acting in isolation, it must be architected holistically with its peers (engine, body, wings, etc)

The Hermagoras Method

- Hermagoras of Temnos (1st century BC) was an ancient Greek teacher of rhetoric in Rome
- Devoted to a technique for discovery of arguments known as "Inventio" under which a topic cannot be deemed complete until all 'arguments' from all perspectives have been evaluated
- Devised a method of dividing a topic into its "seven circumstances" (who, what, when, where, why, in what way, by what means)
- Provided the root for modern techniques to ensure thoroughness in the coverage of a subject:
    - Rudyard Kipling poem "The Six Honest Serving Men"
    - Journalism, education, and police investigation
    - John Zachman's Architecture Framework

SABSA Architecture Perspectives (Columns)

	What	Why	How	Who	Where	When
	Asset Perspective	Risk Perspective	Process Perspective	People Perspective	Location Perspective	Temporal Perspective
Overview	What matters most: assets, goals, objectives, the vision for the future	Motivating factors and risk context: the need to protect against damaging threat events and gain benefit from opportunities	The "How to": Process (method) and capability (means)	Governance, trust and relationships	Jurisdiction, locations and environment	Time and sequence dependencies

Architecture Columns - Benefits

Holistic, Systemic Understanding

- Application of Hermagoras' Method is of great benefit to Architecting complex environments
- A viewpoint (layer of abstraction) can now be considered from six perspectives (columns)
- Enables the SABSA Architect to work holistically by detecting, understanding, modelling and resolving the complex interactions between perspectives
  - Inter-connectivity
  - Inter-dependency
  - Systemic relationships

Architecture Columns - Benefits

Traceability from Consistency of Perspective

- Consistent perspectives (columns) apply through multiple viewpoints (layers of abstraction)
- Enables the SABSA Architect to leverage complex system engineering, top-down, black-box techniques to achieve traceability of decisions
  - Traceability to justify & articulate benefits of solutions & innovations
  - Traceability to demonstrate complete coverage of requirements
  - Traceability through-life
- Results in solutions being deployed because they are demonstrably required not because they are on a checklist, standard, or declared to be “best practice”

The SABSA Matrix

A Structured Problem Solving Framework

- The combination of 6 layers of abstraction with 6 perspectives creates a 6*6 matrix
- Embodies the "mental model" of the SABSA Architect
- Summarises the structured thought process required to solve complex problems
- Results in integrated, meaningful artefacts rather than isolated solutions
  - Business-driven
  - Systemically understood

The SABSA Matrix - Adaptability

Interpreted for Purpose

- The generic matrix is just a structure: the Architect's problem solving "mental model"
  - The top-down structure consists of layers representing the different levels of abstraction (nomenclature, syntax, semantics, morphology, level of detail) required for each viewpoint
  - The lateral structure consists of columns representing different perspectives
- Although the structure remains stable, each cell of the matrix (abstraction and perspective) adopts particular nomenclature, syntax, semantics, morphology and level of detail, depending upon what is being architected
  - e.g. The Logical abstraction of the Process perspective is the generic "Logical Process" but may be referred to as "Information flows and transformations" in Process Engineering
  - e.g. Security Architecture nomenclature differs from that of Total Quality Engineering

From "What is Architecture?" No matter the culture, sector, or environment, Architecture processes remain the same ***Royal Institute of British Architects (RIBA)***

The SABSA Matrix

Interpreted for Enterprise Security Architecture

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision Goals, Targets, Value & Assets	Enterprise Risk Opportunities & Threats	Enterprise Value Chain Value Chain, Core Processes & Capabilities	Enterprise Governance Culture, Org. Structure & Relationships	Enterprise Geography Territories, Jurisdictions & Sites	Enterprise Time Dependence Time & Sequence Dependencies
Conceptual	Attributes Framework Attributes Taxonomy & Profile	Risk & Policy Frameworks Enablement & Control Objectives, Policy Architecture	Process Framework Process Strategy & Architecture	Governance & Trust F'works Ownership & Trust Relationships	Domain Frameworks Security Domain Framework	Time Framework Architecture Roadmap
Logical	Information Information Architecture & Model	Policy Domain Policy & Risk Model	Info Processing & Services Information Flows & Functional Transformations, SSOA	Trust Model Domain Governance & Trust Model	Logical Domains Domain Model & Inter-domain Associations	Time Framework Information & Service Time & Sequence Models
Physical	Data Data Architecture	Practices & Procedures Risk Management Practices & Procedures	Data Comms & Mechanisms Security Mechanisms	Data & System Governance User Interface, Identity & Access Systems	Infrastructure Domains Platforms, Networks & Devices	Processing Schedule Data Processing & Comms Time & Sequence Dependencies
Component	Products & Tools Processors & Repository Standards & Configuration	Risk Standards Risk Management Standards	Protocol Standards Protocol & Comms Standards & Configurations	I&AM Standards Identity & Access Standards & Configuration	Location Standards Node & address Standards & Configurations	Time Standards Time & Sequence Standards & Configuration
Management	Delivery & Continuity Operational Excellence & Resilience Activities	Risk Management Risk Management Activities	Process Management Capability & Service Management Activities	Governance Management Governance, Governance Management Activities	Environment Management Environment & Infrastructure Management Activities	Time & Sequence Management Time Management Activities

SABSA as an Holistic Technique

The Matrix is not a Checklist

- The SABSA Matrix embodies the technique to name, define and specify each Architecture element in context
- But it is not a checklist of artefacts and elements in isolation
- Elements relate to each other
- The Architecture as a whole, its constituent strategies, frameworks, models and elements, also relate to the complex environment in which they exist
- The SABSA approach is not to merely populate the Matrix cells with deliverables in isolation, it is to create the structures and techniques to define artefacts holistically

Vertical Relationships - Explicit

Example – Business Driven not in Isolation

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Dependence
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & trust Frameworks	D	
Logical	Information	Policy	Information Processing & Services	Trust Model	Logical Domains	Time & Sequence Model
Physical	Data	Practices & Procedures	Data Comms & Mechanisms	Data & System Governance		
Component	Products & Tools	Risk Standards	Protocol Standards	I&AM Standards	Location Standards	Time Standards
Management	Delivery & Continuity	Risk Management	Process Management	Governance Management	Environment Management	Time & Sequence Management

The Enterprise Risk Context is the need to protect against damaging threat events and gain benefit from opportunities

The strategy for dealing with that Risk Context is an explicit vertical relationship - a framework defining risk management objectives

Vertical Relationships - Implicit

Example – Risk Management Objectives are Influenced by All Perspectives

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Dependence
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & trust Frameworks	D	
Logical	Information	Policy	Information Processing & Services	Trust Model	Logical Domains	Time & Sequence Model
Physical	Data	Practices & Procedures	Data Comms & Mechanisms	Data & System Governance		
Component	Products & Tools	Risk Standards	Protocol Standards	I&AM Standards	Location Standards	Time Standards
Management	Delivery & Continuity	Risk Management	Process Management	Governance Management	Environment Management	Time & Sequence Management

Risk management objectives are driven explicitly by risk context

Risk management objectives are driven implicitly by the context provided by other perspectives

Lateral Relationships - Systemic

Example – Peer Elements are Inter-related, Not Isolated

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)		
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance		
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & trust Frameworks	Domain Framework	Time Framework
Logical	Information	Policy	Information Processing & Services	Trust Model		
Physical	Data	Practices & Procedures	Data Comms & Mechanisms	Data & System Governance		
Component	Products & Tools	Risk Standards	Protocol Standards	I&AM Standards		
Management	Delivery & Continuity	Risk Management	Process Management	Governance Management	Management	Management

The perspectives at any layer of abstraction are systemically related to each other

- Influence each other
- Are influenced by each other

The policy framework & risk management framework are not in isolation

Risk management objectives influence, and are influenced by, peer elements

Holistic Relationships

Example – Holistic Risk Management Objectives

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Dependence
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & trust Frameworks	Domain Framework	Time Framework
Logical	Information	Policy	Information Processing & Services	Trust Model		
Physical	Data	Practices & Procedures	Data Comms & Mechanisms	Data & System Governance	Infrastructure	Processing
Component	Products & Tools	Risk Standards	Protocol Standards	I&AM Standards		
Management	Delivery & Continuity	Risk Management	Process Management	Governance Management		

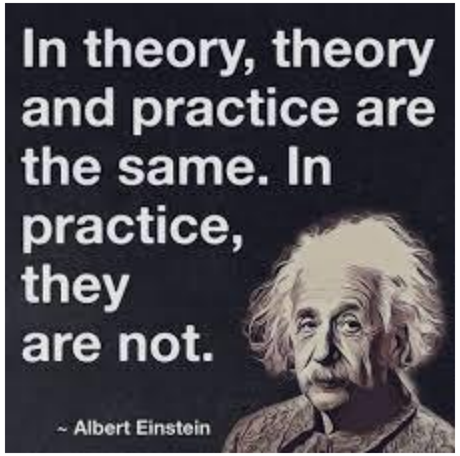
Risk management objectives are driven explicitly by risk context

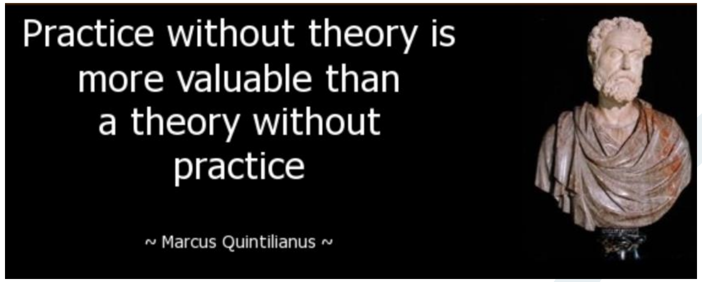
Risk management objectives are driven implicitly by the context provided by other perspectives

Risk management objectives influence, and are influenced by, peer elements

Architect's Dilemma – Unattainable Idealism

- Architect's "Ivory Tower"
- Enterprise Architecture rarely starts from a 'green field'
- How to ever complete the strategy in ever-changing complexity
    - Idealist strategy is overcome by operational practicality
- Scope is rarely 'all of enterprise' in practice
    - Budget & support challenges
- How to define the starting point
    - Scope the initiative / project
    - Write and issue an RFP
- How to deliver 'something' before 'everything'





SABSA Calibrated Architecture

SABSA's Unique Capability to Calibrate Architecture

- What must be architected, if not the whole enterprise?
  - A perspective of enterprise
    - e.g. governance architecture
  - A new approach
    - e.g. Agile, DevOps, Digital transformation
  - A solution
    - e.g. Incident management, end-point security, or DLP
- The SABSA "mental model" to solve a complex problem is consistent whatever the problem space
- A single method can be calibrated for:
  - Scope
  - Scale
  - Time
  - Budget

SABSA A series of integrated frameworks, models, methods and processes, used independently or as an holistic integrated technique
SABSA Foundation

Calibrated by Scale – Analysis Levels

Level	Description
Macro	**Enterprise Architecture** The target-state for 'all of Enterprise' as a complex system: • Across each of the 6 perspectives • Through each of the 6 layers of abstraction • Through-life
Meso	**Architecture** A mid-range population for a specific community (such as a business function or unit), an enterprise approach (such as Agile, DevOps, Digital Transformation or Product R&D). Falls between Macro and Micro levels and determines traceable connections between them
Micro	**Solutions Architecture** Architecture applied to provide a suite of solutions in a class (such as Incident Management or I&AM), or a solution in a particular specialised setting (such as individual applications, infrastructure components, or products)

Calibrated by Scale – Analysis Level Conventions

Conventions for Architecture Layers to Apply to Analysis Levels

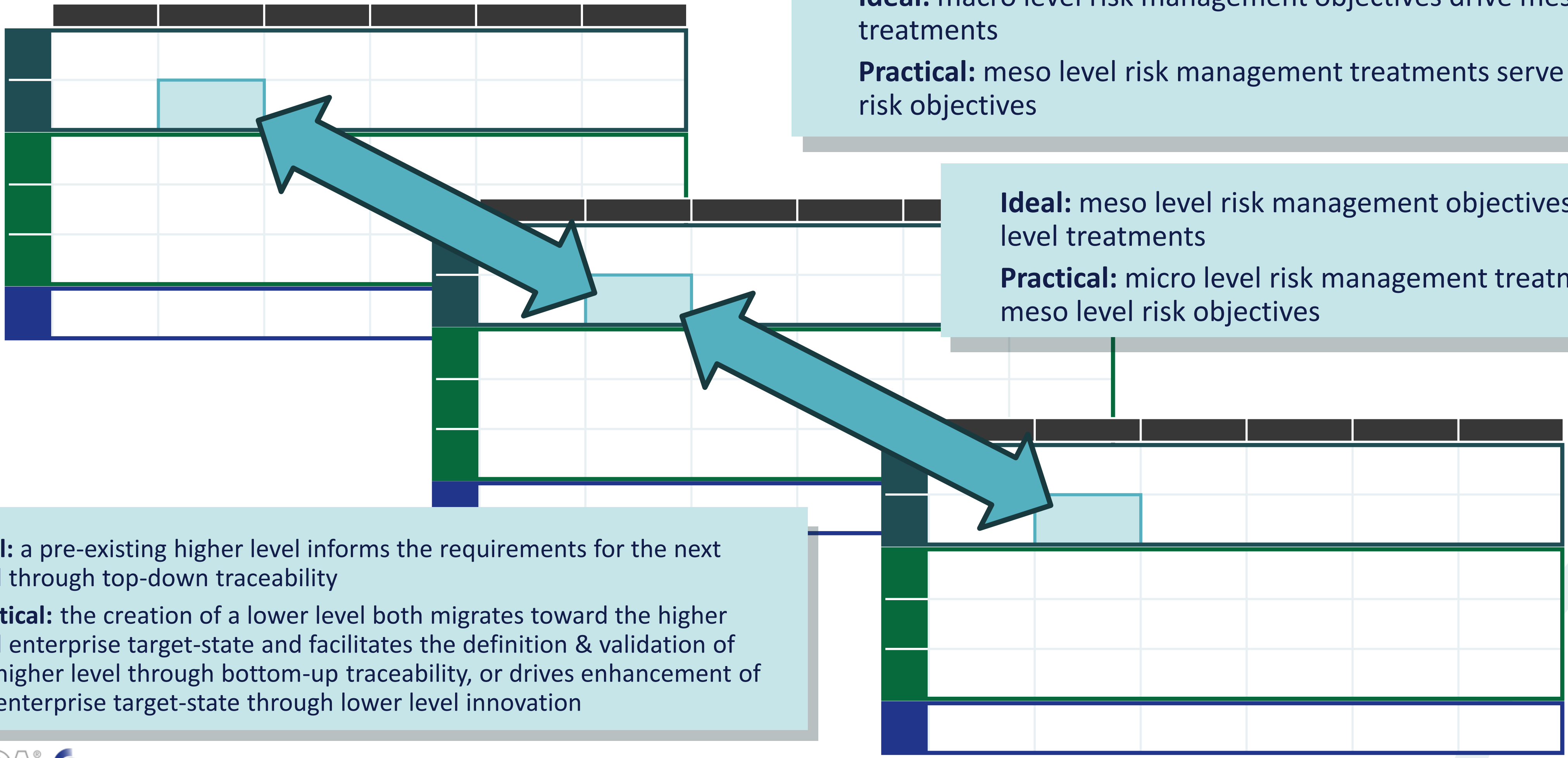
Level	Conventions
Macro	Defines the end goal Delegates requirements to, and is served by, the Meso level Specified independently of the Meso level which is treated as a black box Has no interface with the Micro level
Meso	Serves the requirements of the Macro level Is not an end goal in itself but a means to the Macro end goal Delegates requirements to, and is served by, the Micro level Specified independently of the Micro level which is treated as a black box
Micro	Serves the requirements of the Meso level Is not an end goal in itself but a means to the Meso goal

Calibrated by Scale – A Context for Innovation

Cell to Cell Example (valid for any cell)

Ideal: macro level risk management objectives drive meso level treatments

Practical: meso level risk management treatments serve macro level risk objectives



Ideal: meso level risk management objectives drive micro level treatments

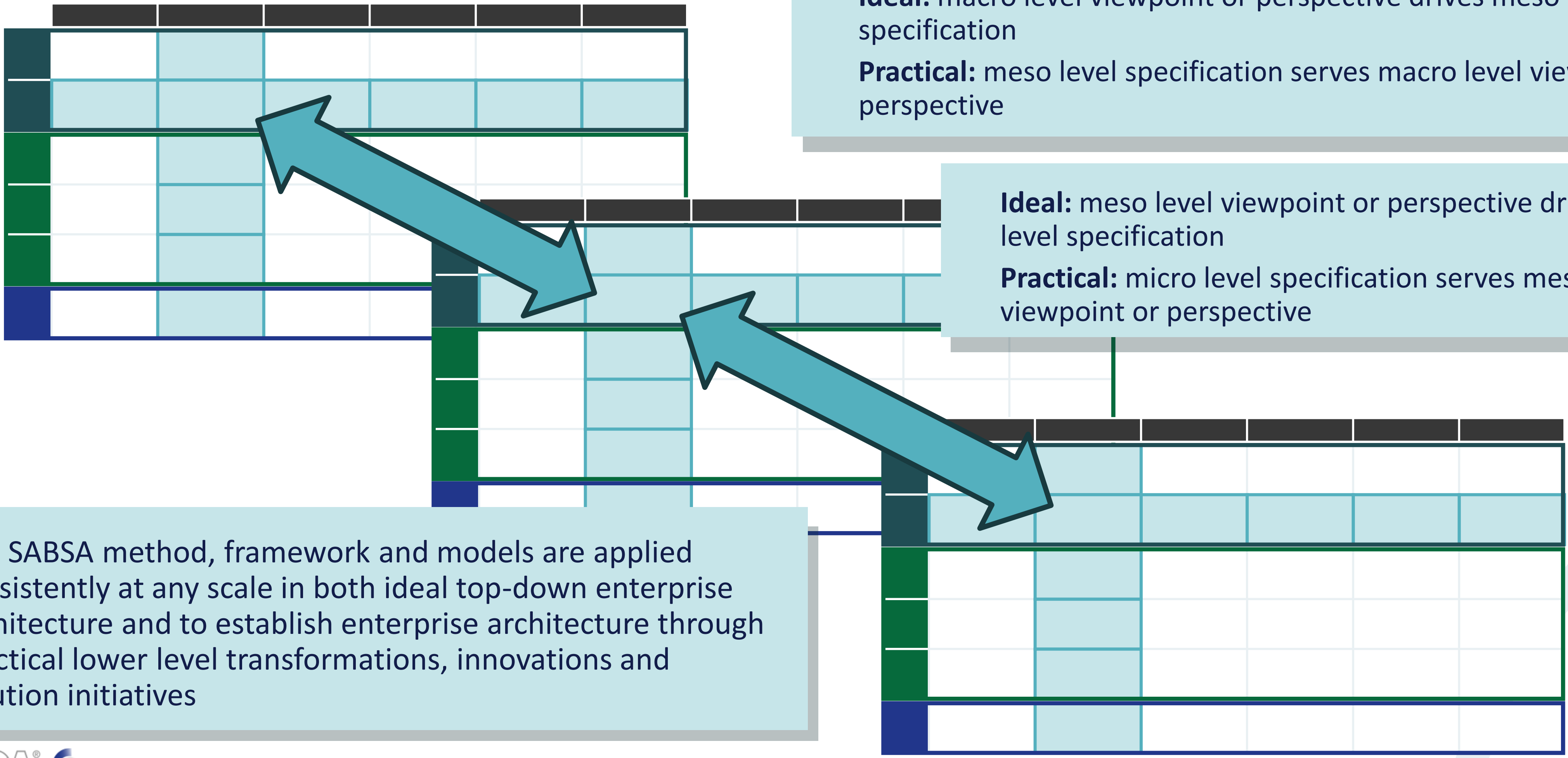
Practical: micro level risk management treatments serve meso level risk objectives

Ideal: a pre-existing higher level informs the requirements for the next level through top-down traceability

Practical: the creation of a lower level both migrates toward the higher level enterprise target-state and facilitates the definition & validation of the higher level through bottom-up traceability, or drives enhancement of the enterprise target-state through lower level innovation

Calibrated by Scale – A Context for Innovation

Cell to Cell Example (valid for any cell)



Ideal: macro level viewpoint or perspective drives meso level specification

Practical: meso level specification serves macro level viewpoint or perspective

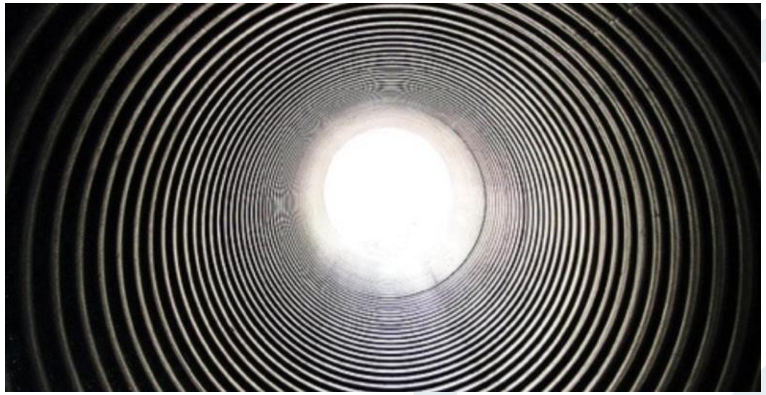
Ideal: meso level viewpoint or perspective drives micro level specification

Practical: micro level specification serves meso level viewpoint or perspective

The SABSA method, framework and models are applied consistently at any scale in both ideal top-down enterprise architecture and to establish enterprise architecture through practical lower level transformations, innovations and solution initiatives

Architect's Dilemma – Tunnel Vision

- The approach to create vertically-related, calibrated, architectures solves many problems but it may create a different one: Tunnel Vision
- Any sub-level below Enterprise is by definition not Enterprise, it is only one particular viewpoint or aspect of Enterprise
- Natural bias / tunnel vision issues:
  - Looking 'downward' from a level, we see multiple dependencies and relationships: many contributing "means to an end", but looking 'upward' from a level, we may see an exclusive relationship to the higher level: a single "means to an end"
  - Focus on our own areas of expertise and interest causes peer architectural abstractions to be excluded from our view, or missed, even if they contain more appropriate options



SABSA Systemic Vision

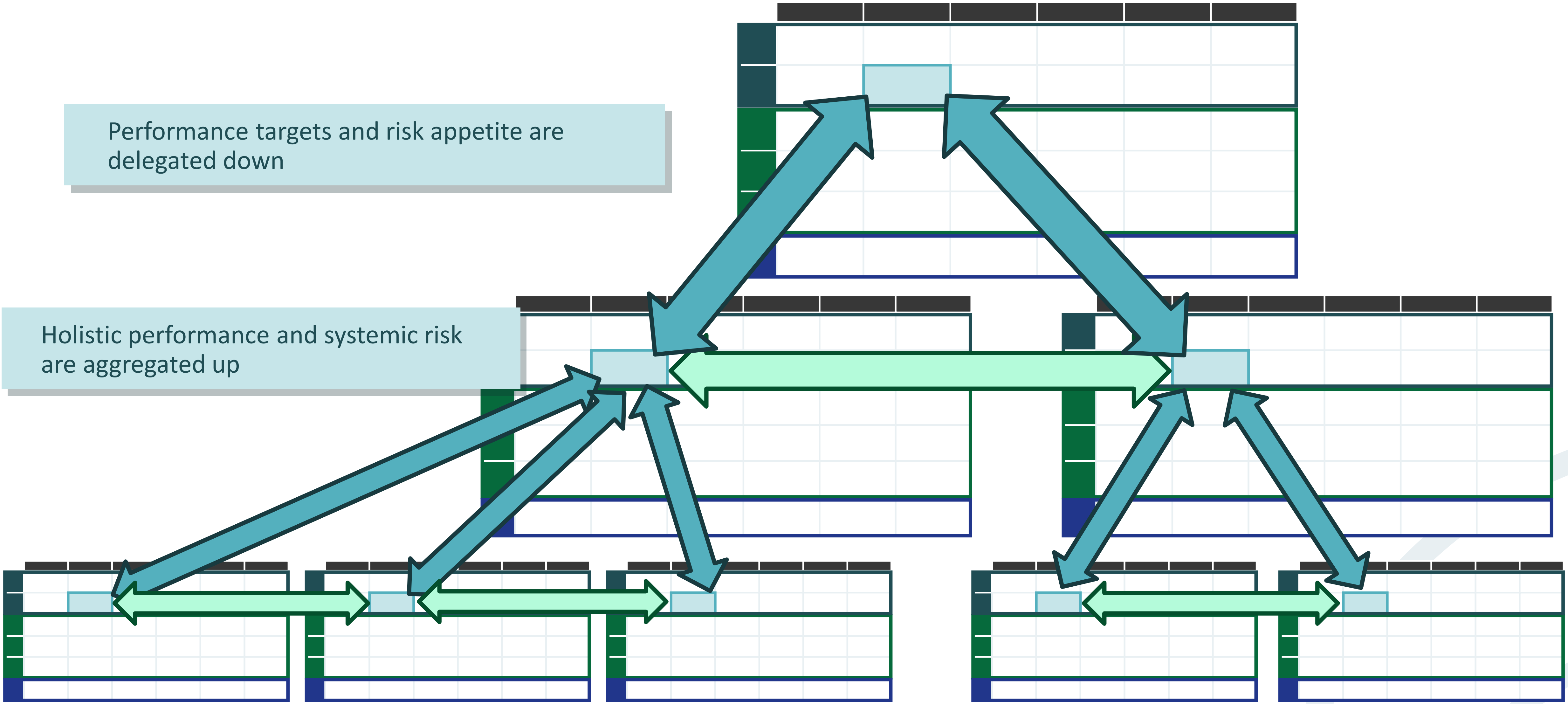
Enable non-enterprise architecture in an enterprise context

- A key role of a true Enterprise Architecture method is to create the structure that enables non-Enterprise Architects to act in an holistic Enterprise context
- The consistency of SABSA structures (method, framework and models) irrespective of the scale or scope to which they applied enables:
  - Vertical traceability to context
  - Peer systemic relationships to be modelled, understood, and acted upon

SABSA Systemic Vision - Example

Performance targets and risk appetite are delegated down

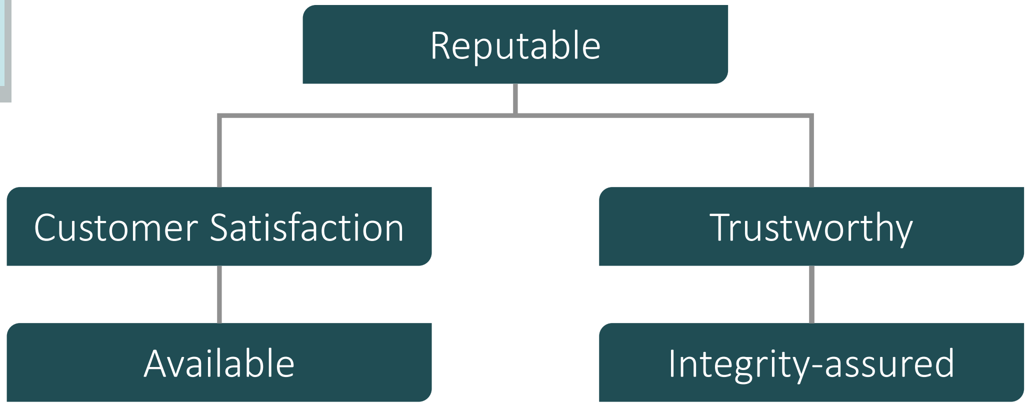
Holistic performance and systemic risk are aggregated up



SABSA Risk Distribution & Performance Aggregation Structure

Attributes Dependency

Distribute risk appetite and performance targets through a dependency tree



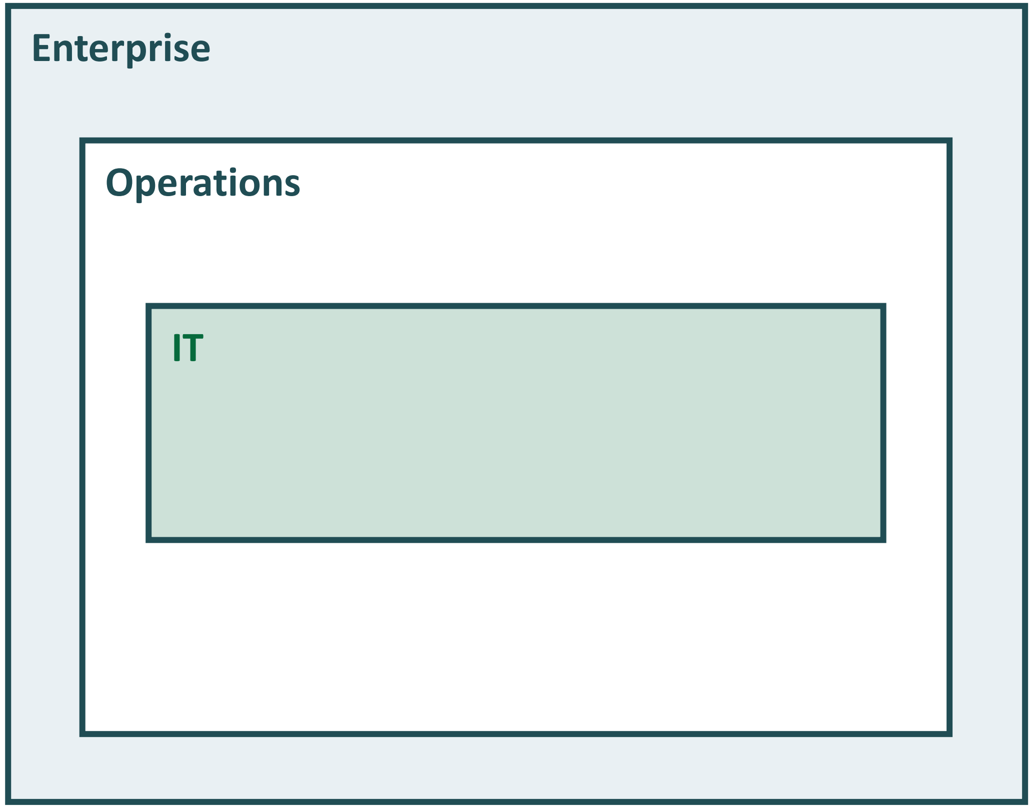
Aggregate compliance to appetite and performance against targets

Attributes provide the normalised definition to distribute and aggregate what is at risk

SABSA Risk Distribution & Performance Aggregation Structure

Domain Hierarchy

Distribute dominion of authority through the Domain model to lower authorities



Aggregate distributed dominions to higher Domain Authority

Domains provide the normalised structures to distribute and aggregate dominion of authority over risk

What is the SABSA Risk Strategy Framework?

SABSA Risk Strategy Framework

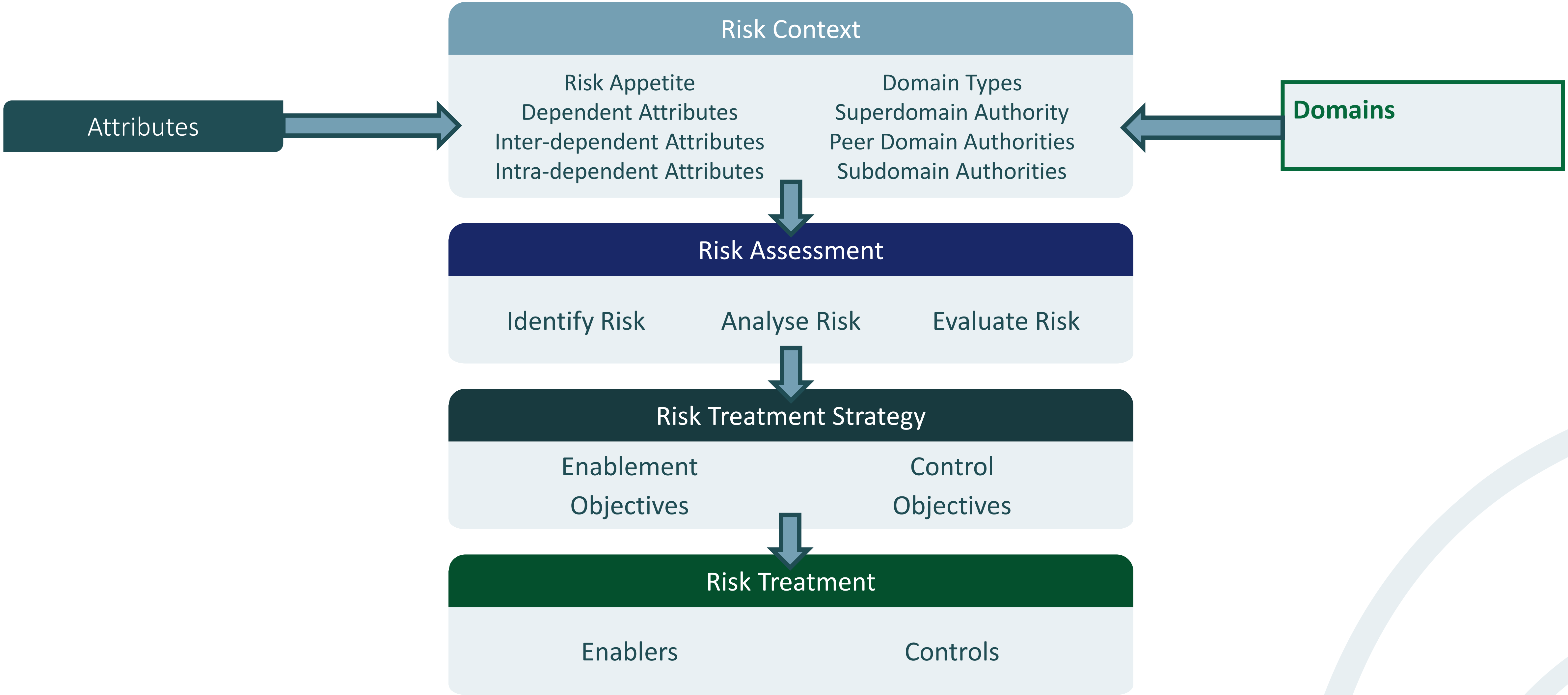
The structured SABSA concepts and techniques that support our work, simplify complexity, and inform risk decisions

The application of the SABSA Risk Strategy Framework results in risk treatment strategy comprised of control objectives to manage potentially negative outcomes and enablement objectives to manage potentially beneficial outcomes

SABSA Risk Strategy Framework - Purpose

- Achieve an appropriate balance between realising opportunities for gains while minimising losses
- Apply an architecturally structured and comprehensive approach
- Integrate and align risk silos to holistically embed risk management into all levels and perspectives of Enterprise
- Traceably align risk management activities to Enterprise context
- Customise ‘risk thinking’ to be instinctive to the Enterprise culture
- Provide a method to include and engage Stakeholders at all levels in meaningful terms
- Deliver clarity and certainty of risk ownership and accountability
- Empower risk owners to make objective and proportionate risk decisions in-context
- Cater for the systemic, interconnected, interdependent nature of risk complexity
- Create a robust method that offers pre-emptive early warning capability and dynamically adapts to complex disruption and organic innovation

SABSA Risk Strategy Framework



Fundamentals of Governance in SABSA

Section 3

Open Discussion – What is Governance?

What is Governance?

Governance The way in which an organisation is controlled ***OED***

Governance Authority and control: the way in which something is managed ***Collins***

Governance The process of overseeing control and direction ***Merriam Webster***

SABSA Governance

The process of allocating and enacting authority, roles and responsibilities to direct and manage a Domain

SABSA Security Governance

The process of allocating and enacting authority, roles and responsibilities to direct and manage Domain security

What is the SABSA Governance Framework?

SABSA Governance Framework

The structured SABSA concepts and techniques that support our work, simplify complexity, and make informed decisions regarding roles and responsibilities

The application of the SABSA Governance Framework results in an architected Governance model that defines roles & responsibilities, and associated communications & reporting structures

SABSA Governance Framework Purpose

- Understand and communicate the dependencies between Domains of a complex system
- Resolve the competing and conflicted interests of parties in a complex system
- Allocate and enact clear Accountability within a complex system
- Allocate and enact clear Responsibilities within a complex system
- Define the necessary channels and types of communication required between Accountable and Responsible parties
  - Who should be Consulted to understand requirements
  - Who should be Informed of Responsibility to meet requirements
  - Who should be Informed of Performance and Compliance

Governance Traceability

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Dependence
	Goals, Targets, Value & Assets	Opportunities & Threats	Value Chain, Core Processes & Capabilities	Culture, Org. Structure & Relationships	Territories, Jurisdictions & Sites	Time & Sequence Dependencies
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & Trust Frameworks	Domain Framework	Time Framework
	Attributes Taxonomy & Profile	Enablement & Control Objectives	Process Strategy & Architecture	Ownership & Trust Relationships	Security Domain Framework	Architecture Roadmap

Explicit Governance Traceability

The Governance Framework represents the authority, roles and responsibilities within the Enterprise structure and relationships, aligned to its culture

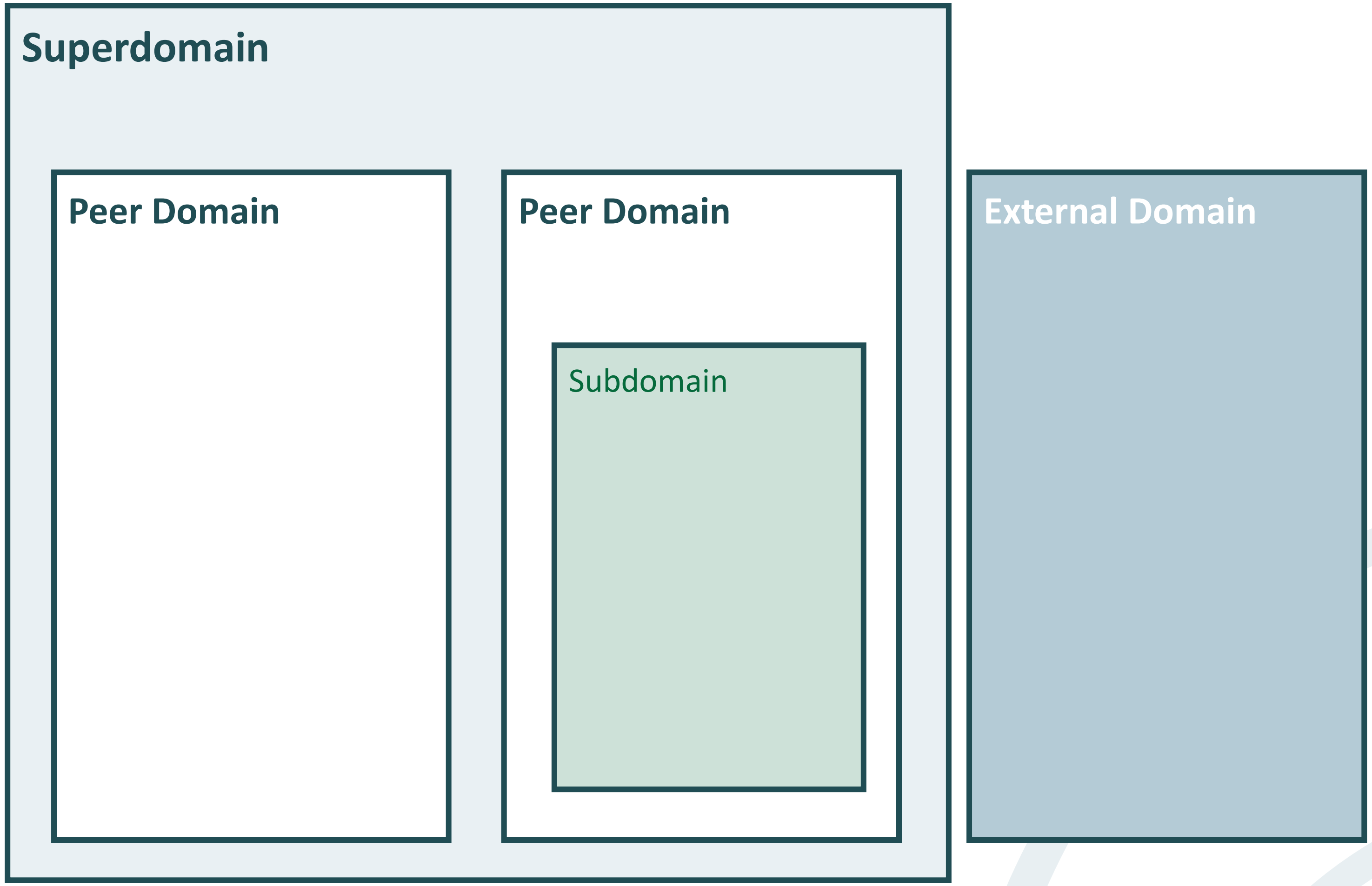
Implicit Governance Traceability

However, the Enterprise Domain structure is not an organisation chart, so the Governance Framework must also be capable of representing authority, roles and responsibilities for:

- Goals & assets
- Risk & policy
- Capabilities & processes
- Locations, sites & jurisdictions
- Time & sequence dependencies

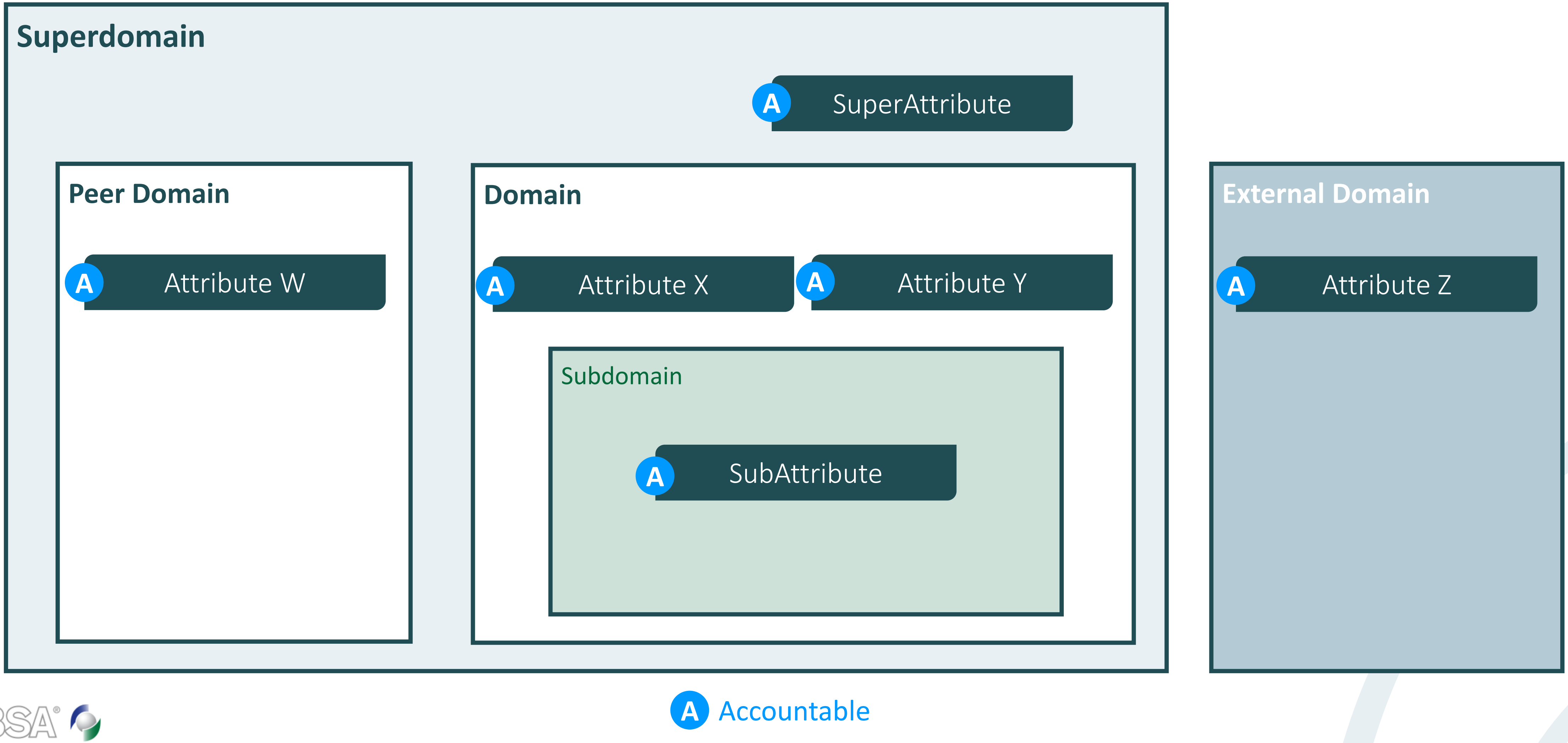
Authority in a Complex System

- The Domain Authority is accountable for ("owns") the risk to, and the performance of, the Attributes in a Domain
  - The Domain defines the type and scope of the Authority's dominion
  - The Attributes, as the 'assets' of the Domain, define what the Authority has dominion over
- However, the Domain is not in isolation but exists in the risk and performance context of other Domains in a complex dependency structure
- The Domain:
  - Serves its Superdomain
  - May interact with Peer Domains
  - May distribute Risk Appetite and Performance Targets to its Subdomain(s)



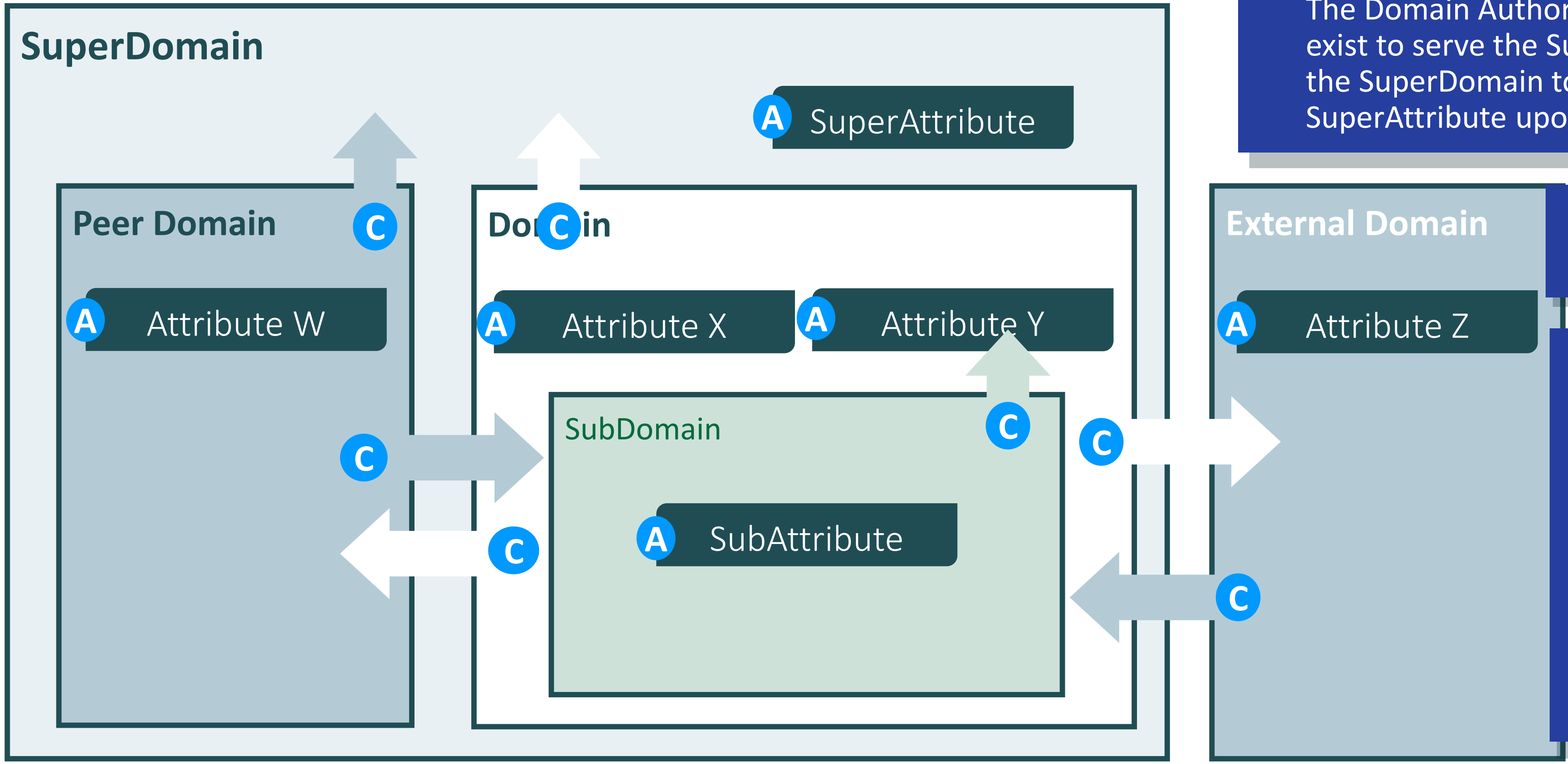
Accountability Model

Each domain authority is accountable for Attributes in their Domain



Consultation Model

Consult SuperDomain and Peers to determine Attribute Dependency



The Domain Authority risk appetite & performance targets exist to serve the SuperDomain Authority, and must consult the SuperDomain to identify dependencies of the SuperAttribute upon Attributes X and Y

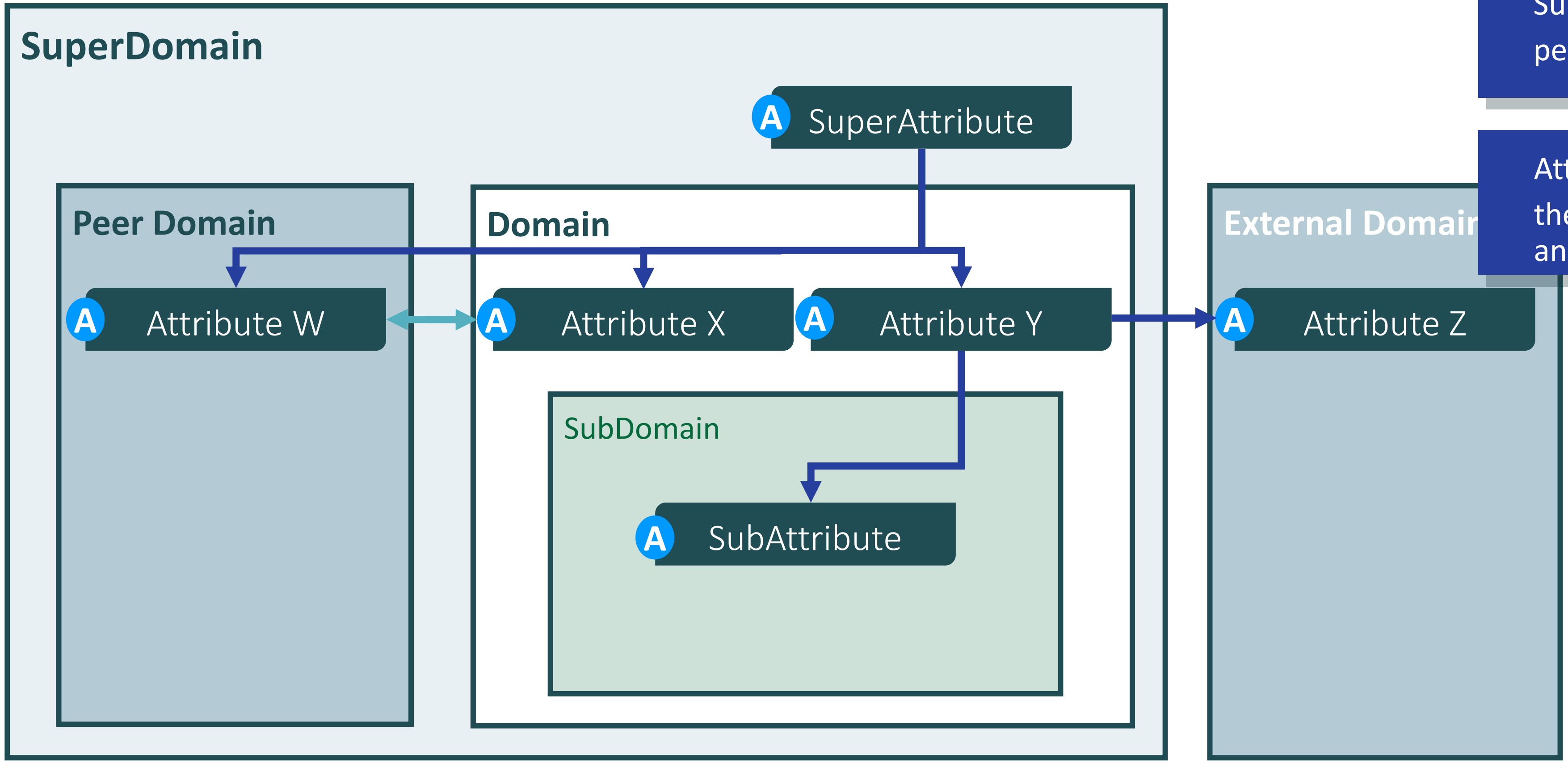
Similarly, the SubDomain Authority consults the Domain Authority

The Domain Authority risk appetite & performance targets may interact with those of the Peer Domain as they share a common Superdomain, and must consult the Peer Domain to identify dependencies of Attributes X and Y upon Attribute W. Similarly, the Peer Domain must consult the Domain to identify dependencies of Attribute W upon Attributes X and Y

C Consult   A Accountable

Attribute & Domain Dependency Model

Dependency Type Example



SuperAttribute is dependent upon the risk and performance of Attributes W, X and Y

Attribute Y is dependent upon the risk and performance of the SubAttribute and Attribute Z

Attributes W and X are inter-dependent:

Attribute W is dependent upon the risk and performance of Attribute X

Attribute X is dependent upon the risk and performance of Attribute W

Attributes X and Y are independent: Their success does not depend upon the others' risk and performance

Delegated Responsibility: Custodians & Trustees

Responsibility delegated with or without policy authority

- Accountability and liability cannot be delegated
- A Domain may delegate responsibility in one of two ways

Responsible Custodians (RC)
Owner of Attributes upon which the Domain depends
Comply with the Risk Appetite of the Domain's Attribute(s)
Meet part or all of the Performance Target of the Domain's Attributes
Has no policy authority over the Domain
By default, all responsible Domain's are custodians

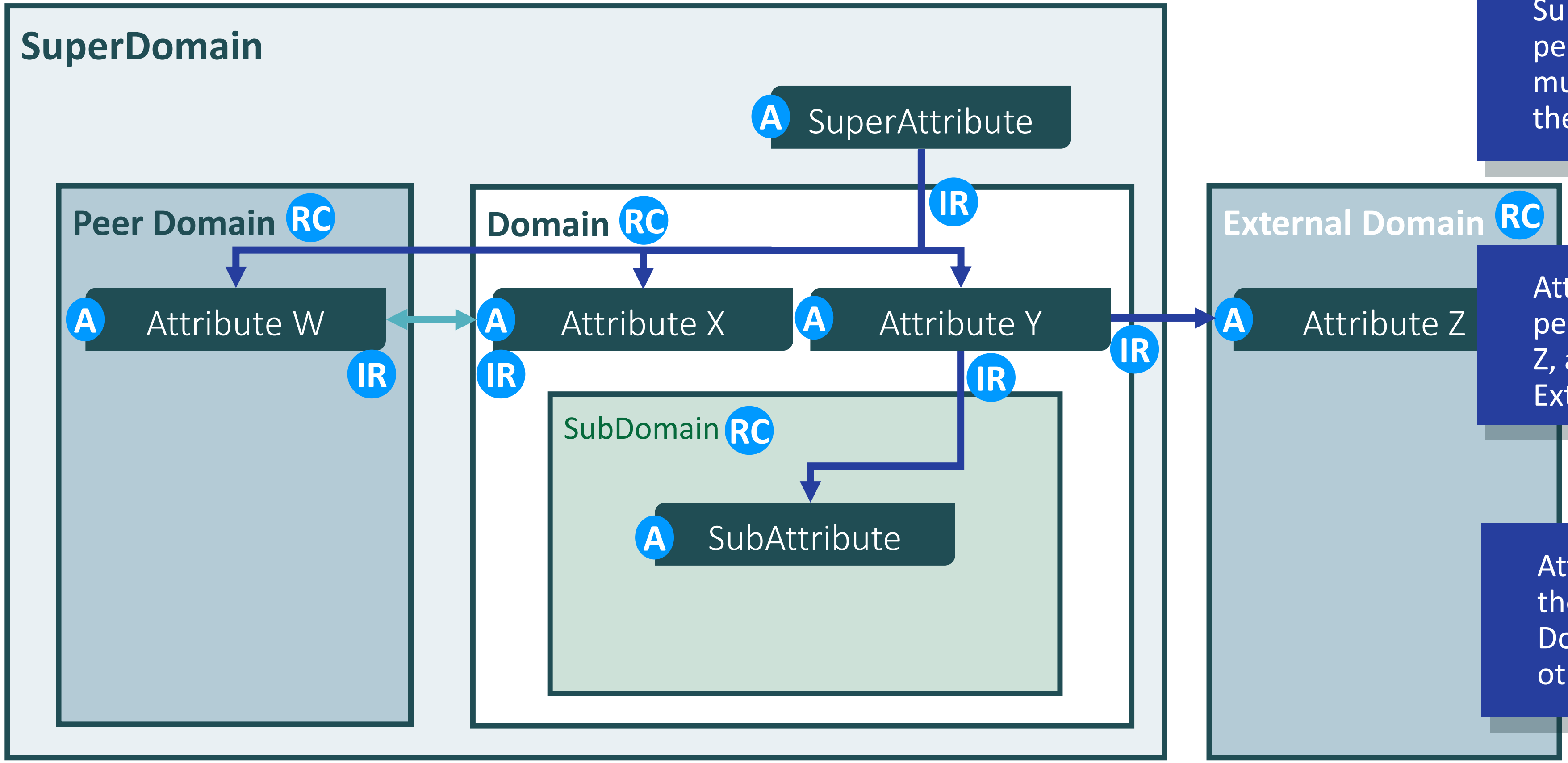
Responsible Trustees (RT)
Usually assigned only when the Domain Authority is:
--Inexperienced, unqualified, vulnerable
- Not in a position to make an informed decision
Acts as policy authority on behalf of the Domain Authority
Makes policy decisions for the Domain but is not accountable

Retained Responsibility

Where no domain exists to which responsibility can be delegated, a Domain Authority may be both Accountable and Responsible

Responsibility Model

Accountable authorities delegate responsibility in the direction of dependency



Superattribute is dependent upon the risk and performance of Attributes W, X and Y, and must Inform the Domain and Peer Domain of their Responsibilities IR

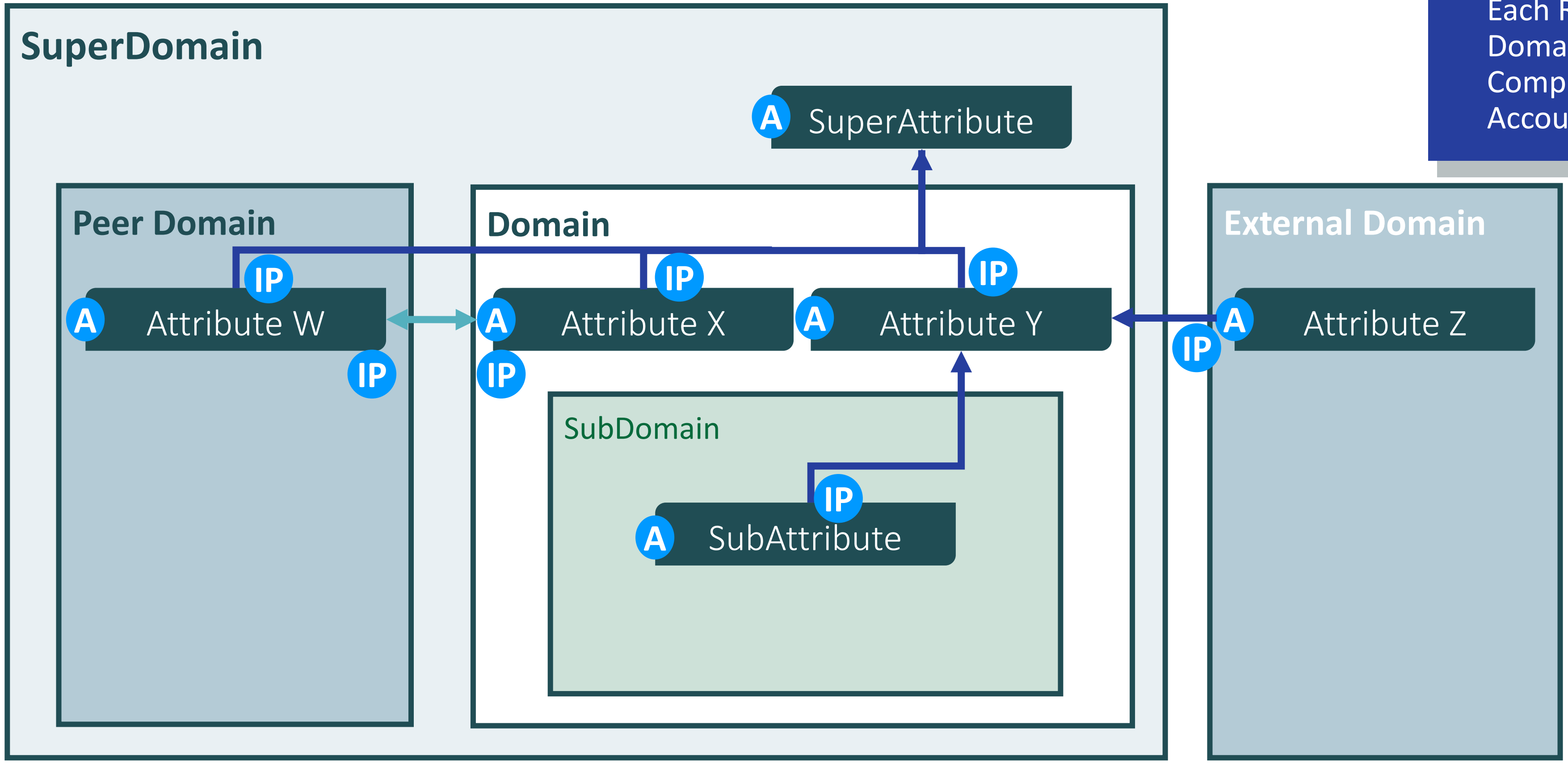
Attribute Y is dependent upon the risk and performance of the SubAttribute and Attribute Z, and must Inform the Subdomain and External Domain of their Responsibilities IR

Attributes W and X are inter-dependent upon the other's risk and performance, and the Domain and Peer Domain must Inform each other of their Responsibilities IR

RC Responsible Custodian IR Inform Responsibility

Reporting Model

Responsible authorities inform performance to dependent Accountable authorities



Each Responsible Domain informs the Accountable Domain on the degree of Performance and Compliance of the Attributes upon which the Accountable Domain depends IP

The Subdomain reports on the SubAttribute to the Domain IP

The External Domain reports on Attribute Z to the Domain IP

The Peer Domain reports on Attribute W to the Domain and SuperDomain IP

The Domain reports on Attribute X to the Peer Domain and SuperDomain IP

The Domain reports on Attribute Y to the SuperDomain IP

IP Inform Performance

Roles & Responsibilities Model - Example

Accountable: DOMAIN			
Attribute: ATTRIBUTE X			
	Consulted (to determine dependent Attributes)	Responsible (dependency) (and informed of responsibility)	Informed (dependent) (of performance & compliance)
External Authority			
SuperDomain	C		IP (SuperAttribute depends on X)
Peer Domain	C		
Peer Domain (of dependent Attribute)			IP (Attribute W depends on X)
Peer Domain (of dependency Attribute)		R IR (Attribute X depends on W)	
External Domain	C		
External Domain (of dependent Attribute)			
External Domain (of dependency Attribute)			
SubDomain (of dependency Attribute)			

Roles & Responsibilities Model - Example

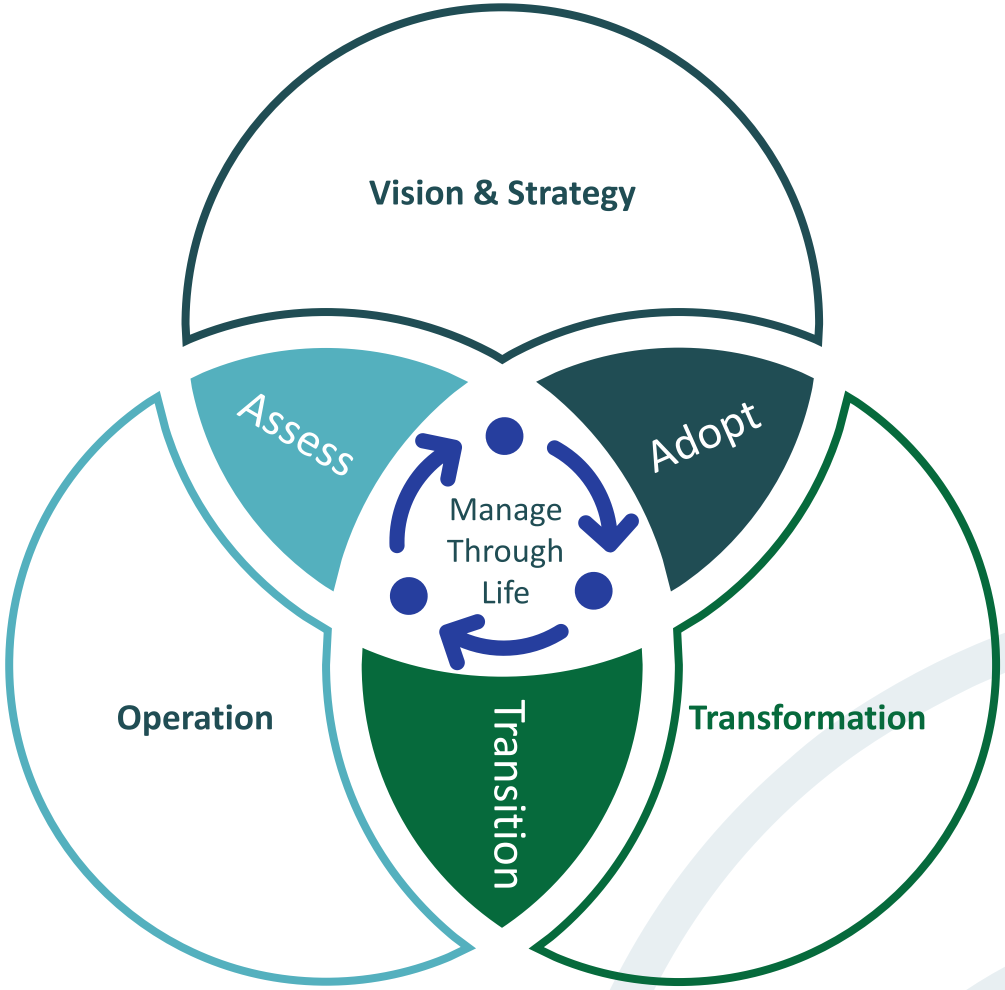
Accountable: DOMAIN

Attribute: ATTRIBUTE Y

	Consulted (to determine dependent Attributes)	Responsible (dependency) (and informed of responsibility)	Informed (dependent) (of performance & compliance)
External Authority			
SuperDomain	C		IP (SuperAttribute depends on Y)
Peer Domain	C		
Peer Domain (of dependent Attribute)			
Peer Domain (of dependency Attribute)			
External Domain	C		
External Domain (of dependent Attribute)			
External Domain (of dependency Attribute)		R IR (Attribute Y depends on Z)	
SubDomain (of dependency Attribute)		R IR (Attribute Y depends on SubAttribute)	

SABSA Governance Framework

Accountable Domain Authority	Strategy	Identify dependent Attributes: Consult Superdomain, Peer Domains & External Authorities Determine: Risk Appetite, Performance Targets & Objectives Set: Policy to meet objectives
	Adopt	Identify dependencies: Subdomains, Peer Domains & External Domains Inform: Dependencies of responsibility
Responsible Domain Authorities	Transform	Design: Controls & Enablers to meet Objectives Design: Systems, Processes & Resourcing Models
	Transition	Implement: Controls & Enablers Establish: Systems, Processes & Resources
	Operate	Monitor Performance: Controls & Enablers Manage: Systems, Processes & Resources
	Assess & Report	Assess: Performance of Attributes against Risk Appetite & Performance Targets Report: Performance of Attributes against Risk Appetite & Performance Targets



Fundamentals of Assurance in SABSA

Section 4

Open Discussion – What is Assurance?

What is Assurance? Sectoral Definitions

Assurance Pursuant to an accountable relationship between two or more parties, an IT audit and assurance professional is engaged to issue a written communication expressing a conclusion about the subject matters for which the accountable party is responsible. Assurance refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter. ***ISACA***

Assurance Initiative An objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the enterprise. ***ISACA***

Assurance Assurance is grounds for confidence that an IT product meets its security objectives. Assurance can be derived from reference to sources such as unsubstantiated assertions, prior relevant experience, or specific experience. However, the CC provides assurance through active investigation. Active investigation is an evaluation of the IT product in order to determine its security properties. ***Common Criteria***

What is Assurance? Definitions

Assurance A positive declaration intended to give confidence ***Cambridge***

Assurance Abjective certainty; being certain as to a fact, certitude; confidence, trust ***OED***

Assurance Confidence of mind or manner: easy freedom from self-doubt or uncertainty ***Merriam Webster***

SABSA Assurance

SABSA Assurance

Providing defined levels of confirmation, trust and confidence that the SABSA Architecture artefacts and related management processes meet defined target requirements and target properties

SABSA Assurance Management

The process of managing assurance, including governing, planning and executing an enterprise assurance programme to provide confirmation, trust and confidence that Architecture artefacts and processes meet target requirements and properties such as: Business-driven; complete; resilient; fit-for-purpose; managed within risk appetite; performing as expected

SABSA Assurance Process

The set of active investigation activities that comprise 'assurance management' including audits, tests, reviews, checks & balances

What is the SABSA Assurance Framework?

SABSA Assurance Framework

The structured SABSA concepts and techniques that support our work, simplify complexity, and make informed decisions regarding assurance

The application of the SABSA Assurance Framework results in a set of architected assurance processes that provide defined levels of confirmation, trust and confidence that Architecture artefacts and processes meet target requirements and properties

What is the Subject of The SABSA Assurance Process?

The SABSA Assurance Framework assures SABSA artefacts & processes

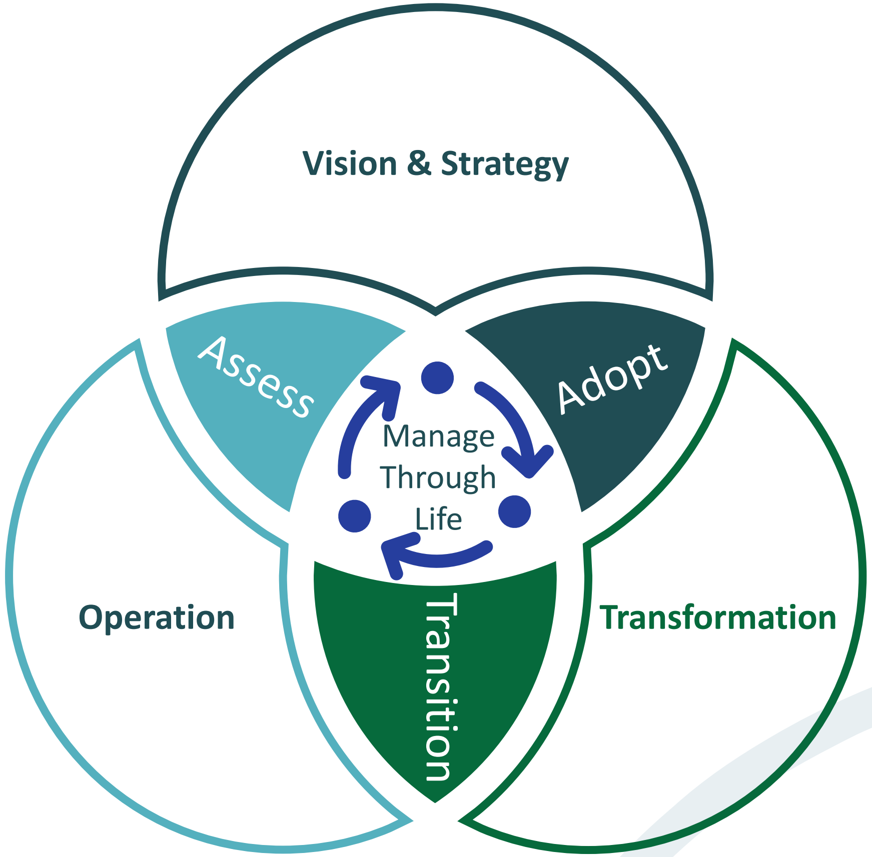
	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Dependence
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & trust Frameworks		
Logical	Information	Policy	Information Processing & Services			
Physical	Data	Practices & Procedures	Data Comms & Mechanisms	Data & System		
Component	Products & Tools	Risk Standards	Protocol Standards			
Management	Delivery & Continuity	Risk Management	Process Management			

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Management	Delivery and Continuity	Risk Management	Process Management	Governance, Management	Environment Management	Time 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	Analyse Requirements	Assess Risks	Manage Value Chain	Manage Relationships	Manage Facilities	Manage Time
Conceptual	Define Requirements	Define Risk Objectives	Manage Processes	Define Trust Relationships	Define Domains	Define Time Framework
Logical	Manage Information	Manage Policy	Manage Services	Manage Roles	Manage Domains	Manage Time Model
Physical	Manage Data	Manage Practices	Manage Mechanisms	Manage Access	Manage Infrastructure	Manage Processing Schedule
Component	Manage Configuration	Manage Standards	Manage Protocols	Manage Entities	Manage Addressing	Manage Timing

SABSA®

SABSA Assurance Framework Purpose

- Articulate the needs of the parties in a complex system for confirmation, trust and confidence
- Define assurance targets and properties in-context
- Define assurance levels required
- Define the assurance activities necessary to provide confirmation, trust and confidence commensurate with each required Assurance level
- Ensure that a dependent domain authority or element can trust its dependencies to deliver required benefits and operate within risk appetite
- Ensure that a domain authority or element upon which another depends is meeting its risk and benefit obligations



The SABSA Assurance Framework provides confirmation, trust and confidence that the requirements for architecture artefacts have been defined and validated, and that the architectural processes through-life have been conducted to a level commensurate with requirements

Assurance Requirements & Target Properties

Provide confirmation, trust & confidence that architecture:

- Is business-driven
- Is traceable – that each artefact & process meets its explicit & implicit requirements
- Delivers the required capabilities to the defined performance level
- Operates within risk appetite
- Delivers the business benefits for which it was commissioned
- Is complete
- Is of adequate quality
- Is resilient & robust
- Is governable & is being governed properly
- Is manageable & is being managed properly
- Functions as intended
- Is fit-for-purpose
- Etc.

The Need for Assurance Levels

Provide confirmation, trust & confidence that architecture:

Scope	Investigations can involve varied volumes of artefacts & processes
Depth	Investigations can involve varied levels of granularity and detail
Diligence	The degree of rigour to be applied in the investigation has varied levels of structure and formality

Assurance Levels - Influences

Critically / Impact

	Safety (S)	Environmental (E)	Operational (O)	Cost (C)
Catastrophic I	Single death or multiple serious injuries or severe occupational illnesses	Major widespread damage or serious breach of legislation. Ineffective control measures	Loss of the platform or equipment	Greater than £500k
Critical II	A single severe injury or occupational illness or multiple minor occupational illnesses	Noticeable widespread impact on the environment. Control measures minimally effective	Loss of mission capability	Between £200k and £500k
Marginal III	At most a single minor injury or a single minor occupational injury	Minor impact on the environment. Control measures substantially effective	Limited mission capability	Limited mission capability
Negligible IV		Little impact. Control measures comprehensive	Minimal disruption to mission capability	Less than £10k

From Living RCM

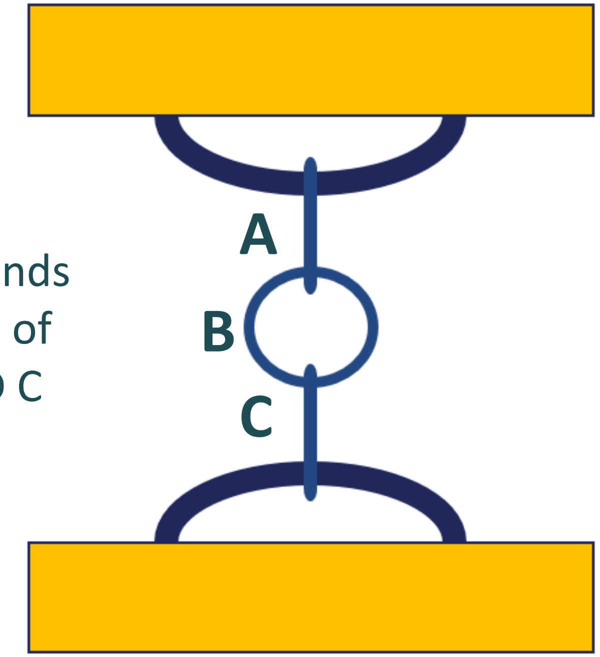
The level of assurance required increases with the degree of criticality, independently of loss probability

Assurance Levels - Influences

Dependency condition

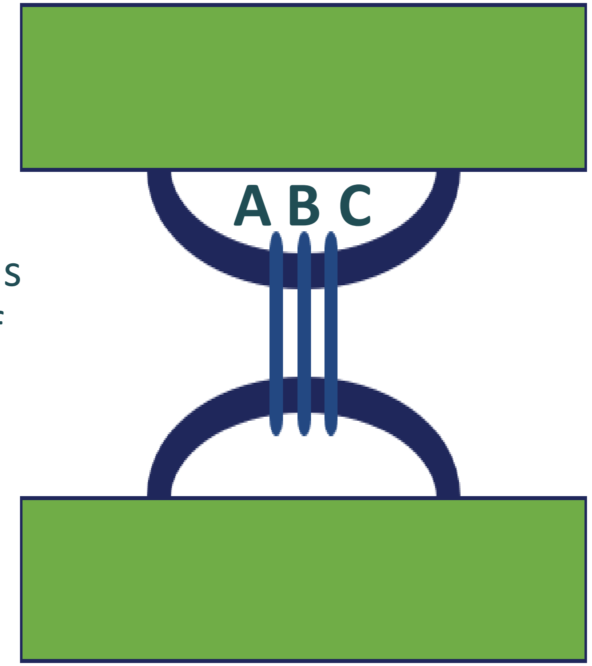
AND condition

Success depends
upon success of
A AND B AND C



OR condition

Success depends
upon success of
A OR B OR C



AND dependencies increase risk and decrease resilience

OR dependencies decrease risk and increase resilience

Assurance Levels - Influences

Pure / inherent risk in the operating environment

Assurance Levels - Influences

- Residual risk in the operating environment

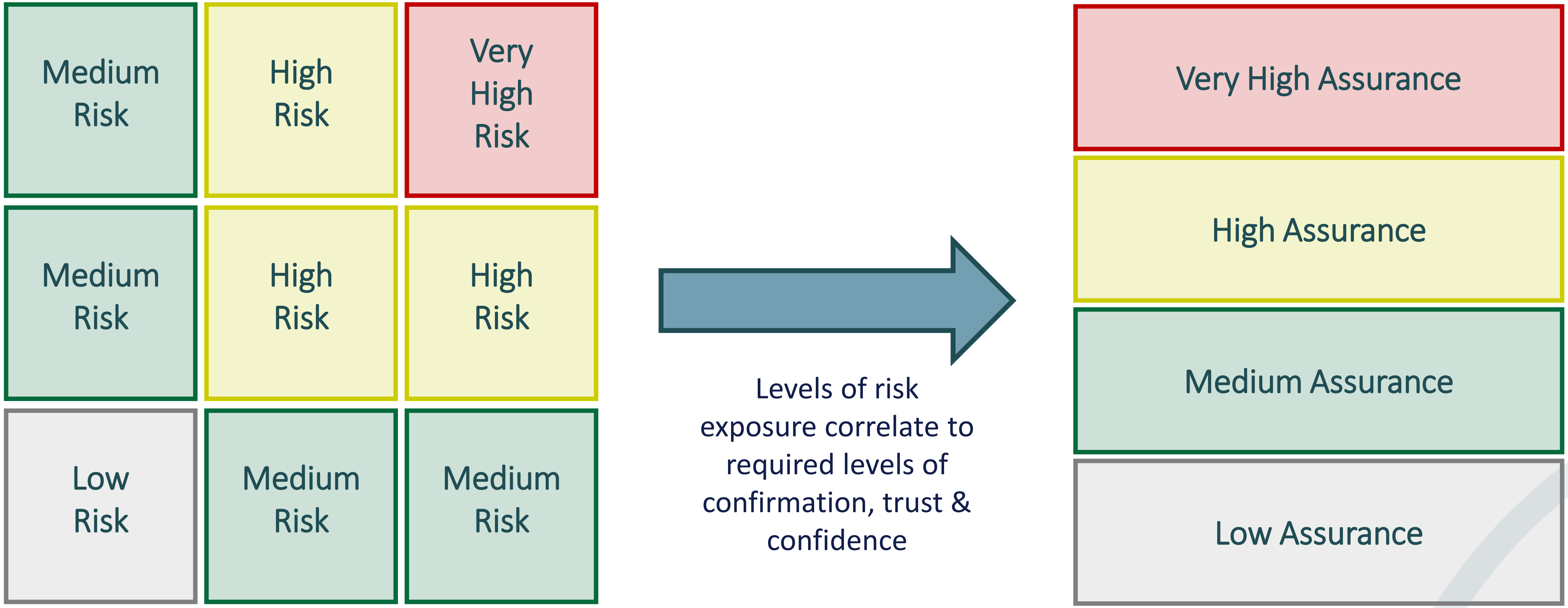
Assurance Levels - Influences

Maturity Level

5 Optimised	The SABSA artefact, its underlying processes, and the artefacts and processes with which it is integrated and aligned, are holistically and continuously optimised to meet changing business requirements
4 Monitored	The SABSA artefact and its underlying processes are monitored and measured through-life, performance is reported to appropriate Domain Authorities, and are assured to the level specified by an assurance framework
3 Defined	The SABSA artefact is created using a formal process, under the dominion of an identifiable authority, is documented and communicated to all relevant stakeholders, and is integrated and aligned with all other relevant SABSA or wider-Enterprise processes and artefacts
2 Informal	The SABSA artefact is created and maintained using similar but non-standardised processes, unsupported by policy, without assigned governance roles, and is not integrated and aligned with other SABSA or wider-Enterprise processes and artefacts
1 Unreliable	The SABSA artefact is developed and maintained using ad hoc processes applied inconsistently and in isolation
0 Non-existent	The SABSA artefact and the process to develop and maintain it do not exist

Determine Assurance Levels

Example – correlated to risk standard



4 Risk Levels

4 Assurance Levels

Catalogue Assurance Activities

Activities to provide confirmation, trust & confidence

- Audit or assess compliance against defined standards or policies
- Review against 'desired practice' or performance target
- Peer review
- Inspection
- Testing processes & systems
- Validation & verification
- Quality control & quality assurance
- Accreditation
- Process analysis
- Event monitoring

Common Criteria Example

6.2.4 Assurance through evaluation

28 Evaluation has been the traditional means of gaining assurance, and is the basis of the CC approach. Evaluation techniques can include, but are not limited to:

a) analysis and checking of process(es) and procedure(s);

b) checking that process(es) and procedure(s) are being applied;

c) analysis of the correspondence between TOE design representations;

d) analysis of the TOE design representation against the requirements;

e) verification of proofs;

f) analysis of guidance documents;

g) analysis of functional tests developed and the results provided;

h) independent functional testing;

i) analysis for vulnerabilities (including flaw hypothesis);

j) penetration testing.

Define Assurance Model In-context

Populate assurance activities required for each defined level

		Assurance Evaluation Subject					
		Assets	Risk	Process	People	Location	Time
Assurance Level	Level 1						
	Level 2						
	Level 3						
	Level n						

Assurance Activities

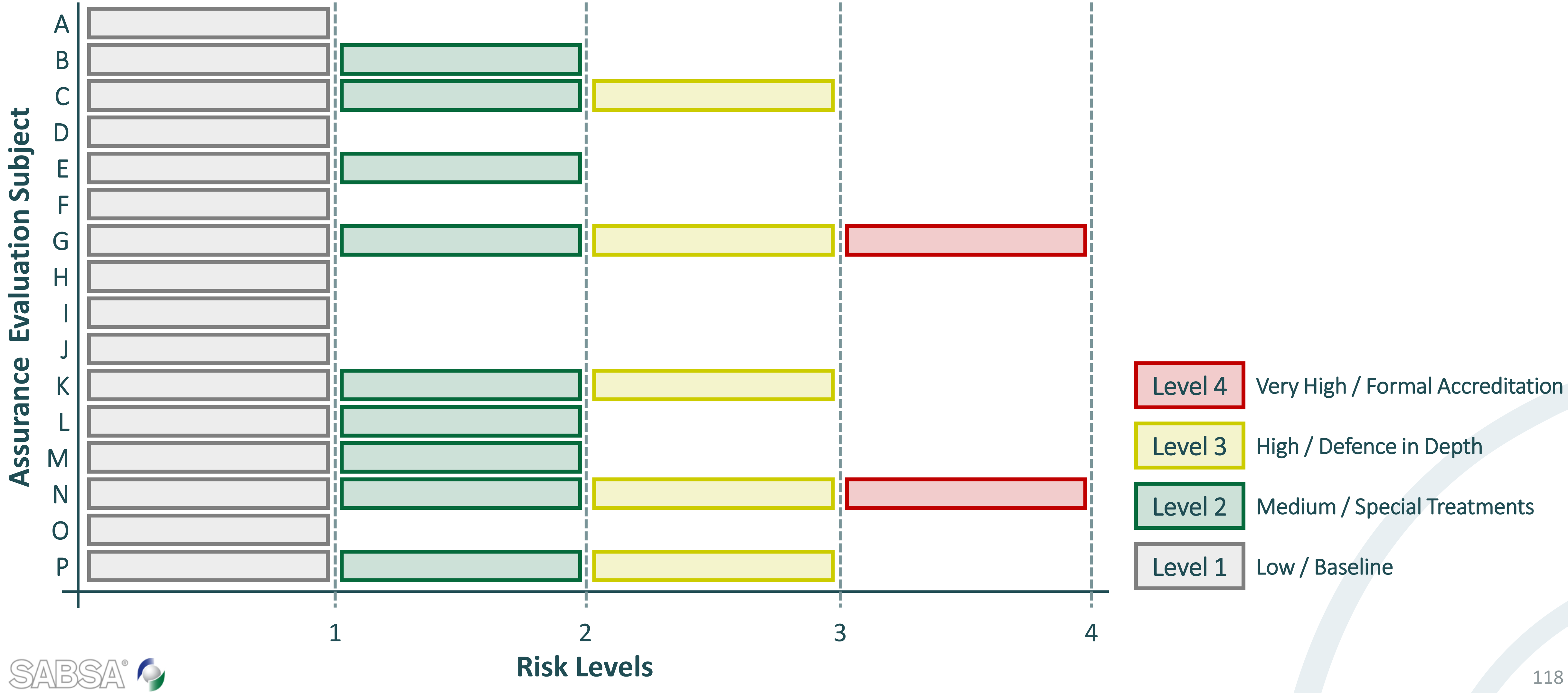
Assurance Activities

In a National Security context, the People subject may require a set of assurance activities of greater scope, depth & diligence to provide level 1 Assurance than those required in other contexts

In an Oil & Gas context, the Location / Environment subject may require a set of assurance activities of greater scope, depth & diligence to provide level 1 Assurance than those required in other contexts

Assurance Needs Assessment

Example – Assurance levels driven by risk standard

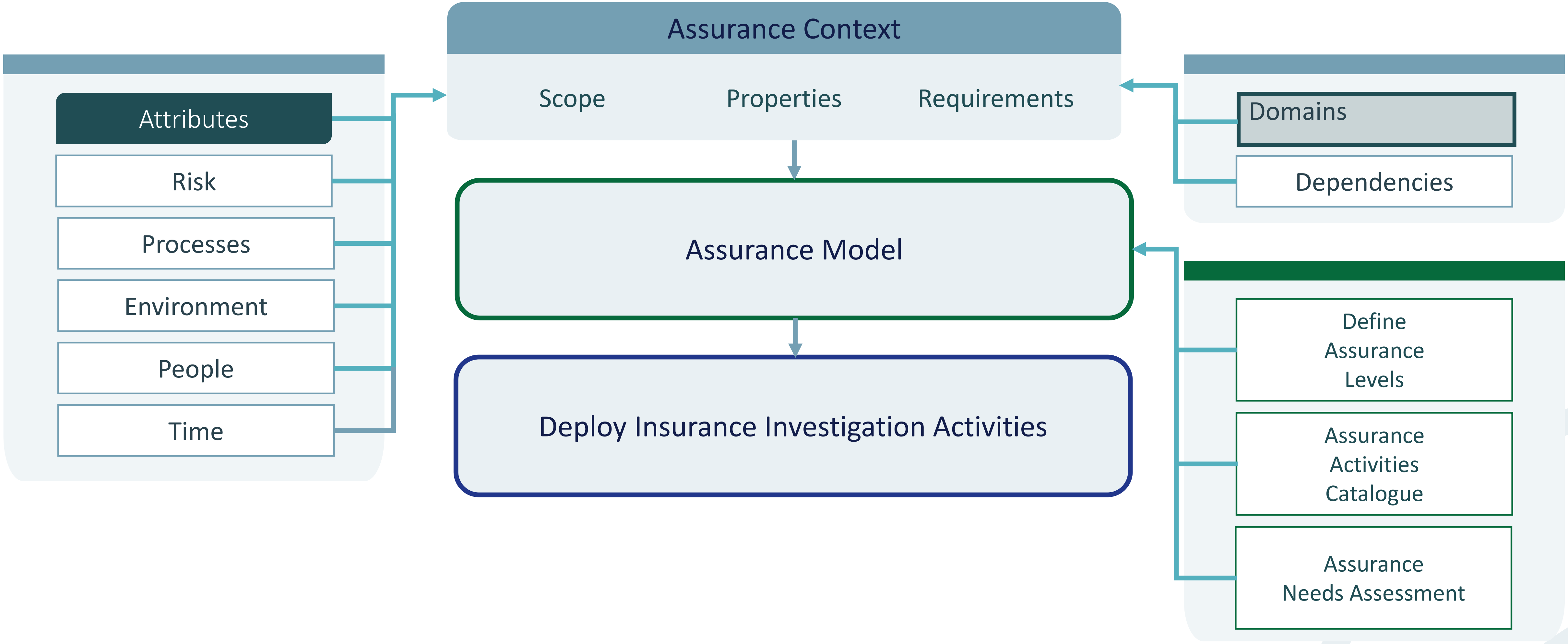


Example – Security Assurance Model for Agile

Assurance Evaluation Subject: Security Code in Agile Development					
Agile Attributes Framework	Agile Risk & Policy Frameworks	Agile Process Framework	Agile Governance & trust Frameworks	Agile Domain Framework	Agile Time Framework
Early Continuous Valuable Business-enabling Customer-empowering Accountability Design integrity	Maintain holistic security posture. Mitigate inherent risks of Agile Risk balanced control objectives v enablement objectives	Re-usable security patterns Continuous embedded risk analysis & security testing	Definition of dominions of authority for Product Owner, Scrum Master, Security & Risk	Definition of interactions and collaboration between Product Owner, Scrum Master, Security & Risk	Fail fast. Risk analysis in definition of "ready" Security testing in definition of "done"

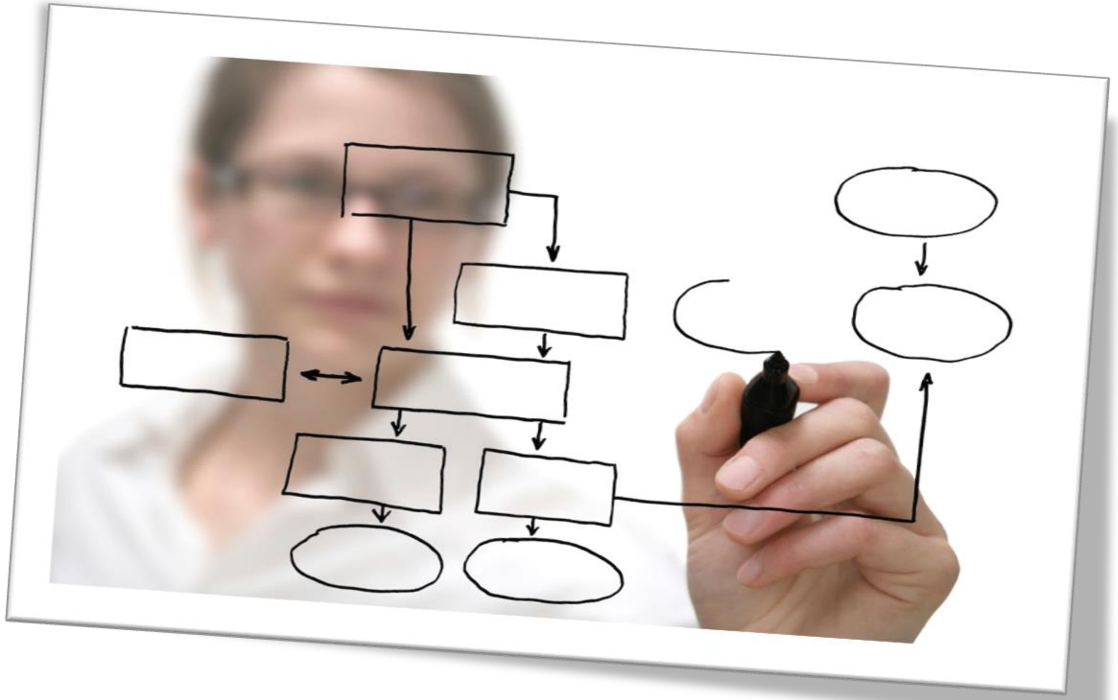
Code Type	Assurance Need / Level		Assurance Activity
Not security relevant	Level 0	Low Assurance	No activities required
Security relevant	Level 1	Medium Assurance	Scrum Master self-determination
Security code	Level 2	High Assurance	Security Dept participation in Agile Sprints & Scrums
Critical security code	Level 3	Very High Assurance	Security Dept participation in Agile Sprints & Scrums Security Dept provide resource for full code audit

SABSA Assurance Framework



Workshop A1-2

Current-state Evaluation Part 2



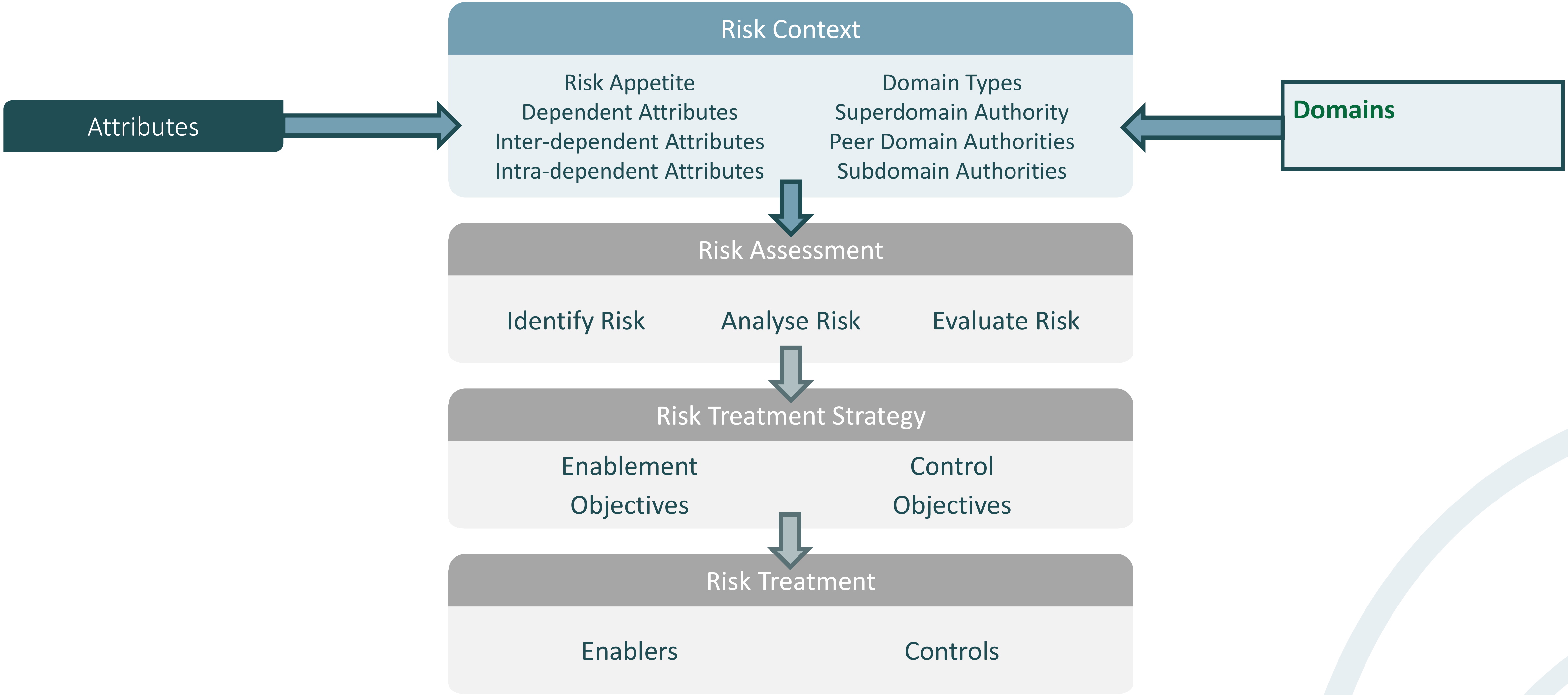
A1 – Unit 2

Risk Context

Risk Context

Section 5

Scope


Attributes
Risk Context
Risk Appetite
Dependent Attributes
Inter-dependent Attributes
Intra-dependent Attributes
Domain Types
Superdomain Authority
Peer Domain Authorities
Subdomain Authorities
Domains
Risk Assessment
Identify Risk
Analyse Risk
Evaluate Risk
Risk Treatment Strategy
Enablement
Objectives
Control
Objectives
Risk Treatment
Enablers
Controls

ISO 31000 Risk Context

External Risk Context Includes the organisation's external stakeholders, its local, national, and international environment, as well as any external factors that influence its objectives ***ISO 31000***

Risk Context To establish the context means to define the external and internal parameters that organisations must consider when they manage risk ***ISO 31000***

Internal Risk Context Includes the organisation's internal stakeholders, its approach to governance, its contractual relationships, and its capabilities, culture, and standards ***ISO 31000***

But "The Organisation" is a complex system containing a large volume of interacting and interconnected risks

The Need to Architect Enterprise Risk Context

"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.

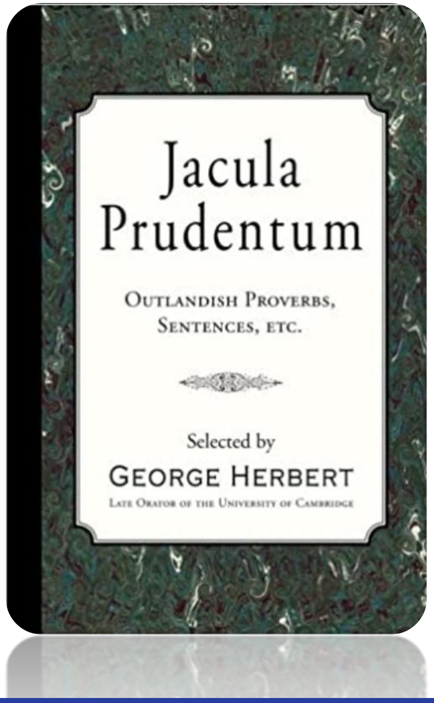
For want of a rider the message was lost.

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 Herbet, Jacula Prudentum, 1651



How does the King manage horseshoe nail risk?

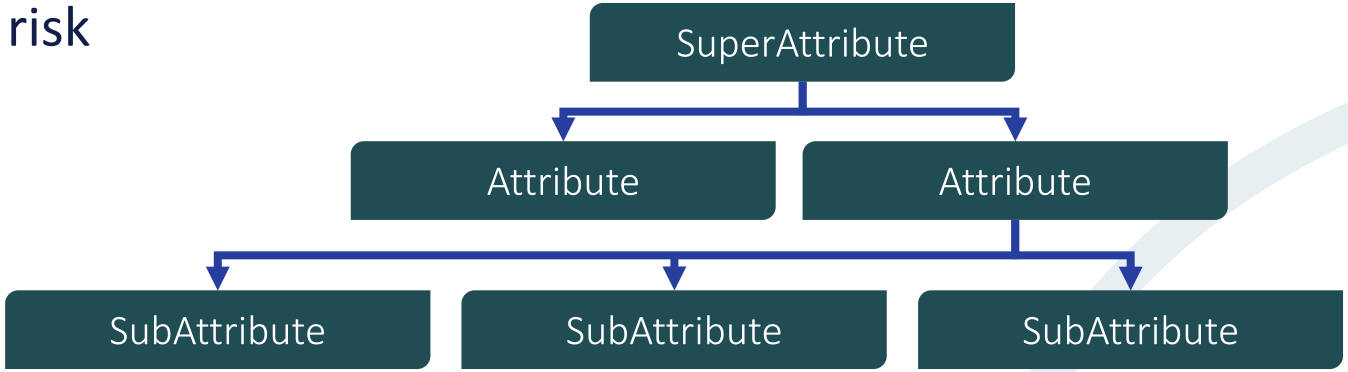
The Enterprise is dependent upon horseshoe nails but the risk context for horseshoe nails differs from the Enterprise risk context and must be calibrated accordingly

Enterprise Success and Dependencies

- Enterprise success factors are represented by measurable Attributes
- The Enterprise is performing to current requirements if:
  - The SuperAttribute performance target is being met
  - The SuperAttribute is operating within risk appetite
- An Attribute is dependent upon its SubAttributes to first:
  - Meet performance targets
  - Operate within risk appetite

SABSA Risk

The positive or negative effect of uncertain events on Attributes



Authority for Managing Success & Risk is Distributed

Relative Superdomains, Subdomains & Peer Domains

Superdomain

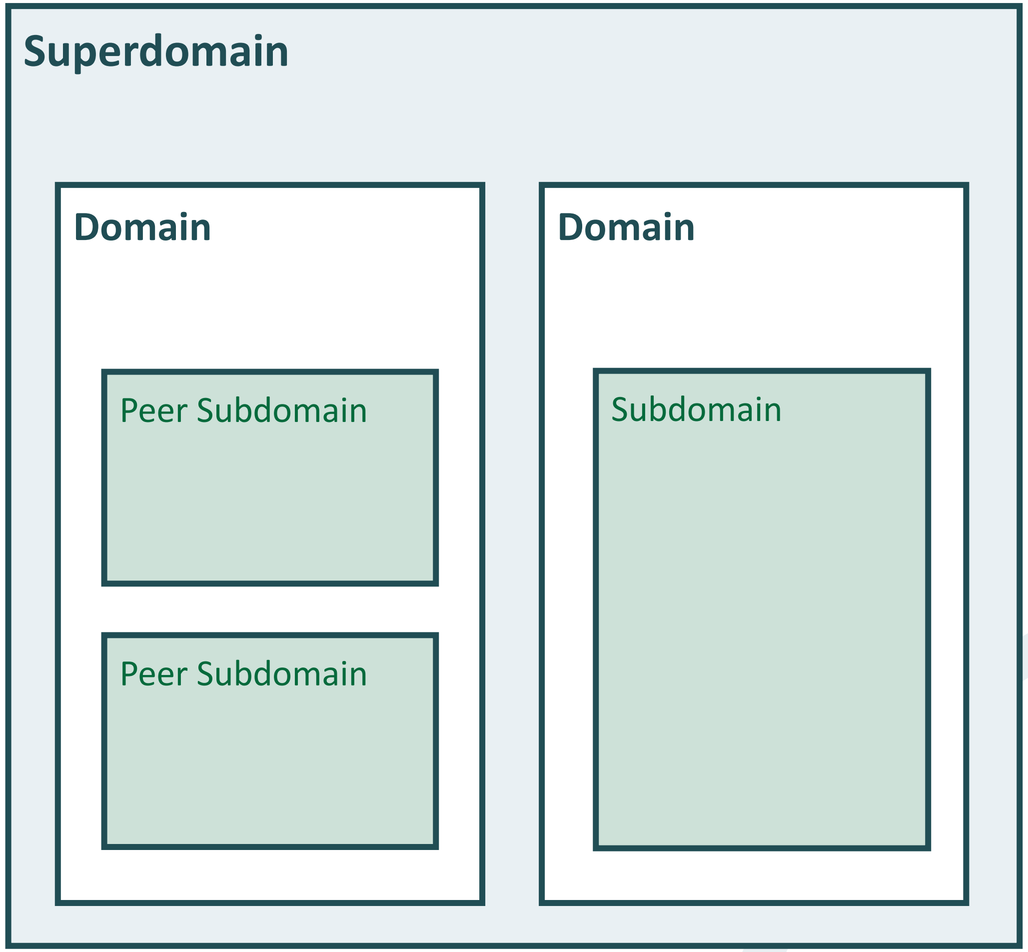
A set of elements, area of knowledge or activity, subject to the common dominion of a single accountable authority, that has delegated and authorised risk and performance dependencies to a lower authority(ies)

Subdomain

A set of elements, area of knowledge or activity, subject to the common dominion of a single accountable authority, serving risk and performance dependencies delegated from, and authorised by, a higher authority

Peer Domains

Subdomains serving risk and performance dependencies delegated from, and authorised by, an immediate common higher authority



Inter-connected Risk Context

Avoiding risk silos

- The distribution and aggregation structure deals will vertical systemic risk interactions but risks can also interact laterally
- Treating a risk in one Domain has damaging or beneficial consequences for other domains
- Failure to treat a risk in one Domain has damaging or beneficial consequences for other domains

Inter-connected Risk Context

CIO

Collaborative

I&AM Program

Access Controlled

Digital Transformation Program

Shareable

CIO's objective is to optimise collaboration by providing the right information to all of the right people at the right time

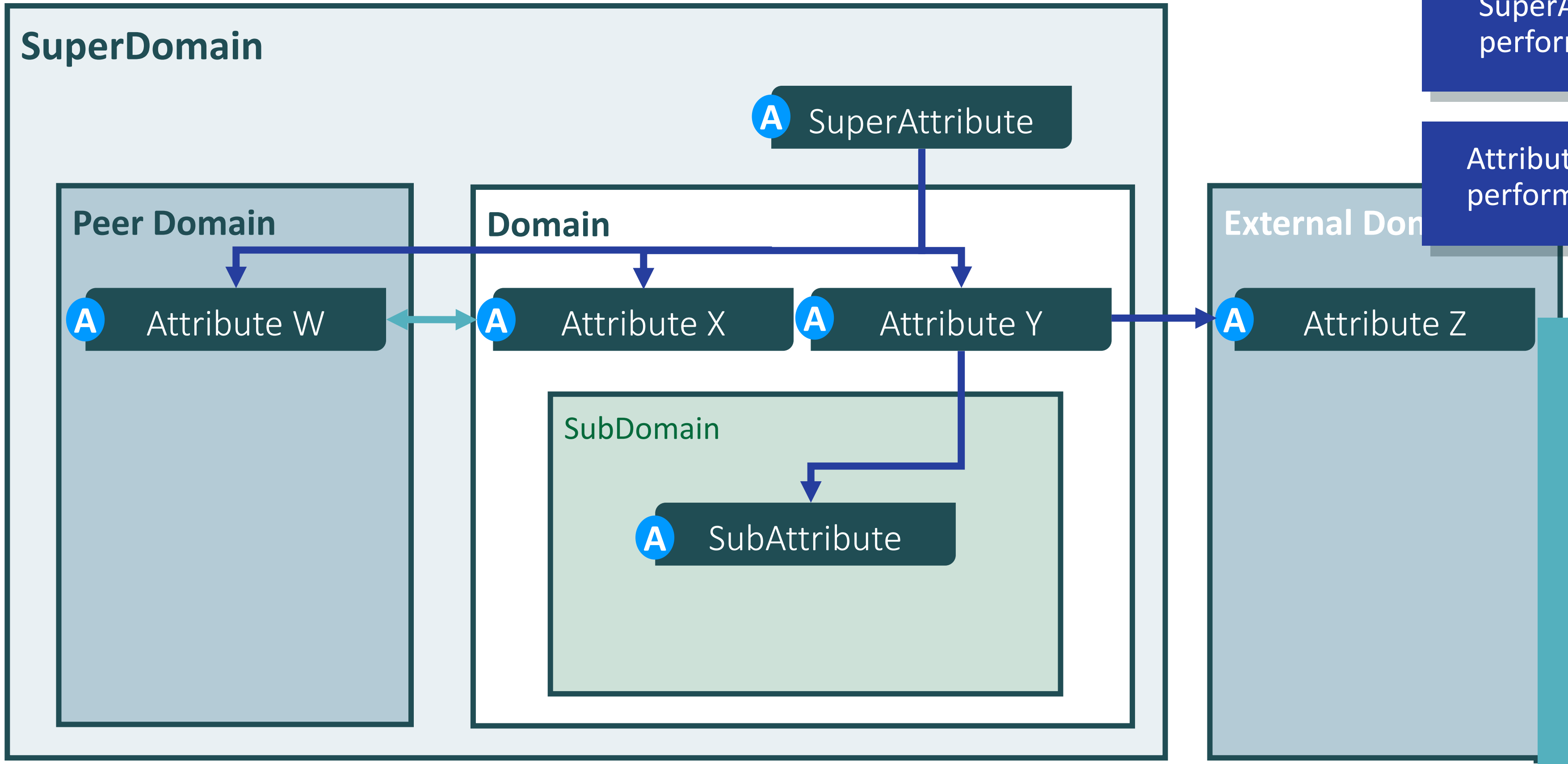
I&AM Program focus is
right information, *right* people, *right* time

Digitisation Program focus is
providing information to *all*

Peer Domains exist to serve the risk appetite and performance targets of their common Superdomain. The Superdomain is accountable for resolving the risk conflict by defining the balance appropriate to the risk context

Each Dependency in a Complex System is a Risk Relationship

Attribute & domain dependency example revisited



SuperAttribute is dependent upon the risk and performance of Attributes W, X and Y

Attribute Y is dependent upon the risk and performance of the SubAttribute and Attribute Z

Attributes W and X are inter-dependent:

Attribute W is dependent upon the risk and performance of Attribute X

Attribute X is dependent upon the risk and performance of Attribute W

Attributes X and Y are independent: Their success does not depend upon the others' risk and performance

Each Risk Dependency is Also a Trust Relationship

Trust Firm belief in the reliability, truth, or ability of someone or something ***OED***

Trust To believe that someone is good and honest and will not harm you, or that something is safe and reliable ***Cambridge***

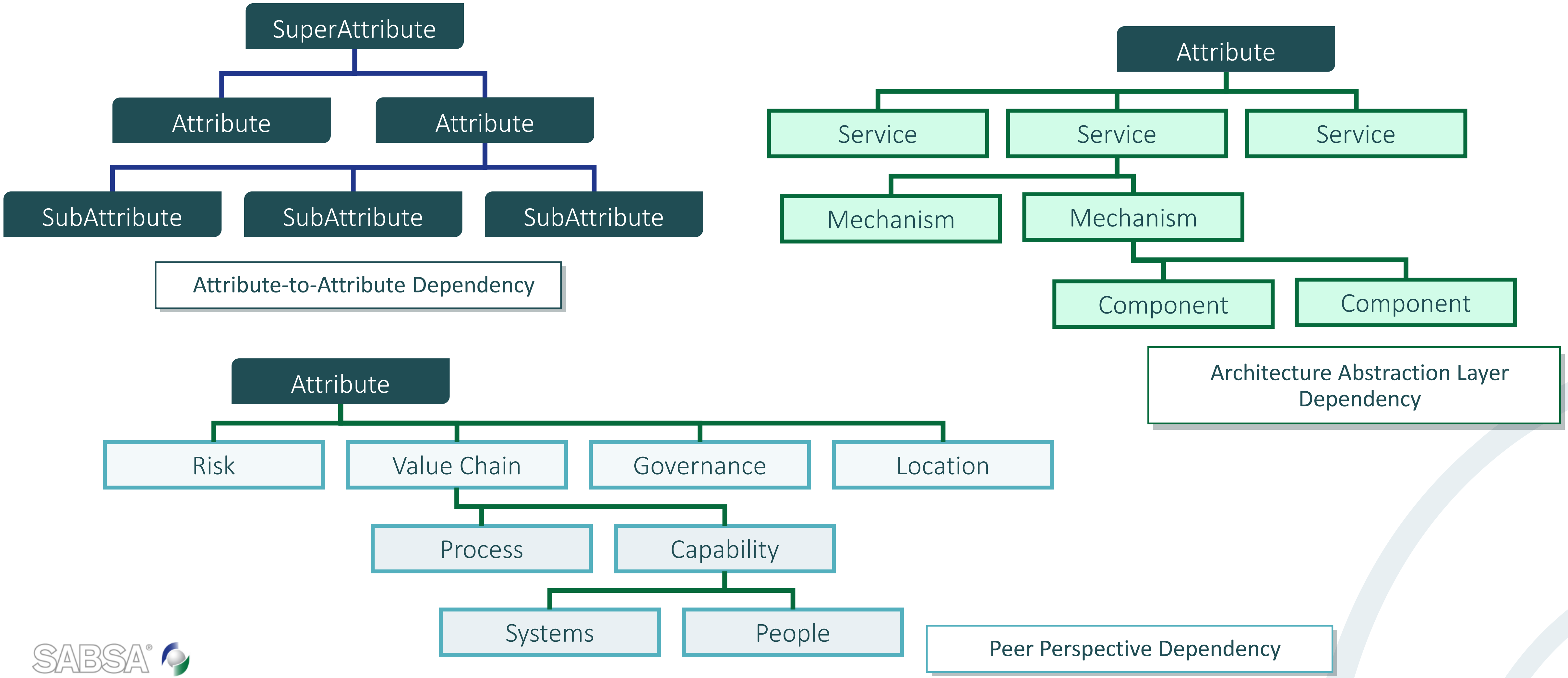
Trust Assured reliance on the character, ability, strength, or truth of someone or something ***Merriam Webster***

SABSA Trust

The state of readiness to accept risk based on the assured belief that the nature and degree of dependency of a Domain or Domain element upon others is satisfied

Risk Dependency Relationships Can Be Explicit or Implicit

Risk & trust dependencies within a complex system



SABSA

Risk Context – The Risk Ownership Challenge

Who owns risk?

- There are many possible risk stakeholders:
  - A person accountable for risk
  - A person or persons who are responsible for managing risk on behalf of the accountable person
  - Person or persons whose decisions or activities affect risk
  - Person or persons whose decisions or activities are affected by risk

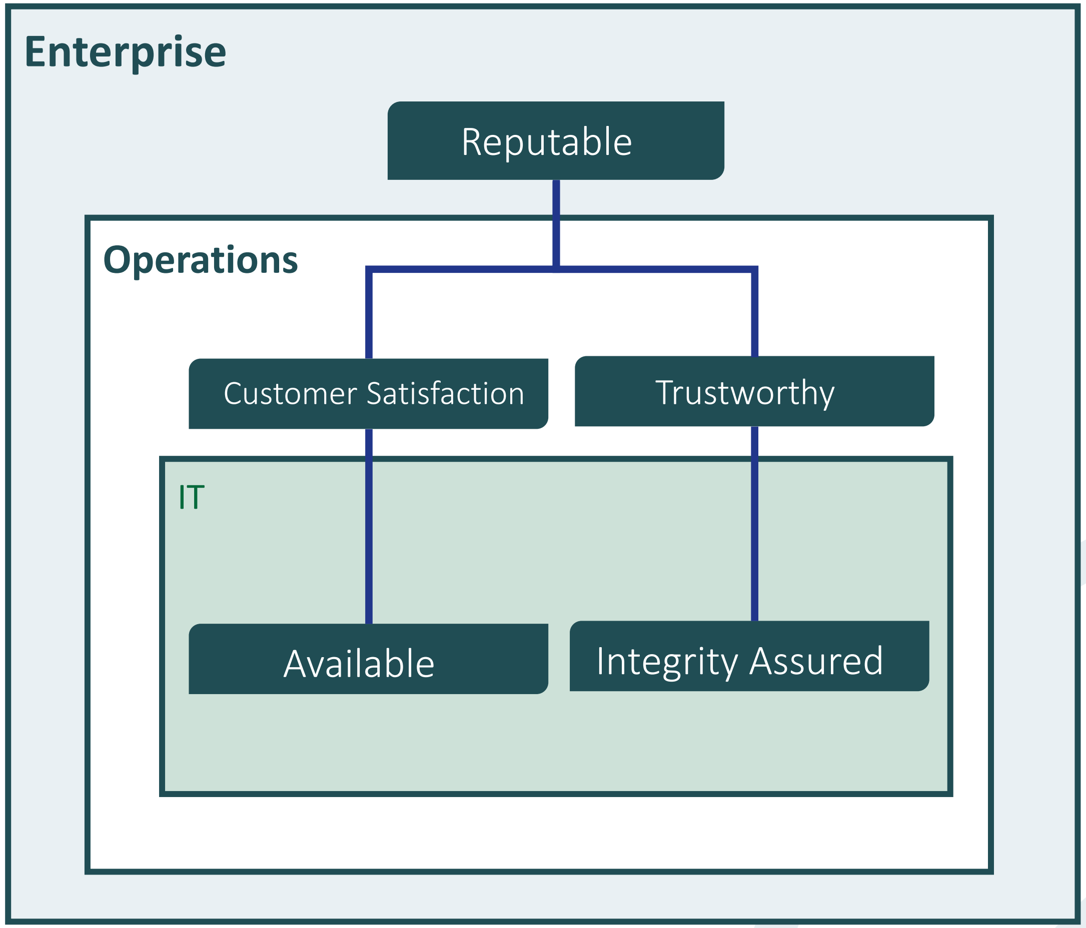
Dear Business Stakeholder, You own the risk of the zero day exploit noted in this report

Systems Risk Report

SABSA Risk Distribution & Performance Aggregation Structure

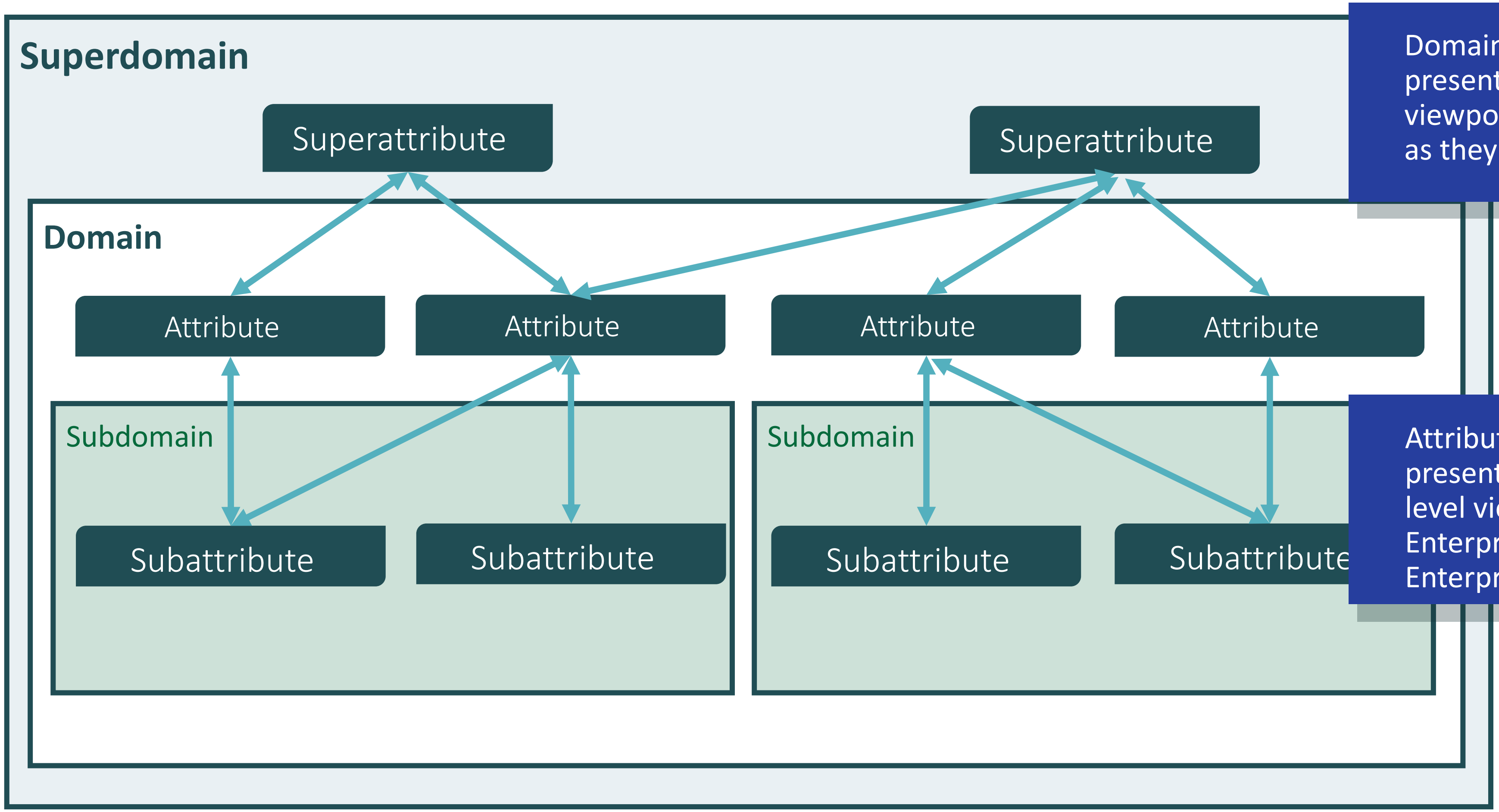
Providing certainty and clarity of risk ownership

- The Domain Authority is accountable for ("owns") the risk to, and the performance of, the Attributes in a Domain
  - The Domain defines the type and scope of the Authority's dominion
  - The Attributes, as the 'assets' of the Domain, define what the Authority has dominion over



Architected Risk & Performance Distribution

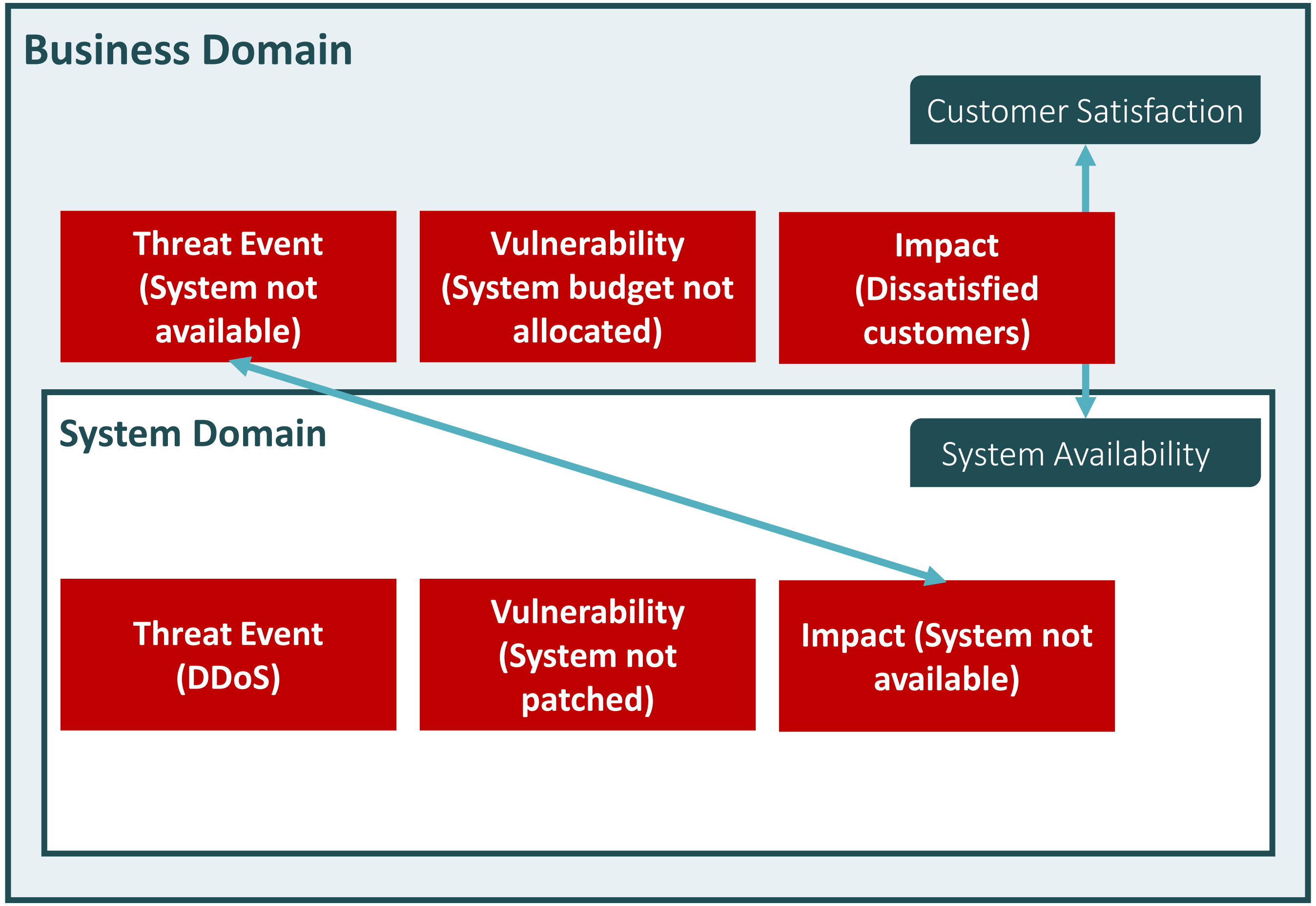
Normalised structure and language provide holistic clarity



Domains provide common structure for presenting authority of any meso or micro level viewpoint, abstraction or aspect of the Enterprise as they relate to the whole macro Enterprise

Attributes provide common language for presenting the requirements of any meso or micro level viewpoint, abstraction or aspect of the Enterprise as they relate to the whole macro Enterprise

Architecting Clarity of Risk Ownership – Whose Risk Context?



The performance target and risk appetite for "Customer Satisfaction" is defined by the Business Domain Authority and distributed to its dependency "System Availability"

The Business Domain Authority is accountable for ensuring that the system domain on which they depend is appropriately budgeted and resourced

The System Domain Authority is accountable for the risk performance of the Attribute "System Availability" and has authority for managing the relevant threats and vulnerabilities within the budget and resource constraints established by the Business Domain Authority

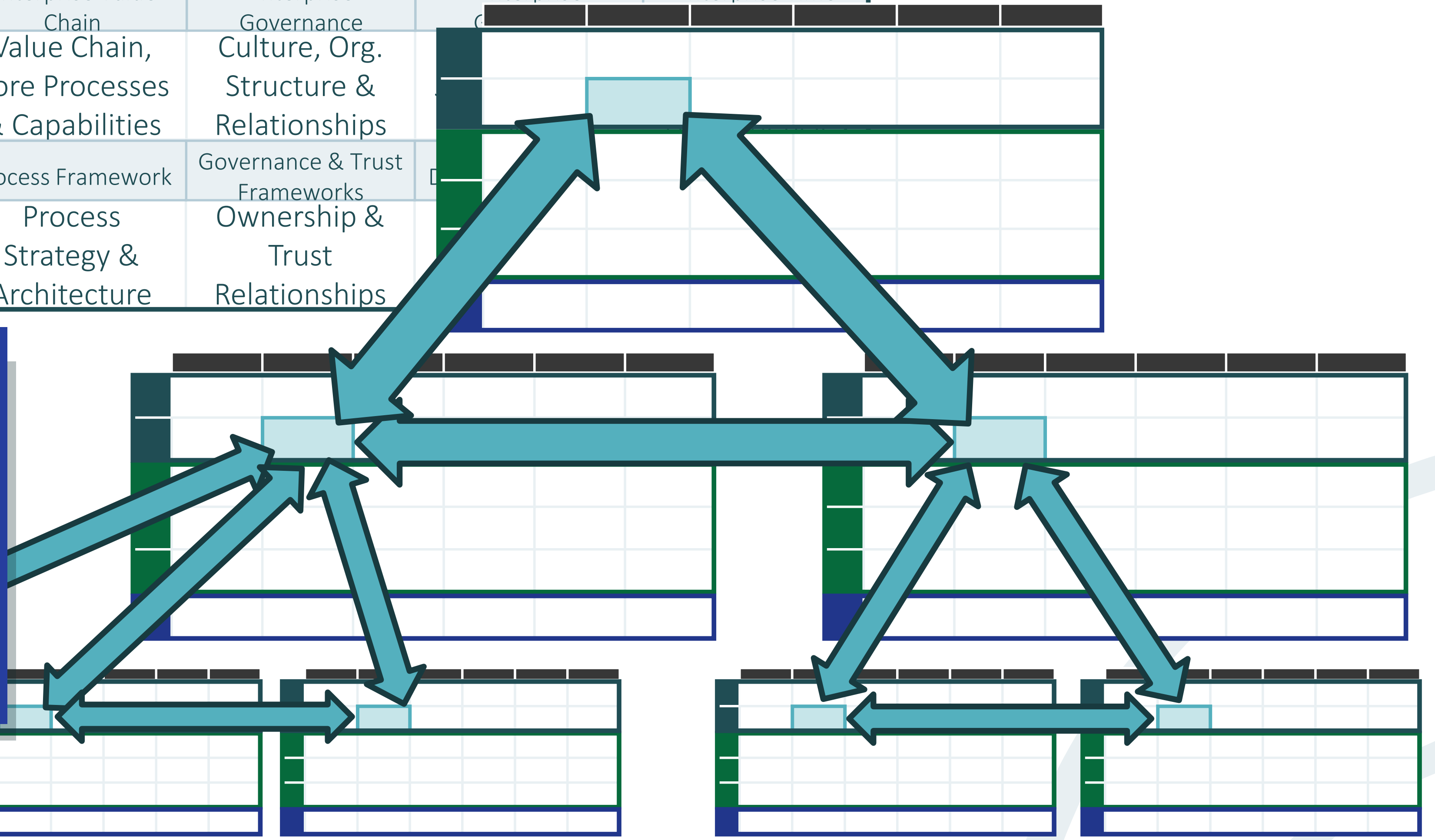
The DDoS attack is not a threat event to the business domain: it is a threat to the system domain

The loss of "System Availability" is the threat to the business domain

Any impact to a Subdomain attribute is a threat event from the perspective of the Superdomain

Architecturally Distributed Risk Context

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise	Enterprise Time
	Goals, Targets, Value & Assets	Opportunities & Threats	Value Chain, Core Processes & Capabilities	Culture, Org. Structure & Relationships		
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & Trust Frameworks		
	Attributes Taxonomy & Profile	Enablement & Control Objectives	Process Strategy & Architecture	Ownership & Trust Relationships		



Any Subdomain exists to serve the risk appetite and performance targets of its Superdomain, in harmony with its peers. The Risk Context for any Domain at any level is therefore its Superdomain and Peer Domain's:

- Goals and assets
- Capabilities and processes
- Relationships and people
- Locations, sites and jurisdictions
- Time and sequence dependencies

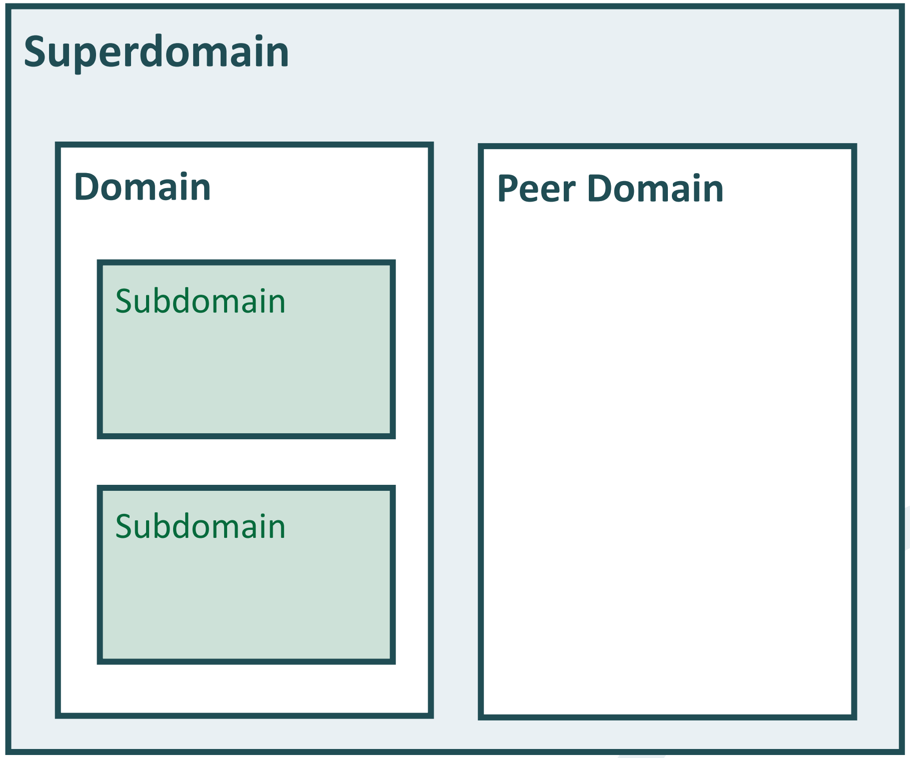
SABSA®

Risk Owner Filter

Understand the owner's viewpoint within the complex system

- The Architect needs to:
  - See the 'big picture'
  - Have the means to communicate that the 'big picture' of full traceability exists
- Flawed temptation to present the 'big picture' for all consumers and expect them to understand it

Layers are closed: Interfaces between layers are defined only for layers directly above and below
Ref "Architecture Layers – Conventions"



The context for any risk owner consists of the dependent trust relationships with their immediate Superdomain, Peers, and Subdomains

SABSA Architected Risk Context

To truly define risk context we must deconstruct enterprise complexity

Risk Context To establish the context means to define the external and internal parameters that organisations must consider when they manage risk ***ISO 31000***

External Risk Context Includes the organisation's external stakeholders, its local, national, and international environment, as well as any external factors that influence its objectives ***ISO 31000***

Internal Risk Context Includes the organisation's internal stakeholders, its approach to governance, its contractual relationships, and its capabilities, culture, and standards ***ISO 31000***

SABSA Risk Context

The external and internal parameters that domains must consider when they manage risk

SABSA External Risk Context

The domain's environment represented by its Superdomain and Peer Domain stakeholders and their Attribute objectives, as well as those of domains outside the Enterprise with which it interacts

SABSA Internal Risk Context

The domain authority's Attribute objectives, and their delegation to subdomain authorities

Risk Context Calibration

The SABSA frameworks enable articulation of risk context for any element

		What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
The Context **For** Agile	**Contextual (Enterprise Macro)**	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Dependence
		Shareholder Value, Reputation & Brand, Market Share	Harness change for Competitive Advantage	Optimised Value Chain	Customer Relationships, 'Can do' Culture, Agility to adapt to 'new normal' stakeholder expectations	Global Jurisdictions, Digital Workplace	Faster time to market
The Context **Of** Agile	**Contextual (Agile Meso)**	Agile Vision	Agile Risk	Agile Value Chain	Agile Governance	Agile Location	Agile Time Dependence
		Better ways to develop working software, Early & continuous delivery of value	Customer satisfaction / discontent	Digital Transformation Programme – Processes & Capabilities	Agile-enabled Org Structure, Business & Dev-Ops in collaboration	Seamless across physical & Virtual extended environments, Empowering supportive & trusting environment	Digital Transformation Roadmap & Dependencies, Program Cycles

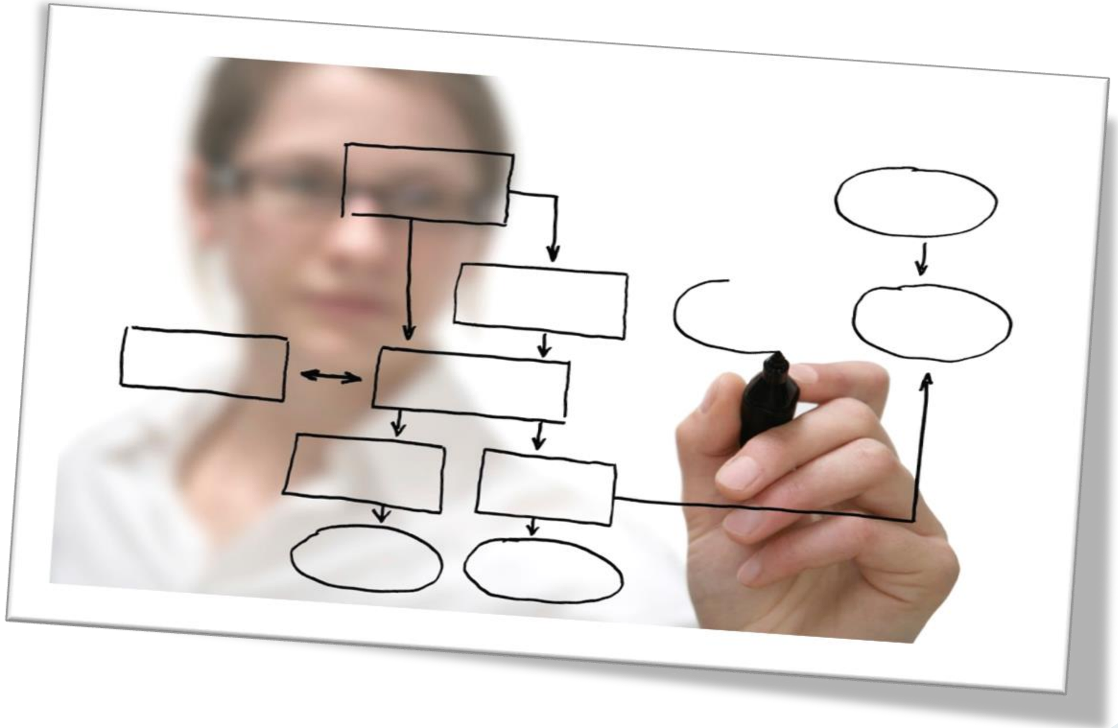
Risk Context Calibration

And ultimately create visibility & traceability of complex risk connectivity

Contextual (Agile Meso)	Agile Vision	Agile Risk	Agile Value Chain	Agile Governance	Agile Location	Agile Time Dependence
	Better ways to develop working software, Early & continuous delivery of value	Customer satisfaction / discontent	Digital Transformation Programme – Processes & Capabilities	Agile-enabled Org Structure, Business & Dev-Ops in collaboration	Seamless across physical & Virtual extended environments, Empowering supportive & trusting environment	Digital Transformation Roadmap & Dependencies, Program Cycles
Conceptual (Agile Meso)	Agile Attributes Framework	Agile Risk & Policy Frameworks	Agile Process Framework	Agile Governance & Trust Frameworks	Agile Domain Framework	Agile Time Framework
	Early, Continuous, Valuable, Business-enabling, Customer-empowering, Accountability, Design integrity	Maintain holistic security posture, Mitigate inherent risks of Agile, Risk balanced control objectives v enablement objectives	Re-usable security patterns, Continuous embedded risk analysis & security testing	Definition of dominions of authority for Product Owner, Scrum Master, Security & Risk	Definition of interactions and collaboration between, Product Owner, Scrum Master, Security & Risk	Fail fast, Risk Analysis in definition of "ready", Security testing in definition of "done"
Logical (Agile Meso)	Information Assets	Risk Policies	Process Maps & Services	Trust Relationships	Domain Models	Calendar & Timetable
	Features, Product backlog items, User Stories, Models (MBSE)	Individuals & interactions over processes & tools, Working software over extensive documentation, Customer collaboration over contract negotiation, Responding to change over following a plan	Sprint ceremonies, Servant leadership, Continuous integration, Continuous delivery	Inform, consult & reporting relationships for: Virtual teams; T-shaped individuals; Product owner; Scrum Master; Security; Risk	Secure working environment (physical or virtual), Co-location, Kanban boards, Project rooms, Conference facilities	Time-boxed sprints, Definition of "ready", Definition of "done"

Workshop A1-3

Architected Risk Context



Stakeholder Identification & Engagement

Section 6

Interested Parties

Each risk has a variety of possible stakeholders

- Accountable authority
  - Domain authority for an attribute
- Accountable authority dependencies
  - Domain authority depends upon those to whom responsibility has been delegated to:
    - Comply with Domain policy
    - Meet Domain performance targets
    - Ensure domain operates within risk appetite
    - Design, implement or manage risk treatments
  - Domain authority may depend upon PeerDomains who could systemically impact negatively or positively the performance of the Domain
- Dependent Domain authorities
  - SuperDomain or PeerDomain authorities who could be systemically impacted negatively or positively and depend upon the performance of the Domain

Traditional RACI

A process focus

Role	Description
Responsible	The person or people responsible for getting the job done
Accountable	"The buck stops here" – only one person can be accountable for each activity
Consulted	The people whose opinions are sought
Informed	The people that are kept up-to-date on progress

	1st Level	2nd Level	3rd Level	Service Desk Manager	Incident Manager	IT Manager	Customer
Incident submitted to Service Desk	R	-	-	A	-	-	R
Incident detection and recording	R	R	-	A	-	-	-
Determine type of call (Incident, Change, Request)	R	R	-	A	-	-	I
Follow Priority 1 Incident process	R	I	I	R	A, R	I	I
Follow Change process	R	R	-	A	-	-	I
Provide customer with reference number	R	R	-	A	-	-	I
Initial support and classification	R	R, C	-	A	I	-	I
Escalation to right support group	R	I	I	A	C	I	I
Monitoring of progress of Incident (chasing 2nd and 3rd level support)	A	R	R	R	I	R	-
Communicate status updates to customer	R	C	C	A	I	I	I
Investigation and diagnosis	R	R,C	R,C	R	A	R	-
Escalate using escalation process	R	R	R	R,C	A	R	-
Resolution and recovery	R	R,C	R,C	R,C	A	R	I
Customer approval of solution	R	I	I	I	R	-	A
Closure	R	I	I	A	I	I	R

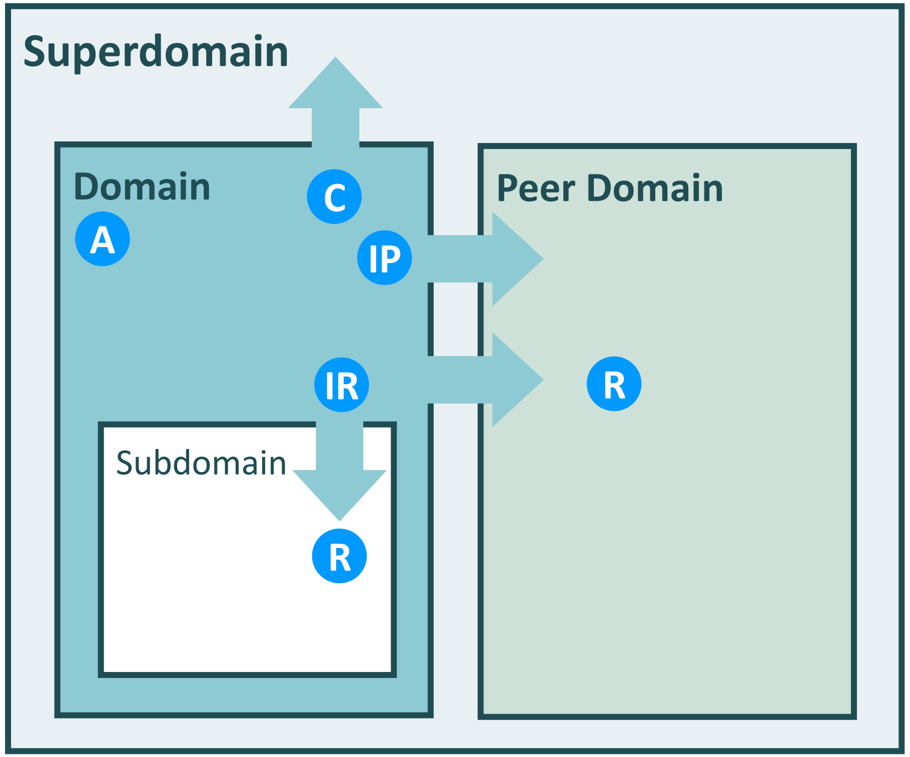
Does a traditional process-focused RACI provide sufficient scope and flexibility to model Enterprise Governance?

Does a traditional process-focused RACI deliver sufficient relevance to risk and security considerations such as Risk Ownership?

Stakeholder Types – Possible Extensions

- Informative Communications
  - Inform of responsibility
  - Inform of performance
- Responsibility delegations with or without policy authority
  - Responsible trustee
  - Responsible custodian
  - Support
- Authority & Ownership
  - Attribute risk owner
  - Liable authority
  - Dependent authority
  - Impacted authority (positively or negatively)
  - Risk acceptance / sign-off
- Assurance & Validation
  - Monitor
  - Compliance
  - Audit
  - Test
  - Review
  - Verify

SABSA Domain RACI – Stakeholder Types



Authority	Role	
Domain	Accountable to	SuperDomain
Domain	Consults	SuperDomain
Domain	Informs Performance to	SuperDomain
Domain	Consults	Dependent Peer Domain
Domain	Informs Performance to	Dependent Peer Domain
Domain	Informs of Responsibility to	Dependency Peer Domain
Dependency Peer Domain	Responsible to	Domain
Domain	Informs of Responsibility to	SubDomain
SubDomain	Responsible to	Domain

Domain Traceability

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Dependence
	Goals, Targets, Value & Assets	Opportunities & Threats	Value Chain, Core Processes & Capabilities	Culture, Org. Structure & Relationships	Territories, Jurisdictions & Sites	Time & Sequence Dependencies
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & Trust Frameworks	Domain Framework	Time Framework
	Attributes Taxonomy & Profile	Enablement & Control Objectives	Process Strategy & Architecture	Ownership & Trust Relationships	Security Domain Framework	Architecture Roadmap

Explicit Domain Traceability

A domain can represent the dominion of a single authority accountable for a geographical or logical location, or jurisdiction

Implicit Domain Traceability

A domain can also represent dominion of a single authority accountable for a:

- Set of assets or objectives
- Risk type or category
- Capability or process
- Organisational unit
- Time factor or dependency

Domain Model is an Authority Diagram not an Org Chart

Org charts represent chain of command, not authority & accountability

- Frequently reorganised
- Represents a chain of command, not what we want to achieve
- Communicates organisational positions, not roles
  - Matrix organisations
  - Dotted lines
  - Position within cross-functional process
  - Liaison, dependency, and interaction outside the direct chain of command

Domains Architect Authority & Accountability

Organisational structure and accountability mismatch - example

Business Operations (COO)

Business Availability

Information (CIO)

Information Availability

Data (Data Owner)

Data Availability

Technology (CTO)

Systems Availability

Platform (IT Manager)

Platform Availability

Network (Network Manager)

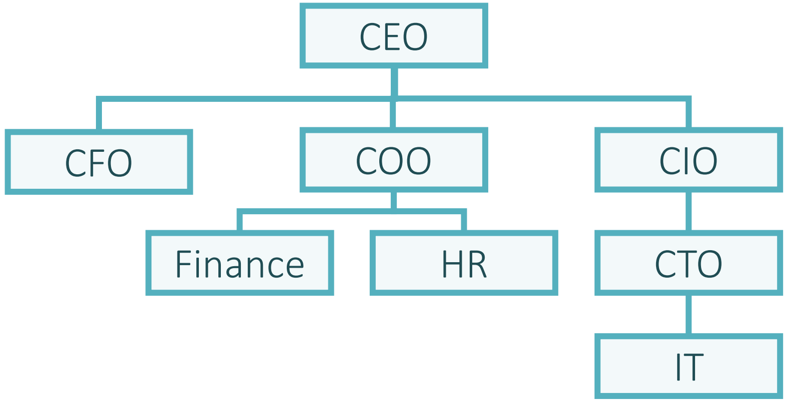
Network Availability

HR (HR Mgr)

Skills Availability

Premises & Equip (Facilities Mgr)

Facilities Availability

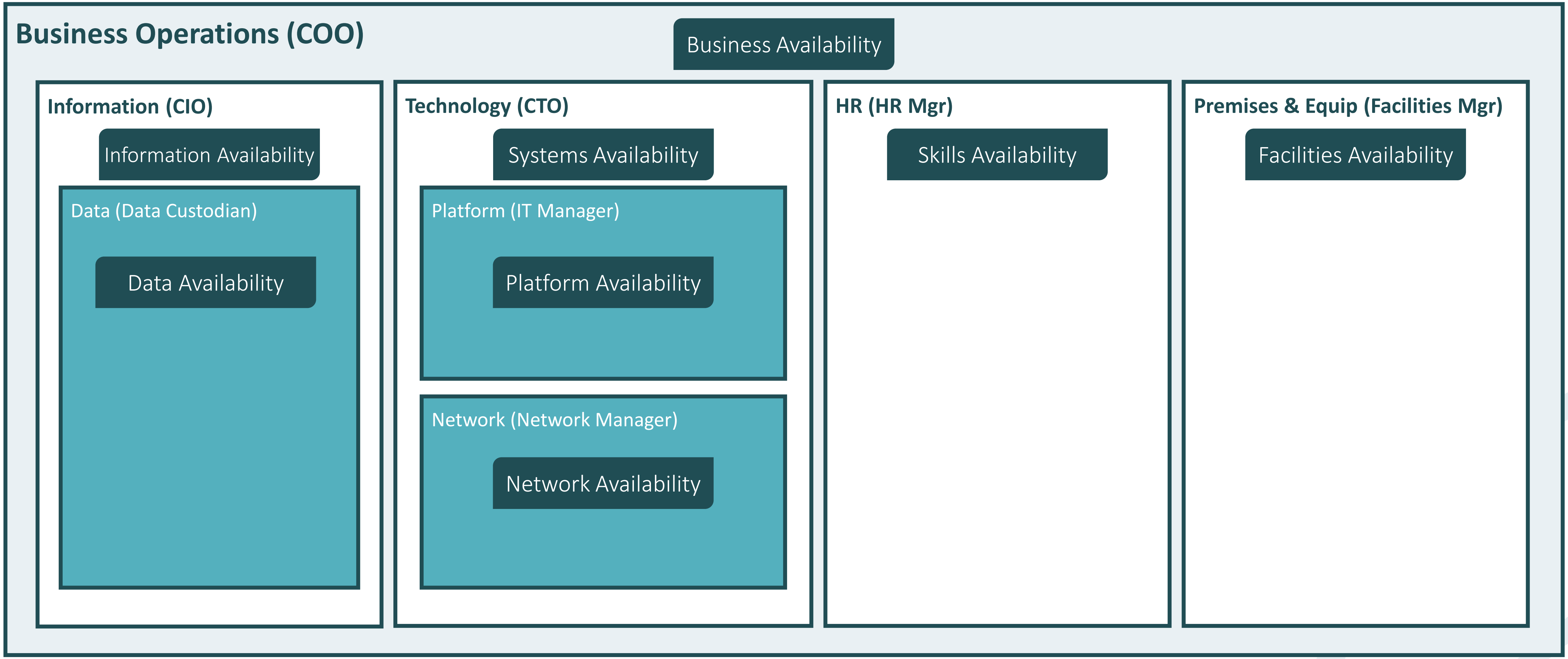


Organisational peers who do not 'report to' each other could form a dependent hierarchy of authorities and accountabilities

Entities who 'report to' a higher organisational position may in reality be authority and accountability peers

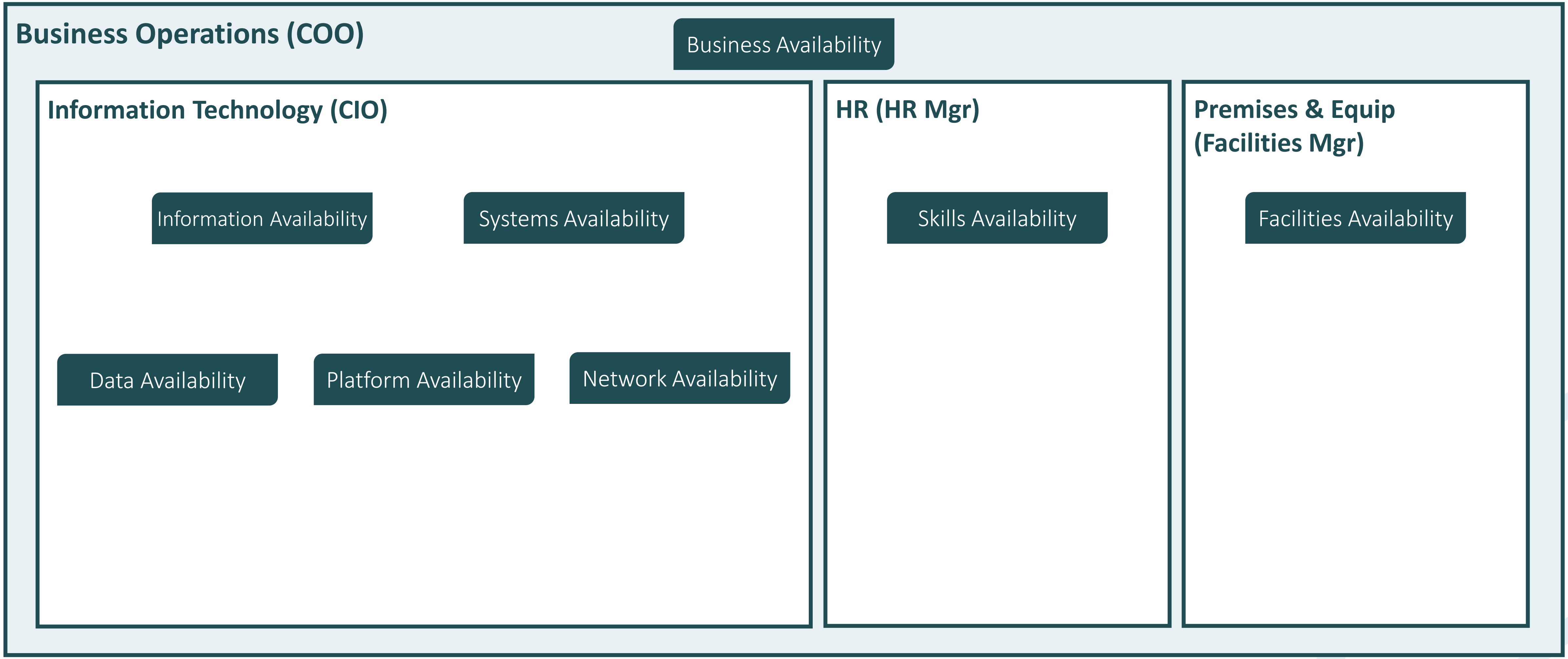
Domain Layers – Authority Delegation

Fully delegated accountable authority - example



Domain Layers – Authority Delegation

Partially delegated accountable authority - example



Align With Enterprise Culture

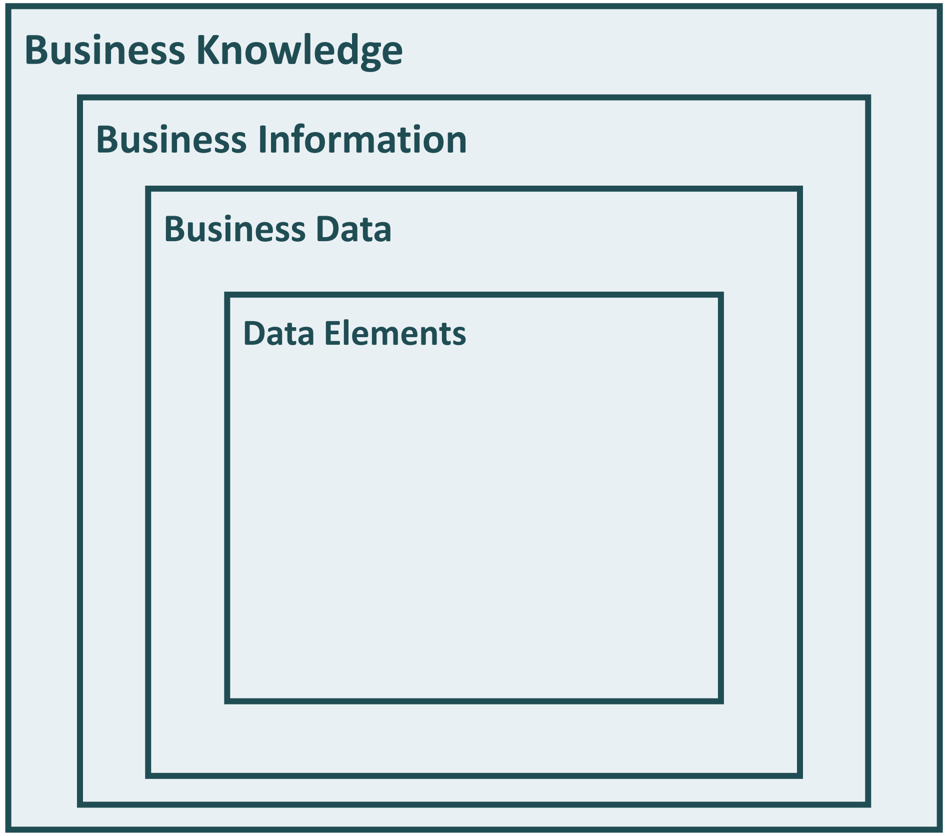
Understand the domain authority's perspective

- The Architect needs to communicate the Domains of accountability and authority to align with Enterprise culture
- An Enterprise can see itself in many possible ways

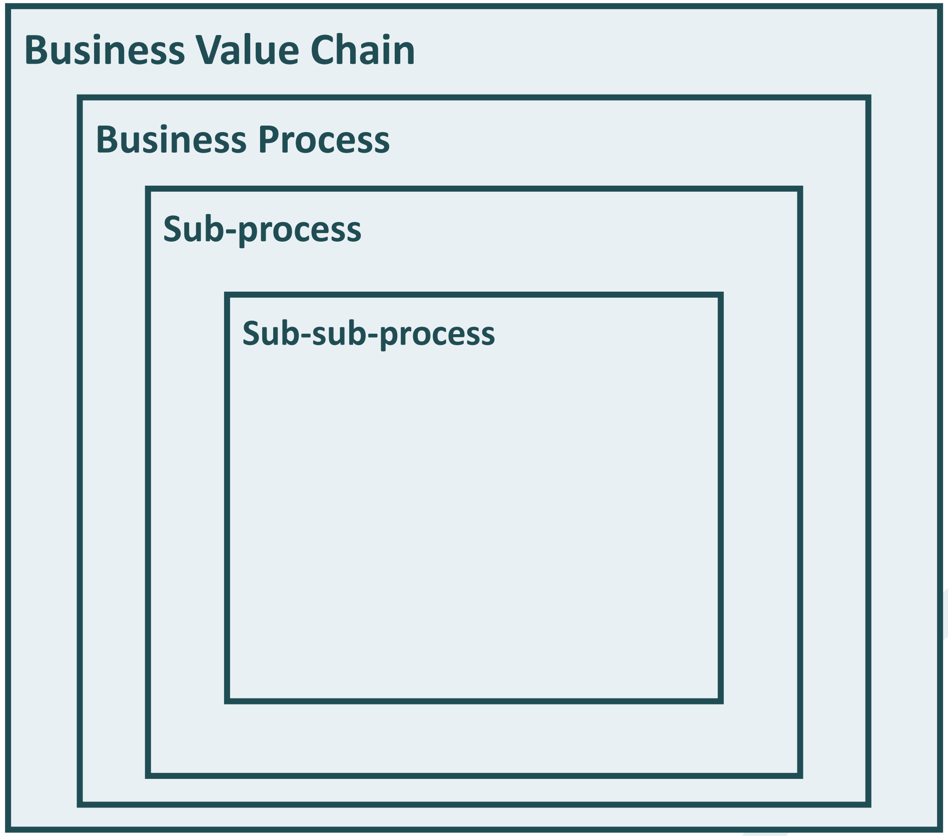
Diverse Stakeholder Perspectives

Example perspectives & layers of abstraction

Chain of Command Perspective



Dependency Perspective



Governance, risk and assurance relate to all of these elements

Diverse Stakeholder Perspectives

Example perspectives & layers of abstraction

Information Asset Perspective

- **Enterprise**
  - **Division**
    - **Department**
      - **Team**

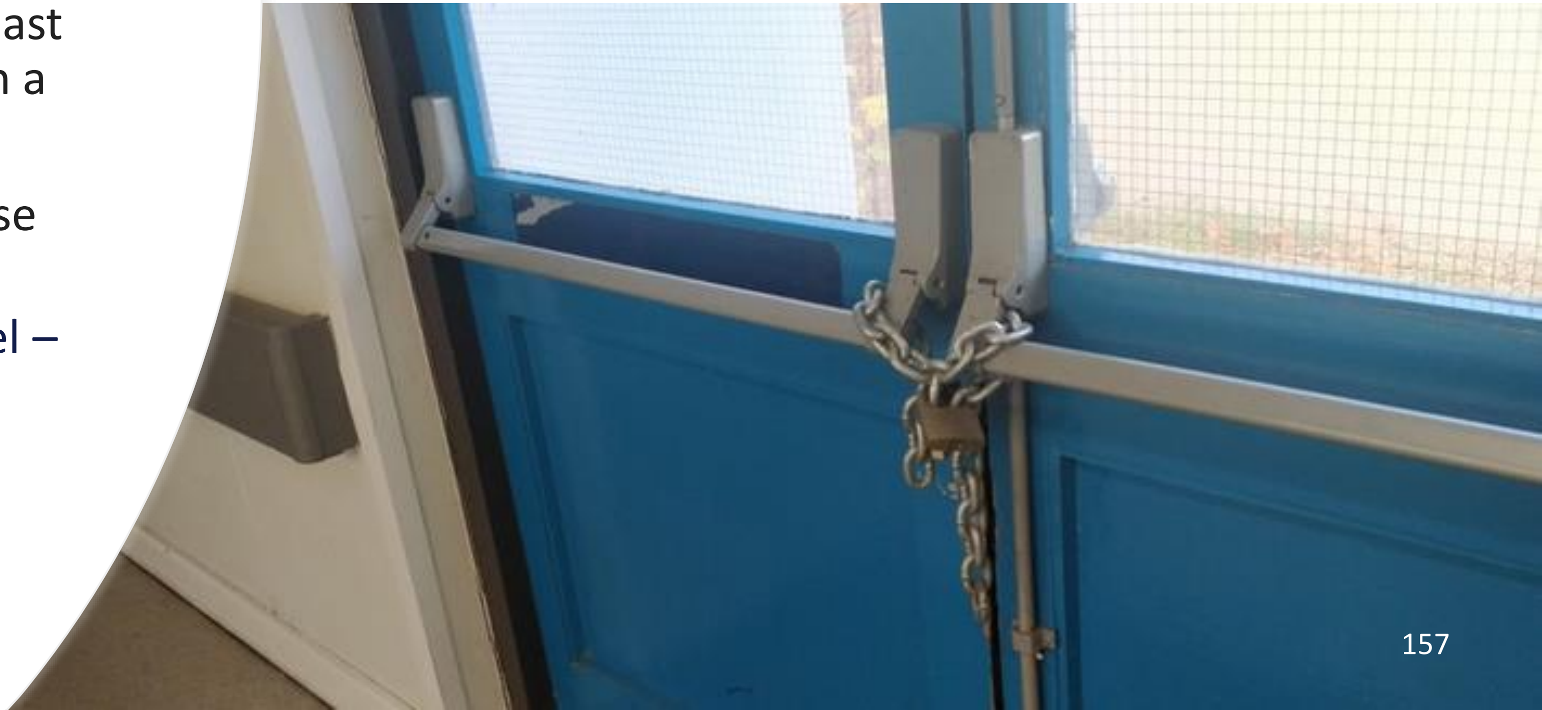
Process Perspective

- **Target**
  - **Target Dependency**
    - **Sub-target Dependency**
      - **Sub-sub-target Dependency**

Governance, risk and assurance relate to all of these elements

Domains Have Interacting, Systemic & Conflicting Risks

- If there's a risk associated with taking a course of action, there's also a risk of not doing so.
- Risks interact - if you mitigate a risk in a domain, you almost certainly increase at least one other risk at the same time (possibly in a different domain)
- For super domain authorities, the enterprise view of risk is what matters
  - Aggregated risks at the enterprise level – the "big picture"
  - Avoiding risk silos – seeing risks holistically



Domain Lens

An authority's view through complexity

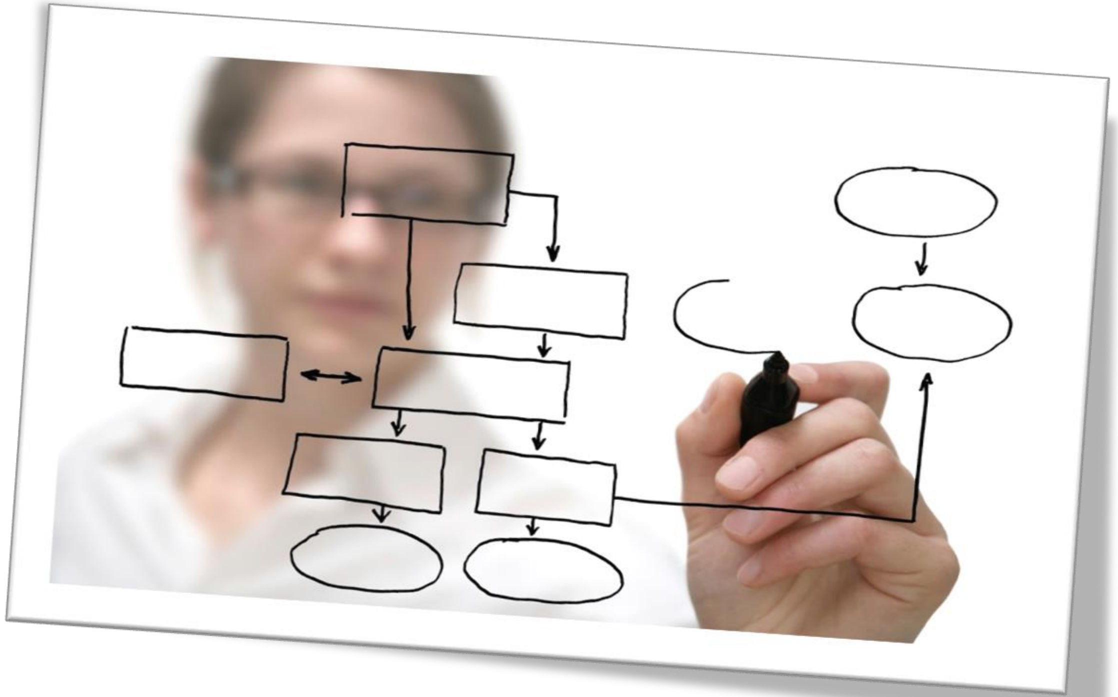
- Apply a lens to Enterprise complexity to view it in the most appropriate way for the stakeholder authority(ies) who are consumers of the Domain Architecture
- Consider the explicit and implicit domain traceability – Domains to represent:
    - Sets of assets or objectives
    - Risk types or categories
    - Capabilities or processes
    - Organisational units
    - Geographical or logical locations, or jurisdictions
    - Performance criteria or deadlines
- Consider the choice of Attributes Taxonomy
    - Already validated
    - Stakeholders already engaged
    - Emotional connection has been established
    - Common language enables collaborative modelling through varying perspectives

Common Language & Consistent Structure

Ensures completeness of stakeholders and dependencies

Workshop A1-4

Stakeholder Identification & Engagement



A1 – Unit 3

Risk Assessment

Scope

Attributes

Risk Context

Risk Appetite
Dependent Attributes
Inter-dependent Attributes
Intra-dependent Attributes

Domain Types
Superdomain Authority
Peer Domain Authorities
Subdomain Authorities

Domains

Risk Assessment

Identify Risk | Analyse Risk | Evaluate Risk

Risk Treatment Strategy

Enablement Objectives | Control Objectives

Risk Treatment

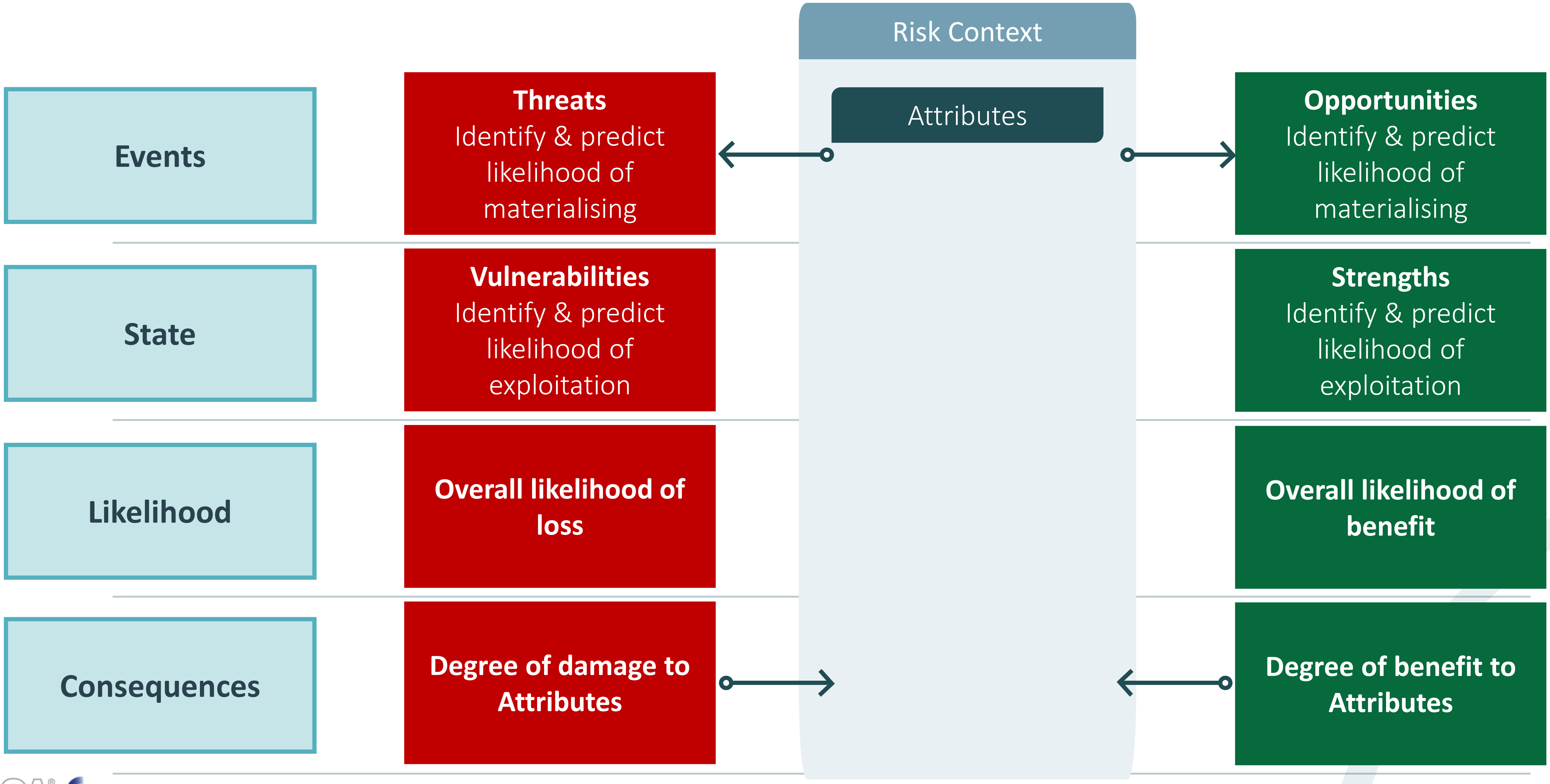
Enablers | Controls

What is Risk Assessment?

- Risk Assessment is the process of identifying, analysing, and evaluating risk
- The purpose is to:
  - Identify possible relevant future events
  - Predict the probability of possible future events
  - Estimate the consequences of possible future events in a prioritised order
  - Evaluate the degree to which the consequences of future events are acceptable
  - Inform a subsequent plan of action for unacceptable consequences

Ultimately, risk assessment should define and communicate priorities for action

SABSA Balanced Risk Assessment Model



Identify Risk

Section 7

Risk Assessment - Identification

- Risk identification is the process of finding, recognising, and describing the sources, nature, and circumstances of events that could influence the achievement of objectives
- It involves identification of:
  - The risk environment
  - The possible events (opportunities and threats) that could occur
  - The state (strength and weakness)
  - The potential consequences (damage and benefit) of the possible events

Register of Risk Elements

Attributes
(what we value)

Threat (event with negative impact)	**Vulnerability** (weakness exploited by the threat)	**Impact** (negative consequences to Attributes)
Opportunity (event with positive benefit)	**Strength** (capability to grasp the opportunity)	**Benefit** (positive consequences to Attributes)
Register of Events Threats & Opportunities	Register of States Strengths & Weaknesses	Attributes Register of What Matters Attributes Profile

Registers enable consistency, completeness & re-use. Select from Enterprise Risk Registers the specific risk elements that combine to describe risks in scope (risk assessment scope, domains, attributes, etc)

Create the Event Register – Select a Taxonomy of Event Types

Sample taxonomy – “Enterprise Security Architecture”

- Regulations & Regulators
- Shareholders & Investors
- Political Conditions
- Market Conditions
- Legislation
- Competitors
- Ethical Pressures
- Cultural Pressures
- Economic Conditions
- Outsourced Service Providers

The Enterprise

- Partnerships and JVs
- Natural Disasters
- Governments
- Supply Chain
- Contracts
- Criminals
- Terrorism
- Customers
- Trade Unions
- Climate & Weather

Create the Event Register – Select a Taxonomy of Event Types

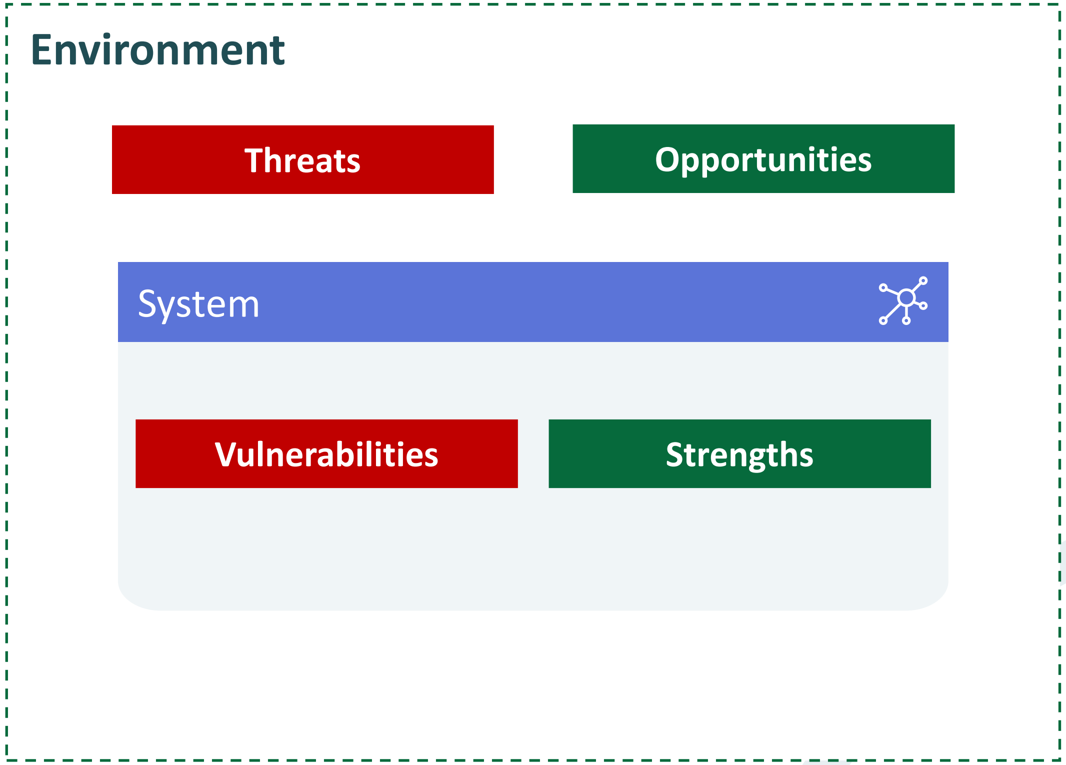
Sample taxonomy – COSO

Economic	Natural	Political	Social	Technological
Capital availability	Emissions & waste	Governmental changes	Demographics	Interruptions
Credit issuance, default	Energy	Legislation	Consumer behaviour	Electronic commerce
Concentration	Natural disaster	Public policy	Corporate citizenship	External data
Liquidity	Sustainable development	Regulation	Privacy	Emerging technology
Financial markets			Terrorism	
Unemployment				
Competition				
Mergers & acquisitions				

Systems Engineering Perspective

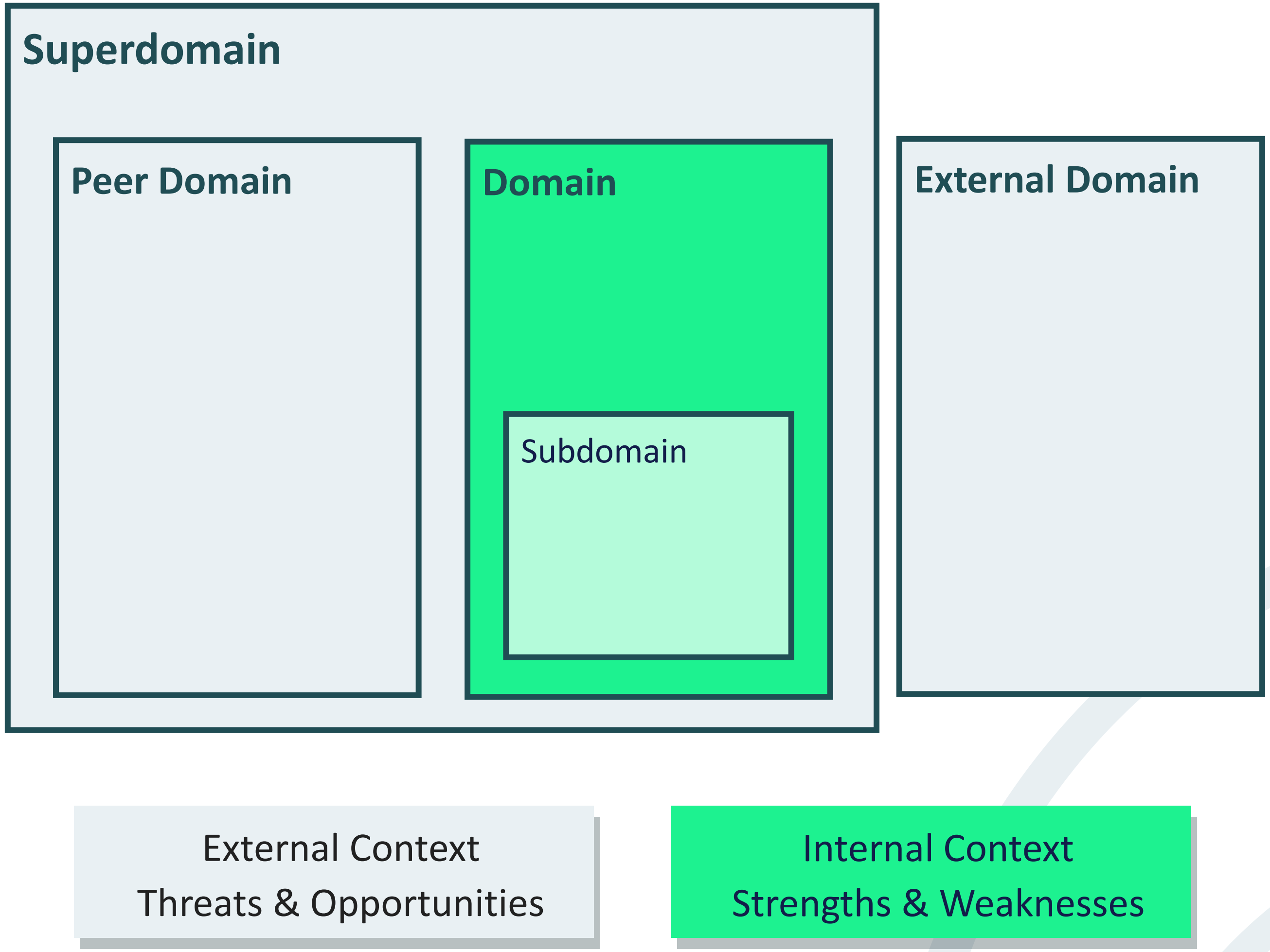
The importance of the risk environment

- The System (Internal Risk Context)
  - Has a boundary
  - Defined as all of the resources (including policy) within the control influence of the system boundary
  - Has control influence over its state of strength or weakness
- The Environment (External Risk Context)
  - The context within which the system exists
  - The system has no control influence over its environment

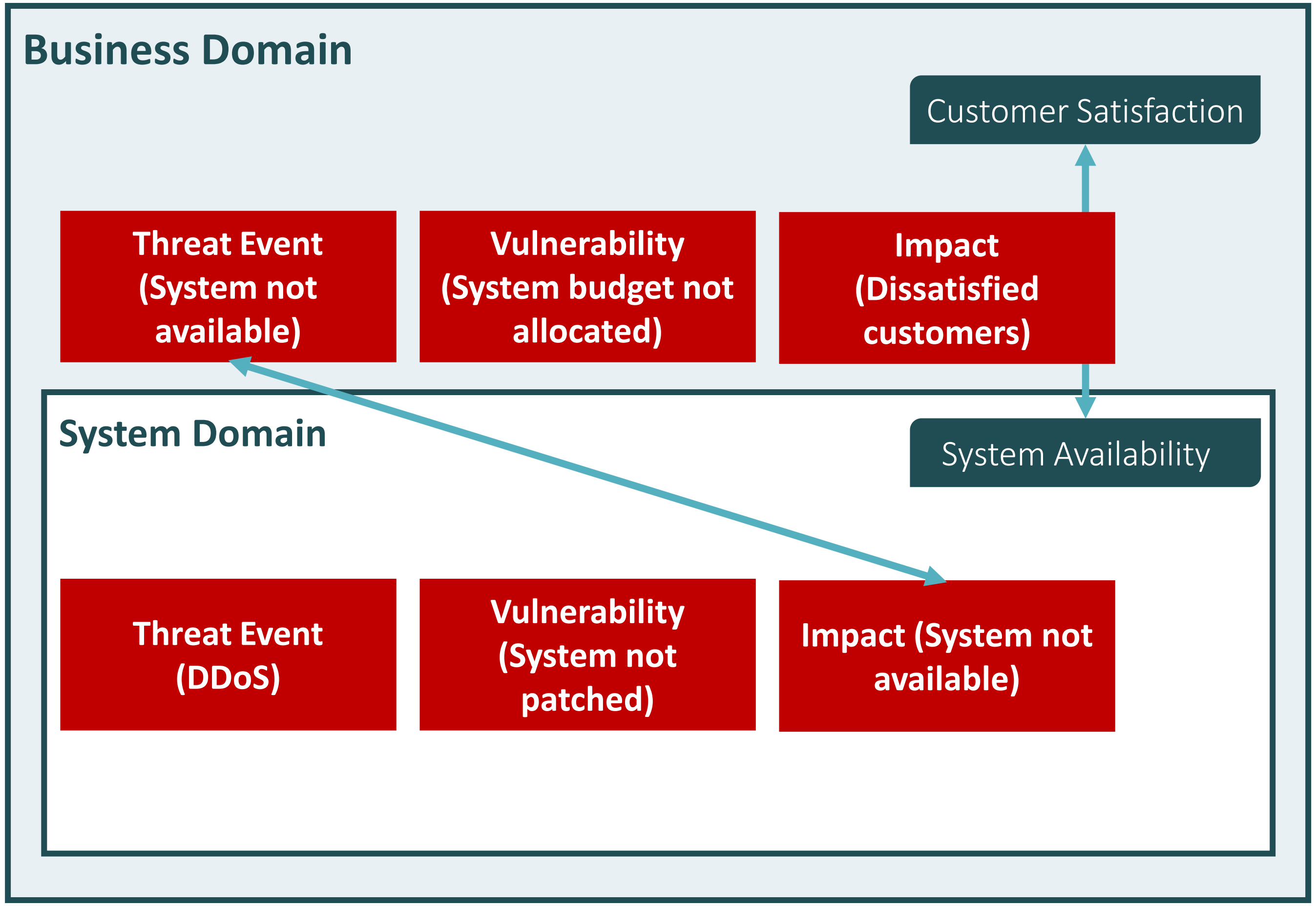


Risk Identification – Scope & Source

- Internal Risk Context
  - The Domain
  - Has a boundary
  - Defined as a set of elements, area of knowledge or activity, subject to the common dominion of a single accountable authority
  - Has authority over its state of strength or weakness
  - Has authority over its subdomains' state of strength or weakness on which it depends
- External Risk Context
  - The environment within which the domain exists
  - The domain has no authority over its environment which is the source of threat & opportunity events



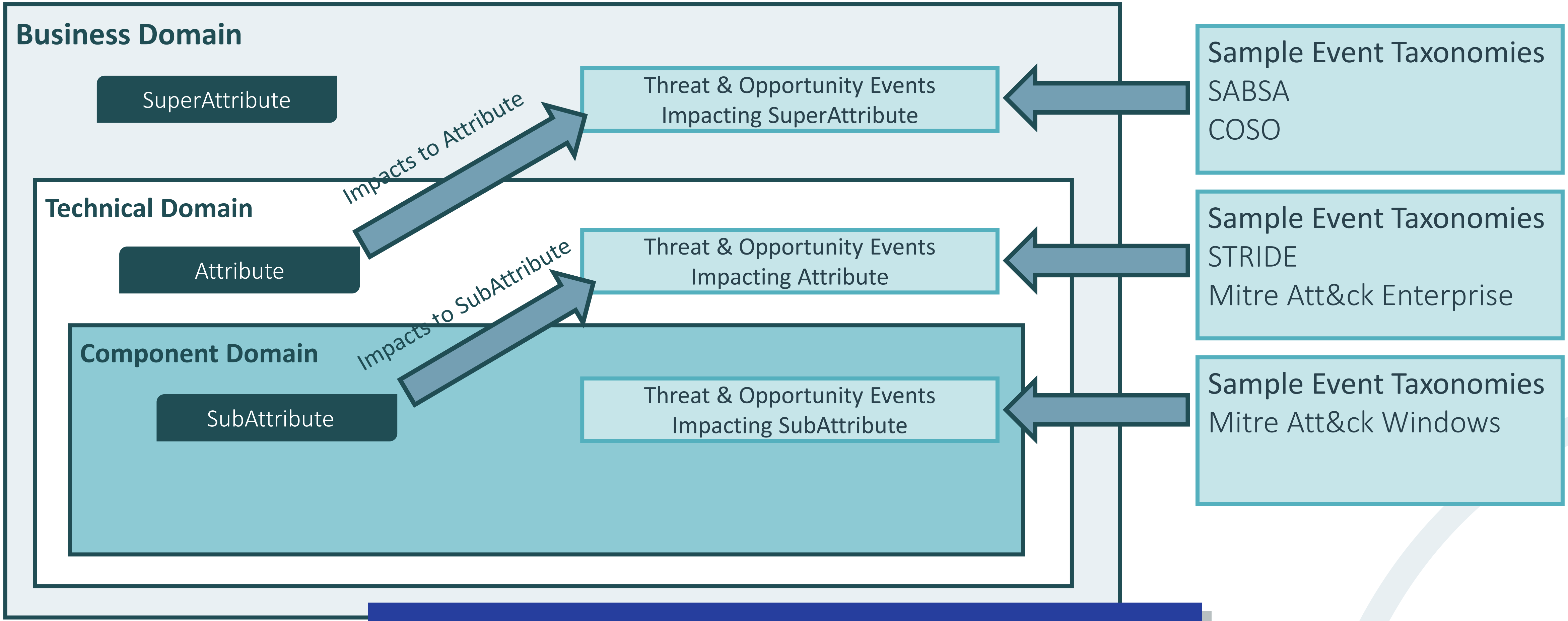
Risk Elements in Context



For Risk Governance to be effective and for Risk Ownership to be clear and obvious, the risk elements (Events, States & Consequences) must be properly allocated to the correct Domains within the complex system

Create the Event Register – Architected Taxonomy

Event taxonomies correlated to domain & attribute layers



Typically, pre-existing registers focus exclusively on threat events and not opportunities

Populating the Event Register

PESTELIM Analysis

Populating the Event Register – SABSA Event Domain Taxonomy

Event Domain	Event Agent Type	Event (Threat & Opportunity) Agents
People	Internal	Employees (past, current, future), Contractors
	External Individuals	Members of the Public, Individual Consumers, Criminals, Terrorists, Third Party Employees (past, current, future)
	External Groups	Customers, Suppliers, Partners, Agents, Shareholders, Regulators, Governments, Criminal Syndicates, Terrorist Groups, Pressure Groups, Competitors, Service Providers, Joint Ventures, Unions
Environment	Natural Events	Natural disasters, Weather conditions
	Accidents	Fire, Flood, Explosion, Collision, Subsidence, Collapse, Sink, Discover
Resources	Critical Infrastructure	Power, Water, Sewage, Drainage, Public Telecomms, Transport, Oil
	Equipment	Industrial Machinery, Plant, Business Equipment
	ICT Infrastructure	Private Telecomms, Platforms, Devices, Peripherals
	Software	Operating Systems, Applications, Code, Malware
Systemic Events	External	Market conditions, Economy, Political Instability, Cultural Shift, Ethical Shift, Supply Chain, Climate Change
	Internal Vertical	Any event within a SABSA domain with negative or positive consequences for its super-domain or sub-domain
	Internal Horizontal	Any event within a SABSA domain with negative or positive consequences for a peer domain

Populating the Event Register – People Domain Example

Event (Threat & Opportunity) Agent	Example Agent	Example Event
Employees (past, current, future), Contractors	Product Developer	Innovation
Employees (past, current, future), Contractors	Accountant	Fraud
Public, Individual Consumers, Criminals, Terrorists, Third Party Employees (past, current, future)	Consumer	Recommendation
Public, Individual Consumers, Criminals, Terrorists, Third Party Employees (past, current, future)	Member of Public	Vandalism
Customers, Suppliers, Partners, Agents, Shareholders, Regulators, Governments, Criminal Syndicates, Terrorist Groups, Pressure Groups, Competitors, Service Providers, Joint Ventures, Unions	Regulator	Favourable Regulation
Customers, Suppliers, Partners, Agents, Shareholders, Regulators, Governments, Criminal Syndicates, Terrorist Groups, Pressure Groups, Competitors, Service Providers, Joint Ventures, Unions	Market Competitor	Aggressive Competition

Populating the Event Register – Environment Domain Example

Event (Threat & Opportunity) Agent	Example Agent	Example Event
Natural disasters, Weather conditions	Unseasonal Mild Weather	Increase Walk-in Business
Natural disasters, Weather conditions	Natural Disaster	Tsunami
Fire, Flood, Explosion, Collision, Subsidence, Collapse, Sink, Discover	Accidental Discovery	Discover Penicillin
Fire, Flood, Explosion, Collision, Subsidence, Collapse, Sink, Discover	Capsize	Oil Pollution

Populating the Event Register – Resources Domain Example

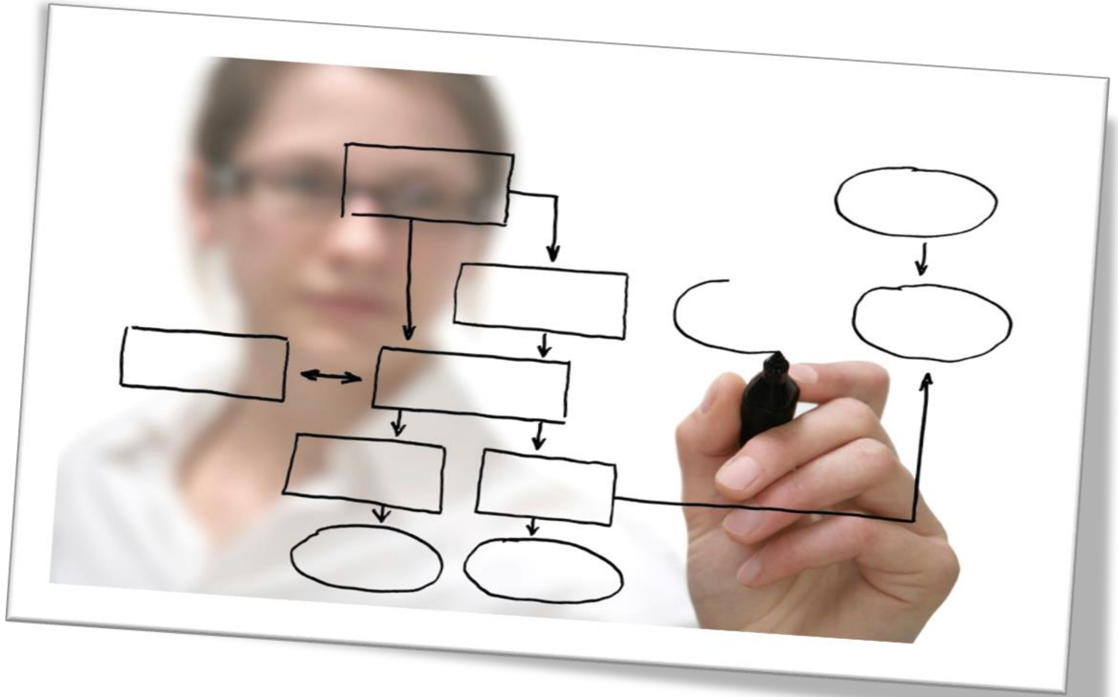
Event (Threat & Opportunity) Agent	Example Agent	Example Event
Power, Water, Sewage, Drainage, Public Telecomms, Transport, Oil & Gas	SmartGrid	Automate Metering
Power, Water, Sewage, Drainage, Public Telecomms, Transport, Oil & Gas	Gas Distributor	Pipeline Failure
Industrial Machinery, Plant, Business Equipment	NextGen Lighting	Increase Energy Efficiency
Industrial Machinery, Plant, Business Equipment	Production Line	Personal Injury
Private Telecomms, Platforms, Devices, Peripherals	New Generation	Automate Process
Private Telecomms, Platforms, Devices, Peripherals	Business Network	Network Failure
Operating Systems, Applications, Code, Malware	New Coding Method	Faster Time to Market
Operating Systems, Applications, Code, Malware	Malware	Code Corruption

Populating the Event Register – Systemic Events Domain Example

Event (Threat & Opportunity) Agent	Example Agent	Example Event
Market conditions, Economy, Political Instability, Cultural Shift, Ethical Shift, Supply Chain, Climate Change	Climate Change	Emerging Green Economy
Market conditions, Economy, Political Instability, Cultural Shift, Ethical Shift, Supply Chain, Climate Change	Economy	Financial Crisis
Any event within a SABSA domain with negative or positive consequences for its super-domain or sub-domain	Confidentiality	Increase Trust
Any event within a SABSA domain with negative or positive consequences for its super-domain or sub-domain	Availability	Decrease Availability
Any event within a SABSA domain with negative or positive consequences for a peer domain	Integrity	Increase Confidence
Any event within a SABSA domain with negative or positive consequences for a peer domain	Compliance	Increase Costs

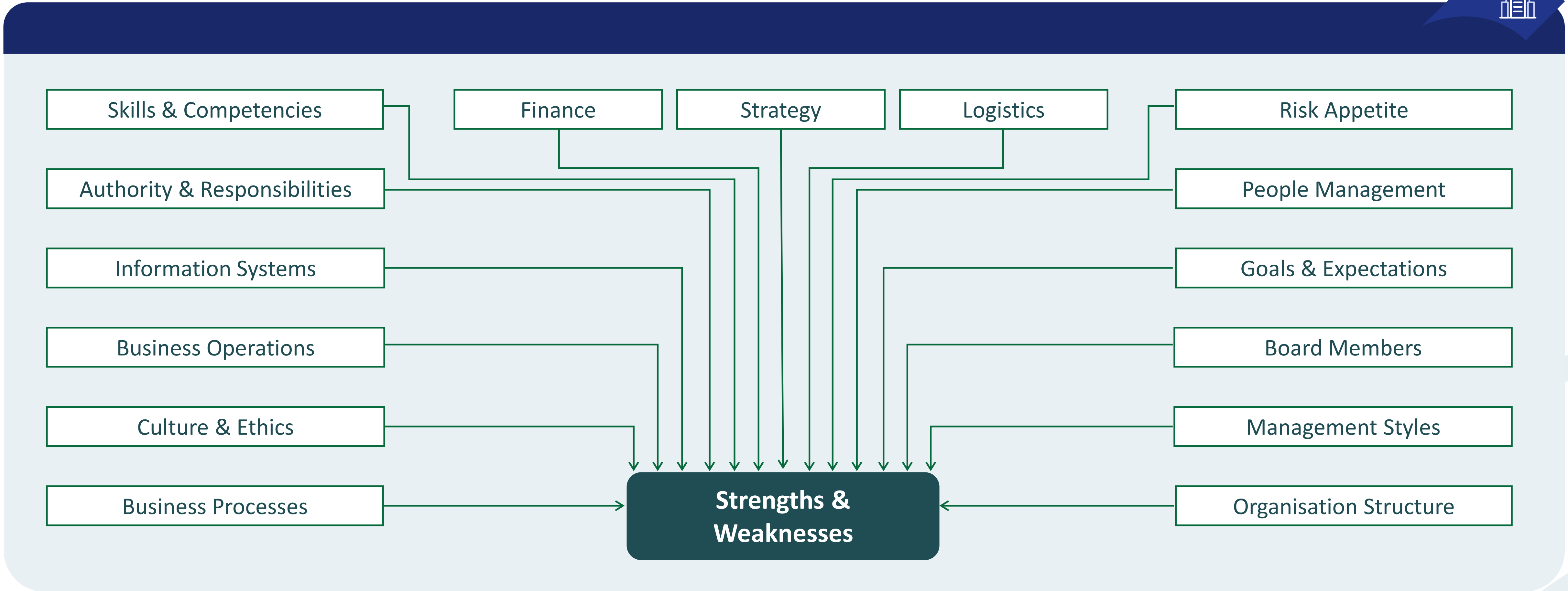
Workshop A1-5

Part 1 – Identify Events



Create the Register of States – Select a Taxonomy

Sample taxonomy – “Enterprise Security Architecture”



Create the Register of States – Select a Taxonomy

Sample taxonomy – COSO

Infrastructure	Personnel	Process	Technology
Availability of assets	Employee capability	Capacity	Data integrity
Capability of assets	Fraudulent activity	Design	Data & system availability
Access to capital	Health & safety	Execution	System selection
Complexity		Suppliers / dependencies	Development & deployment
			Maintenance

Create the Register of States – Select a Taxonomy

Sample technical taxonomy – CVE & NVD

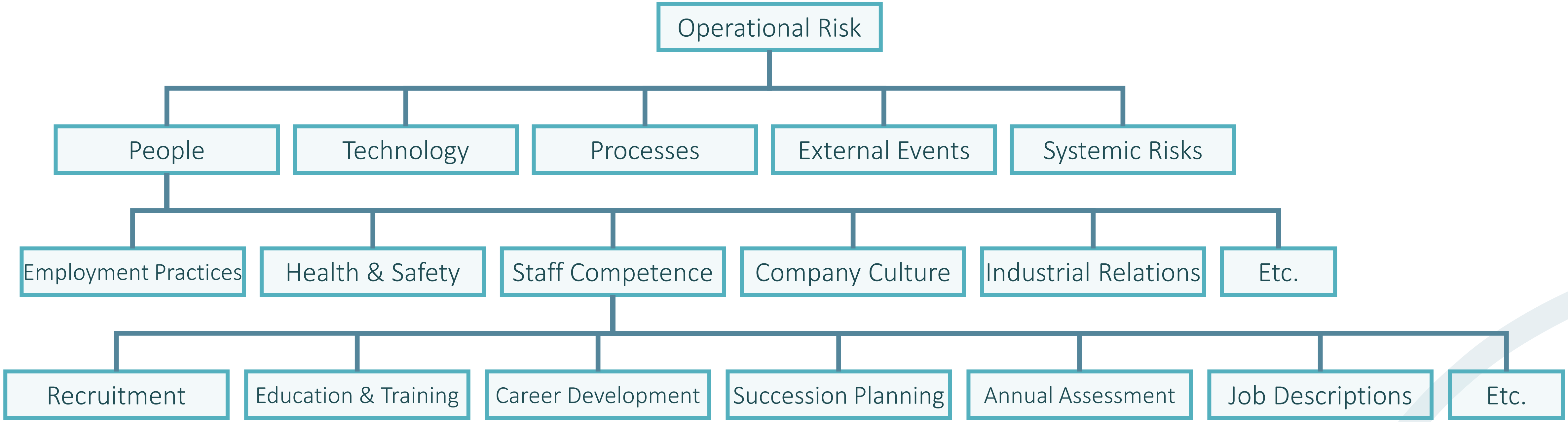
CVE
Common Vulnerabilities & Exposures Glossary (Mitre)

NVD
National Vulnerability Database (NIST)

Typically, pre-existing registers focus exclusively on vulnerability (weakness) state and not strengths

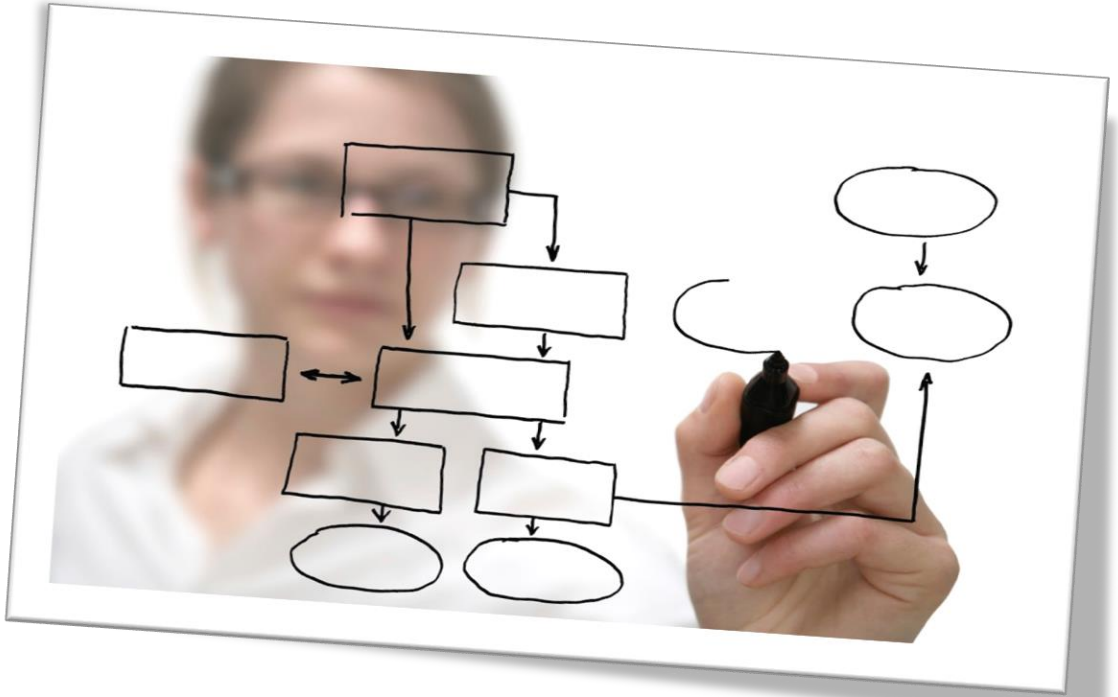
Populate the Register of States – Architected Taxonomy

Correlate layers of abstraction in a dependency tree with domain & attribute hierarchy strengths & weaknesses



Workshop A1-5

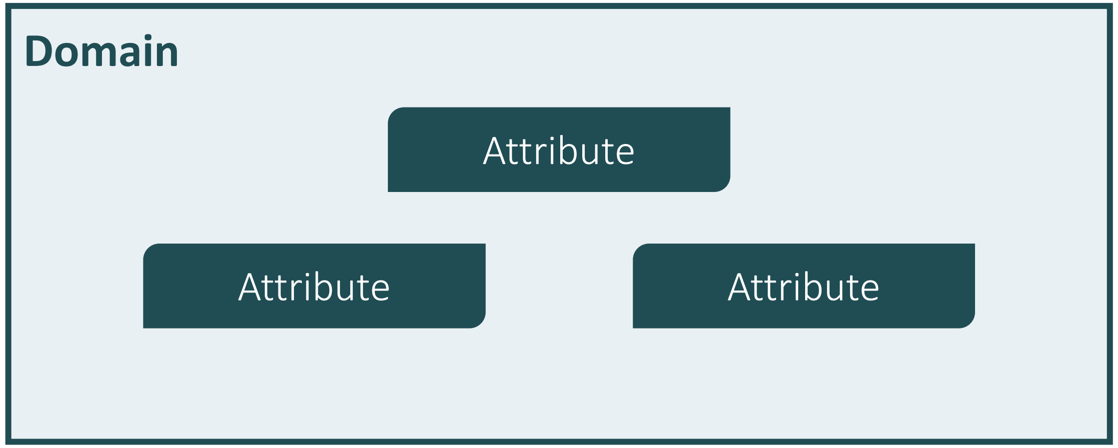
Part 2 – Identify States



Risk Identification - Consequences

Attributes are what matters most to the domain

- Instinctive, natural language for the Domain Authority
- Positive or negative consequences of possible future events upon Attributes
- Negative consequences (damage)
  - Reduction in Attribute performance
  - Failure to meet Attribute performance target
- Positive consequences (benefit)
  - Increase in Attribute performance
  - Increased capability that enables recalibration to a higher Attribute performance target



Remember that systemic consequences through the complex system dependency model can be both positive & negative

Create the Consequences Taxonomy

Attributes classified for aspects of a system

User Attributes		Management Attributes	Operational Attributes	Risk Management Attributes		Legal / Regulatory Attributes	Technical Strategy Attributes	Business Strategy Attributes
Accessible	Motivated	Automated	Available	Access-controlled	Flexibly Secure	Admissible	Architecturally Open	Brand Enhancing
Accurate	Protected	Change-managed	Detectable	Accountable	Identified	Compliant	COTS / GOTS	Business-Enabled
Anonymous	Reliable	Continuous	Inter-Operable	Assurable	Independently Secure	Enforceable	Extendible	Competent
Consistent	Responsive	Controlled	Productive	Assuring Honesty	In our sole possession	Insurable	Flexible / Adaptable	Confident
Current	Transparent	Cost-Effective	Recoverable	Auditable	Integrity-Assured	Legal	Future-Proof	Culture-sensitive
Duty Segregated	Supported	Efficient		Authenticated	Non-Repudiable	Liability Managed	Legacy-Sensitive	Enabling time-to-market
Educated & Aware	Timely	Maintainable		Authorised	Owned	Regulated	Migratable	Governable
				apturing New Risks	Private	Resolvable	Multi-Sourced	Providing Investment Re-use
				onfidential	Trustworthy	Time-bound	Scalable	Providing Return on Investment
		Supportable		Crime-Free				Reputable

It makes sense that the consequences taxonomy is the same taxonomy used for assets – the Attributes taxonomy which is already culturally aligned and accepted

Create the Consequences Taxonomy

Attributes classified to align with cultural values

Stakeholder Groups	Core Values				
	Impartiality	Integrity	Respect	Service	Transparency
Electors, Candidates Scrutineers, Media	Secrecy of the Vote	Confidence & Perception	Privacy	Accessibility Impartiality	Transparency
Senior Management	Reputation Equity	Governability	Compliance	Financial Viability	Auditability
Operations Staff		Accuracy Anonymity Authentication Integrity Verifiability		Availability Reliability Future Sensitivity Modularity	

Create the Consequences Taxonomy

Attributes classified for balanced scorecard alignment

Financial	Customer	Internal Process	Learning & Growth
Cost Effective	Cust. Focused	Automated	Competent
Liability Managed	Engaged	Productive	Confident
Profitable	Retention	Repeatable	Empowered
Providing ROI	Trusted	Scalable	Trained
…	…	…	…
	..	..	..
.	.	.	.

Create the Consequences Taxonomy

Attributes classified to align with stakeholder interests

CEO	CFO	COO	CIO	CTO	CSO
Compliant	Cost Effective	Available	Accurate	Accessible	Access Controlled
Governed	Liability Managed	Change Managed	Private	Agile	Assured
Legal	Profitable	Productive	Reliable	Scalable	Authenticated
Reputable	Providing ROI	Resilient	Timely	Standards Compliant	Confidential
…	…	…	…	…	…
	..	..	..	..	..
.	.	.	.	.	.

Create the Consequences Taxonomy

Attributes classified for enterprise risk category alignment

Financial	Operational	Reputational	Health & Safety
Cost Effective	Available	Brand Enhancing	Accountable
Liability Managed	Change Managed	Culture Sensitive	Educated & Aware
Profitable	Efficient	Compliant	Risk Assessed
Providing ROI	Protected	Confident	Safe
…	…	…	…
	..	..	..
.	.	.	.

SABSA®

Create the Consequences Taxonomy

Attributes classified to align with value chain elements

People Capability

Entity	Customer
Accountable	Accessible
Competent	Accurate
Confident	Culture Sensitive
Diversity	Loyal
Empowered	Private
Equality	Simple
Ethical	Smooth

Process

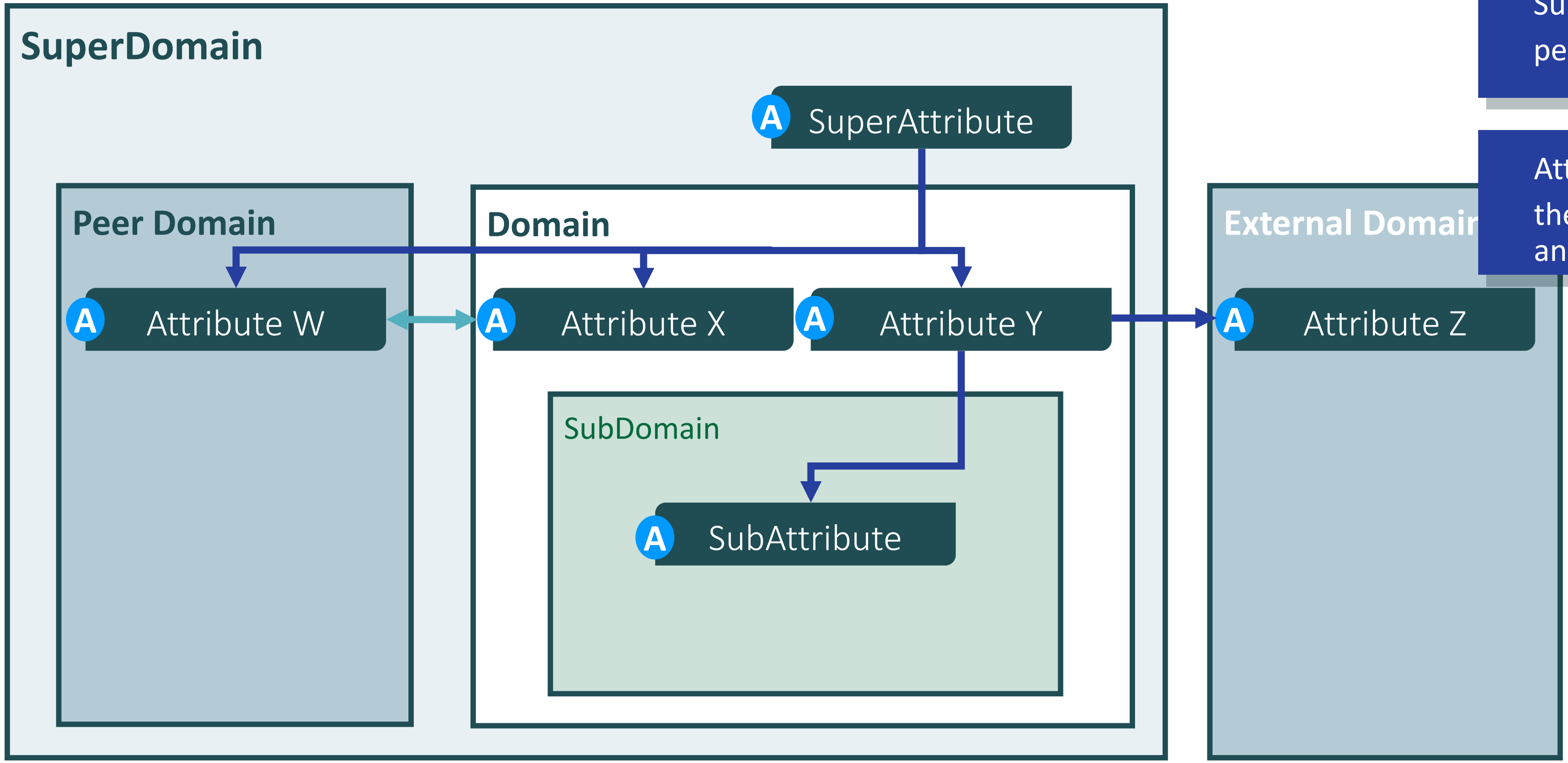
Agile	Automated
Brand Enhancing	Efficient
Governed	Productive
Quality	Repeatable
Timely	

Technology Capability

Architecturally Open	Assured
Available	Extendible
Integrated	Migratable
Protected	Reliable
Scalable	Shareable
Supportable	Total-cost-of-ownership
Trustworthy	Time-to-Market

Consequences for Whom?

Attribute & domain dependency example revisited



SuperAttribute is dependent upon the risk and performance of Attributes W, X and Y

Attribute Y is dependent upon the risk and performance of the SubAttribute and Attribute Z

Attributes W and X are inter-dependent:

Attribute W is dependent upon the risk and performance of Attribute X

Attribute X is dependent upon the risk and performance of Attribute W

Attributes X and Y are independent: Their success does not depend upon the others' risk and performance

Attributes Have Interacting, Systemic & Conflicting Risks

Interactions between value chain domains

People Capability

Entity

- Accountable
- Competent
- Confident
- Diversity
- Empowered
- Equality
- Ethical

Customer

- Accessible
- Accurate
- Culture Sensitive
- Loyal
- Private
- Simple
- Smooth

Process

- Agile
- Brand Enhancing
- Governed
- Quality
- Timely
- Automated
- Efficient
- Productive
- Repeatable

Technology Capability

- Architecturally Open
- Available
- Integrated
- Protected
- Scalable
- Supportable
- Trustworthy
- Assured
- Extendible
- Migratable
- Reliable
- Shareable
- Total-cost-of-ownership
- Time-to-Market

Attributes Have Interacting, Systemic & Conflicting Risks

Interactions in SABSA perspectives

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Dependence
	Goals, Targets, Value & Assets	Opportunities & Threats	Value Chain, Core Processes & Capabilities	Culture, Org. Structure & Relationships	Territories, Jurisdictions & Sites	Time & Sequence Dependencies

Profitable	Risk Managed	Controlled	Accountable	Segregated	Time-to-Market
Reputable	Liability Managed	Quality	Skilled	Compliant	Resilient

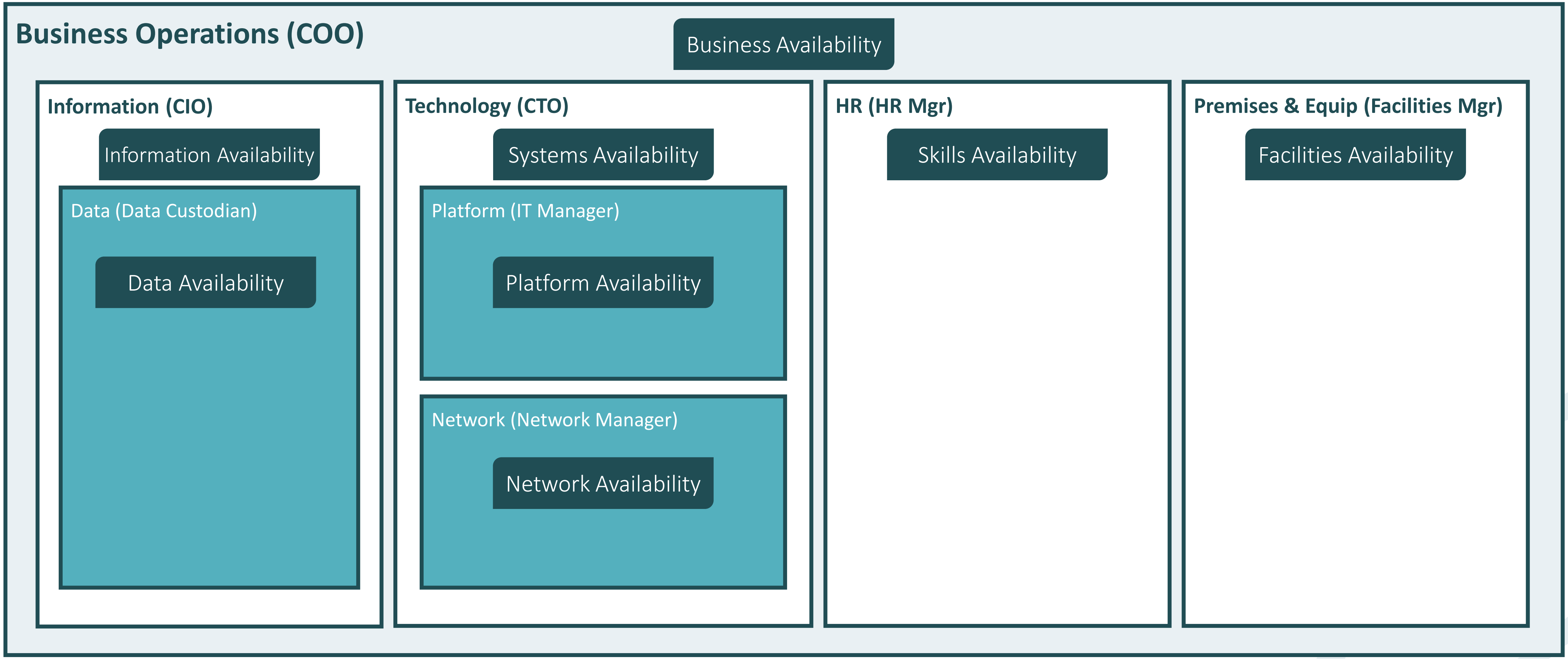
Attributes Have Interacting, Systemic & Conflicting Risks

Interactions between risk type domains

Financial	Operational	Reputational	Health & Safety
Cost Effective	Available	Brand Enhancing	Accountable
Liability Managed	Change Managed	Culture Sensitive	Educated & Aware
Profitable	Efficient	Compliant	Risk Assessed
Providing ROI	Protected	Confident	Safe
…	…	…	…
	..	..	..
.	.	.	.

Populate the Consequences Register

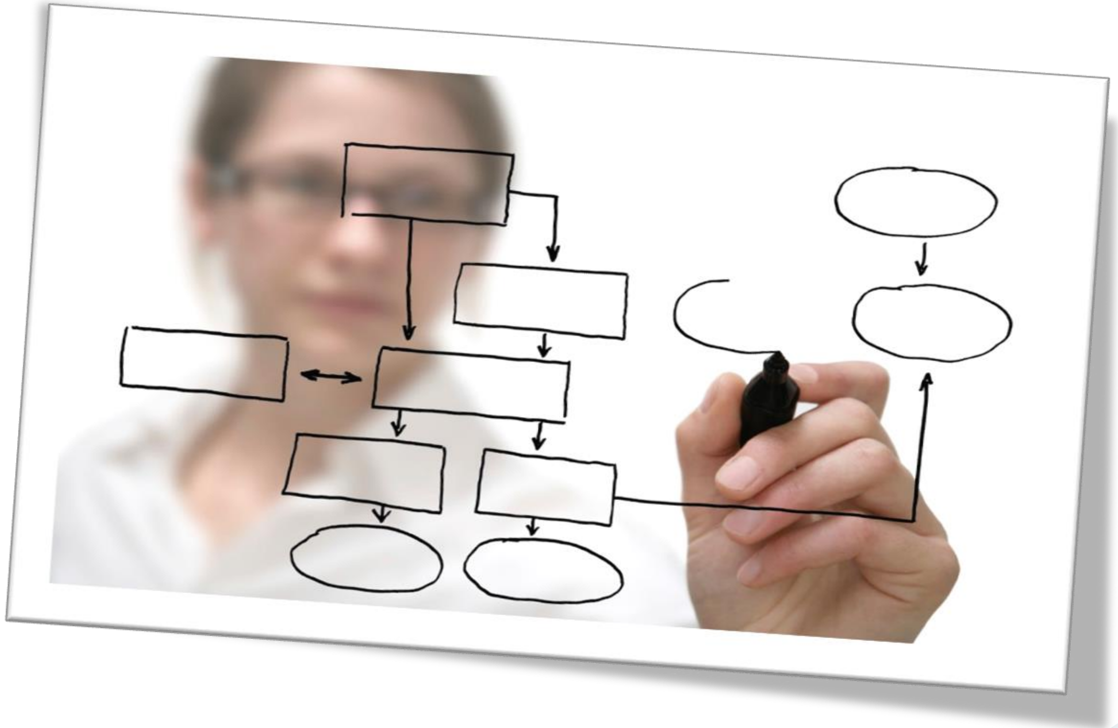
Assemble the dependency tree



SABSA®

Workshop A1-5

Part 3 – Identify Consequences



Analyse Risk

Section 8

There are three kinds of manager:

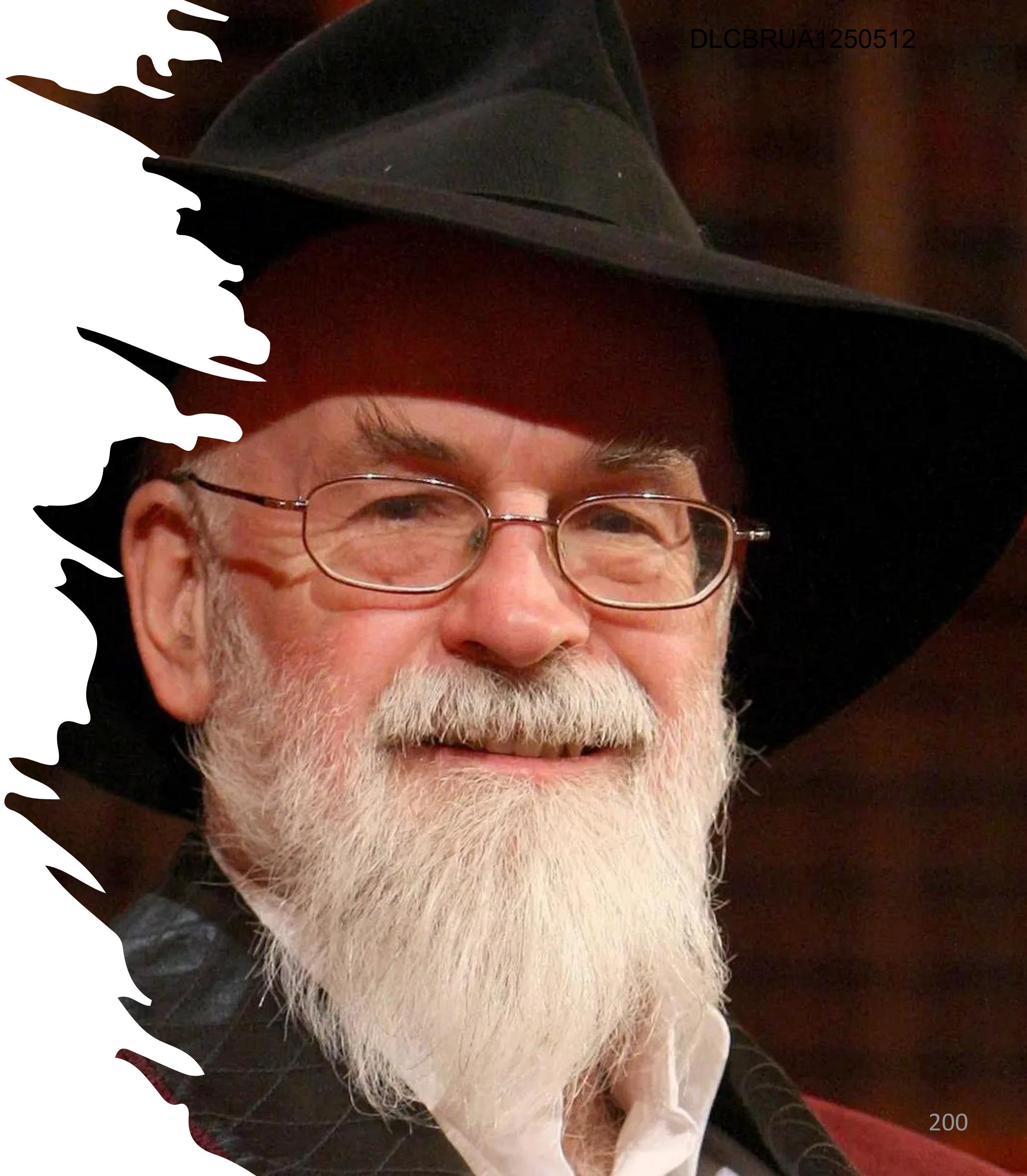
One who can tell me what has happened

One who can tell me what is happening

And one who considers that the other two lack ambition

Terry Pratchett, The Last Continent

Assessment is Future-Focused



Risk Assessment – Analysis

- Risk analysis is the process of understanding the degree to which the identified risks could influence the achievement of objectives
- It involves estimation of the:
  - Likelihood of the possible risk events happening within a given time period
  - Level of magnitude of the possible consequences (damage and benefit) of the possible events

Probability & Likelihood Calculation is Not as Easy as it May Appear

The Monty Hall Problem

Risk Assessment – Analysis: Constraints

Constraints to successful analysis

Constraint	SABSA Approach
Subjective	Overcome "assessment bias" and perception of specialist expertise, or area of interest, through an holistic in-context approach
Vague	Provide measurable, definitive risk level parameters
Inconsistent	Apply an Architectural structure to ensure consistent, uniform understanding between domains

An alternative definition of risk

Risk in a complex system is the degree to which the chances of achieving our goals are affected by things we cannot control, predict, understand, or easily measure

Risk Assessment – Analysis: Likelihood

- Likelihood is the chance that something might happen in our risk context within a given time frame
- Consists of two factors:
  - The likelihood that an event (opportunity or threat) will materialise
  - The likelihood that, at the same time, our state of strength or weakness permits it to have consequences for our risk context

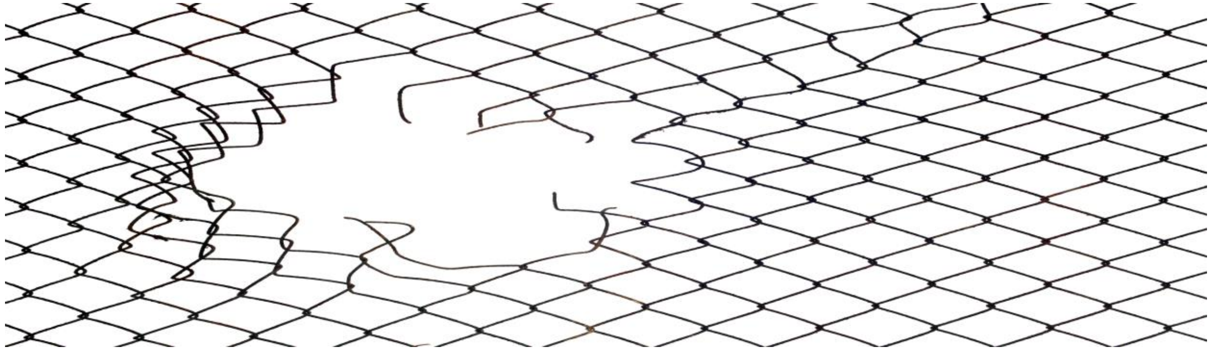
Likelihood Measurement Approaches

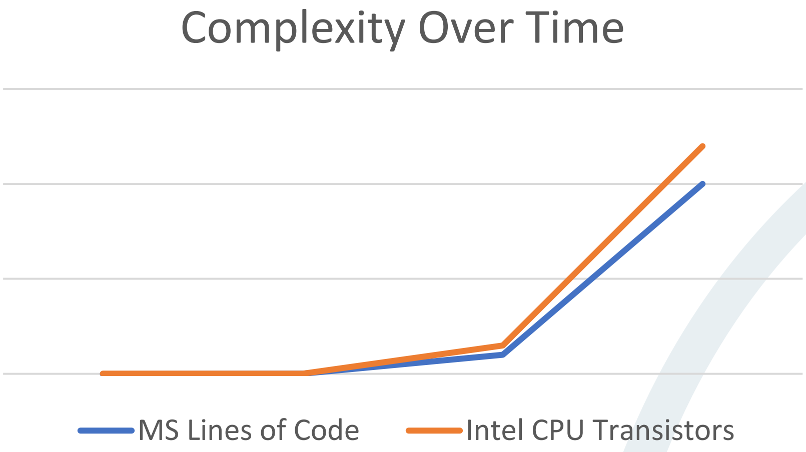
Quantitative	Qualitative	Semi-quantitative
The results can be measured or counted, and any other person trying to quantitatively assess the same situation should end up with the same results Accurate quantitative evaluations can be better relied upon as truth	More subjective than quantitative evaluation. Two individuals evaluating the same thing may end up with different or conflicting results. Qualitative evaluations may involve value judgments and emotional responses Qualitative evaluations may also entail truths, but these truths are harder to get at, and evaluators may not always agree	An intermediary level created by evaluating with a score based on scales or representative numbers . It offers a more consistent and rigorous approach than qualitative assessment with less ambiguity. It does not require the same mathematical skills as quantitative risk assessment, nor does it require the same amount of data, which means it can be applied where precise data is missing Evaluators are likely to agree but truth is not definitive
Probability on a scale of 0.00 to 1.00 or 0% to 100%	High / Medium / Low Very likely / Likely / Unlikely	High >≠ 66.66% Medium >≠ 33.33% ,<= 66.66% Low ≠< 33.33%

Risk Likelihood – Event Analysis Challenge

Issues with the threat-based approach

- Quantification requires good actuarial data which we don't often have
- Statistical data is often not relevant in a dynamic technical environment
- The past is not always a reliable predictor of the future in a rapidly changing system
- "Scare tactics" ask for investment to treat negatives
- Technical threats and vulnerabilities are not well understood by the SuperDomain





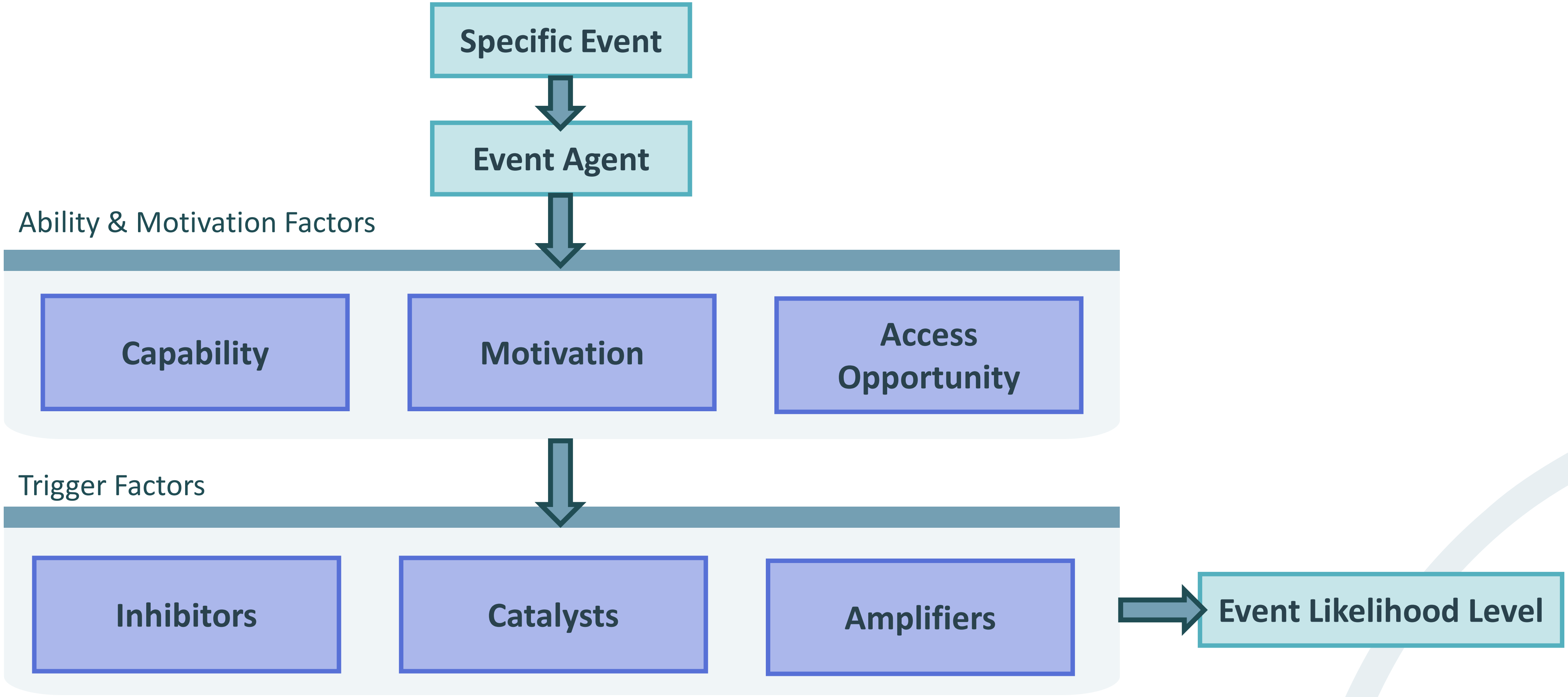
Risk Likelihood – Event Analysis Options

- Binary decision – is it credible that the event will materialise within the time frame?
  - Credible events treated as probable and likelihood analysis is biased toward state
  - Fanciful events treated as improbable and not analysed further
- Determine event probability level based on advice and guidance from industry subject matter experts who may claim to have actuarial information or intelligence
  - Including parties with vested interest - vendors
- Take a formal structured approach to likelihood analysis
- Other?

Objective is to rate possible events with the greatest possible credibility of rating, in the shortest possible time, with the least possible effort

Event Likelihood Level – A Structured Approach

Event scenario analysis framework



Event Likelihood – A Structured Approach

Parameter	Description	Example
Specific Event	A threat/opportunity selected from threat/opportunity database or taxonomy	Unauthorised code inserted into an application to either: defraud or sabotage the organisation
Event Agent	An entity that may execute the threat or opportunity – the event originator	Disaffected employee working in the systems development team
Capability	Level of resources expected to be under the control of the agent	Full skill set and tool set required for the task
Motivation	What motivates the agent	Personal gain or revenge
Access opportunity	Description of the opportunity for access available to threat / opportunity agent & prevalence of accesses	Full access to development code and development environment
Catalysts	Events or changes in circumstances that make the agent decide to act	Redundancy of employee Employee runs up debts Introduction of bonus scheme
Inhibitors	Factors that may deter the agent from executing the event	Fear of being detected, losing job and gaining a criminal record
Amplifiers	Factors that may encourage the agent to execute the event	Belief that rogue code can be hidden and not attributed to an individual

Event Likelihood Level – Agent Capability Factors

Capability Factor	Description
Finance	Money to finance the activities
Technical equipment	Computers, specialised networking equipment, etc
Software	Software tools to perform detailed analysis, probing and penetration of systems, or research & innovation
Facilities	Buildings, services and general support
Expertise	People who are educated, trained or competent in the techniques to be applied in executing the activities
Literature	Books, manuals, instructions and other documentation containing details of how to execute the activities
Experience	People with previous experience of executing the activities

Event Likelihood Level – Agent Motivation Factors

Motivation Factor (Personal Gain)
Finance
Revenge
Knowledge or information
Power and influence
Peer recognition and respect
Satisfy curiosity
Satisfy personality trait
Terrorising groups or individuals
Enhance personal status within group

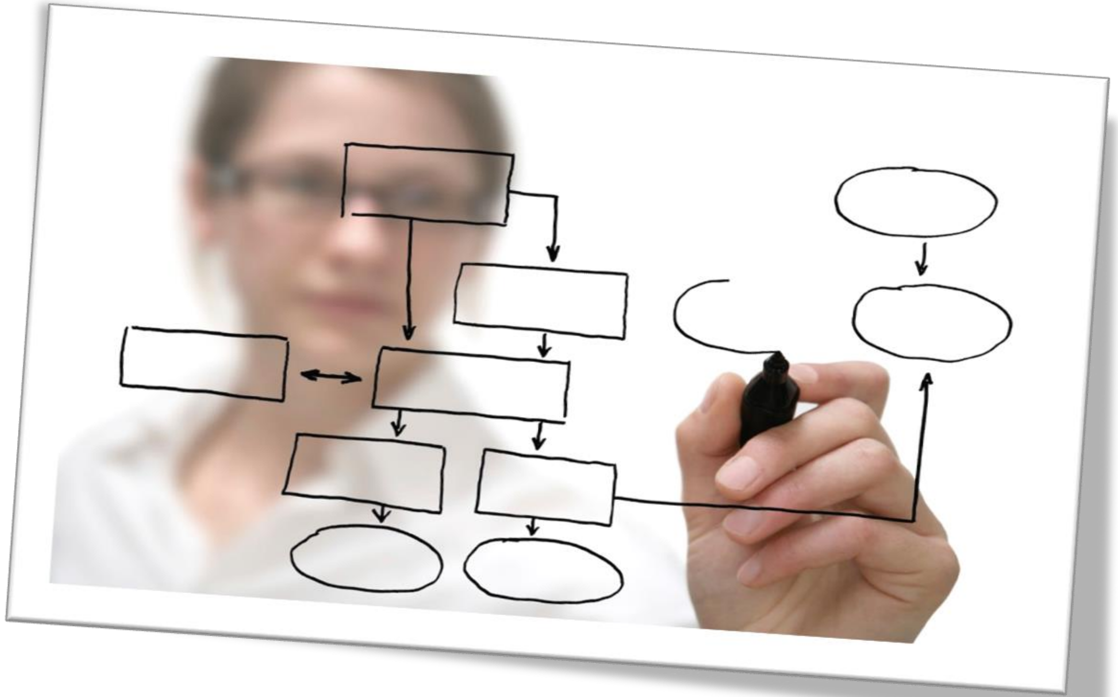
Motivation Factor (Group Gain)
Furthering aims of political group
Furthering aims of criminal group
Furthering aims of religious group
Furthering aims of social or cultural group
Furthering aims of a body corporate
Terrorising groups or individuals
Competitive advantage

Event Likelihood Level – Trigger Factors

Inhibitors	**Catalysts (Candidate KRIs)**	**Amplifiers**
Fear of capture	External events that trigger a response	Peer pressure
Fear of failure	Changes in personal circumstances creating a ‘need’	Fame
Insufficient access limiting the opportunity	Step changes in level of access increasing the opportunity	Easy access providing high level of opportunity
High level of technical difficulty	Step changes in level of difficulty through new technologies and tools/ demonstrable increased prevalence	Ease of execution because of low level of technical difficulty
High cost of participation	Step changes in level of cost	Low cost of participation
Sensitivity to adverse public opinion	Dramatic changes in public opinion and cultural values	Belief in sympathetic public opinion

Workshop A1-6

Part 1 – Assess Event Likelihood



Risk Likelihood – State Analysis Options

- Meaningful states (strengths & weaknesses) are treated as possible and risk analysis is biased toward impact assessment
  - Binary decision – is it credible that:
    - The weakness is meaningful – it could be demonstrably exploited within the time frame
    - The strength is meaningful – we can leverage it to grasp an opportunity within the time frame
- Determine state (strength & weakness) level based on advice and guidance from industry subject matter experts who may claim to have actuarial information or intelligence
  - Including parties with vested interest - vendors
- Take a formal structured approach to state analysis using testing, systems analysis, process analysis, actuarial data
- Other?

Objective is to rate possible states (strengths & weaknesses) with the greatest possible credibility of rating, in the shortest possible time, with the least possible effort

State Analysis – Structured Methods: CVSS Example

Common Vulnerability Scoring System Version 3.1 Calculator

Base Score

Attack Vector (AV)
Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)
Low (L) | High (H)

Privileges Required (PR)
None (N) | Low (L) | High (H)

User Interaction (UI)
None (N) | Required (R)

Scope (S)
Unchanged (U) | Changed (C)

Confidentiality (C)
None (N) | Low (L) | High (H)

Integrity (I)
None (N) | Low (L) | High (H)

Availability (A)
None (N) | Low (L) | High (H)

Severity	Base Score
None	0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Environmental Score

Confidentiality Requirement (CR)
Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)
Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)
Not Defined (X) | Low (L) | Medium (M) | High (H)

Select values for all base metrics to generate score

Modified Attack Vector (MAV)
Not Defined (X) | Network | Adjacent Network | Local | Physical

Modified Attack Complexity (MAC)
Not Defined (X) | Low | High

Modified Privileges Required (MPR)
Not Defined (X) | None | Low | High

Modified User Interaction (MUI)
Not Defined (X) | None | Required

Modified Scope (MS)
Not Defined (X) | Unchanged | Changed

Modified Confidentiality (MC)
Not Defined (X) | None | Low | High

Modified Integrity (MI)
Not Defined (X) | None | Low | High

Modified Availability (MA)
Not Defined (X) | None | Low | High

Temporal Score

Exploit Code Maturity (E)
Not Defined (X) | Unproven (U) | Proof-of-Concept (P) | Functional (F) | High (H)

Remediation Level (RL)
Not Defined (X) | Official Fix (O) | Temporary Fix (T) | Workaround (W) | Unavailable (U)

Report Confidence (RC)
Not Defined (X) | Unknown (U) | Reasonable (R) | Confirmed (C)

State Analysis – CVSS Base Scoring

Base

The Base Score is a function of the Impact and Exploitability sub score equations. Where the Base score is defined as,

If (Impact sub score <= 0) *0 else,*
Scope Unchanged₄ $Roundup(Minimum[(Impact + Exploitability), 10])$
Scope Changed $Roundup(Minimum[1.08 \times (Impact + Exploitability), 10])$

and the Impact sub score (ISC) is defined as,

Scope Unchanged $6.42 \times ISC_{\mathrm{Base}}$
Scope Changed $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

Where,

$$ISC_{Base} = 1 - [(1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail})]$$

And the Exploitability sub score is,

$$8.22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$$

State Analysis – CVSS Temporal & Environmental Scoring

Temporal

The Temporal score is defined as,

$$Roundup(BaseScore \times ExploitCodeMaturity \times RemediationLevel \times ReportConfidence)$$

Environmental

The environmental score is defined as,

If (Modified Impact Sub score <= 0) 0 else,

If Modified Scope is Unchanged Round up(Round up (Minimum [(M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)

If Modified Scope is Changed Round up(Round up (Minimum [1.08 × (M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)

And the modified Impact sub score is defined as,

If Modified Scope is Unchanged 6.42 × $[ISC_{Modified}]$

If Modified Scope is Changed 7.52 × $[ISC_{Modified} - 0.029]$-3.25× $[ISC_{Modified} \times 0.9731 - 0.02]$ 13

Where,

$$ISC_{Modified} = Minimum\ [[1 - (1 - M.IConf \times CR) \times (1 - M.IInteg \times IR) \times (1 - M.IAvail \times AR)], 0.915]$$

The Modified Exploitability sub score is,

$$8.22 \times M.AttackVector \times M.AttackComplexity \times M.PrivilegeRequired \times M.UserInteraction$$

4 Where "Round up" is defined as the smallest number, specified to one decimal place, that is equal to or higher than its input. For example, Round up (4.02) is 4.1; and Round up (4.00) is 4.0.

CVSS Base Score:

Impact Subscore:

Exploitability Subscore:

CVSS Temporal Score:

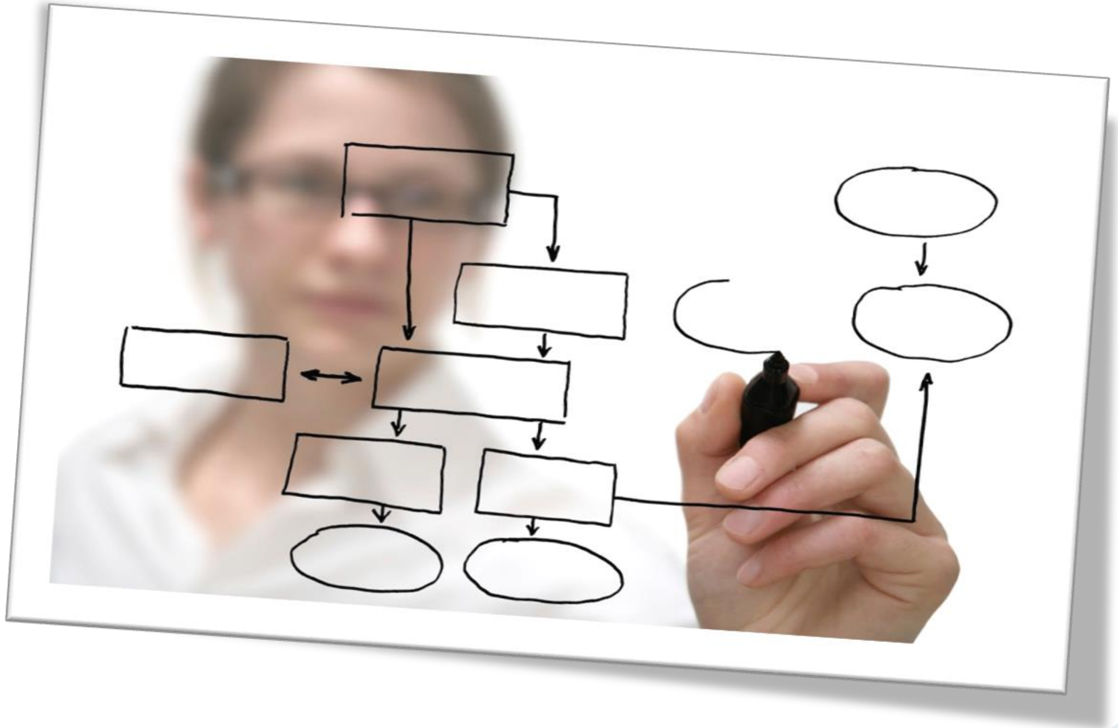
CVSS Environmental Score:

Modified Impact Subscore:

Overall CVSS Score:

Workshop A1-6

Part 2 – Assess State



Risk Period / Holding Period Challenge

- What time frame is appropriate for assessing likelihood?
- Over what period is a risk “in play”?
  - Almost every scenario will occur over the course of an aeon
  - Almost no scenario will occur over the course of a nanosecond
- Extremities of risk period definitions:
  - Time period during which the risk is approximately certain
  - Time period during which the risk is approximately irrelevant

Holding Period A holding period is the amount of time the investment is held by an investor, or the period between the purchase and sale of a security ***Bank for International Settlements***

Likelihood is the chance that something might happen in our risk context *within a given time frame* ***ref “Analysis – Likelihood”***

Risk Period / Holding Period - Approaches

Likelihood Rating	Occurrence Spectrum
Almost certain	Event will occur one or more times in a year
Likely	Event will occur one time in three years
Possible	Event will occur one time in ten years
Unlikely	Event will occur one time in fifty years
Almost impossible	Event will occur one time or less in one hundred years

Likelihood Rating	Frequency Within Risk (Holding) Period
Almost certain	Event will occur more than 100 times in a year
Likely	Event will occur more than 50 times in a year
Possible	Event will occur more than 10 times in a year
Unlikely	Event will occur at least 1 time in a year
Almost impossible	Event will not occur within in a year

The risk (holding) period is clearly contextual.

Does your corporate risk standard enforce a fixed risk period for likelihood calculations across the entire Enterprise, irrespective of the risk context?

Overall Risk Likelihood

Overall likelihood combines the two independent measures of event & state

Likelihood consists of two factors:

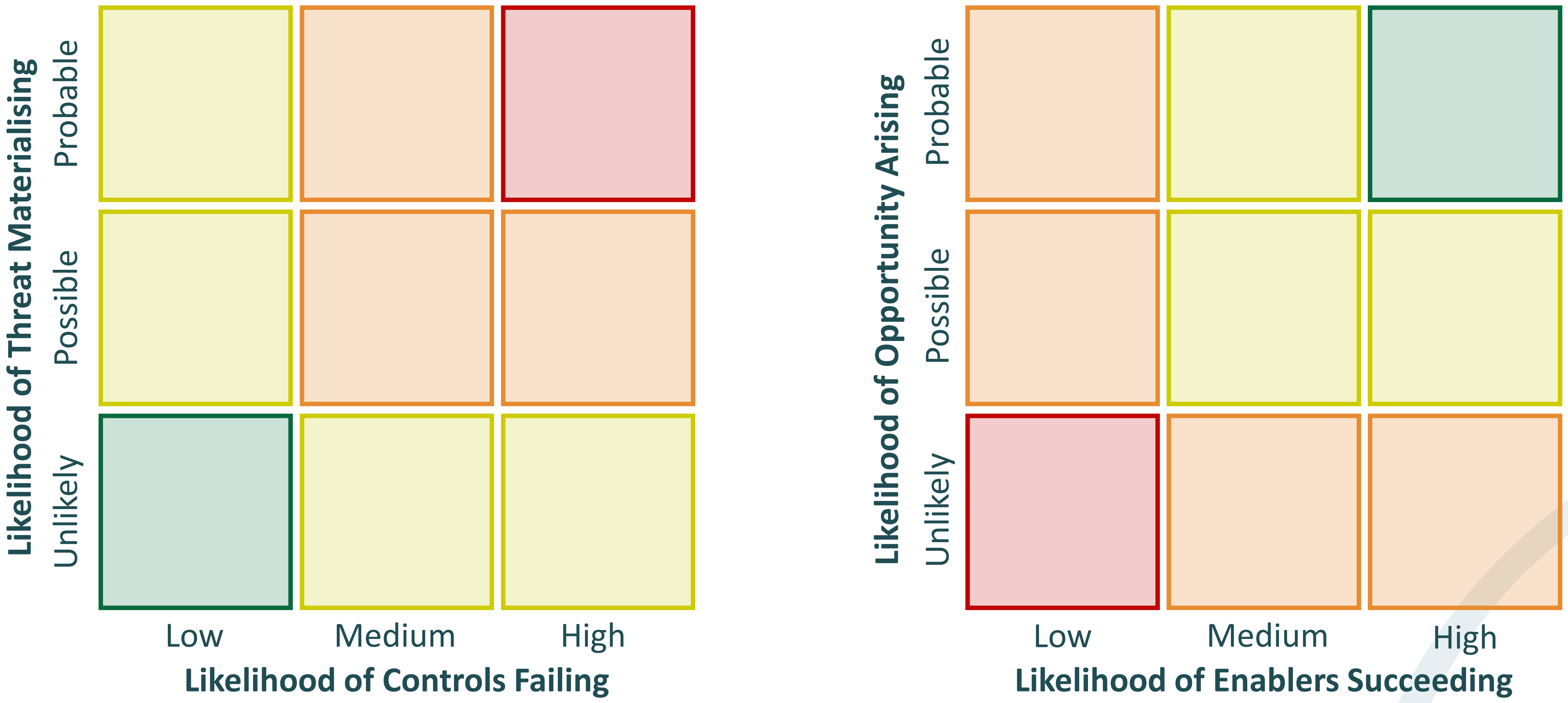
The likelihood that an event (opportunity or threat) will materialise

The likelihood that, at the same time, our state of strength or weakness permits it to have consequences for our risk context ***Ref " Analysis – Likelihood"***

Overall likelihood (the combination of the likelihood that an event will materialise with the likelihood that, at the same time, our controls will fail or enablers succeed) can be determined using any combination of qualitative, quantitative, and semi-quantitative techniques

The Risk Architect must define a spectrum of likelihood levels / ratings from the likelihood heatmap resulting from the combination of the two measures

Risk Likelihood - Qualitative



Risk Likelihood - Quantitative

Likelihood of Threat Materialising (rows) × Likelihood of Controls Failing (columns)

	01	02	03	04	05	06	07	08	09	10
10	10	20	30	40	50	60	70	80	90	100
09	9	18	27	36	45	54	63	72	81	90
08	8	16	24	32	40	48	56	64	72	80
07	7	14	21	28	35	42	49	56	63	70
06	6	12	18	24	30	36	42	48	54	60
05	5	10	15	20	25	30	35	40	45	50
04	4	8	12	16	20	24	28	32	36	40
03	3	6	9	12	15	18	21	24	27	30
02	2	4	6	8	10	12	14	16	18	20
01	1	2	3	4	5	6	7	8	9	10

Likelihood of Opportunity Arising (rows) × Likelihood of Enablers Succeeding (columns)

	01	02	03	04	05	06	07	08	09	10
10	11	12	13	14	15	16	17	18	19	20
09	10	11	12	13	14	15	16	17	18	19
08	9	10	11	12	13	14	15	16	17	18
07	8	9	10	11	12	13	14	15	16	17
06	7	8	9	10	11	12	13	14	15	16
05	6	7	8	9	10	11	12	13	14	15
04	5	6	7	8	9	10	11	12	13	14
03	4	5	6	7	8	9	10	11	12	13
02	3	4	5	6	7	8	9	10	11	12
01	2	3	4	5	6	7	8	9	10	11

Risk Likelihood – Semi-Quantitative

Likelihood of Threat Materialising (rows) / Likelihood of Controls Failing (columns)

	Almost Impossible	Unlikely	Possible	Likely	Almost Certain
10	Very Unlikely	Likely	Very Likely	Very Likely	Almost Certain
09	Very Unlikely	Possible	Likely	Very Likely	Very Likely
08	Very Unlikely	Possible	Likely	Likely	Very Likely
07	Very Unlikely	Possible	Possible	Likely	Very Likely
06	Very Unlikely	Possible	Possible	Likely	Likely
05	Very Unlikely	Unlikely	Possible	Possible	Possible
04	Very Unlikely	Unlikely	Unlikely	Possible	Possible
03	Almost Impossible	Very Unlikely	Unlikely	Unlikely	Unlikely
02	Almost Impossible	Almost Impossible	Very Unlikely	Very Unlikely	Unlikely
01	Almost Impossible	Almost Impossible	Almost Impossible	Very Unlikely	Very Unlikely

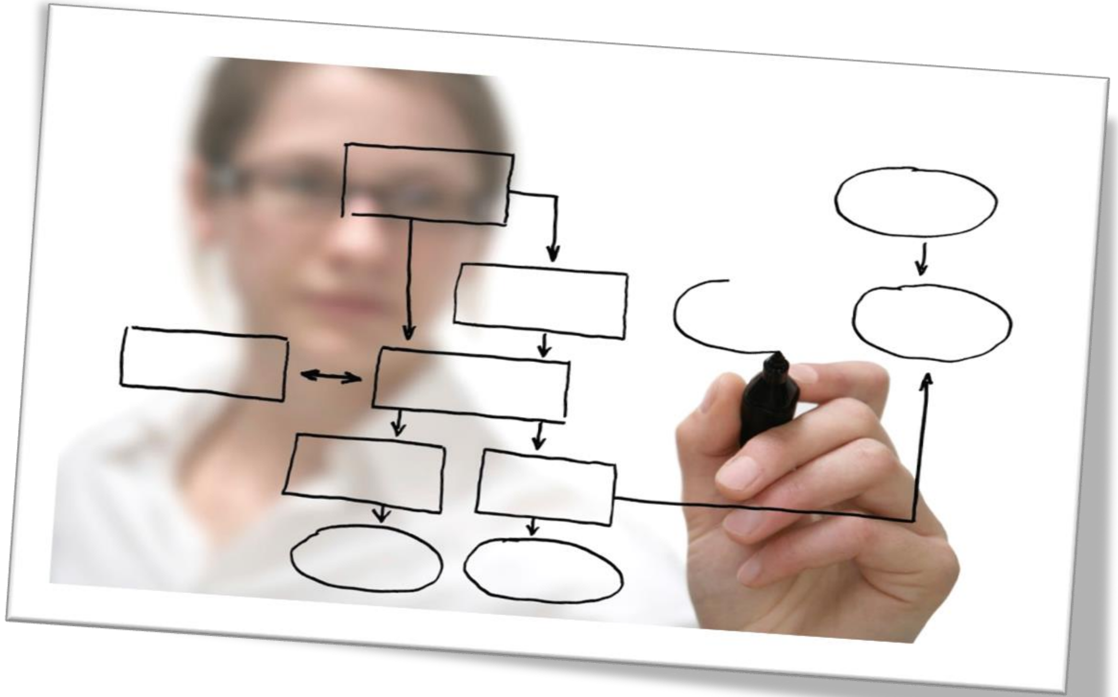
Likelihood of Opportunity Arising (rows) / Likelihood of Enablers Succeeding (columns)

	01	02	03	04	05	06	07	08	09	10
High	10	20	30	40	50	60	70	80	90	100
Medium	5	10	15	20	25	30	35	40	45	50
Low	1	2	3	4	5	6	7	8	9	10

SABSA®

Workshop A1-6

Part 3 – Assess Likelihood



Assess Consequences

The SABSA Attributes Profile – Attributes are measurable

Context
Analysed, Published or interpreted

Attribute Definition

Name:
Definition:

Attribute Taxonomy

Classification:

Attribute Profile

Measurement Approach:
Metric:
Performance Target:

SABSA Attributes Taxonomy

The classification and visual presentation of the SABSA Attributes, or a subset of Attributes, catalogued to represent particular Enterprise aspects or stakeholder requirements

SABSA Attributes Profile

Attribute Definition + Attribute Measurement

The SABSA Attributes in full measurable form comprised of Name, Definition, Measurement Approach, Metric, and Performance Target

Attributes Measurement Framework

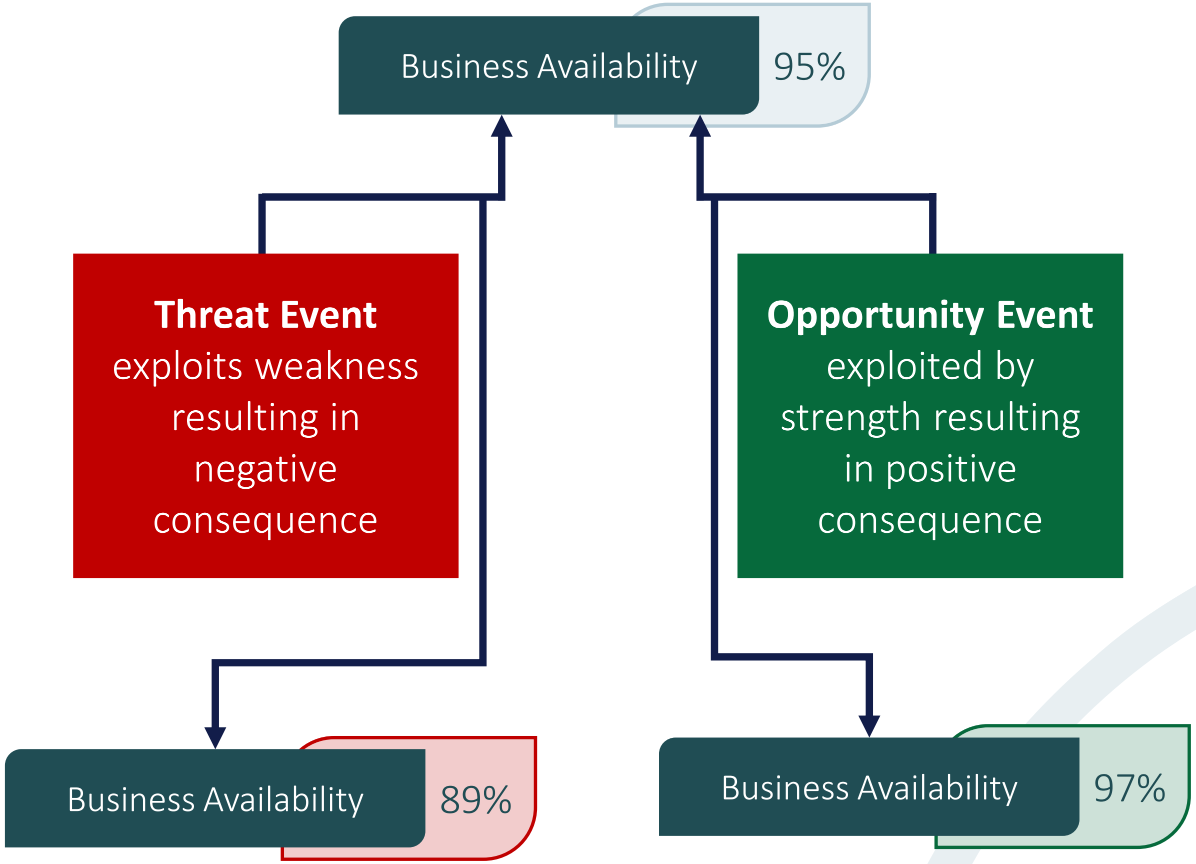
Measurement Approach	Metric	Performance Target
High level statement of the approach to obtaining a measurement Includes the purpose of measuring: ▪ Describe current-state ▪ Compare current-state with a different entity or time ▪ Predict state or trend Includes a verb such as: ▪ Survey ▪ Monitor ▪ Collect Determines the most suitable metric type for the purpose: ▪ Hard (quantitative, objective, verifiable) ▪ Soft (qualitative, subjective, open to opinion)	The means to articulate, and the structure to format, the measure Includes a variable: ▪ Value ▪ Percentage ▪ Volume ▪ Time ▪ Ranking ▪ Scale	The populated metric Includes a mathematical operator: ▪ True or false ▪ = ▪ > or <

Attributes Profile – Measurement Examples

Attribute	Measurement Approach	Metric	Performance Target
Contented	Monitor trend of ice cream volume consumed	Hard metric: Scoops per week	30 scoops per week
Available	Monitor uptime of broadband network service	Hard metric: Percentage per time period	99.999% per week as required by TC5632A: Consumer Service Terms & Conditions
Usable	Survey wholesale customers about online ordering experience	Average monthly satisfaction rating 1 – 5 where 5 is best	Satisfaction rating 4.5

SABSA Approach to Assessing Consequences

- Attributes represent the assets stakeholders care most about
- All Attributes have performance targets
- Impact is expressed as positive or negative consequences of potential events upon Attribute Performance



Assess Consequences – Consequence Levels

As with likelihood, the architect must determine a scale of consequences

Qualitative

Attribute	Performance significantly exceeds target
Attribute	Performance exceeds target
Attribute	Performance marginally exceeds target
Attribute	Performance meets target
Attribute	Performance marginally misses target
Attribute	Performance misses target
Attribute	Performance significantly misses target

Quantitative

Attribute	98%
Attribute	96%
Attribute	95%
Attribute	94%
Attribute	92%

Semi-Quantitative

Attribute	>97.5%	Highly Beneficial
Attribute	95%> <97.5%	Beneficial
Attribute	95%	95%
Attribute	90%< >95%	Damaging
Attribute	<90%	Devastating

Risk Likelihood – Analysis: Level

- Risk level is the magnitude of the event
- It is the combination of the likelihood of a potential event with the scale of its estimated consequences
- Organisations use a variety of qualitative, quantitative, and semi-quantitative multi-point scales to create risk heatmaps

Risk Level Common level of risk categories include : extreme risk, high risk, moderate risk, and low risk. A high risk event would have a high likelihood of occurring and a severe impact if it actually occurred ***ISO 31000***

Attributes

Threat Rating	Vulnerability Rating	Impact Rating
Opportunity Rating	Strength Rating	Benefit Rating

Risk to Attributes = Overall Likelihood of Event * Consequence of event

Output from Overall Likelihood Analysis is now input with Consequence Level Analysis to assess the overall Risk Level

Approach to Risk Level – Define Taxonomy of Risk Levels

Risk levels are represented in a risk heatmap

- Remember what we are trying to achieve
- Risk is the consequences of events upon objectives
- Ultimately, risk assessment should define and communicate priorities for action
- Objective of assessment is to rate possible risks with the greatest possible credibility of rating, in the shortest possible time, with the least possible effort required to inform the business of priorities

Risk Level Heatmap - Qualitative

Likelihood	Significant Damage	Damage	Marginal Damage	Marginal Benefit	Benefit	Significant Benefit
High	Very High -	High -	Medium -	Medium +	High +	Very High +
Medium	Very High -	High -	Medium -	Medium +	High +	Very High +
Low	High -	Medium -	Low -	Low +	Medium +	High +

Consequences

Risk Level Heatmap - Quantitative

Rating	Mid-point Multiplier				
90+	95	-237.5	-118.75	118.75	237.5
60+	75	-187.5	-93.75	93.75	187.5
40+	50	-12.5	-62.5	62.5	125
20+	35	-87.5	-43.75	43.75	87.5
10+	15	-37.5	-18.75	18.75	37.5
5+	7.5	-18.75	-9.375	9.375	18.75
>0	2.5	-6.25	-3.125	3.125	6.35
	Rating	Loss >2.5%	Loss <2.5%	Gain <2.5%	Gain >2.5%
	Multiplier	-2.5	-1.25	+1.25	+2.5

Likelihood

Consequences

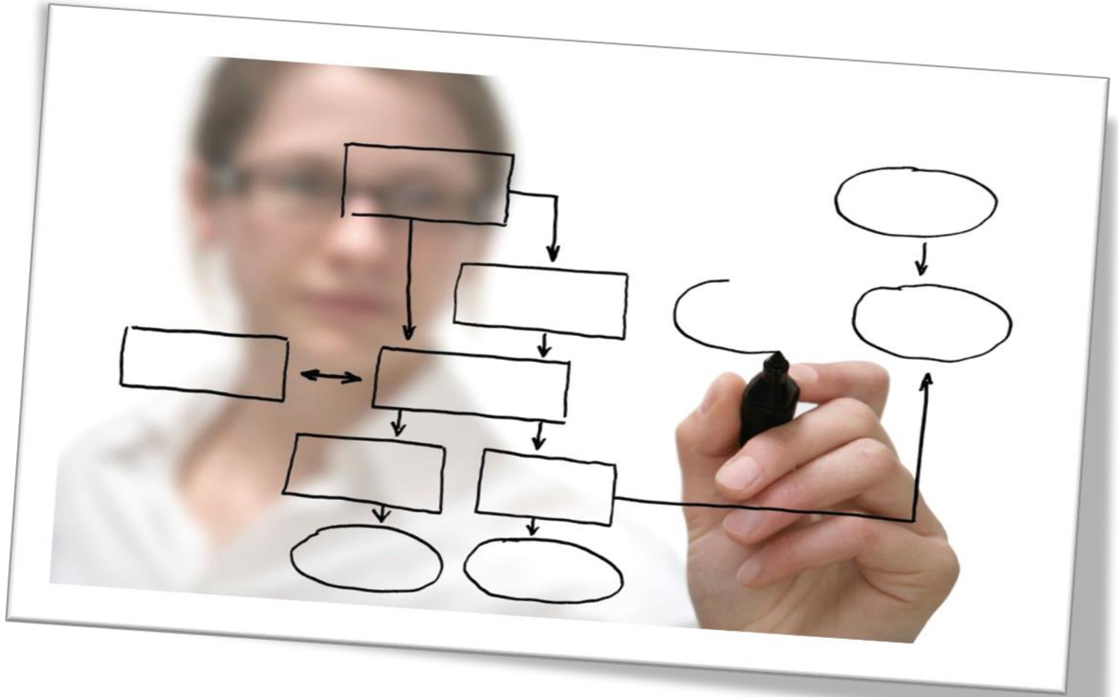
Risk Level Heatmap – Semi-Quantitative

Likelihood	Loss >2.5%	Loss <2.5%	Gain <2.5%	Gain >2.5%
Almost Certain	Very High	High	High	Very High
Very Likely	High	Medium	Medium	High
Likely	High	Medium	Medium	High
Possible	Medium	Low	Low	Medium
Unlikely	Low	Very Low	Very Low	Low
Very Unlikely	Very Low	Negligible	Negligible	Very Low
Almost Impossible	Negligible	Negligible	Negligible	Negligible

Consequences

Workshop A1-6

Part 4 – Assess Risk



Evaluate Risk

Section 9

SABSA®

Risk Assessment – Evaluation

- Risk standards traditionally define Risk Evaluation as a process to compare risk analysis results with risk criteria and cost benefit in order to determine whether or not a specified level of
risk is acceptable or tolerable

Risk Evaluation Making a decision about the level or priority of each risk through the application of the criteria developed when the context was established. Risks are prioritised for attention, and cost benefit analysis is used to determine whether risk treatment is worthwhile ***ISO 31000***

Risk Evaluation Determination of risk management priorities through establishment of qualitative and/or quantitative relationships between benefits and associated risks ***ISO 31000***

The Need to Define Evaluation Criteria

- The purpose of risk evaluation is to make decisions based on the outcomes of risk analysis:
  - About which risks need treatment
  - About treatment priorities
- Risk evaluation involves:
  - Comparing the level of risk found during the analysis process with risk criteria established when the context was considered
  - Considering the risk analysis results in the context of the domain’s objectives
  - Considering the risk analysis results holistically in the domain’s context, dependents and dependencies
  - Where a choice is to be made between options, higher potential losses may be associated with higher potential gains and the appropriate choice will depend upon context, risk appetite and culture

Evaluation Criteria

Considerations include

- Risk Appetite
- Risk Tolerance
- Total cost of risk
- Cost benefit
- Balance of positive and negative consequences for the Domain
- Balance of positive and negative consequences for the Domain's dependents
- Holistic evaluation for the Enterprise as a whole

Risk Appetite

What is the domain authority prepared to lose in pursuing a gain?

- Evaluation of gambling in a casino presents a balanced risk heatmap that indicates a balance of probability of loss (the probability of loss is higher than the probability of gain)
- In a “perfect risk” world, casinos would have no customers
- But casino customers don’t operate in “perfect risk” balance
- And neither do Business owners!

Risk is not a “High” Risk because a high number was calculated in the analysis but because the result of the analysis shows it to be beyond the risk owner’s appetite

Risk Appetite – The Key to Defining Risk Levels

Risk appetite is the inverse of performance target

Attribute Profile

Measurement Approach:
Metric:
Performance Target:

- Every attribute is measurable and has a performance target
- Failure to achieve the target is by definition unacceptable

Attribute	Measurement Approach	Metric	Performance Target	Risk Appetite
Contented	Monitor trend of ice cream volume consumed	Scoops per week	30 scoops per week	0 ice cream scoops
Available	Monitor uptime of broadband network service	Percentage per time period	99.999% per week as required by TC5632A: Consumer Service Terms & Conditions	0.001% downtime
Usable	Survey wholesale customers about online ordering experience	Average monthly satisfaction rating 1 – 5 where 5 is best	Satisfaction rating 4.5	Loss of 0.5 stars

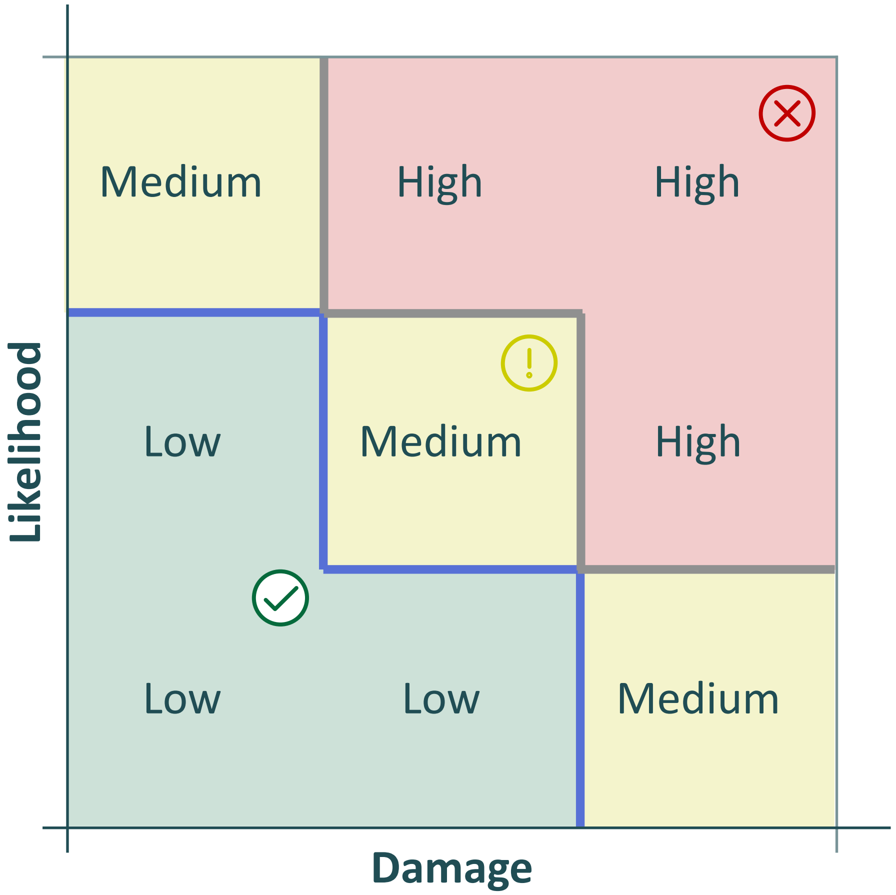
Appetite must be represented on the scaling and design of the heatmap

Implies introduction of a secondary threshold to provide early warning alerts of potentially impending failure to perform within targets

Risk Heatmap Must Incorporate Thresholds

- Are we operating within desired limits?

Risk Levels Determine Priority



Unacceptable Risk
Beyond risk appetite
Urgent treatment required to bring risk within appetite

Warning
Within risk appetite
Treatment required to prevent escalation

Acceptable Risk
Within risk appetite
No treatment required

Primary Risk Threshold (appetite indicator)

Secondary Risk Threshold (early warning indicator)

Appetite for Gain – Why We Are Prepared To Accept Risk

Implication that “Risk Appetite” should be split into appetite for loss & gain

Attribute	Measurement Approach	Metric	Performance Target	Appetite for Loss	Appetite for Gain
Contented	Monitor trend of ice cream volume consumed	Scoops per week	30 scoops per week	0 ice cream scoops	2 ice cream scoops per week
Available	Monitor uptime of broadband network service	Percentage per time period	99.999% per week as required by TC5632A: Consumer Service Terms & Conditions	0.001% downtime	99.9995% per week
Usable	Survey wholesale customers about online ordering experience	Average monthly satisfaction rating 1 – 5 where 5 is best	Satisfaction rating 4.5	Loss of 0.5 stars	Growth to 4.6 stars

Risk Tolerance

Risk Tolerance The levels of variation the entity is willing to accept around specific objectives ***COSO***

Risk Tolerance The organisation's or stakeholder's readiness to bear the risk ***after*** risk treatment in order to achieve its objectives ***ISO 31000 Guide 73 Risk Management Vocabulary***

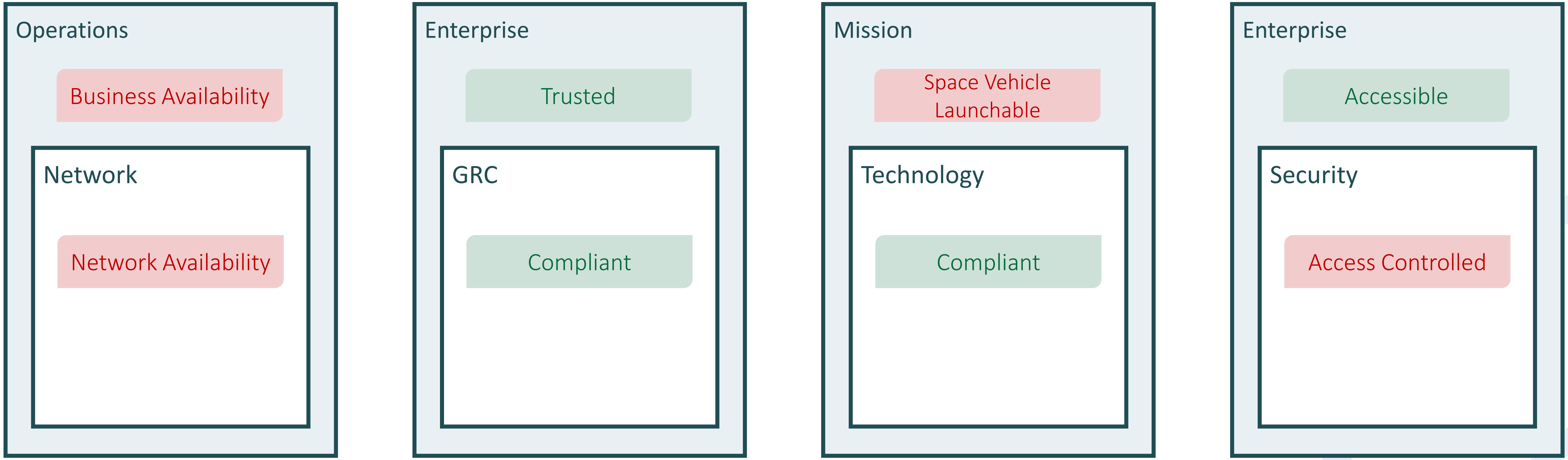
The appetite is defined as 60 but does the tolerance change depending upon criteria such as weather conditions, or proximity of a school?

However we define the terms, we must define the positive and negative boundaries and variances within which we wish to operate in order to consider not just if a risk is acceptable but if it is acceptable in the context of potential gains?

Domain Dependency & Systemic Risk Balance

Relationship can be +to+, -to-, +to- or –to+

- Risk perspectives vary:
  - A high risk to one Domain Authority may be perceived as a low risk to another
- Risks conflict:
  - A negative to one Attribute may be perceived as a benefit to another



Domain Dependency & Systemic Risk Balance

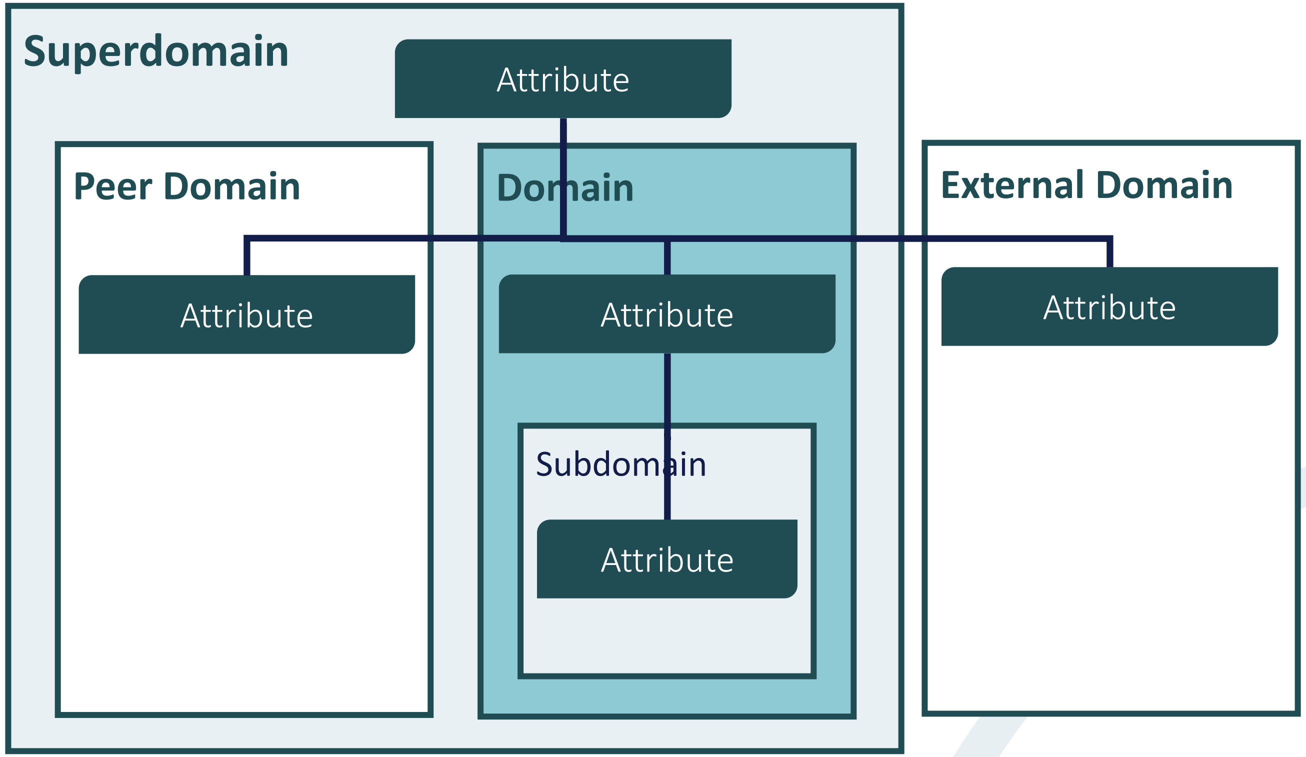
Dependency upon balance

Security, usability & cost do not inter-depend but the Domain/SuperDomain depends upon all 3 to be performing to target – the balance between them must be 'correct' in order for the Domain to meet its targets

SABSA Holistic Risk Evaluation

Enable systemic balanced risk decisions

- In SABSA, Risk Evaluation is performed holistically throughout the domains within the Risk Context:
  - The balance of damage and benefit to all of the inter-dependent Attributes
  - The Domain's internal context
  - The Domain's external context (Superdomain and Peer Domains)
- Extends the concept of cost benefit beyond finance to what matters most to all relevant stakeholders
- Enables systemic understanding



Attributes & Domains as an Holistic Evaluation Structure

Enterprise

Adaptable | Compliant | Community Focused | Customer Satisfaction | Global | Innovative

Profitable | Responsible | Risk Managed | Sustainable | Trusted | Visionary

People Capability

Entity	Customer
Accountable	Accessible
Competent	Accurate
Confident	Culture Sensitive
Diversity	Loyal
Empowered	Private
Equality	Simple
Ethical	Smooth

Process

Agile	Automated
Brand Enhancing	Efficient
Governed	Productive
Quality	Repeatable
Timely	

Technology

Architecturally Open	Assured
Available	Extendible
Integrated	Migratable
Protected	Reliable
Scalable	Shareable
Supportable	Total-Cost-of-Ownership
Trustworthy	Time-to-Market

Identity Program

Access Controlled | Authorised | Credentialed | Identified | Robust | Unique

Authenticated | Compliant | Enrolled | Registered | Unified

Evaluation of Negative Impact In-Context

Enterprise

Adaptable | Compliant | Community Focused | Customer Satisfaction | Global | Innovative

Profitable | Responsible | Risk Managed | Sustainable | Trusted | Visionary

People Capability

Entity
- Accountable
- Competent
- Confident
- Diversity
- Empowered
- Equality
- Ethical

Customer
- Accessible
- Accurate
- Culture Sensitive
- Loyal
- Private
- Simple
- Smooth

Process

- Agile
- Automated
- Brand Enhancing
- Efficient
- Governed
- Productive
- Quality
- Repeatable
- Timely

Technology

- Architecturally Open
- Assured
- Available
- Extendible
- Integrated
- Migratable
- Protected
- Reliable
- Scalable
- Shareable
- Supportable
- Total-Cost-of-Ownership
- Trustworthy
- Time-to-Market

Identity Program

Access Controlled | Authorised | Credentialed | Identified | Robust | Unique

Authenticated | Compliant | Enrolled | Registered | Unified

Evaluation of Enablement In-Context

Enterprise

Adaptable | Compliant | Community Focused | Customer Satisfaction | Global | Innovative

Profitable | Responsible | Risk Managed | Sustainable | Trusted | Visionary

People Capability

Entity

- Accountable
- Competent
- Confident
- Diversity
- Empowered
- Equality
- Ethical

Customer

- Accessible
- Accurate
- Culture Sensitive
- Loyal
- Private
- Simple
- Smooth

Process

- Agile
- Automated
- Brand Enhancing
- Efficient
- Governed
- Productive
- Quality
- Repeatable
- Timely

Technology

- Architecturally Open
- Assured
- Available
- Extendible
- Integrated
- Migratable
- Protected
- Reliable
- Scalable
- Shareable
- Supportable
- Total-Cost-of-Ownership
- Trustworthy
- Time-to-Market

Identity Program

Access Controlled | Authorised | Credentialed | Identified | Robust | Unique

Authenticated | Compliant | Enrolled | Registered | Unified

The Extent & Degree of Systemic Interactions

Interactions must be clear, credible and ideally measureable

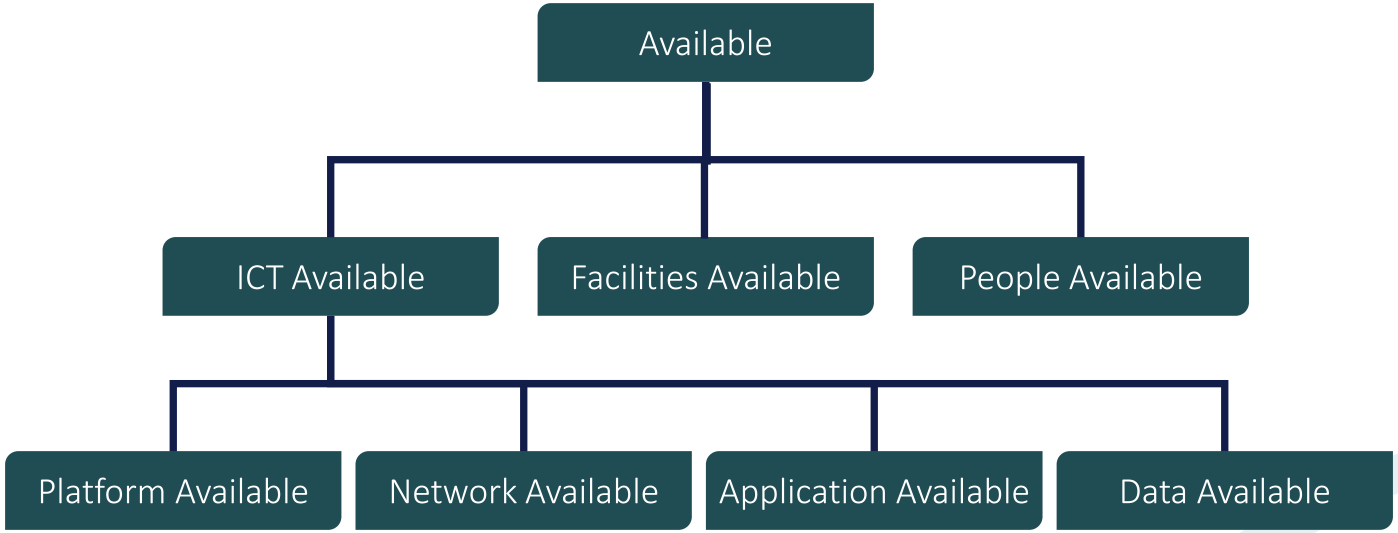
SABSA structures enable us to make a credible assertion that risks to Attributes are inter-connected....but how can the degree of the interaction be measured and evaluated in an aggregated and systemic setting?

- Lies, damned lies, statistics & performance metrics
- Tendency for subdomain to report in the language of the subdomain
  - "I have stopped 5000 viruses!"
- Report in the language of, and to the target of, the Superdomain

Risk Evaluation – Aggregation Complexity Challenge

Status at the enterprise domain is a computation of the subdomains

- Complex mathematics
- Complex politics
- When does the risk to an aggregated Attribute cross the appetite threshold?
  - When any one of its sub-domains is higher than the threshold?
  - When all of its sub-domains are higher than the threshold?
  - When the average rating of the sub-domains is higher than the threshold?
  - Is any sub-domain weighted higher than the others?



If the 4 SubDomain Attributes operate at 99.999% available, does the SuperDomain Attribute operate at 99.999% available?

Domain Dependency & Systemic Risk Balance

Financial Impact

20

10

10

Reputational Impact

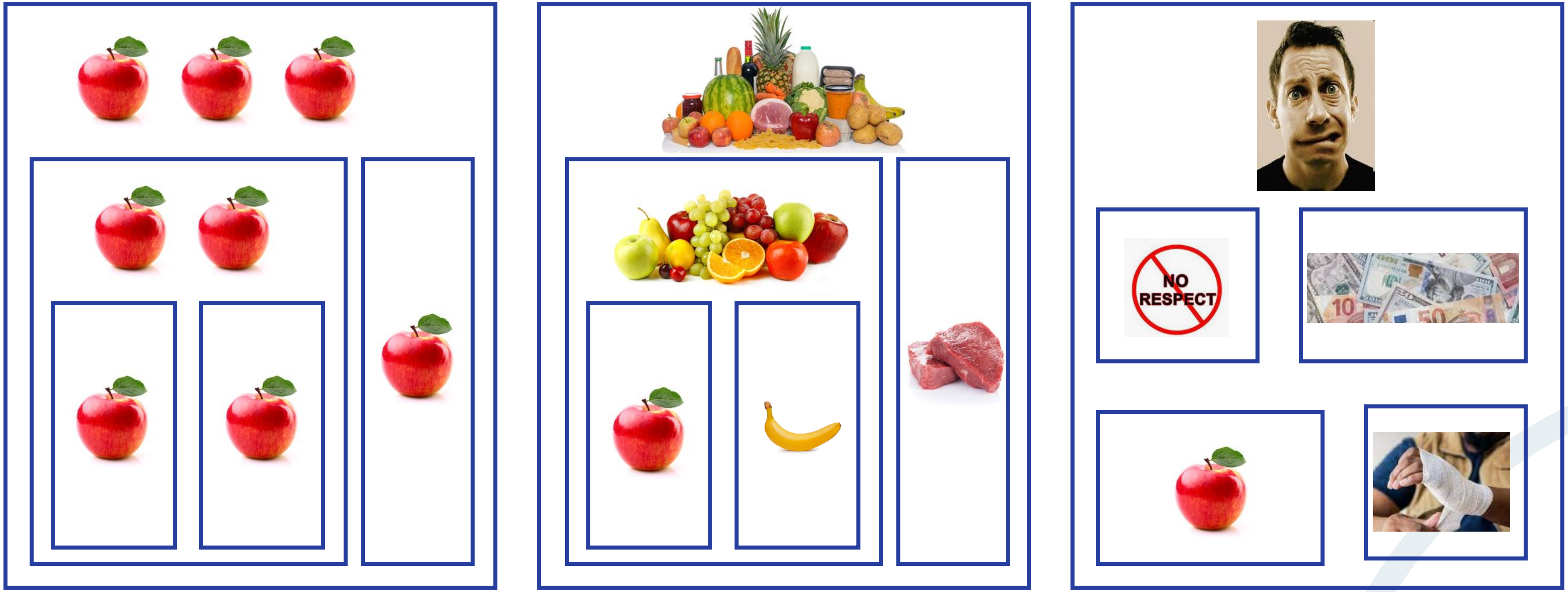
Severe

Severe

Negligible

Health & Safety Impact

Risk Evaluation – Aggregation Articulation Challenge



Total Cost Approach to Risk Evaluation

Cost of action plus cost of inaction

Risk Cost-Benefit Analysis

- To determine if a decision to invest in risk treatment is sound, ascertaining if – and by how much – its benefits outweigh its costs
- To provide a basis for comparing risk treatment investments or decisions, comparing the total expected cost of each option with its total expected benefits

SABSA's normalised language provides the capability to extend the concept of cost benefit beyond finance to what matters most to all relevant stakeholders

Risk Ratings Aggregation Challenges

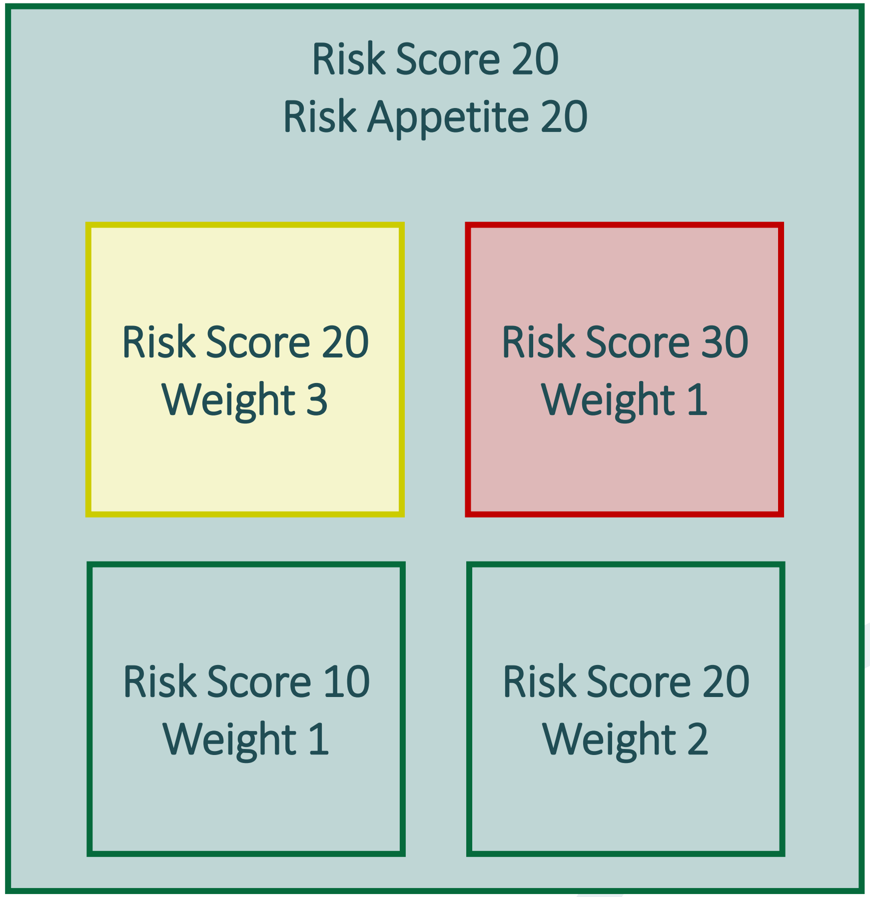
The 'averaging out' issue

- A common approach is that the risk rating in the higher domain is

$$\frac{\text{Sum (sub-domain risk scores * weights)}}{\text{Sum (sub-domain weights)}}$$

$$\frac{(20*3=60)+(30*1=30)+(10*1=10)+(20*2=40)=140}{(3+1+1+2)=7}$$

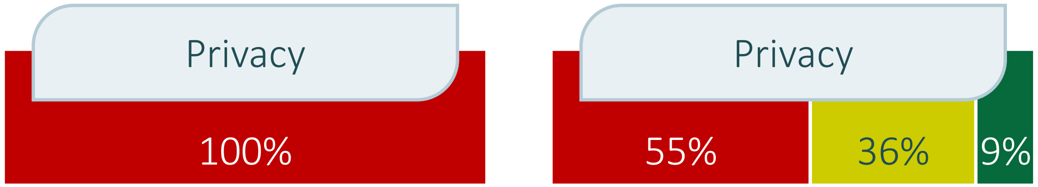
- Issue: the resulting score of 20 is within appetite even though one sub-domain is beyond appetite (it has a score of 30)



Risk Ratings Aggregation Challenges

‘Risk high’ approach to solving ‘averaging out’ issue

- One approach to solving this issue is to ‘carry forward’ the indicators in a way that communicates highest exposure and overall status e.g. “scarfing”
- But in practice this incurs the possibility that a large proportion of “single highest indicators” are red due to the reality of business operations



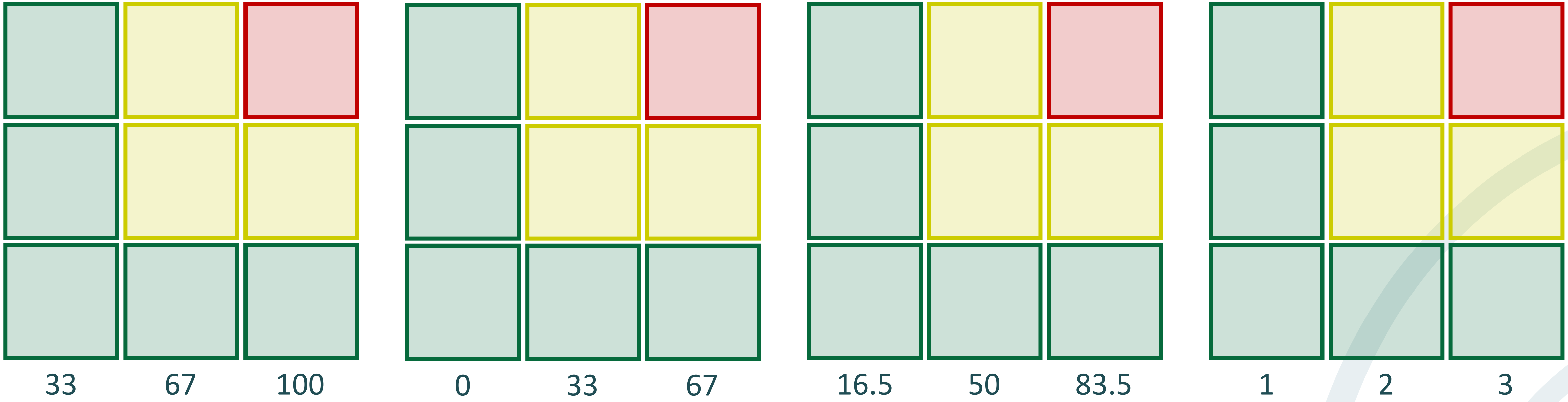
Single Highest Indicator **Proportional Indicator**

Risk Ratings Aggregation Challenges

Distortion from qualification / banding of quantified scores

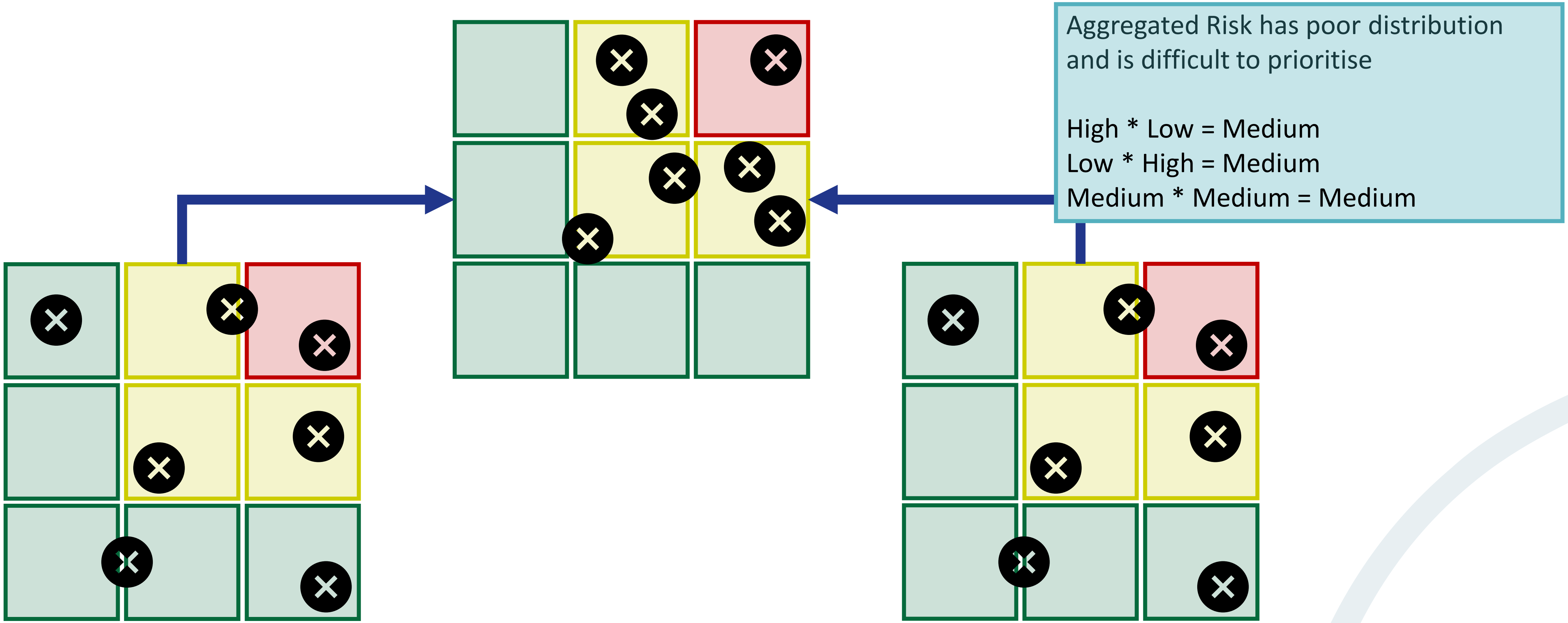
- 2 points - binary (yes/no): 0%, 100%
- 3 points (H / M / L): 0%, 50%, 100%
- 4 points: 0%, 33%, 67%, 100%
- 5 points: 0%, 25%, 50%, 75%, 100%
- …etc

- Average
- Weighted Average
- Low threshold
- High threshold
- …etc



Risk Ratings Aggregation Challenges

Choice of scale affects risk distribution and prioritisation

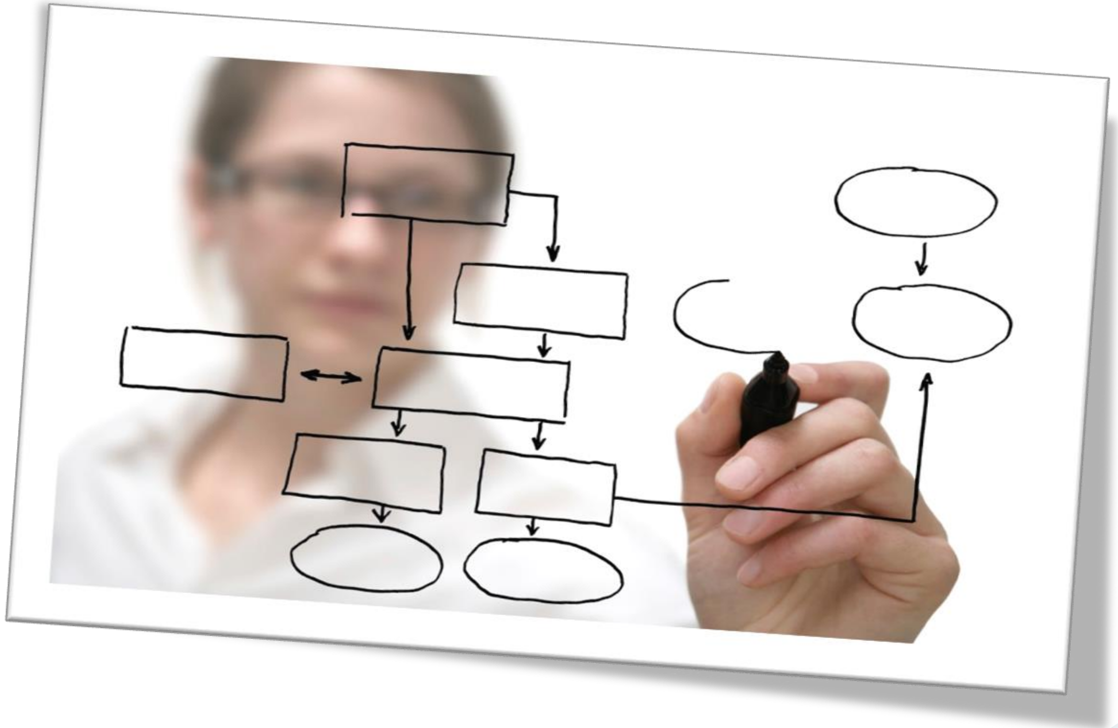


Distributed Risk – Easy to Prioritise

Distributed Risk – Easy to Prioritise

Workshop A1-7

Evaluate Risk



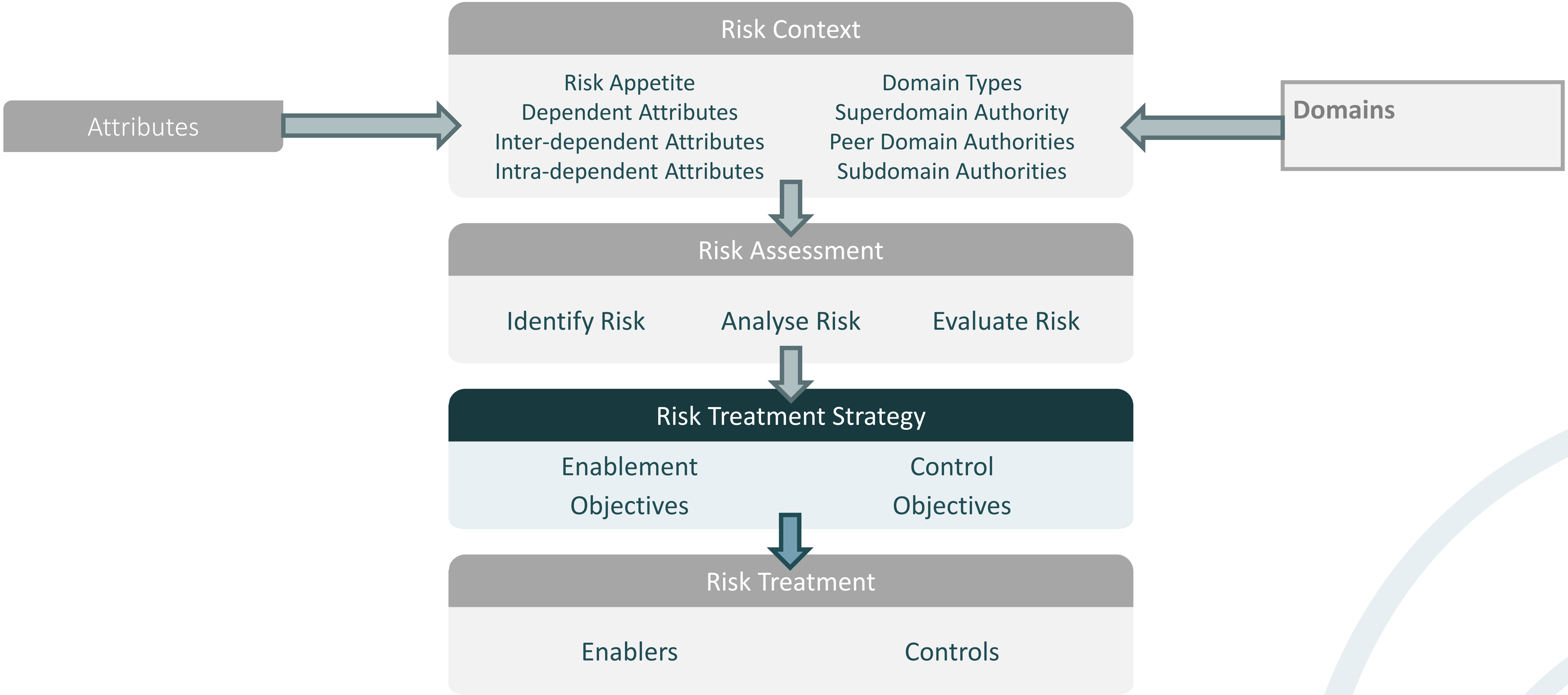
A1 – Unit 4

Risk Treatment

Risk Treatment Strategy

Section 10

Scope


Risk Context
Risk Appetite
Dependent Attributes
Inter-dependent Attributes
Intra-dependent Attributes
Domain Types
Superdomain Authority
Peer Domain Authorities
Subdomain Authorities
Attributes
Domains
Risk Assessment
Identify Risk
Analyse Risk
Evaluate Risk
Risk Treatment Strategy
Enablement
Objectives
Control
Objectives
Risk Treatment
Enablers
Controls

Holistic Enterprise Risk Strategy in SABSA

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Dependence
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & trust Frameworks	Domain Framework	Time Framework
Logical	Information	Policy	Information Processing & Services	Trust Model		
Physical	Data	Practices & Procedures	Data Comms & Mechanisms	Data & System Governance		
Component	Products & Tools	Risk Standards	Protocol Standards	I&AM Standard		
Management	Delivery & Continuity	Risk Management	Process Management	Governance Management		

- Risk management objectives are driven explicitly by risk context
- Risk management objectives are driven implicitly by the context provided by other perspectives
- Risk management objectives influence, and are influenced by, peer elements

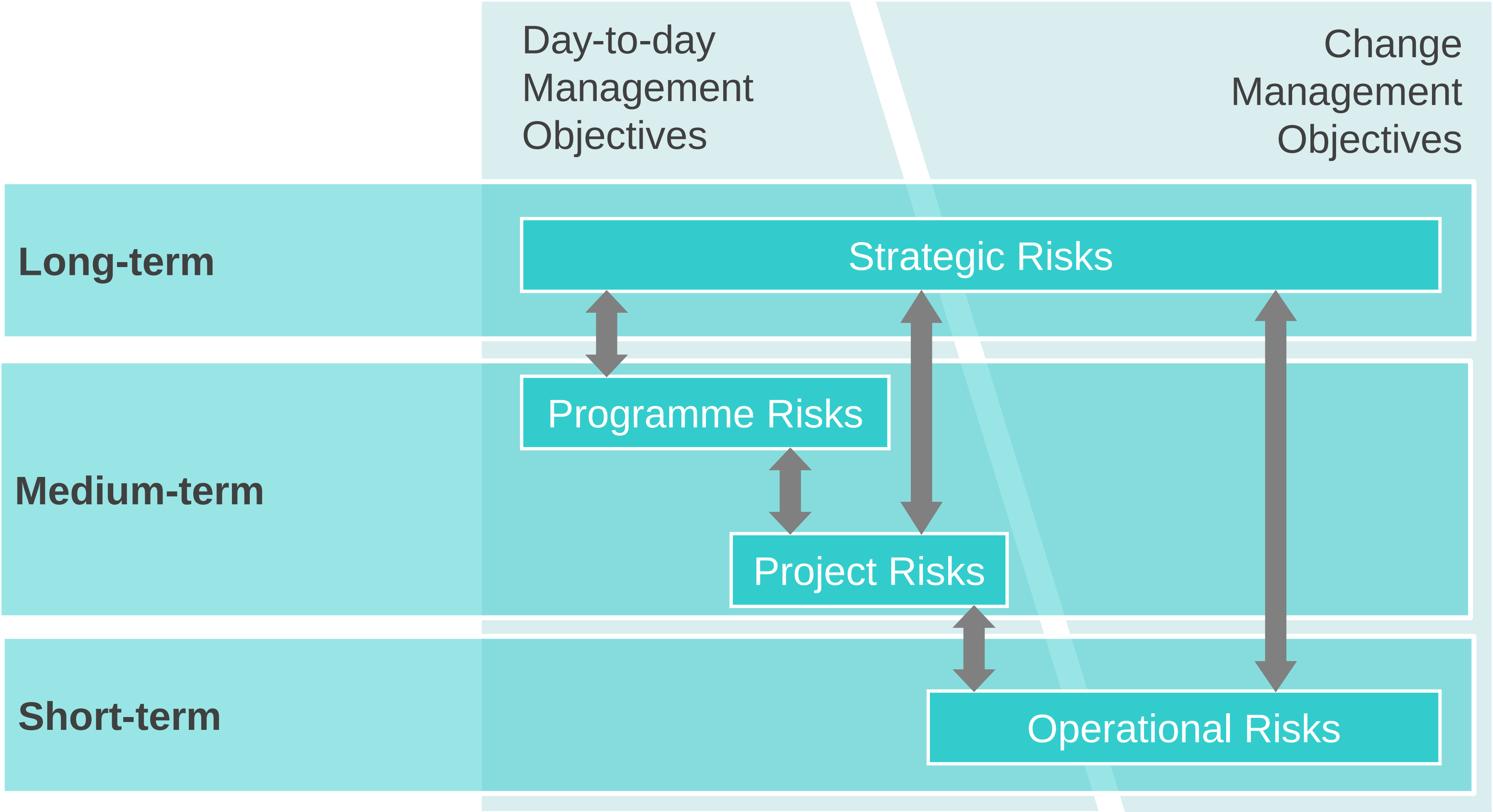
SABSA®

Risk Management Strategy

Risk Management Strategy is the process of selecting options for dealing with evaluated risk

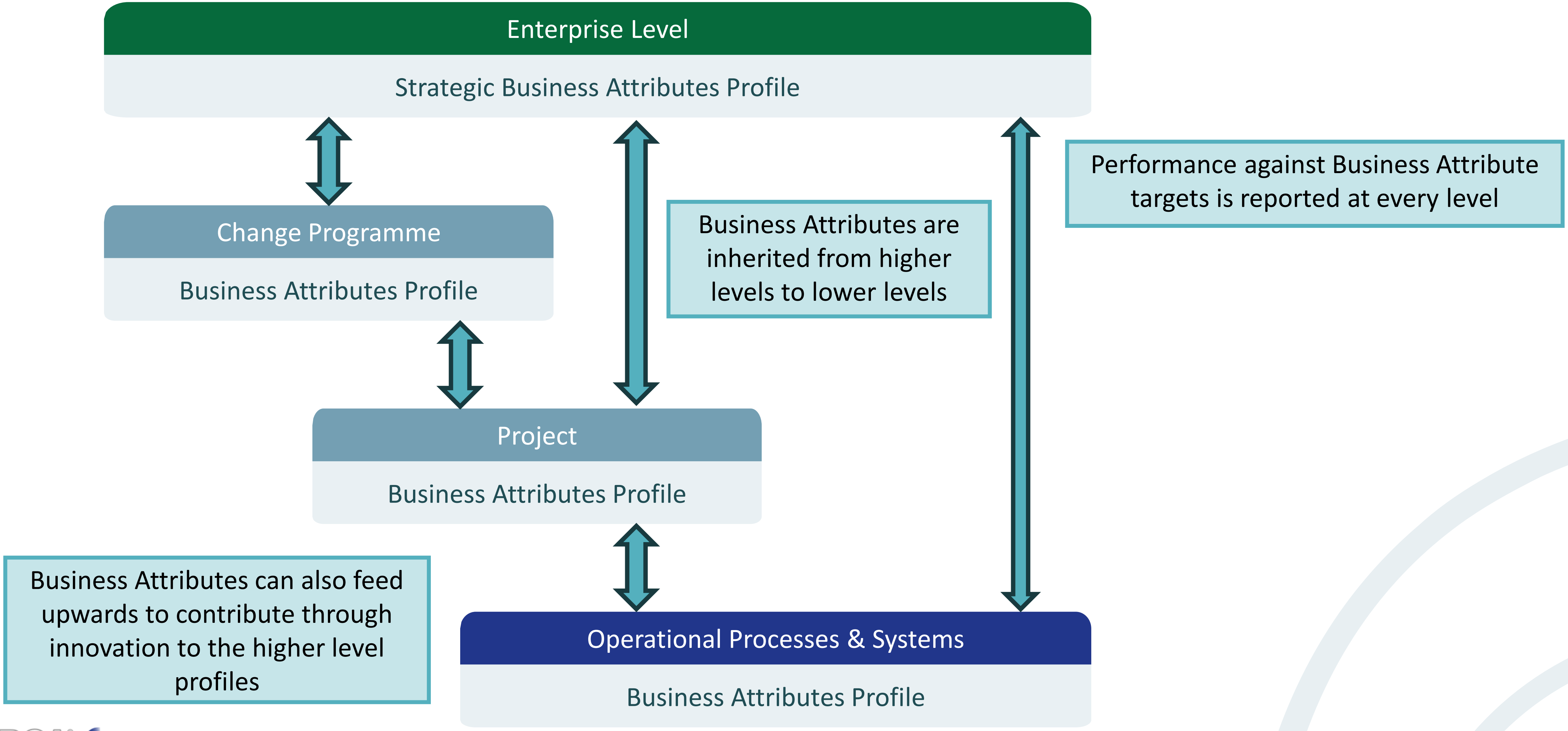
Option	Description
Avoid	Eliminate the risk by avoiding potential events (and therefore the consequences of those events Example: cancel a planned project because potential disruption outweighs the originally intended benefits or it is recognised that the opportunities identified cannot be grasped in practice
Treat	Alter the probability of a event, change the state of strength or weakness, or modify the extent of possible consequences
Transfer	Arrange / contract for another domain authority (internal or external) to assume the risk and its consequences
Retain	Accept the risk and its consequences without taking any action
Increase	Increase the probability of an event in order to pursue greater benefit

Strategic, Transformation & Change Risk



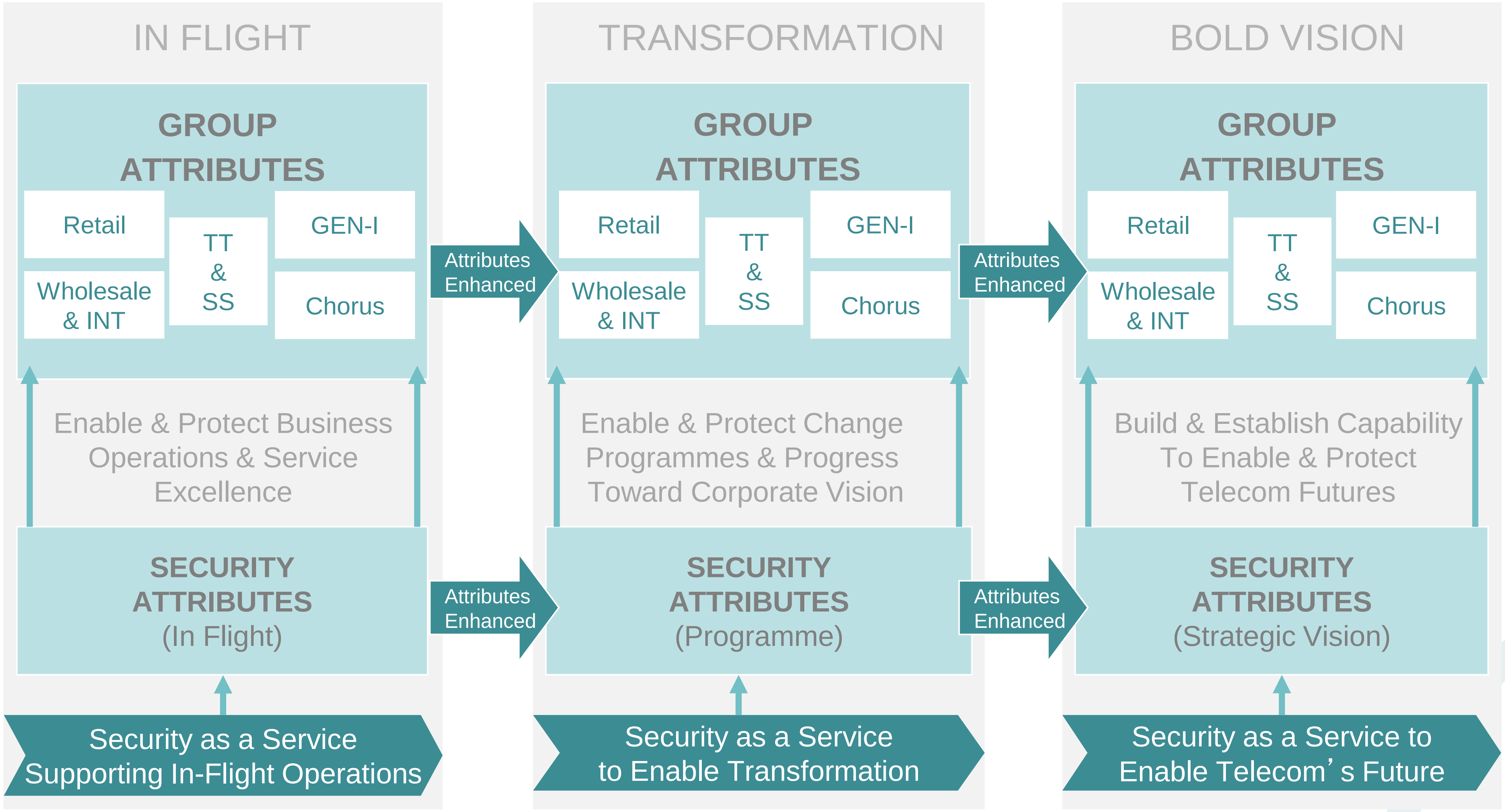
Source: OGC M_o_R 2007

Common Language for Strategic, Transformation & Change Risk



DLCBRUA1250512

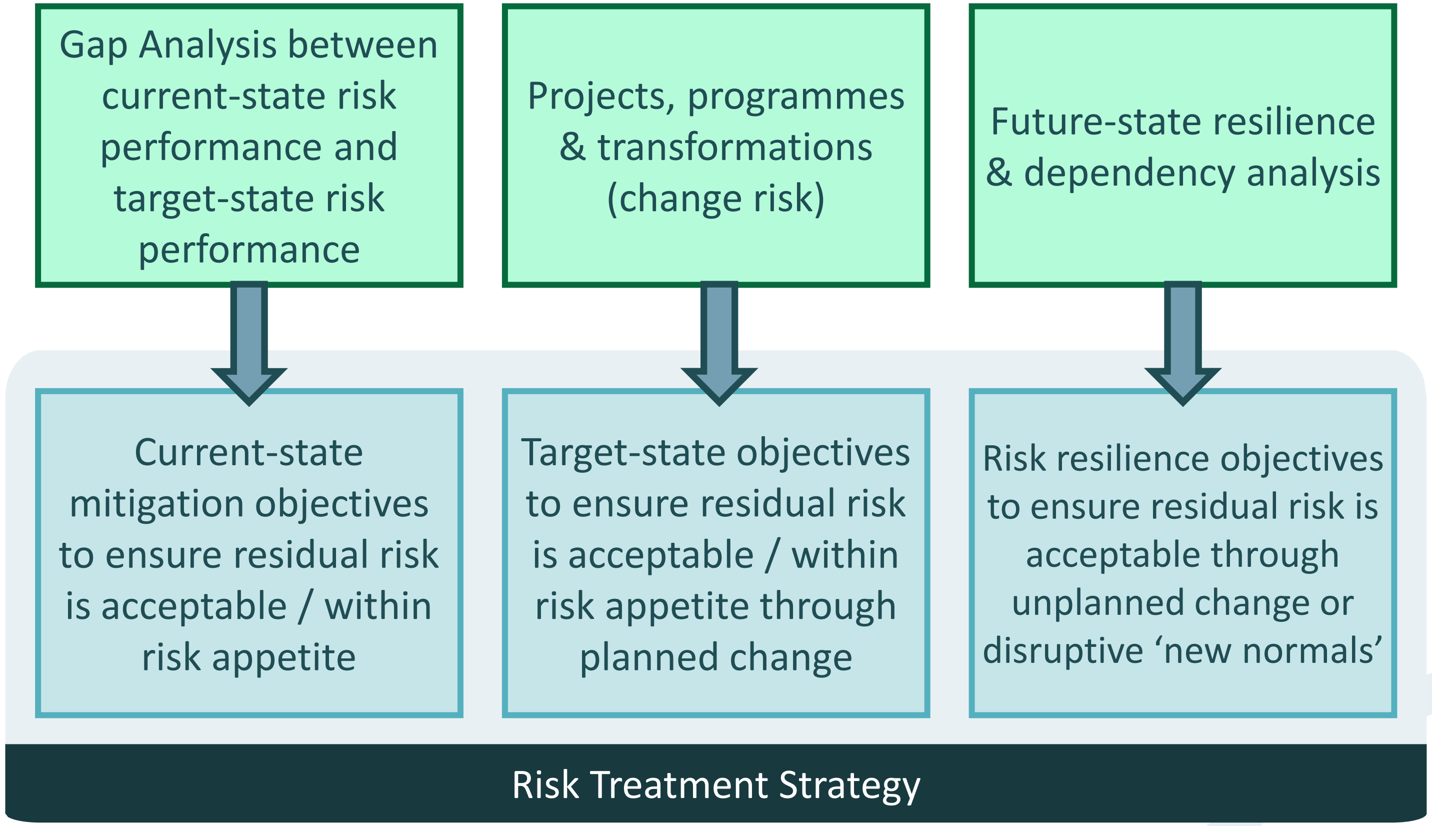
Common Language for Strategic, Transformation & Change Risk



Risk Treatment Strategy

Inherent Risk The level or risk inherent present before any treatment action. The raw state of risk. Sometimes referred to as Pure Risk

Residual Risk The level or risk remaining after treatment of inherent risk. The current risk level after the effect of current risk treatments are considered



Risk Treatment Strategy is the process of defining appropriate risk treatment objectives (enablement and control objectives) for risk evaluated as requiring treatment

Treatment Strategy From Gap Analysis

Current State

Residual Risk beyond appetite

Treatment Strategy

Objectives to bring Residual Risk within appetite

Target State

Residual Risk within appetite

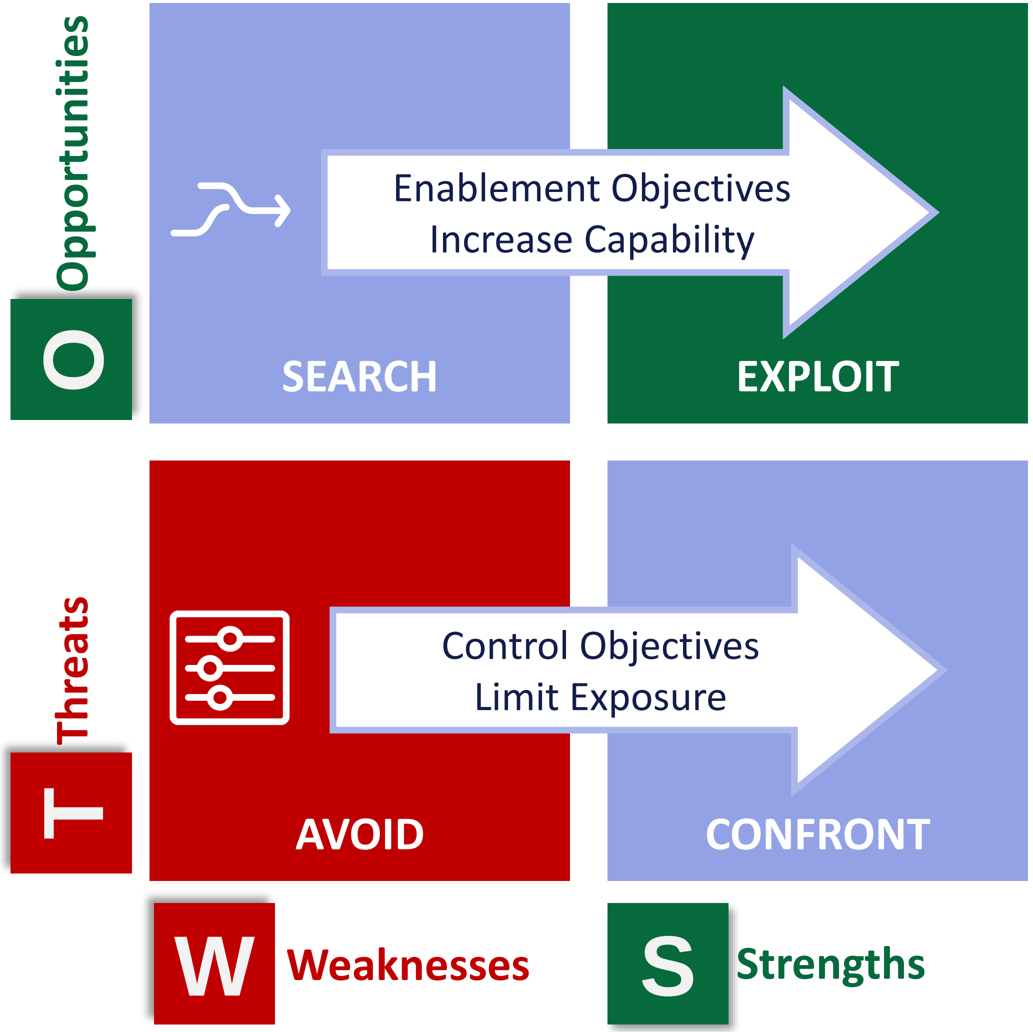
Control Objectives define the intention to limit exposure to potential damage

Enablement Objectives define the intention to increase capability to capitalise benefits

Treatment Strategy from SWOT Analysis

Define enablement objectives to increase capability

Use existing strengths to capitalise opportunities



Define control objectives to limit exposure to damage

Use existing strengths to confront threats

Treatment Strategy from SWOT Analysis

Derive objectives from SWOT analysis

- Common practice to define business and marketing strategy
- Correlate the threats & opportunities output from the external context analysis with the strengths & weaknesses from the internal context analysis

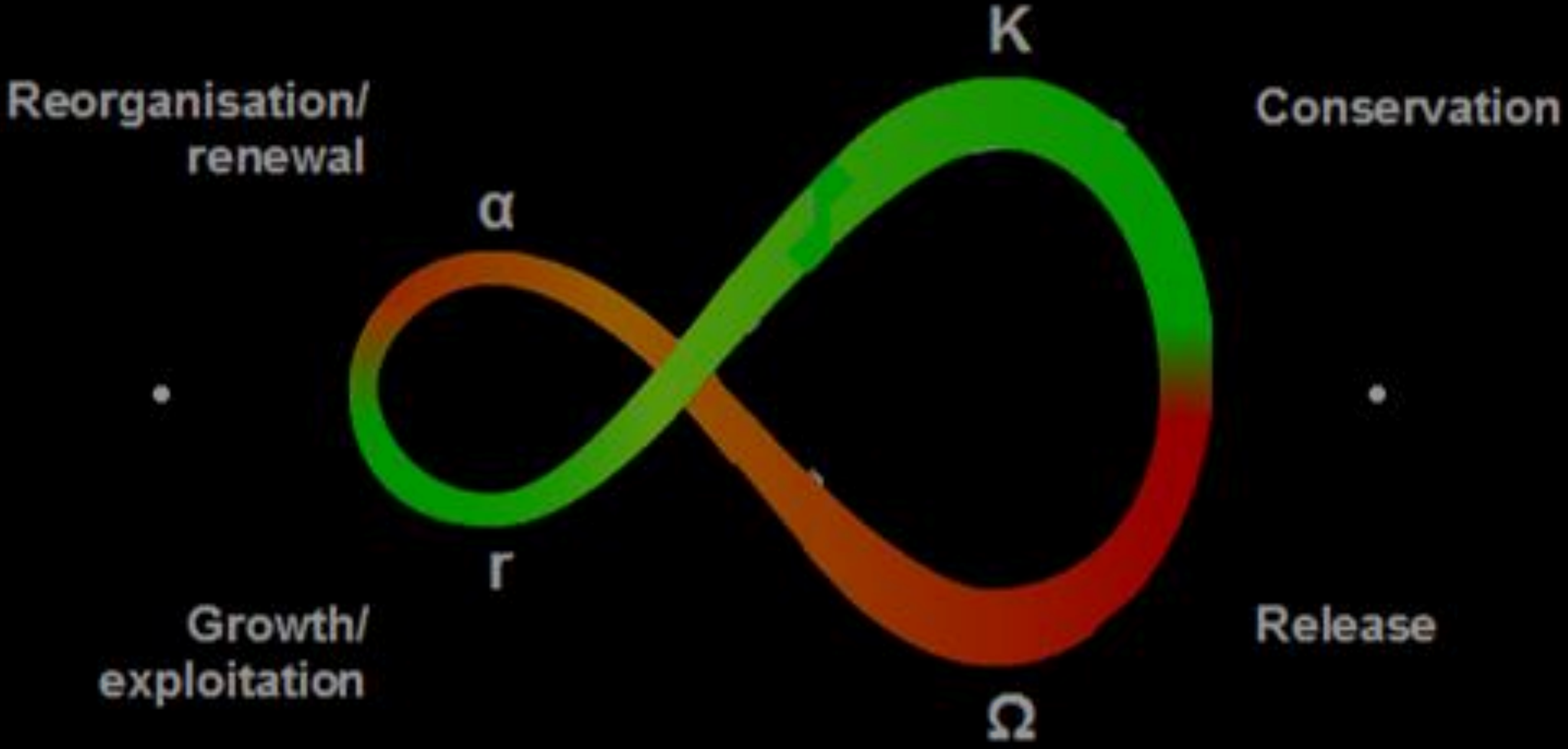
Strength	Weakness	Opportunity	Threat
Mywidgets Inc has strong reputation for quality	Our handmade widgets take long time to manufacture	Developing large-scale market for widgets in China	Large competitors have faster & automated production lines

Control objective: Protect market share from emerging competitors

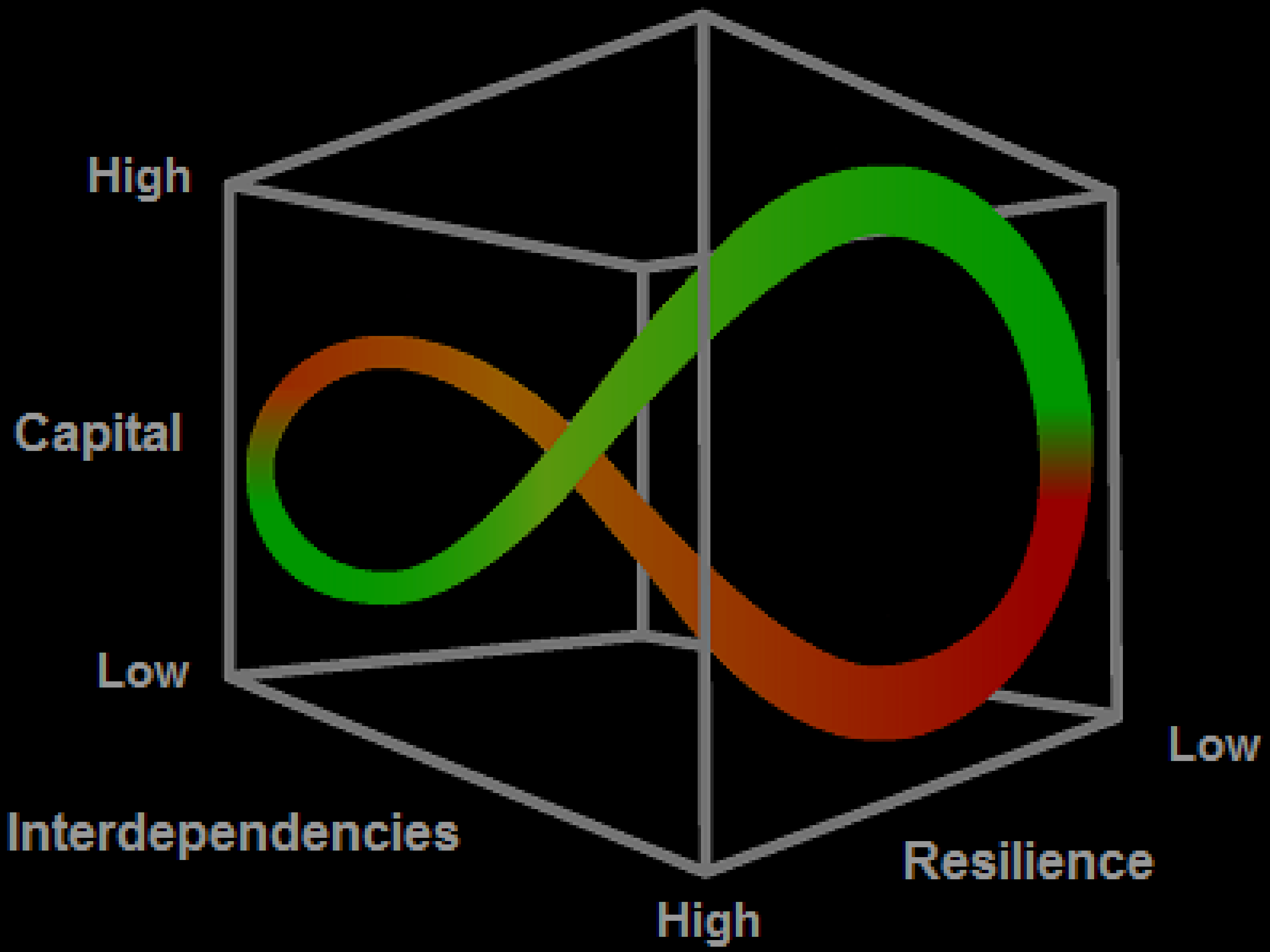
Enablement objective: Leverage automation for faster time-to-market production capability of quality widgets

Treatment Strategy from Emerging Ecosystems Lifecycle

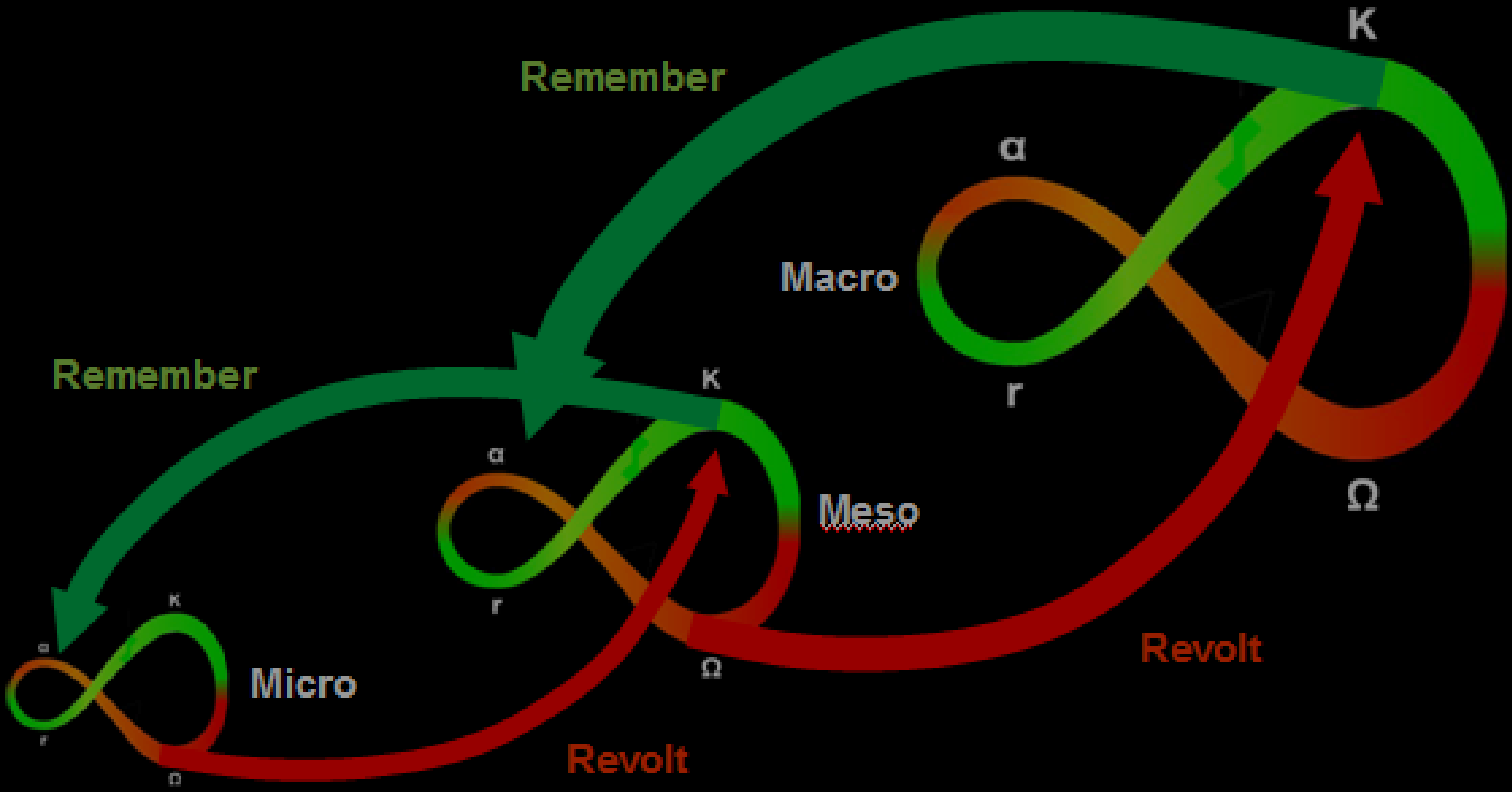
Growth, Destruction, Renewal



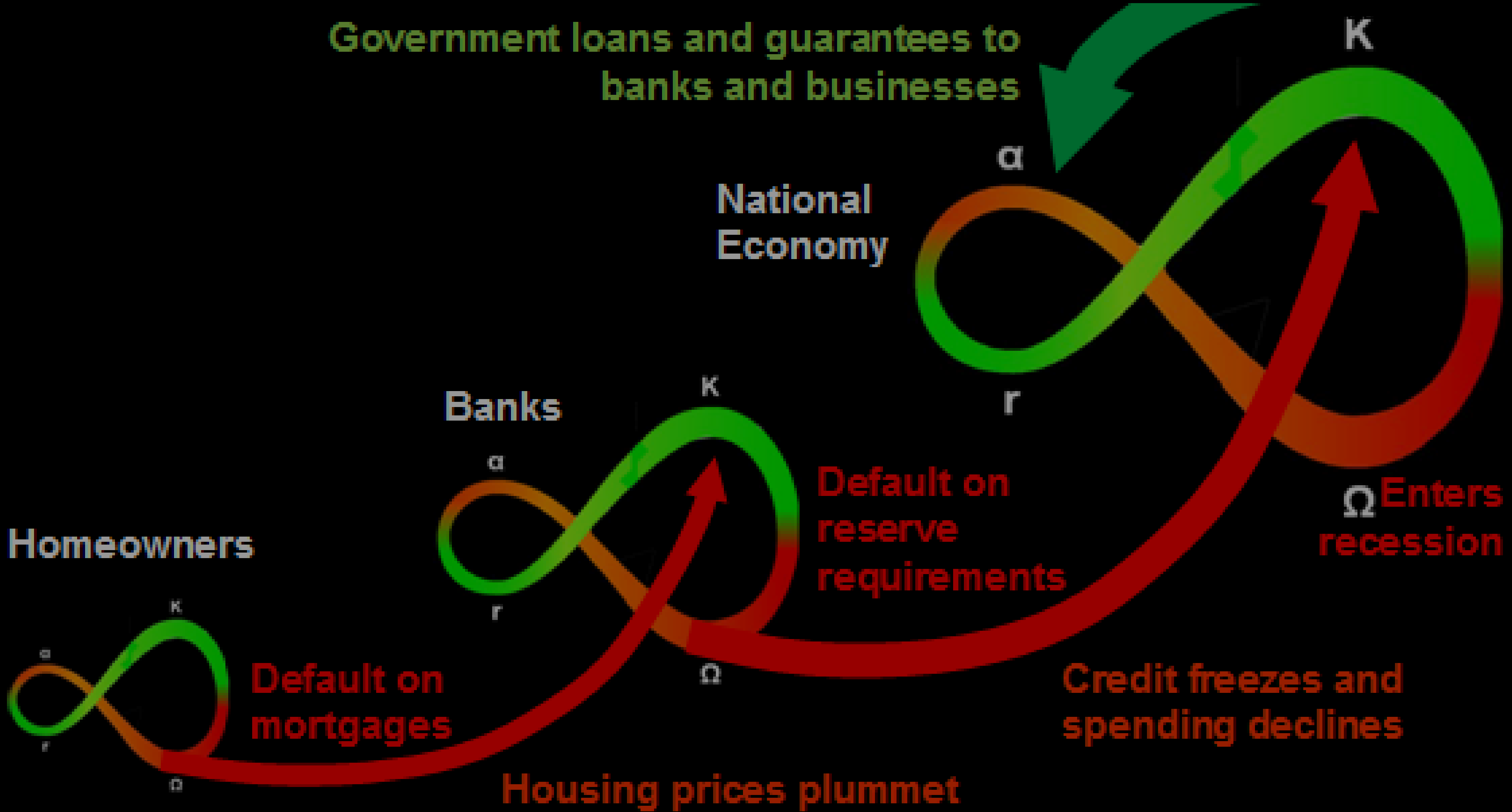
Panarchy – Adaptive Cycle of Renewal



Resilience & Interdependency

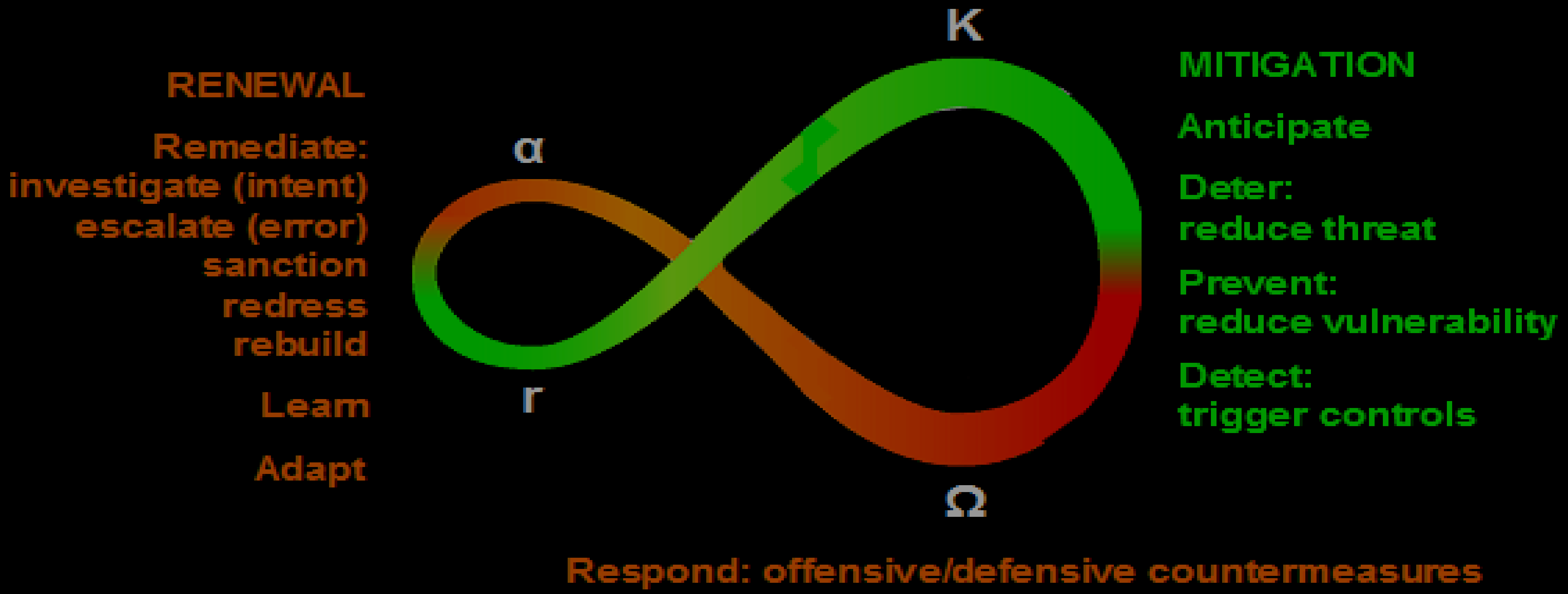


Panarchy – Networked Interactive Cycles



Financial Crisis Example

Implications of Complex System / Network Science



SABSA Lifecycle Strategy | SABSA Domain Hierarchy | SABSA MTCS

Renewal Resilience & SABSA

Treatment Priorities from Current-state Risk Level Heatmap

Likelihood	Significant Damage	Damage	Marginal Damage	Marginal Benefit	Benefit	Significant Benefit
High	Very High -	High -	Medium -	Medium +	High +	Very High +
Medium	Very High -	High -	Medium -	Medium +	High +	Very High +
Low	High -	Medium -	Low -	Low +	Medium +	High +

Consequences

SABSA®

The Architecture Roadmap: Strategy Time & Sequence

Vision

The Vision is about the future. It is the essence of ***what*** we need to achieve. It is embodied by Contextual Architecture.

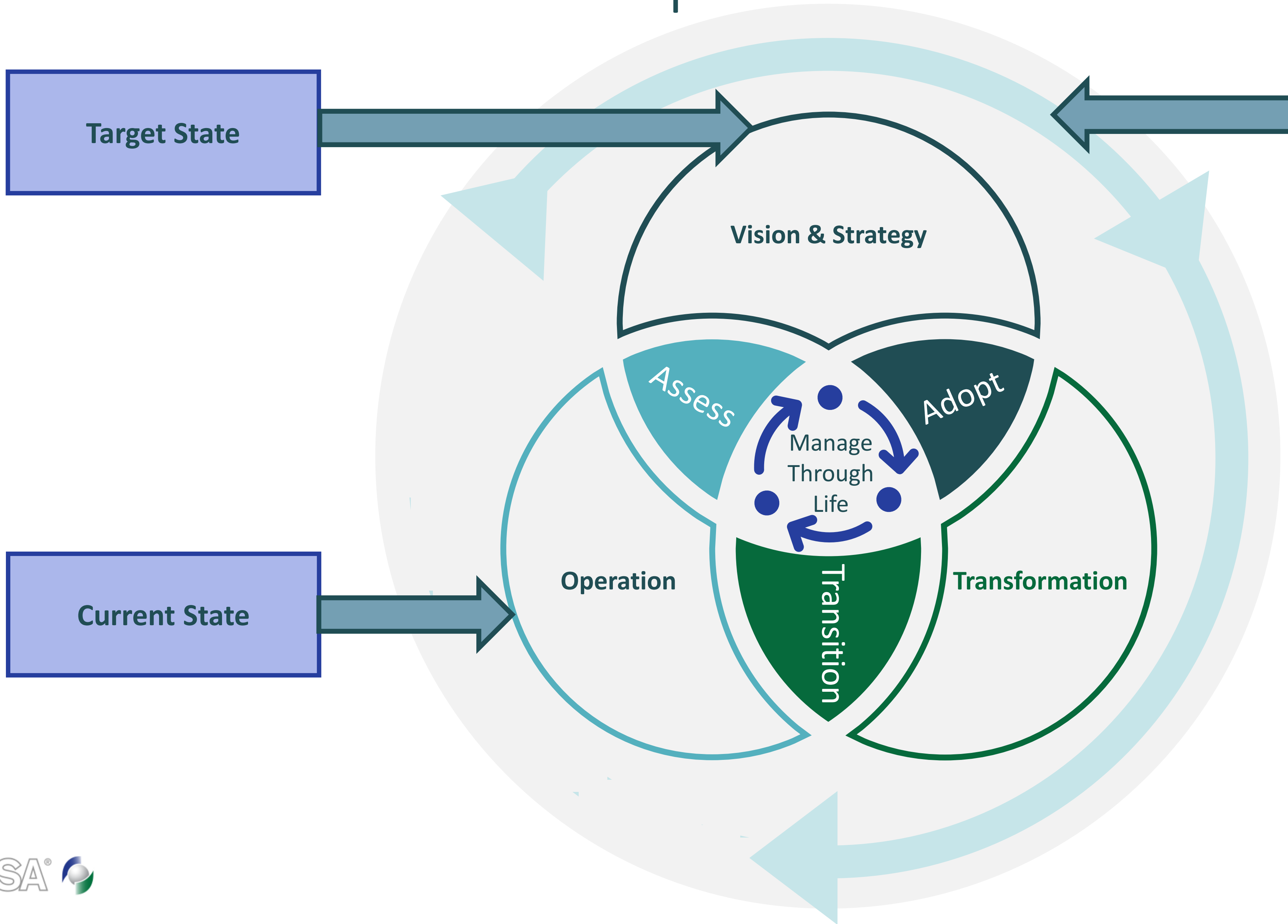
Strategy

The Strategy is ***how*** to turn the vision into reality: how do we get to where we want to be and what must be done to get us there. It sets direction and defines initiatives required to be successful. It is embodied by Conceptual Architecture.

Roadmap

The Strategic Roadmap represents the ***when*** of the strategy. It communicates strategy in terms of time parameters and sequence dependencies for each step required to achieve adoption of strategy and transformation to target-state.

The Role of the Roadmap



Roadmap
The time & sequence dependencies of realising the strategy by transforming the current-state into the target state

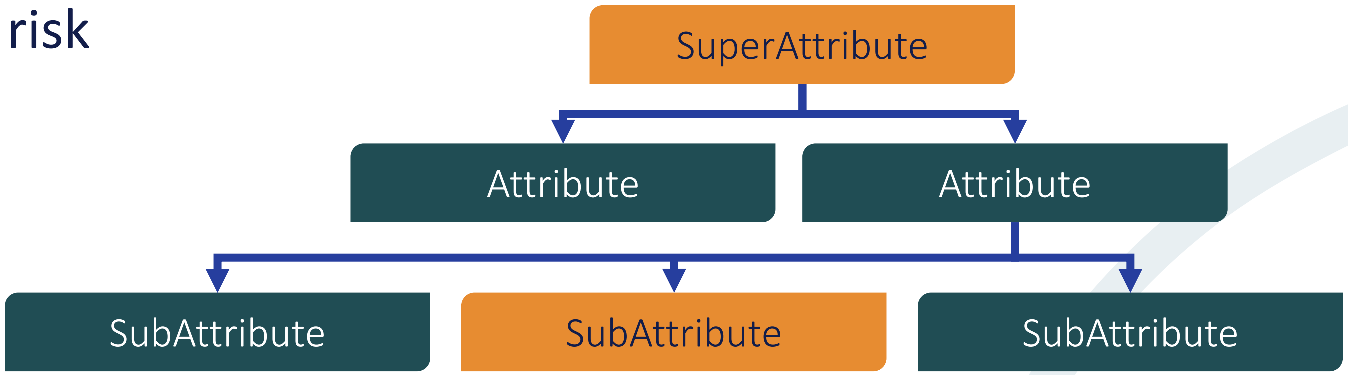
Success and Dependencies

Current-state remediation objectives

- Enterprise success factors are represented by measurable Attributes
- The Enterprise is performing to current requirements if:
  - The SuperAttribute performance target is being met
  - The SuperAttribute is operating within risk appetite
- An Attribute is dependent upon its SubAttributes to first:
  - Meet performance targets
  - Operate within risk appetite

If the SuperAttribute is not performing as required, we must identify which of its dependencies are causing it to fail

What is the best course of action to remediate the issue, increase resilience to failure, or improve performance?



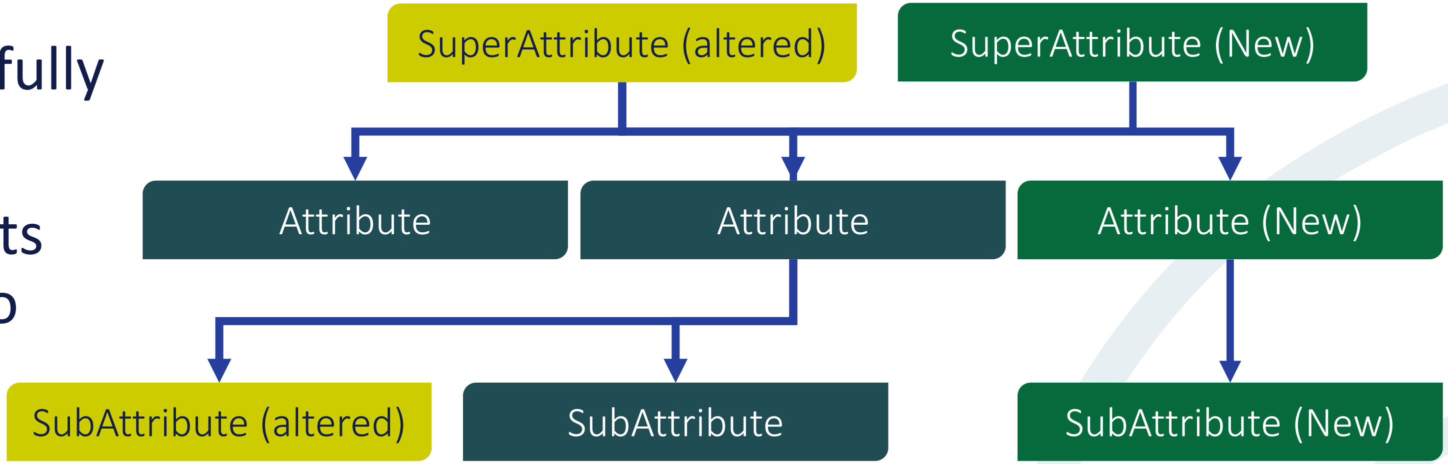
Success and Dependencies

Target-state transformation objectives

- Future Enterprise success factors are represented by measurable Attributes
- The Enterprise Strategy is realised if:
  - Existing SuperAttributes achieve new performance targets and operate within amended risk appetites
  - New SuperAttributes are successfully introduced
- The new or amended Attribute targets are dependent upon SubAttributes to first achieve their respective targets

If a new target-state requirement is defined, we must identify:

- New Attributes upon which the target-state is dependent
- Amendments to existing Attributes performance targets or risk appetite upon which the target-state is dependent
- Where is the best investment to enable us to meet new requirements and grasp new opportunities



Dependency Modelling

- The SABSA Dependency Modelling technique is adapted from original work by John Gordon
- Origins in assessing risk in Critical National Infrastructure
- A method of determining the dependency risk to an enterprise through the use of a graphical model
- Software-based Bayes/fault mode analysis enables faster and effective ‘what if’ visualisation

Keeping it Together

Dependency Modelling

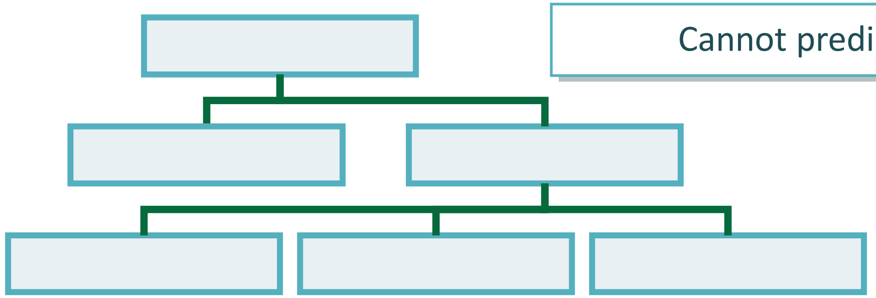
and

Risks to the Infrastructure

John Gordon

Cannot control all dependencies

Cannot predict all failures



Risk increases with lack of understanding of dependencies

Better understanding of dependencies increases resilience to failure

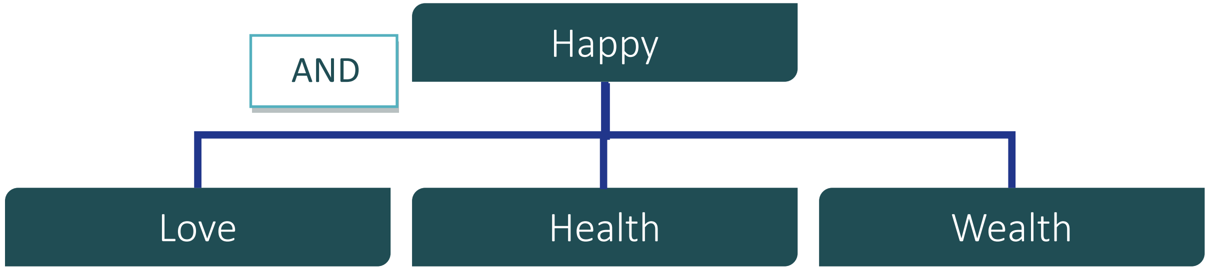
Dependency Model Elements

- Attribute with at least two possible states
  - Success state – performance targets are met / residual risk is within risk appetite
  - Fail state – performance targets are not met / residual risk exceeds risk appetite
- Dependency tree
- Dependency conditions
  - AND/OR
- Probability analysis

Warning/alert state or additional risk levels could be added but are not modelled in these examples

Success State & Dependency & Probability

Attribute Dependency Tree



Success of Attribute ***Happy*** is dependent upon:

Success of Attribute ***Love***

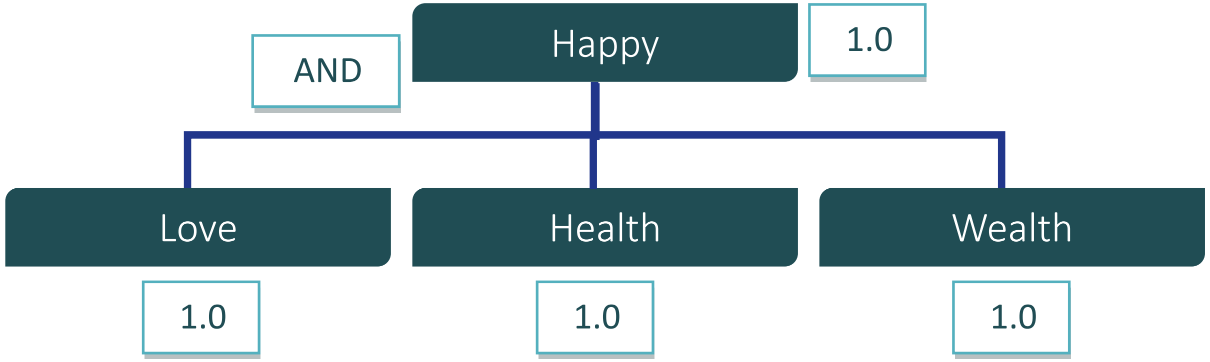
AND

Success of Attribute ***Health***

AND

Success of Attribute ***Wealth***

Attribute Dependency Tree with probability of success



If probability of ***Love*** success state is 1.0

AND

Probability of ***Health*** success state is 1.0

AND

Probability of ***Wealth*** success state is 1.0

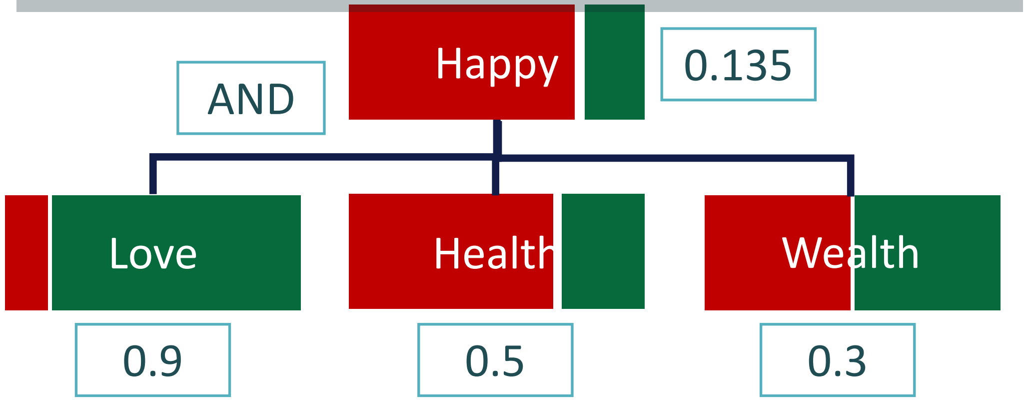
THEN

Probability of ***Happy*** success state is 1.0

Probability with Systemic 'AND' & 'OR' Dependency

Risk assessment tells us that the probabilities of dependency Attributes for ***Happy*** being in success state are:

Love 0.9 ***Health*** 0.5 ***Wealth*** 0.3



Dependency Modelling tells us the probability of ***Happy*** being in success state, given its dependence on ***Love***, AND ***Health***, AND ***Wealth***

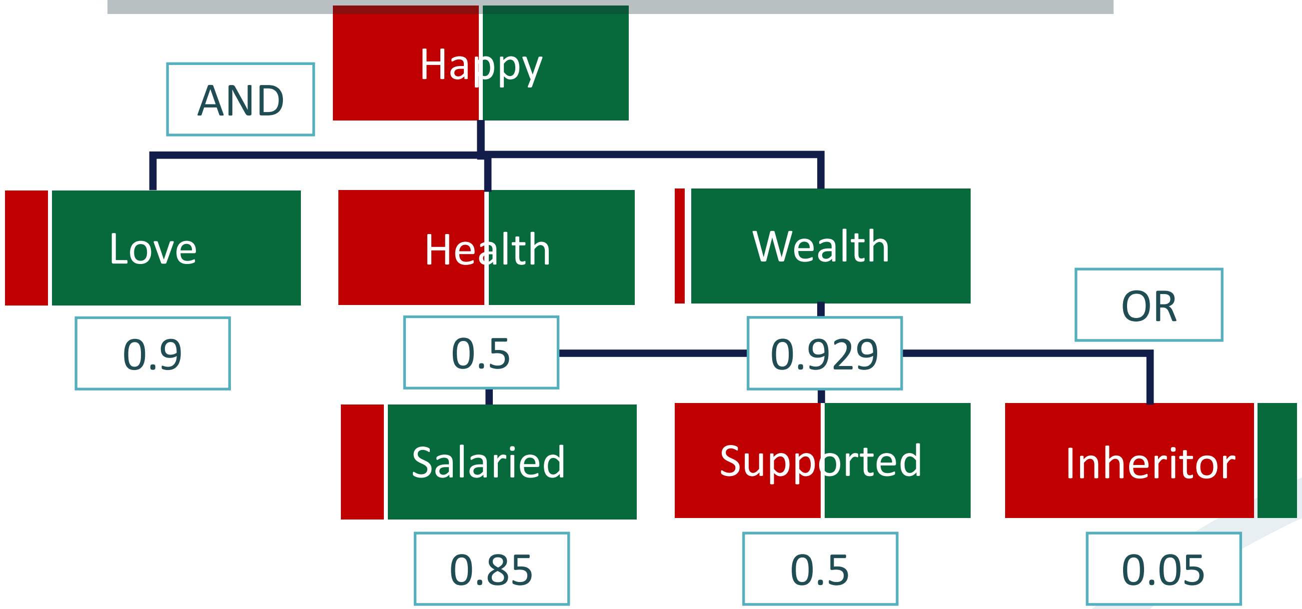
The probability aggregation is

(***Love*** 0.9)*(***Health*** 0.5)*(***Wealth*** 0.3) = ***Happy.***

The probability of ***Happy*** success state = 0.135

Risk assessment tells us that the probabilities of dependency Attributes for ***Wealth*** being in success state are:

Salaried 0.85 ***Supported*** 0.50 ***Inheritor*** 0.05



Dependency Modelling tells us the probability of ***Wealth*** being in success state, given its dependence on ***Salaried***, OR ***Supported***, OR ***Inheritor*** is 0.929

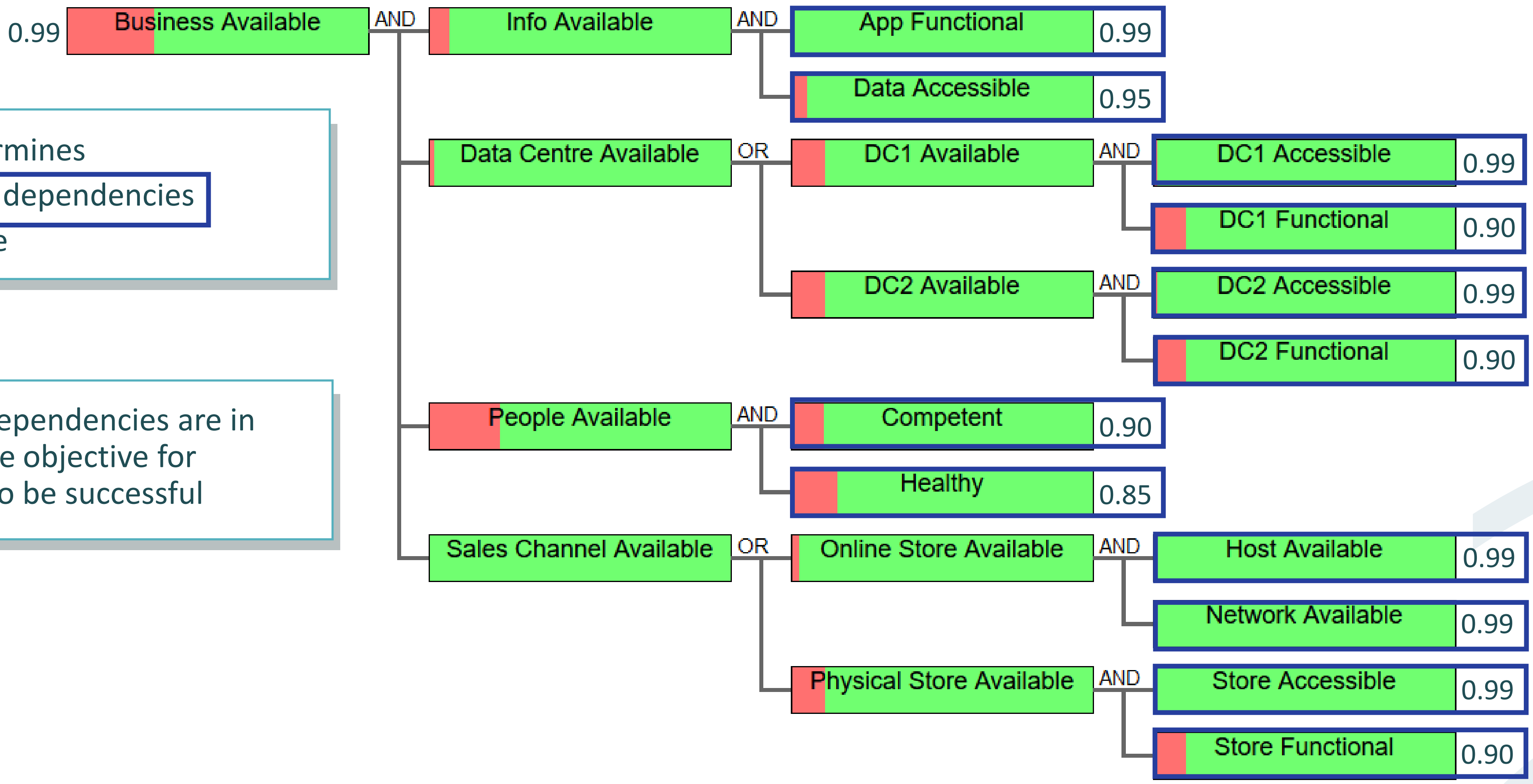
Wealth = 1-(1-0.85)*(1-0.5)*(1-0.05)

This has a systemic effect on the probability of ***Happy*** success which is now: 0.418

Current-state Dependency Model

Risk Assessment determines probability of the end dependencies being in ‘success’ state

The risks to the end dependencies are in context of the ultimate objective for “Business Available” to be successful



SABSA®

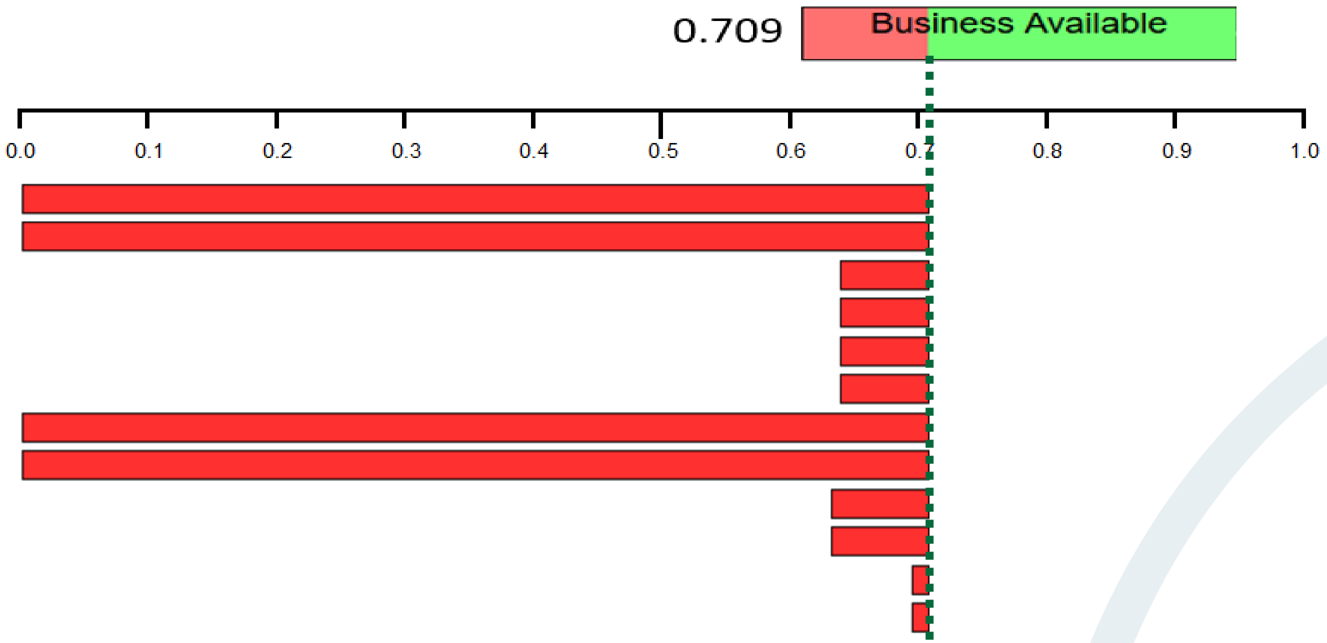
Current-state Dependency Failure Analysis

Which dependency failures have the greatest impact?

- 'What if' a single end-dependency were to fail?
- Does the probability of the SuperAttribute success decrease and, if so, to what extent?
- How sensitive is the SuperAttribute to the failure of its end-dependencies?

Current-state Probability of success

	Business Available probability of success if dependency fails	Business Available change in probability if dependency fails
App Functional	0.000	0.709
Data Accessible	0.000	0.709
DC1 Accessible	0.640	0.069
DC1 Functional	0.640	0.069
DC2 Accessible	0.640	0.069
DC2 Functional	0.640	0.069
Competent	0.000	0.709
Healthy	0.000	0.709
Host Available	0.633	0.076
Network Available	0.633	0.076
Store Accessible	0.697	0.012
Store Functional	0.697	0.012

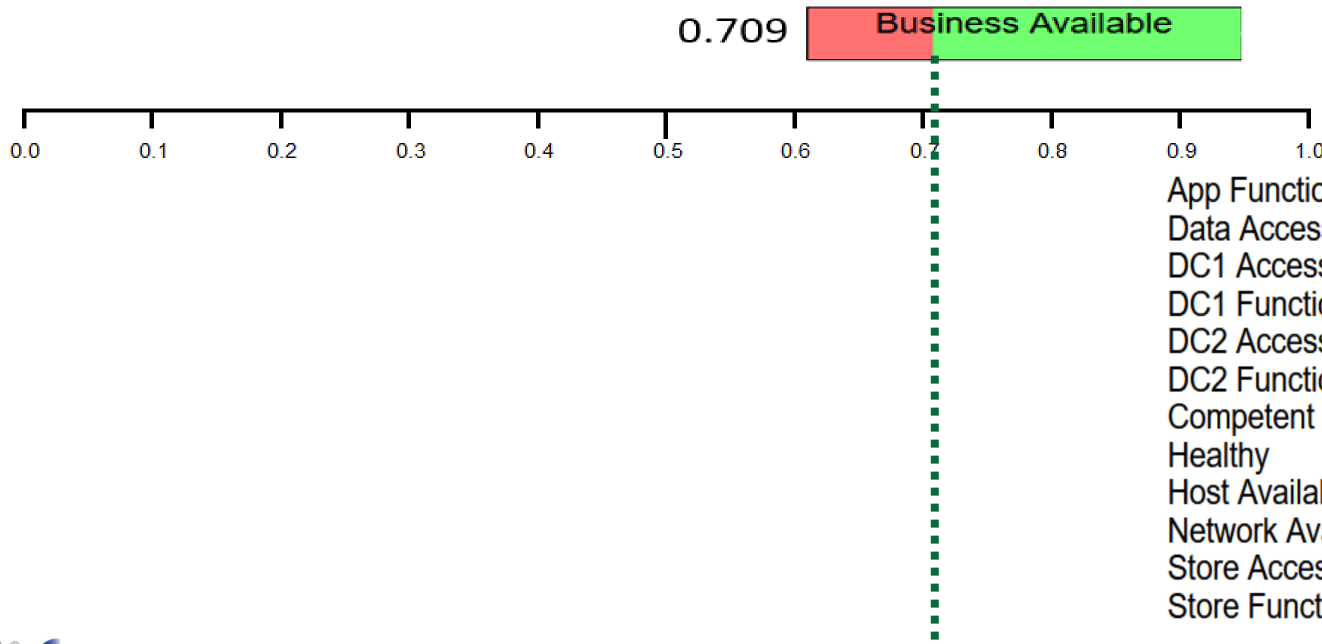


Current-state Dependency Success Analysis

Which dependency successes have the greatest benefit?

- ‘What if’ a single end-dependency were guaranteed to succeed (probability = 1)?
- Does the probability of the SuperAttribute success increase and, if so, to what extent?
- How sensitive is the SuperAttribute to the success of its end-dependencies?

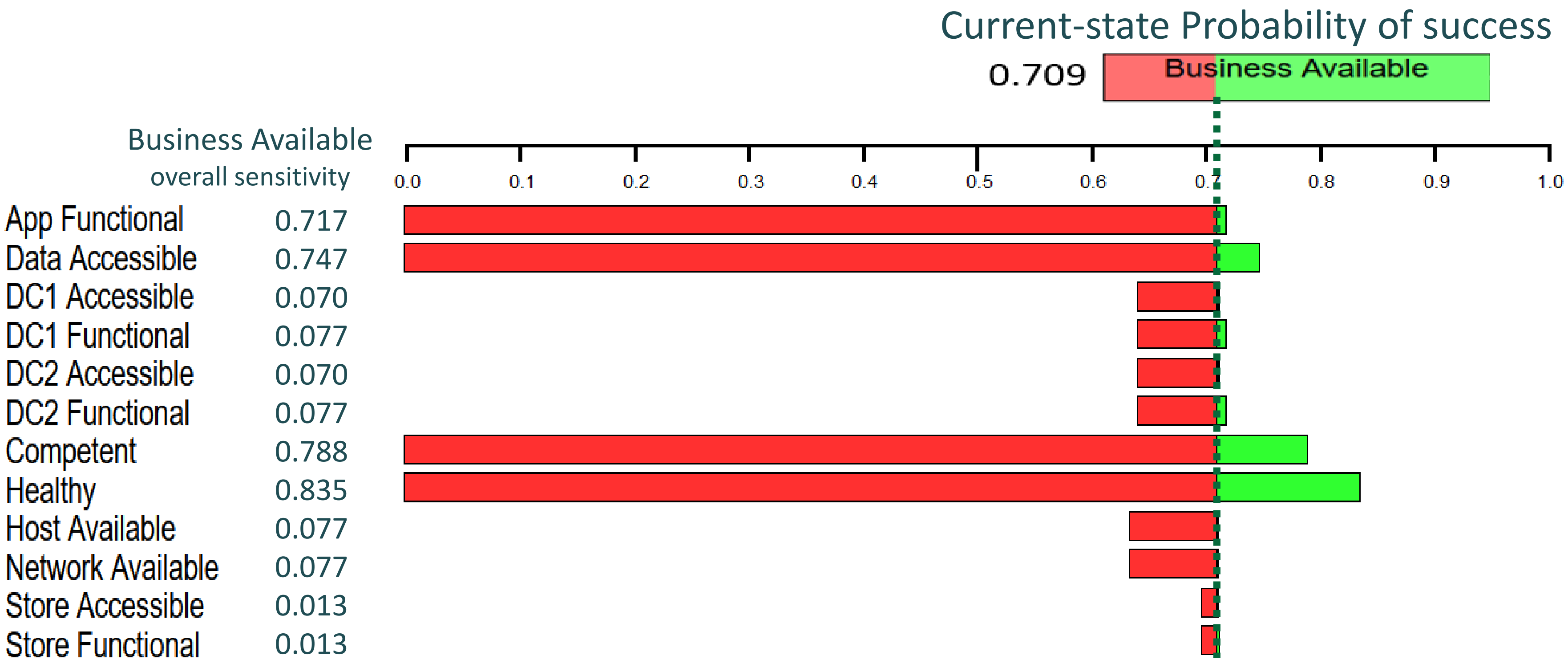
Current-state Probability of success



	Business Available probability of success if dependency succeeds	Business Available change in probability if dependency succeeds
App Functional	**0.717**	**0.008**
Data Accessible	**0.747**	**0.038**
DC1 Accessible	**0.710**	**0.001**
DC1 Functional	**0.717**	**0.008**
DC2 Accessible	**0.710**	**0.001**
DC2 Functional	**0.717**	**0.008**
Competent	**0.788**	**0.079**
Healthy	**0.835**	**0.126**
Host Available	**0.710**	**0.001**
Network Available	**0.710**	**0.001**
Store Accessible	**0.710**	**0.001**
Store Functional	**0.711**	**0.002**

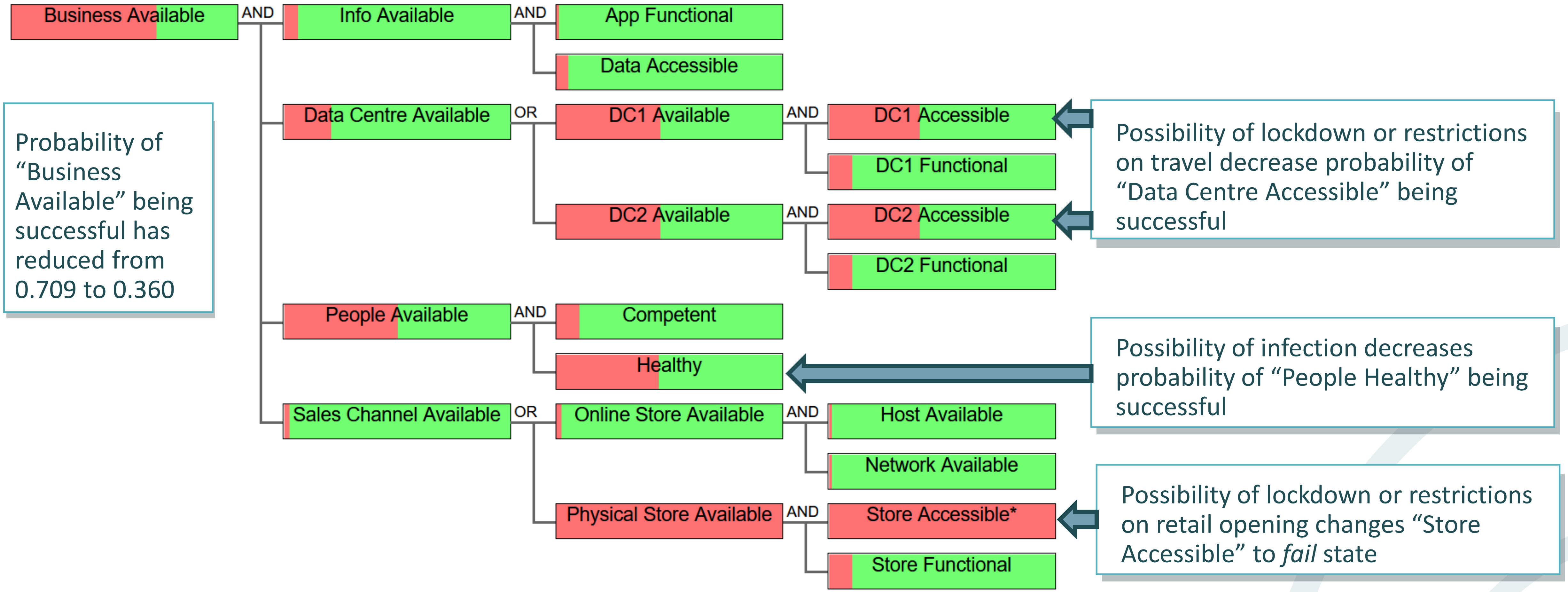
Current-state Overall Sensitivity Analysis

Which dependencies have the greatest overall influence?



New Circumstances – The Need to Adapt

A new normal - pandemic



Sensitivity In New Circumstances

Identify new or amended priorities

New Current-state Probability of success

0.360

	Business Available overall sensitivity	Business Available change in probability if dependency fails	Business Available change in probability if dependency succeeds
App Functional	0.363	0.360	0.003
Data Accessible	0.379	0.360	0.019
DC1 Accessible	0.189	0.114	0.075
DC1 Functional	0.126	0.114	0.012
DC2 Accessible	0.189	0.114	0.075
DC2 Functional	0.126	0.114	0.012
Competent	0.400	0.360	0.040
Healthy	0.654	0.360	0.294
Host Available	0.363	0.360	0.003
Network Available	0.363	0.360	0.003
Store Accessible	0.007	0.000	0.007
Store Functional	0.000	0.000	0.000

While it is important to protect against failure of a number of end-dependencies the greatest enablement comes from increasing Health & Data Centre Accessibility

Health of people which was previously only marginally the most sensitive end dependency now becomes a clear and urgent priority

SABSA

Options for the Treatment Strategy & Roadmap

Manage event, state or consequences

	Manage Probability		Manage Consequences
	Manage Event	**Manage State**	
	Deter threat *Encourage opportunity*	*Decrease weakness* *Increase strength*	*Resilience to negative impact* *Leverage of positive benefit* *Replace 'AND dependencies with 'OR' dependencies*
Health	Vaccination	Isolation	Cannot identify an 'OR' for health
Data Centre Accessible	Decrease travel restrictions	Enable home working	Data Centre Accessible physically OR logically

Model Strategy & Roadmap Options

Which strategy provides the best outcome?

- Which of the identified options to influence the probabilities of the end-dependencies provides greatest outcome?

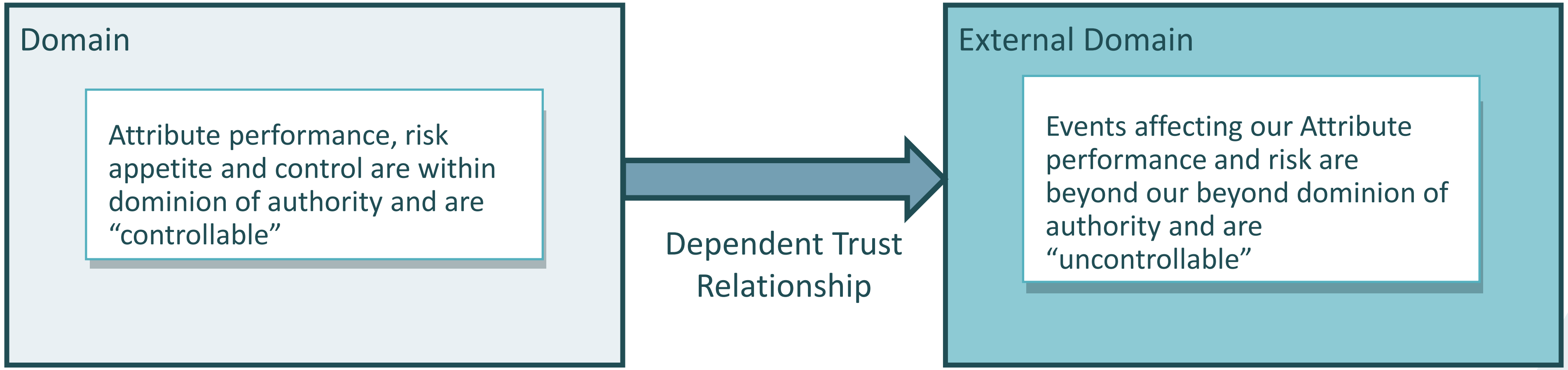
End Dependency	Treatment Strategy	Probability of the Business Available Success
Health	Vaccinate only	From 0.360 to 0.621
	Isolate only	From 0.360 to 0.491
Data Centre Accessible	Remove travel restrictions only	From 0.360 to 0.460
	Provide logical access via home working only	From 0.360 to 0.452

‘Controllable’ Versus ‘Uncontrollable’ Strategy

External domains are beyond dominion of authority

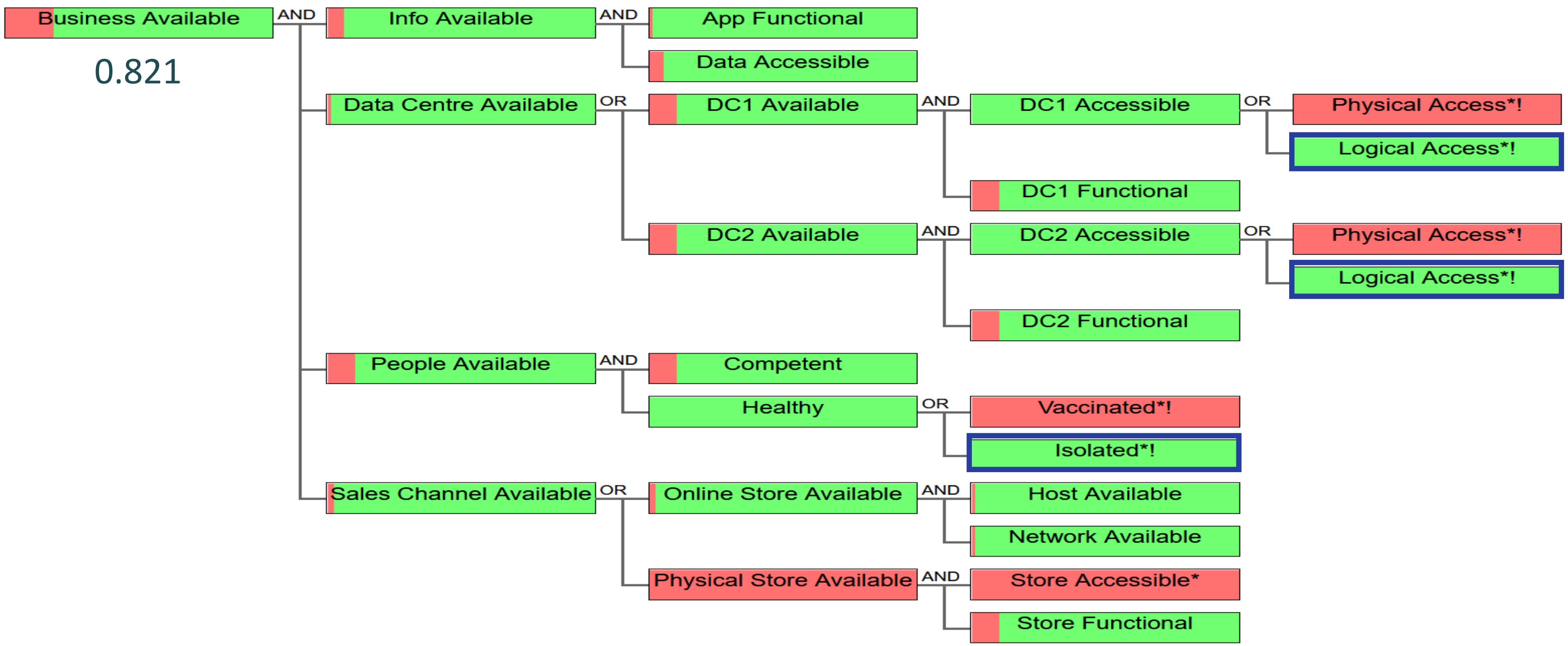
- External domains are uncontrollable
- We cannot exert direct control authority but can attempt to:
  - Deter events that could adversely impact us
  - Encourage events that could positively benefit us

End Dependency	‘Uncontrollables’ Treatment Strategy
Health	Fund vaccination research
Data Centre Accessible	Political lobby to remove travel restrictions



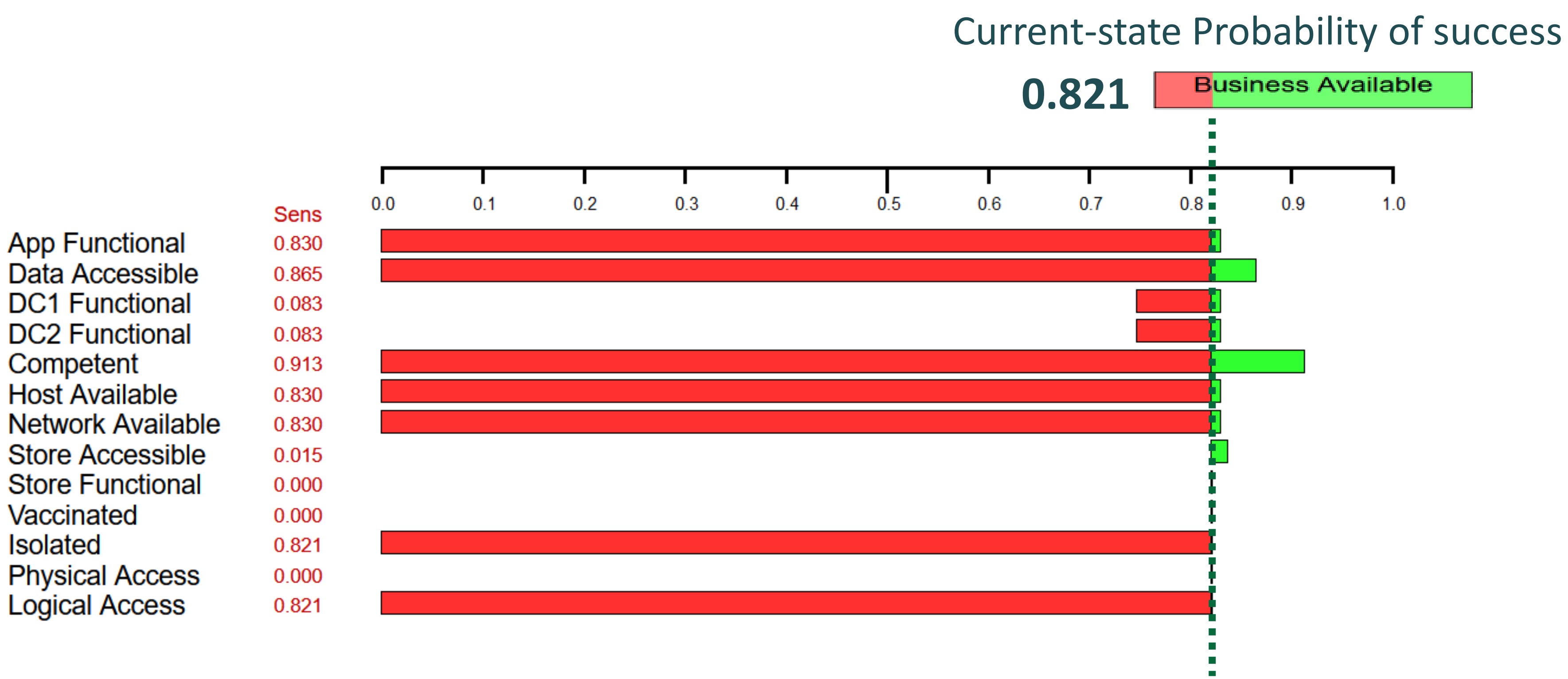
Prioritised First Steps

End Dependency	Treatment Strategy Within Domain of Authority
Health	Isolate our workforce
Data Centre Accessible	Provide logical access via home working



Sequencing Next Steps

New priorities emerge from dependency modelling the new state



Roadmap Dependencies for Redefined “Success”

Risk appetite & performance targets are not static

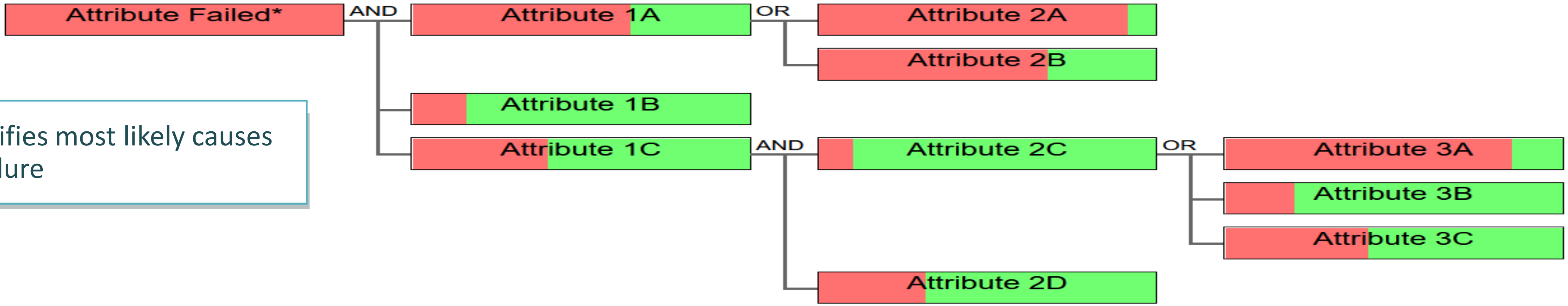
- The Enterprise may redefine “success” by adjusting the required performance target or risk appetite of Attributes
- Priorities can now be modelled by top-down analysis:
  - Set the Attribute to “Fail” to use the Dependency Model to detect most probable cause of failure
  - Set the Attribute to “Success” to use the Dependency Model to detect most likely contributions to success

Online Store Available

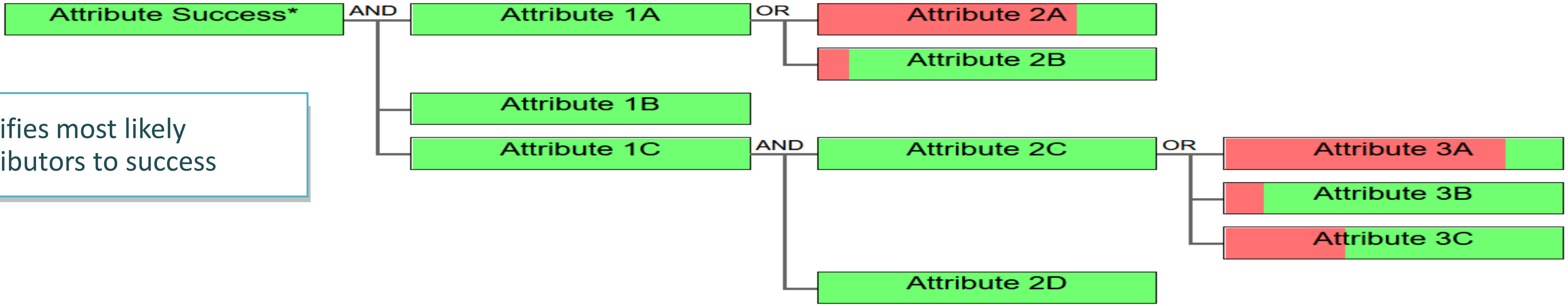
Success state performance targets are met / residual risk is within risk appetite

New Enterprise strategy for the new normal abandons physical stores and has a new focus on online retailing. This changes the definition of success for the Attribute “Online Store Available”

Top-down Failure & Success Analysis



Identifies most likely causes of failure

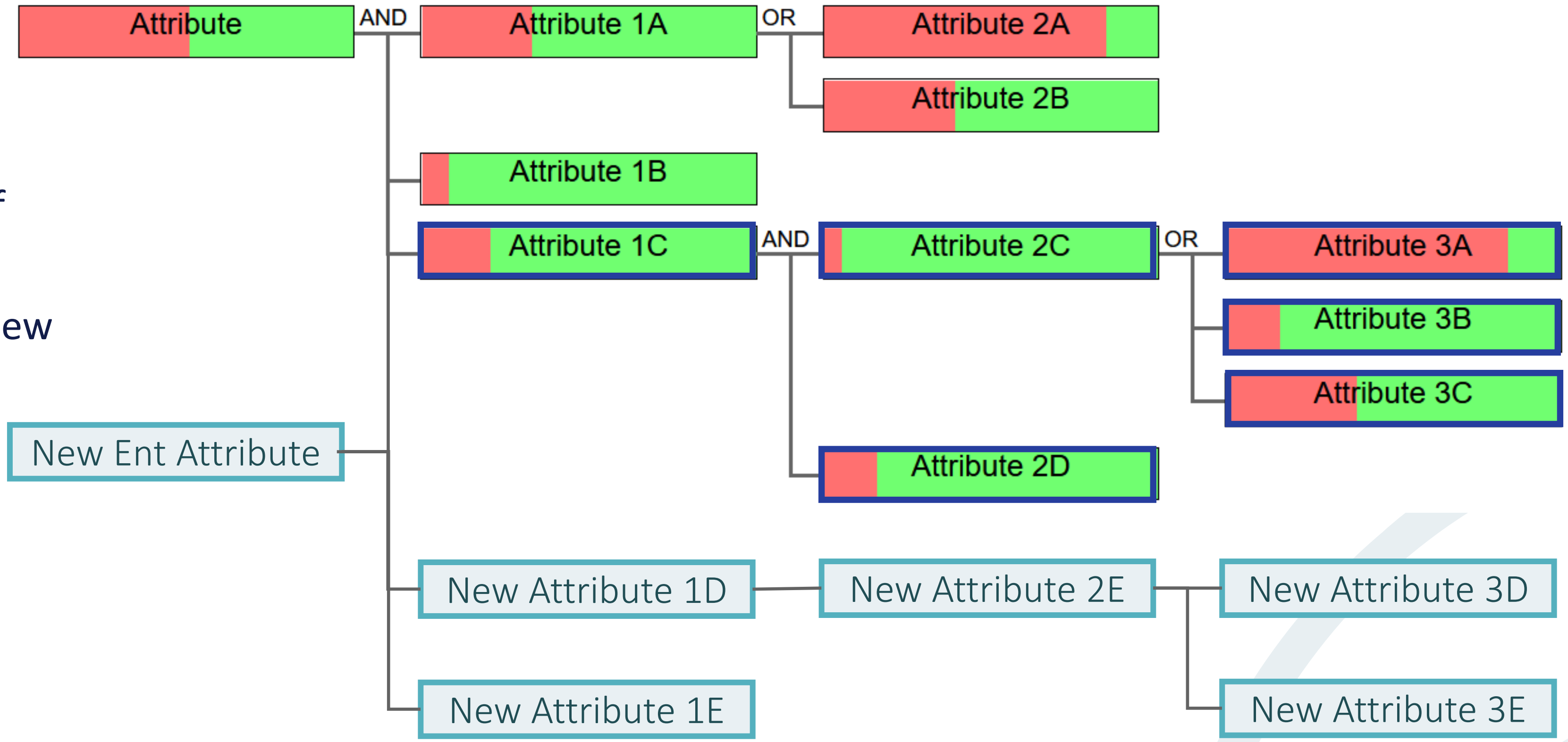


Identifies most likely contributors to success

Strategy Roadmap for a New Vision

Gap analysis between current-state & target-state

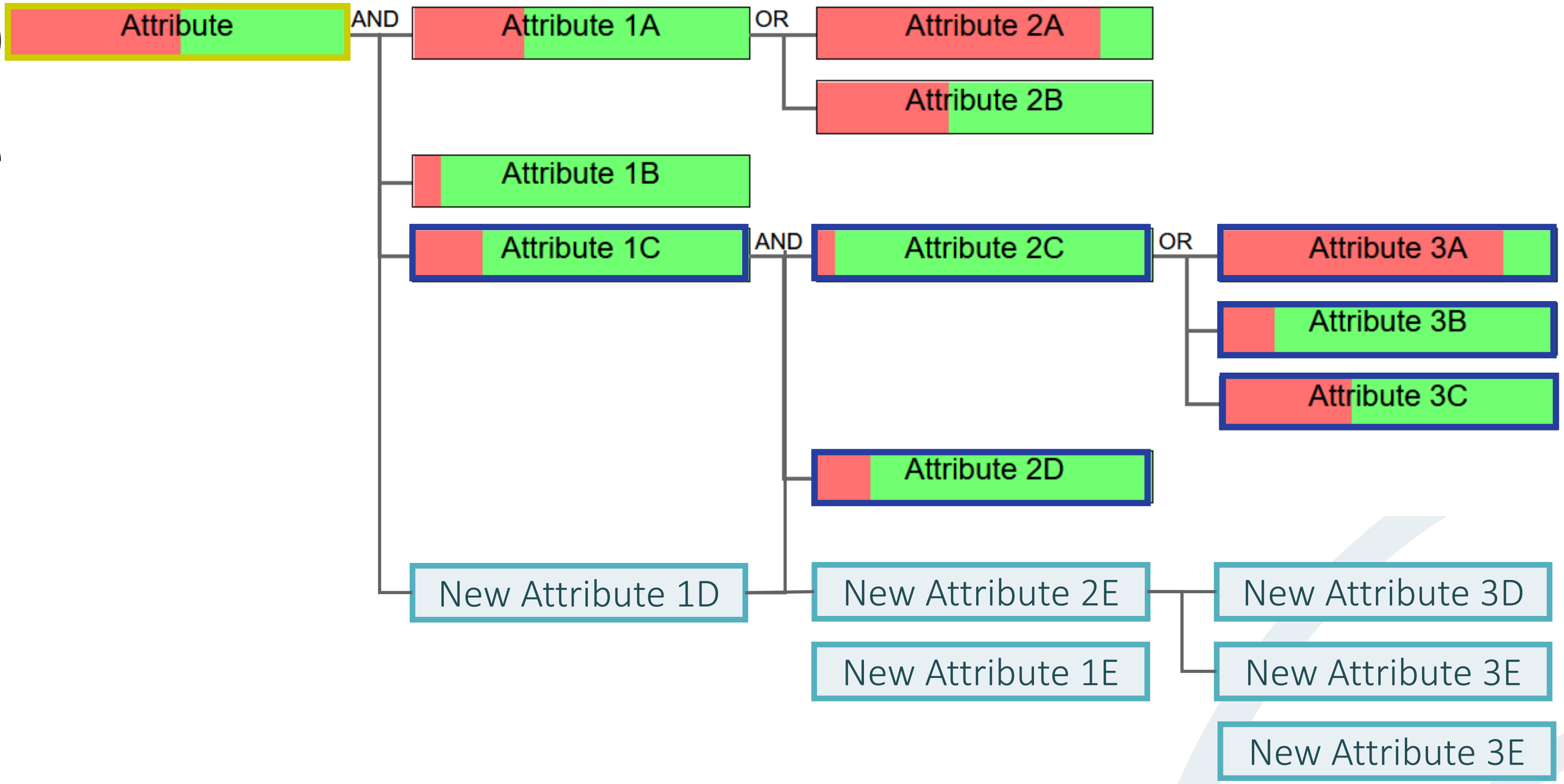
- A gap analysis informs that the Roadmap to meet new Enterprise (macro) level requirements, involves a combination of:
  - Leveraging the knowledge base of existing relevant Attributes and dependencies
  - Introducing new Attributes with new dependencies



Roadmap Implications for a New Non-enterprise Architecture

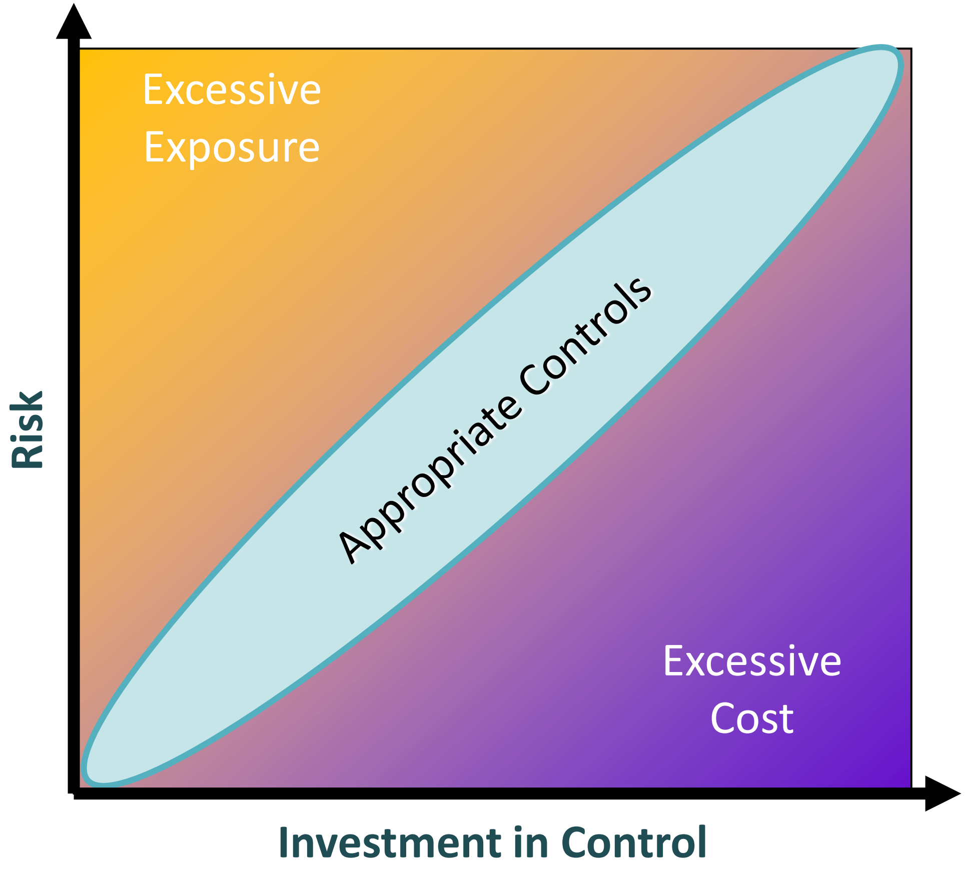
Bi-directional dependency analysis between current-state & target-state

- Analysis informs positive and negative implications of a new non-Enterprise (meso or micro) initiative on SuperAttributes
- It also leverages the knowledge base of existing relevant Attributes and dependencies
- And introduces new Attributes with new dependencies



Risk Finance Strategy

Appropriate risk treatment investment



SABSA®

Risk Finance Strategy

Types of risk finance

- Self-insurance
  - Accepting certain levels of risk
  - Most applicable where there is a diverse portfolio of assets
- Diversification
  - Ensuring that risks are spread across a large number of risk types and asset types
  - Often known as ‘hedging’, especially in financial risk management
  - Especially useful for managing purely financial risk
- Economic capital allocation
  - Sums set aside on the balance sheet to cover unforeseen risk events of significant scale
  - Cannot cover catastrophic loss
- Insurance
  - Designed to transfer risk to a third-party insurer for a fee (insurance premium)
  - Most applicable to catastrophic loss
  - The level of accepted risk is the ‘excess’ on the insurance policy

Risk Finance Strategy

Use of economic capital

- Most often applied to:
  - Certain financial risks such as credit risk and financial market risk
  - Operational risk (although this is more difficult because of the heterogeneous nature of operational risks – you must first separate out the risk types and lines of business and must allow for possible correlation)
- Not really applicable to strategic risk
  - The only mitigation against strategic risk is good strategic judgement, competence of both management and staff and strong governance

Risk Finance Strategy

Calculating economic capital

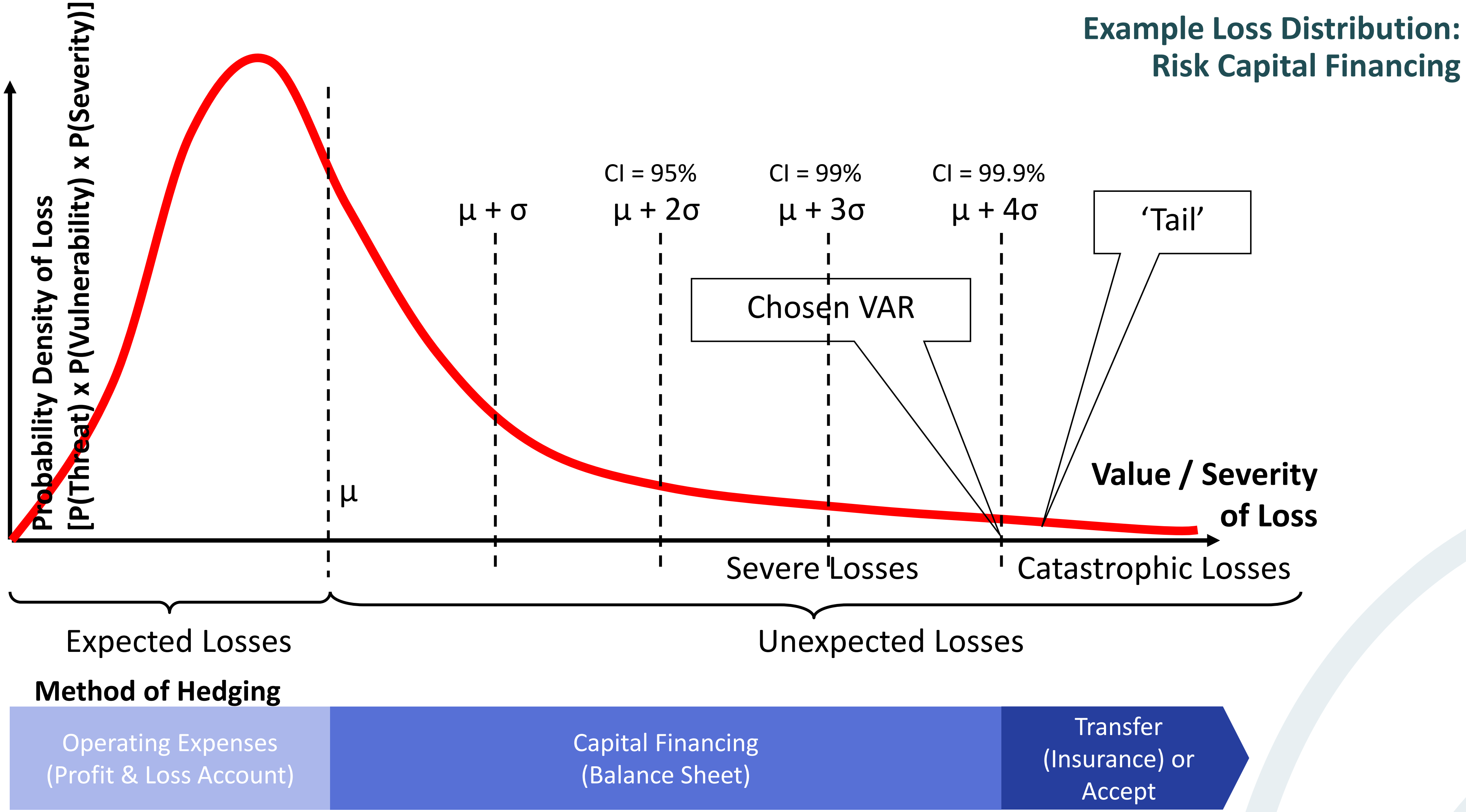
- Create a loss database framework
- Collect loss data and populate the database over several years
- Collate the data into a matrix of line of business versus risk type
  - Identify your different lines of business
  - Identify your principal risk types
- Use the loss data to model two probability distributions for each of the matrix cells:
  - Frequency of loss events within a one-year period (fit the data to a Poisson distribution)
  - Severity of loss (given event) within a one year period (fit the data to a Log-normal distribution)
- Estimate the statistical parameters for these distributions
- Use these probability distributions as the inputs to a Monte Carlo simulation of the loss distribution
- Calculate the capital allocation as a given confidence interval of the simulated loss distribution

Risk Finance Strategy

Modelling economic distributions

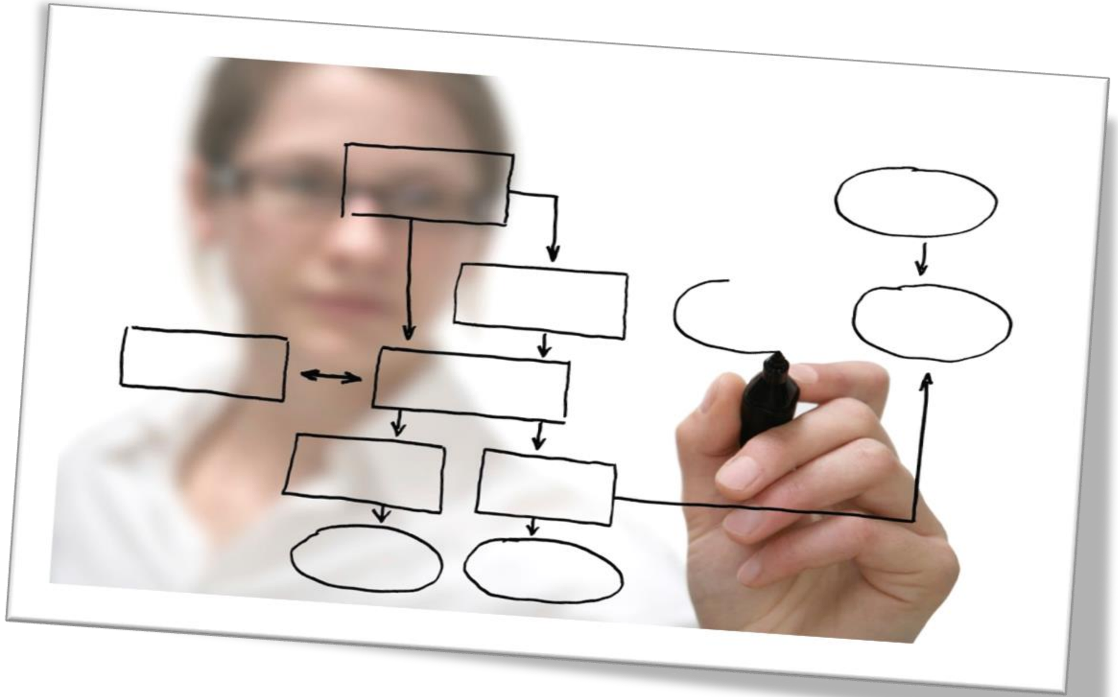
- Collect historical internal loss data
  - Collate according to risk type and line of business
- Statistically analyse the loss data
  - Sample mean (x bar)
  - Sample standard deviation (s)
- Estimate population parameters (from sample statistics)
  - Population mean (μ)
  - Population standard deviation (σ)
- Fit the empirical data to a theoretical loss distribution
  - Frequency of events: Poisson
  - Severity of loss (given event): Log-normal
- Carry out ‘goodness of fit’ tests
  - χ^2 test
- Select a value-at-risk (VAR) confidence level
  - 99%, 99.5% or 99.9%

Risk Finance Strategy



Workshop A1-8

Risk Treatment Strategy

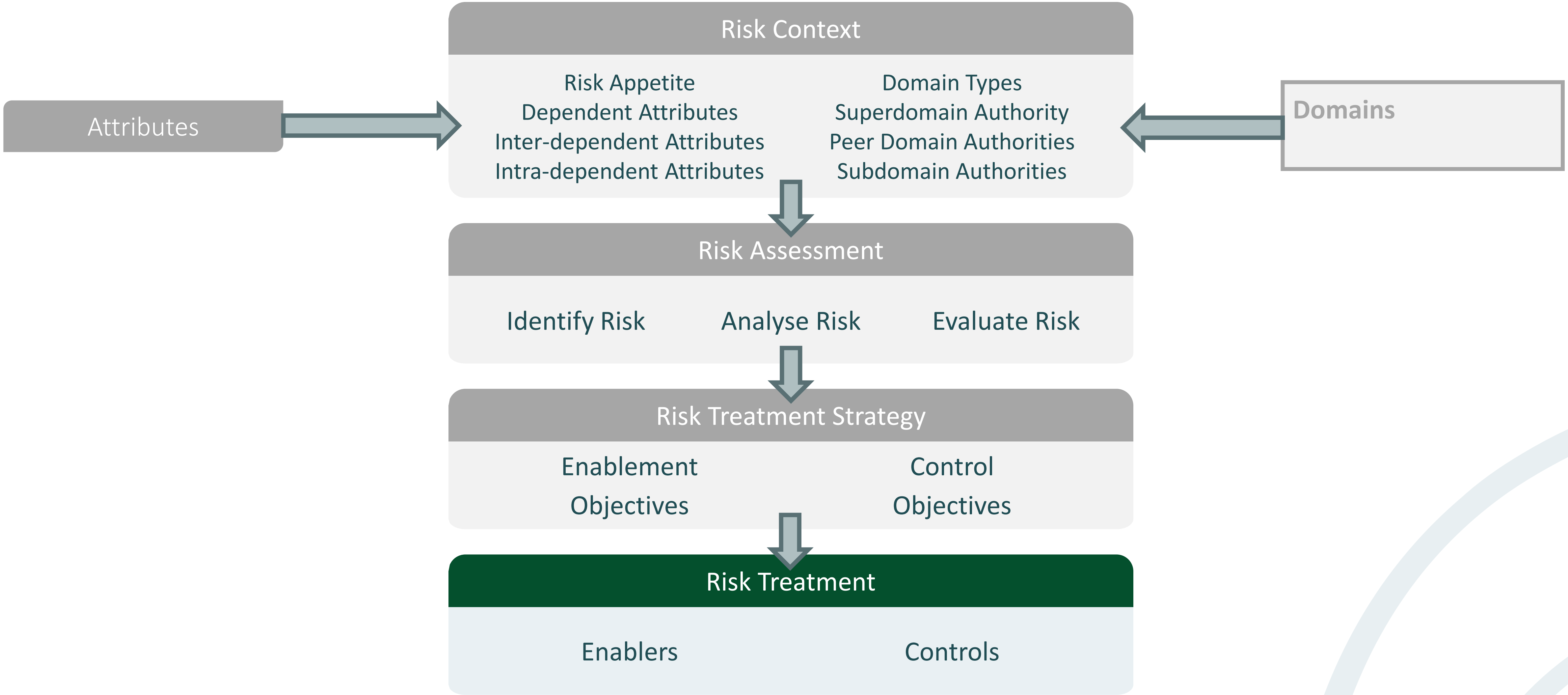


SABSA®

Risk Treatment

Section 11

Scope


Attributes
Risk Context
Risk Appetite
Dependent Attributes
Inter-dependent Attributes
Intra-dependent Attributes
Domain Types
Superdomain Authority
Peer Domain Authorities
Subdomain Authorities
Domains
Risk Assessment
Identify Risk
Analyse Risk
Evaluate Risk
Risk Treatment Strategy
Enablement Objectives
Control Objectives
Risk Treatment
Enablers
Controls

Controls & Enablers

- A control is a risk treatment that reduces the risk of negative impact and protects the target performance level of the Attribute within risk appetite
- An enabler is a risk treatment that increases the potential for positive benefit to the target growth in performance level of the Attribute

Attribute

Controls

Protect from negative consequences

Achieve control objectives to:

- Maintain
- Protect
- Reduce

Enablers

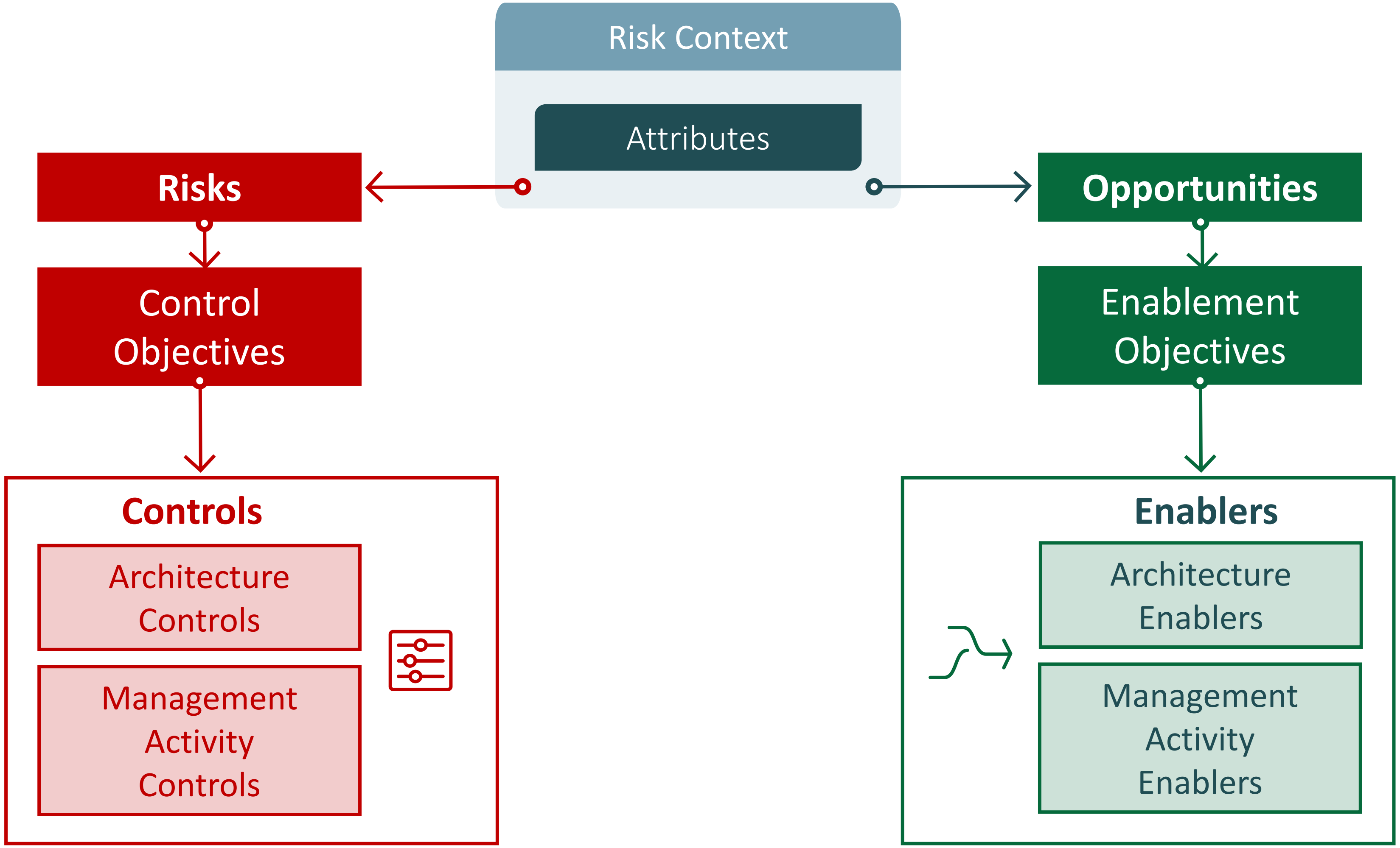
Produce positive consequences

Achieve enablement objectives to:

- Empower
- Grow
- Increase

SABSA®

Controls & Enablers



Controls & Enablers

Logical services, physical mechanisms, components & respective management activities

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Dependence
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & trust Frameworks		
Logical	Information	Policy	Information Processing & Services			
Physical	Data	Practices & Procedures	Data Comms & Mechanisms	System		
Component	Products & Tools	Risk Standards	Protocol Standards			
Management	Delivery & Continuity	Risk Management	Process Management			

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Management	Delivery and Continuity	Risk Management	Process Management	Governance, Management	Environment Management	Time 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	Analyse Requirements	Assess Risks	Manage Value Chain	Manage Relationships	Manage Facilities	Manage Time
Conceptual	Define Requirements	Define Risk Objectives	Manage Processes	Define Trust Relationships	Define Domains	Define Time Framework
Logical	Manage Information	Manage Policy	Manage Services	Manage Roles	Manage Domains	Manage Time Model
Physical	Manage Data	Manage Practices	Manage Mechanisms	Manage Access	Manage Infrastructure	Manage Processing Schedule
Component	Manage Configuration	Manage Standards	Manage Protocols	Manage Entities	Manage Addressing	Manage Timing

Risk Treatment Architecture Layers

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

Architecture Layers – Conventions Revisited

- The end goal is defined by the top layer
- The end goal and requirements to meet the goal are delegated top-down through each successive layer to a level of abstraction and detail that is meaningful at that level
- Each layer is a means to an end, serving the requirements of the layer above
- Layers are closed
  - The layer’s requirements are delegated to the layer directly below which cannot be by-passed
  - Interfaces between layers are defined only for layers directly above and below
- Layers are independent
  - A layer is a black box to the layer above
  - A layer is specified independently of the layer below
- Changes of specification can be made in a layer to meet the requirements of the layer above without effecting the specification of other layers
  - The rubber compound can be changed when it starts to rain so that the performance of the tyres continues to provide the grip required

SABSA Governance Framework Revisited

Accountable Domain Authority	Strategy	Identify dependent Attributes: Consult Superdomain, Peer Domains & External Authorities Determine: Risk Appetite, Performance Targets & Objectives Set: Policy to meet objectives
	Adopt	Identify dependencies: Subdomains, Peer Domains & External Domains Inform: Dependencies of responsibility
Responsible Domain Authorities	Transform	Design: Controls & Enablers to meet Objectives Design: Systems, Processes & Resourcing Models
	Transition	Implement: Controls & Enablers Establish: Systems, Processes & Resources
	Operate	Monitor Performance: Controls & Enablers Manage: Systems, Processes & Resources
	Assess & Report	Assess: Performance of Attributes against Risk Appetite & Performance Targets Report: Performance of Attributes against Risk Appetite & Performance Targets

Domain Authority at any level sets control & enablement objectives but may delegate responsibility to subdomains or peers

From the Domain Authority perspective, SubDomain Authorities are responsible for establishing and operating the controls & enablers required to meet the objectives

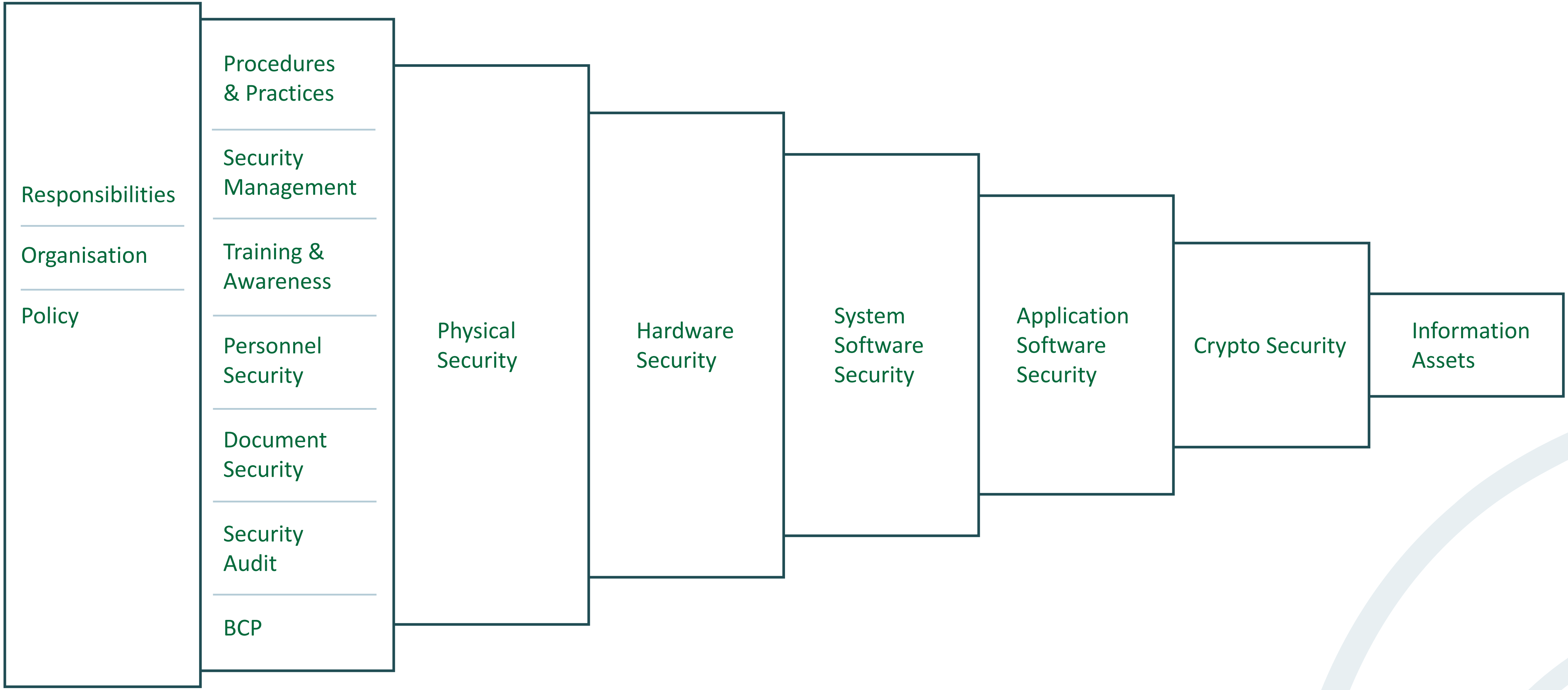
Risk Treatment Capabilities

Manage event, state or consequences

Manage Probability		Manage Consequences
Manage Event	Manage State	
Deter threat *Encourage opportunity*	*Decrease weakness* *Increase strength*	*Resilience to negative impact* *Leverage of positive benefit* *Replace 'AND dependencies with 'OR' dependencies*

Objective is to treat the right element of risk, at the right place, in the right way, at the right time, with the greatest effect on objectives, for the lowest investment

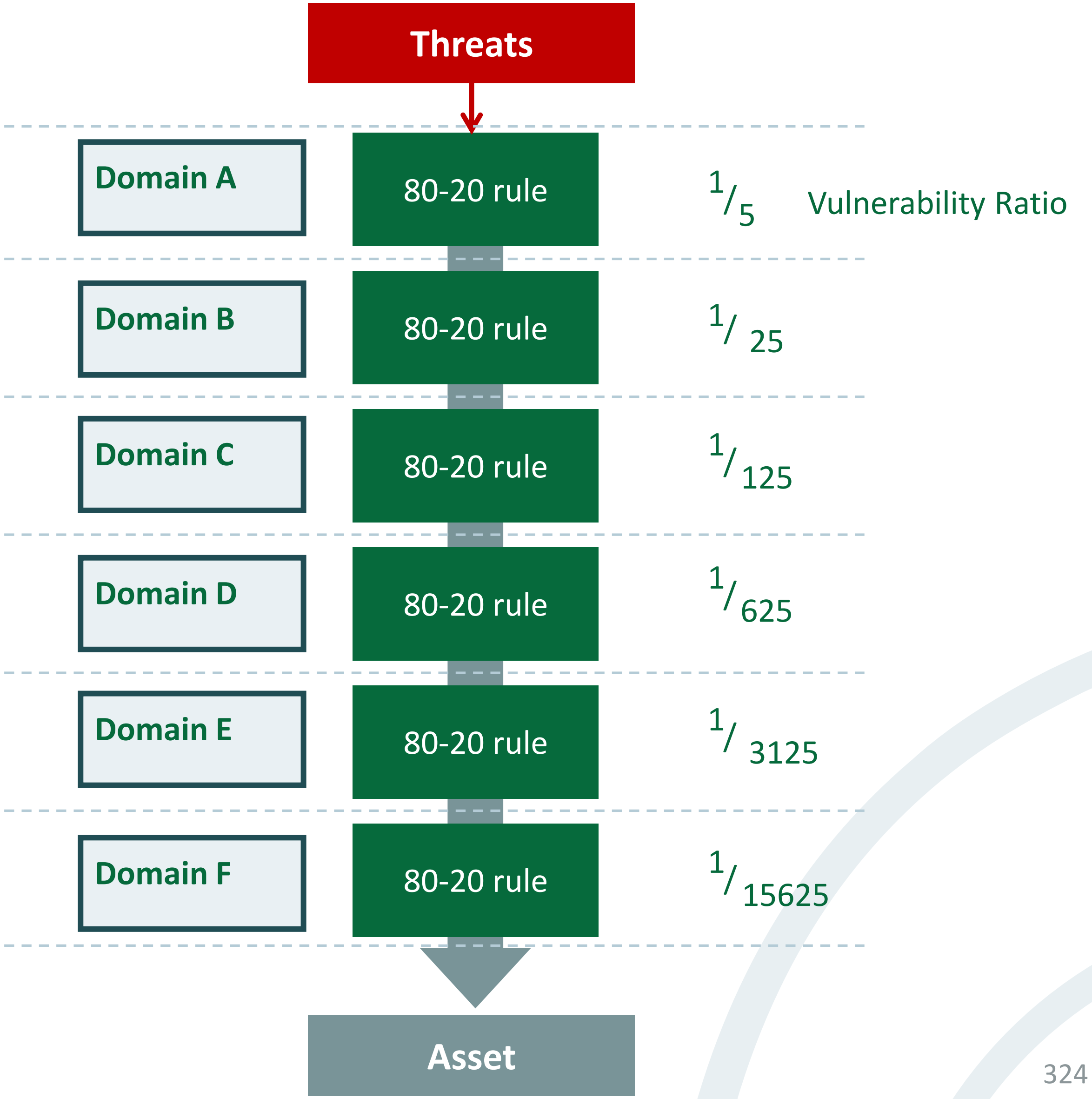
Generic Defence in Depth Layering



SABSA®

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

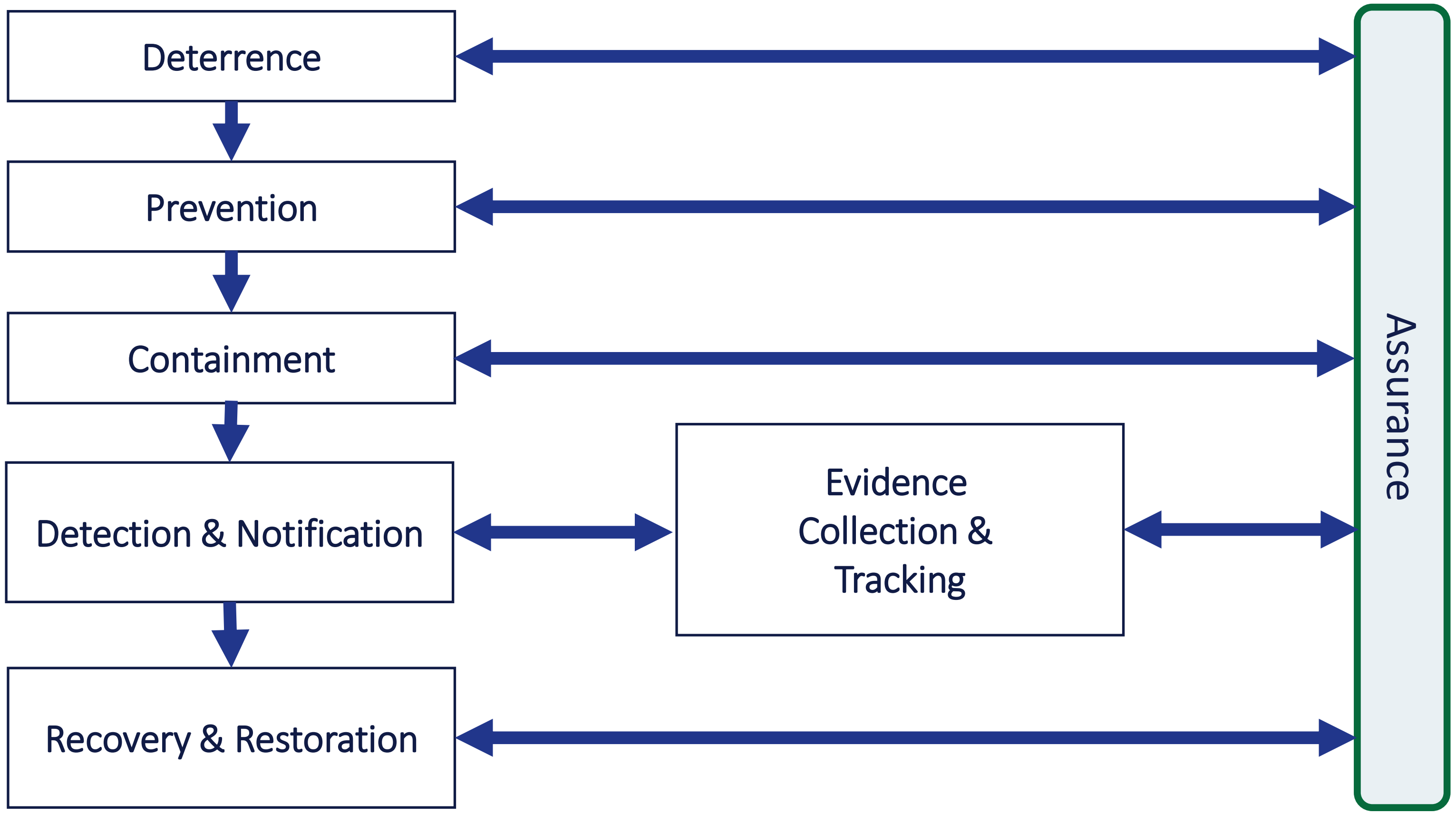


Multi-tiered Controls Strategy Capabilities

Prioritised, proportional, balanced investment

- Over-investment in risk treatments 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

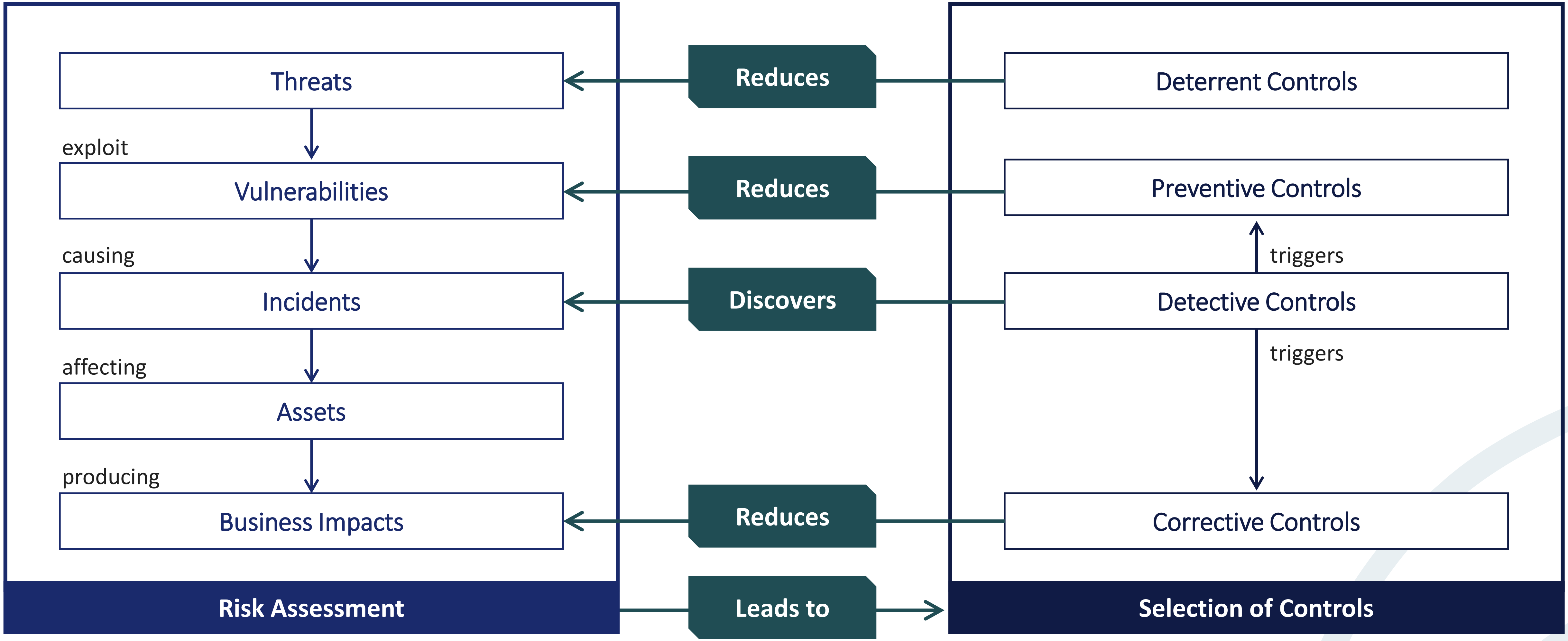
SABSA Multi-tiered Control Strategy



Application of Multi-tiered Treatments

- The multi-tiered controls strategy is modelled 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-tiered Control



Application of Multi-tiered Control Strategy

Attributes

Attribute	Attribute	Attribute
Attribute	Attribute	Attribute

with performance targets & risk appetite thresholds

Risk Assessment Ratings

Threat	**Vulnerability**	-Impact
Opportunity	**Strength**	+Impact

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

Integrated Controls & Enablers Library

Control 1	…	ISO 9.2	CobIT 1.1	PCI
Control 2	…	ISO 8.3	CobIT 1.2	NIST
Enabler 1	…	ISO 7.4	CobIT 1.3	SOX
Enabler 2	…	ISO 6.5	CobIT 1.4	Etc.

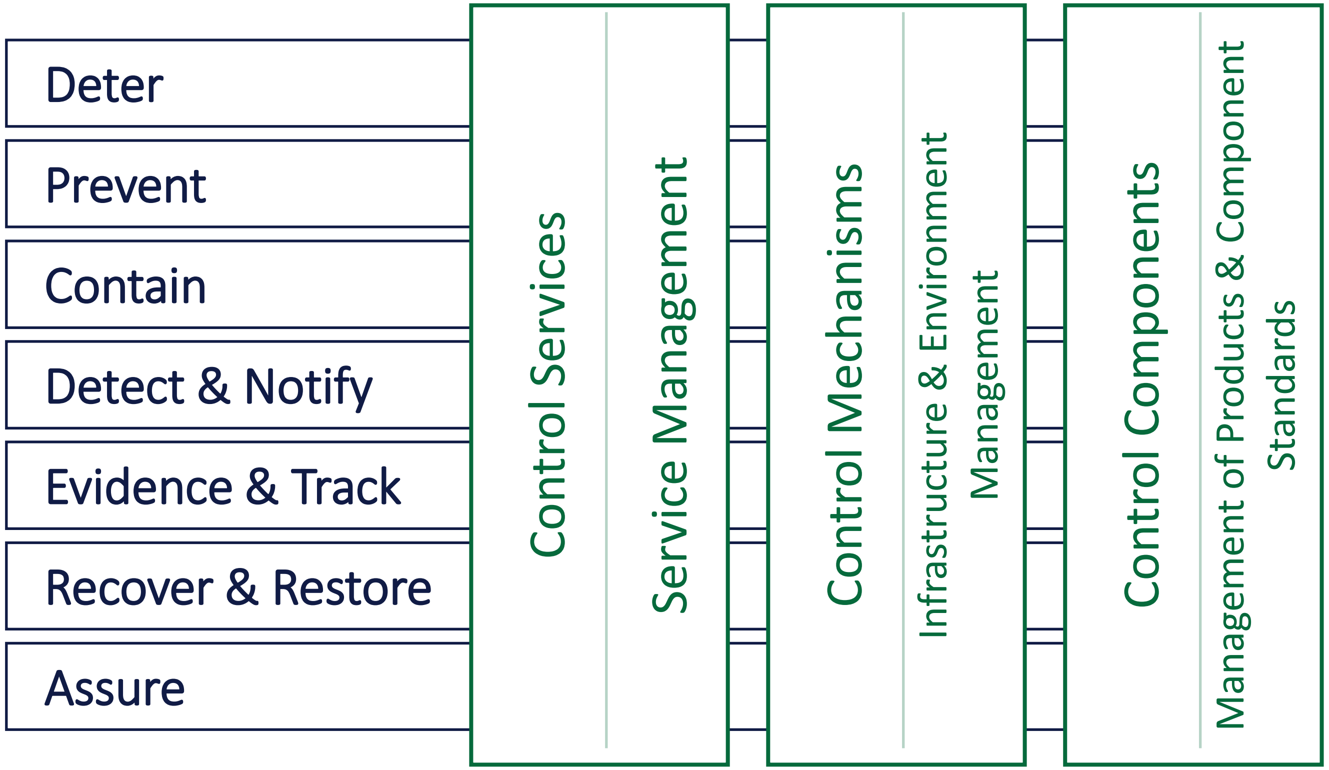
Mapped to all corporate standards

Defence-in-Depth Model Indicators

SABSA MTC	Tech Domain	Etc
Deter	Apps	1
Prevent	Platform	2
Contain	Network	3
Etc.	Etc.	Etc.

Strength-in-Depth Capability Engineering

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



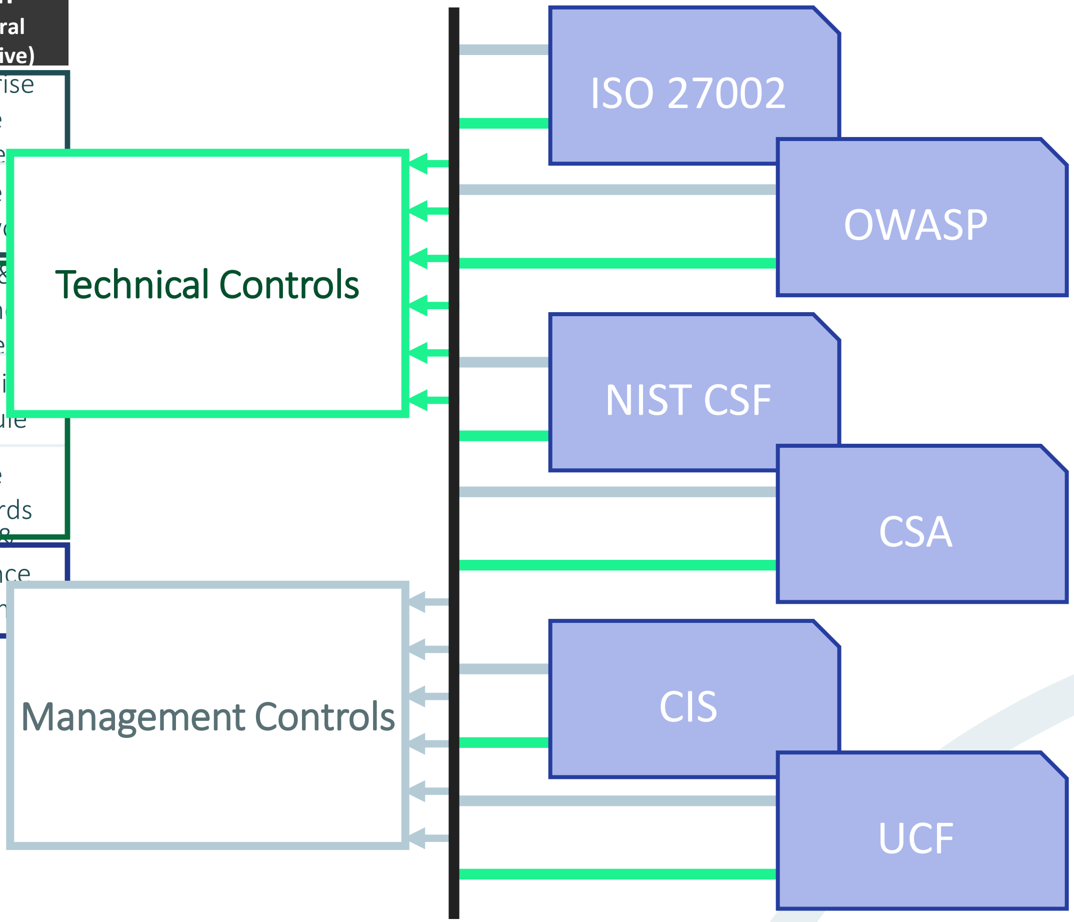
Risk Treatment Integration & Alignment

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Depende
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & trust Frameworks	Domain Framework	Time Framew
Logical	Information	Policy	Information Processing &	Trust Model	Logical Domains	Time & Sequen Mode
Phy						
Manage						

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Management	Delivery and Continuity	Risk Management	Process Management	Governance, Management	Environment Management	Time 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	Analyse Requirements	Assess Risks	Manage Value Chain	Manage Relationships	Manage Facilities	Manage Time
Conceptual	Define Requirements	Define Risk Objectives	Manage Processes	Define Trust Relationships	Define Domains	Define Time Framework
Logical	Manage Information	Manage Policy	Manage Services	Manage Roles	Manage Domains	Manage Time Model
Physical	Manage Data	Manage Practices	Manage Mechanisms	Manage Access	Manage Infrastructure	Manage Processing Schedule
Component	Manage Configuration	Manage Standards	Manage Protocols	Manage Entities	Manage Addressing	Manage Timing



SABSA

SABSA Attributes – Common Language for Integration

ISO/SEC 2700x - Commented version

A8.1.3 Terms and conditions of employment

Control 21 *[Confidentiality, Compliant, Admissible]*

As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.

Implementation guidance

The terms and conditions of employment[209] should reflect the organization's security policy in addition to clarifying and stating [210,211]:

[Confidentiality, Admissible] a) that all employees, contractors and third party users who are given access to sensitive information should sign a confidentiality or non-disclosure agreement[212] prior to being given access to information processing facilities (see also 6.1.5);

b) the employee's, contractor's and any other user's legal responsibilities and rights, e.g. regarding copyright laws, data protection legislation (see also 15.1.1 and 15.1.2);

[Confidentiality, Admissible] c) responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or third party user (see also 7.2.1 and 10.7.3);

[Confidentiality] d) responsibilities of the employee, contractor or third party user for the handling of information received from other companies or external parties;

[Private, Compliant] e) responsibilities of the organization for the handling of personal information, including personal information created as a result of, or in the course of, employment with the organization (see also 15.1.4);

f) responsibilities that are extended outside the organization's premises and outside normal working hours, e.g. in the case of home-working (see also 9.2.5 and 11.7.1);

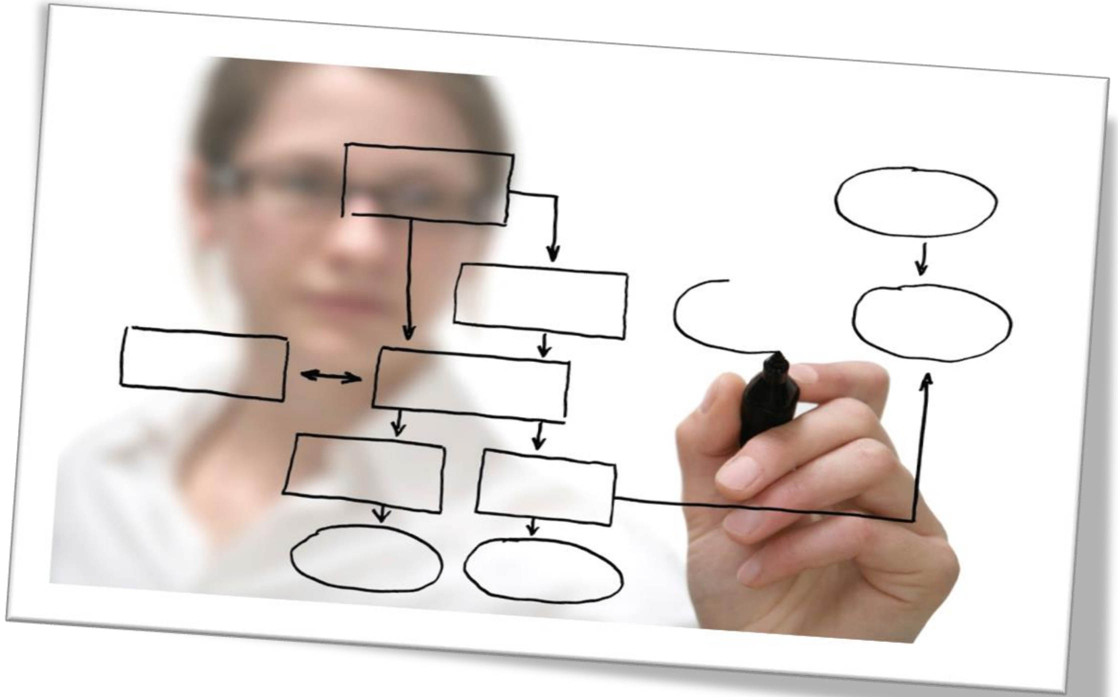
g) actions to be taken if the employee, contractor or third party user disregards the organization's security requirements (see also 8.2.3).

Extract reproduced with permission from Hans Hopman

SABSA®

Workshop A1-9

Risk Treatment



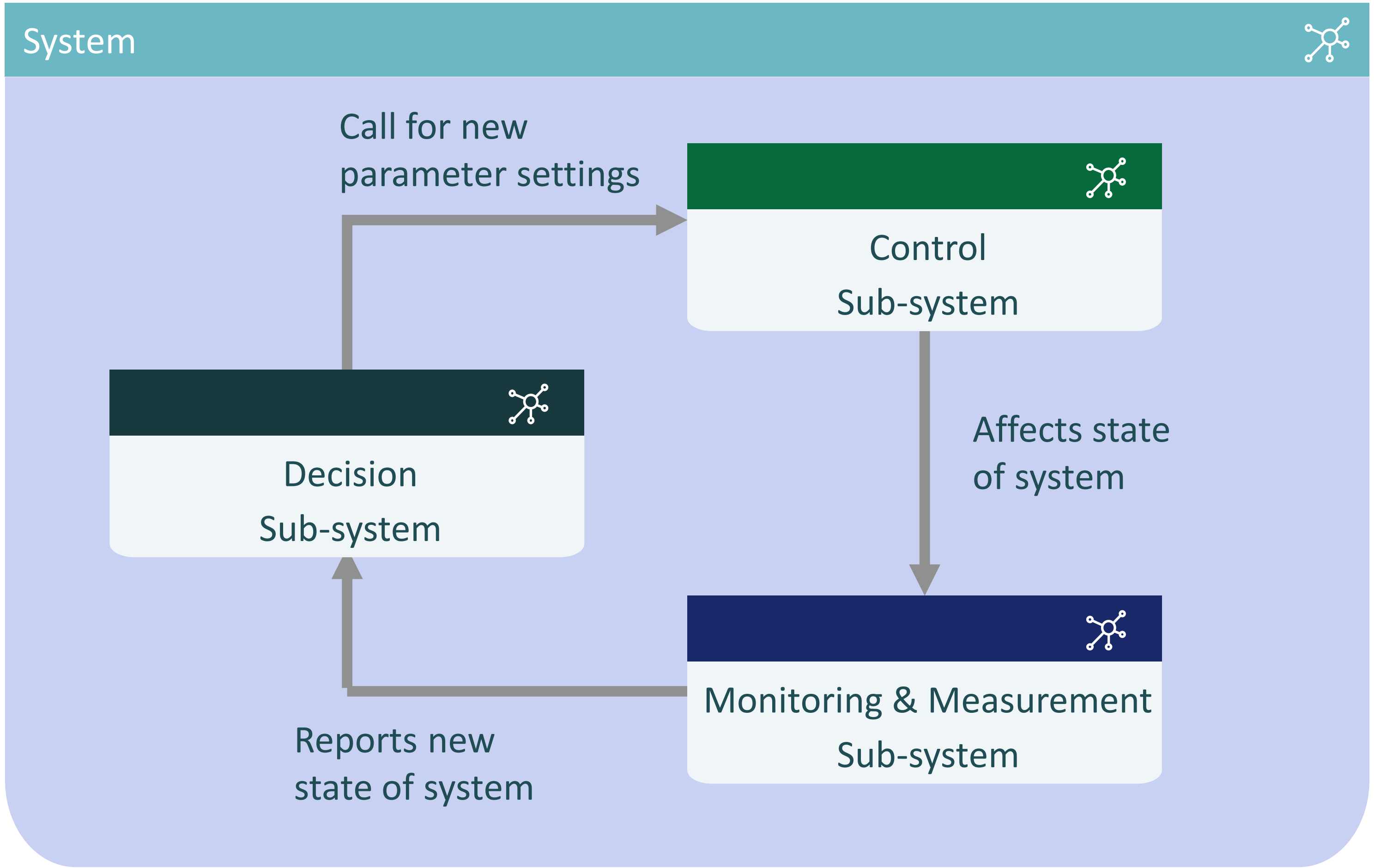
A1 – Unit 5

Risk Management

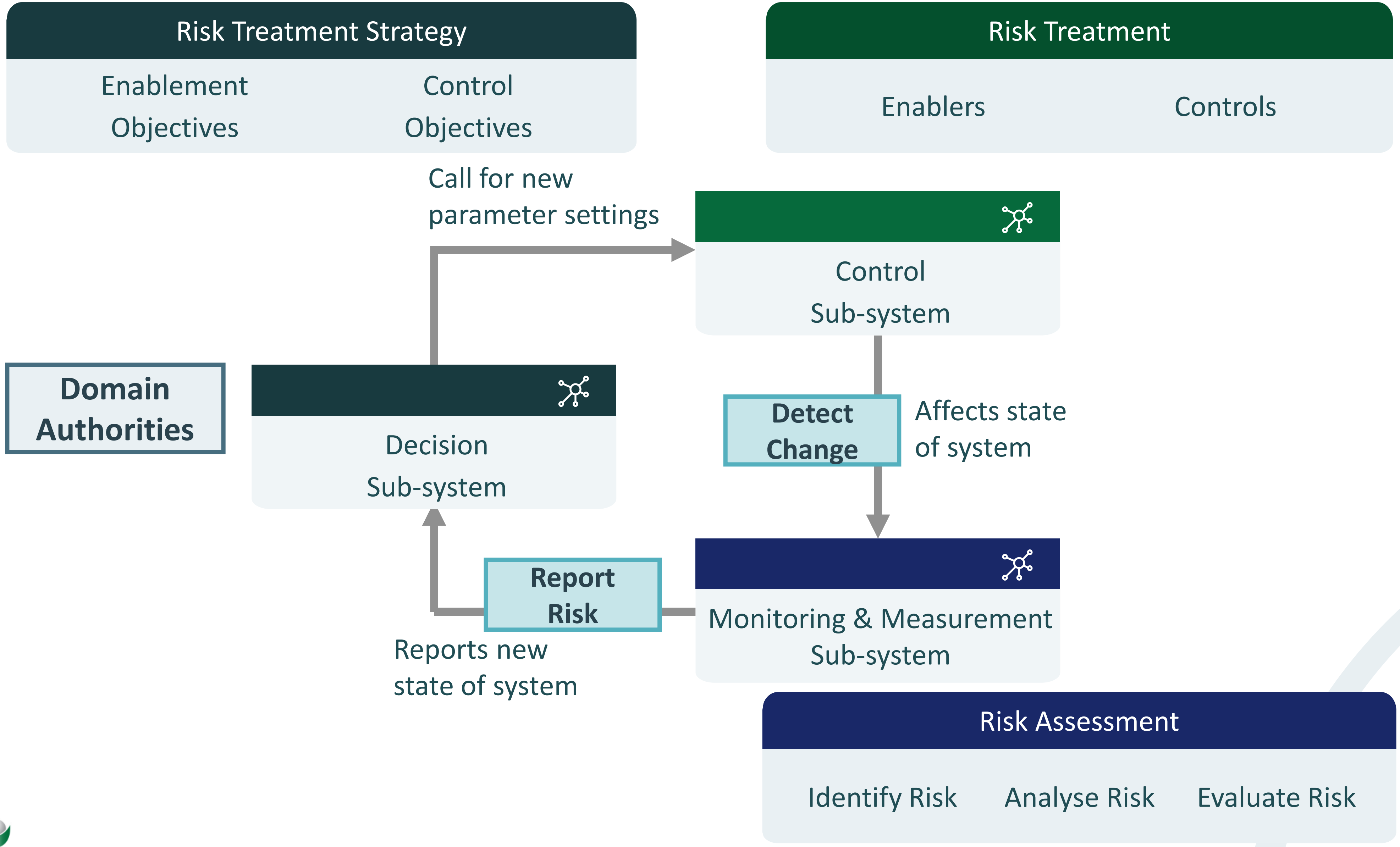
Risk Management

Section 12

Feedback Control Loop System



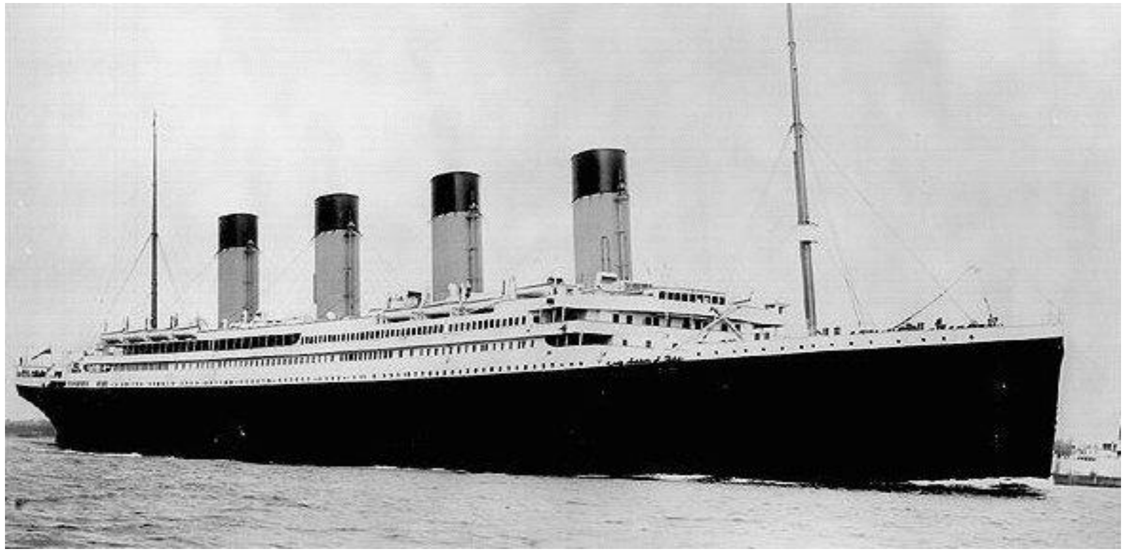
Risk Management Feedback Control System



Risk Management - Monitor

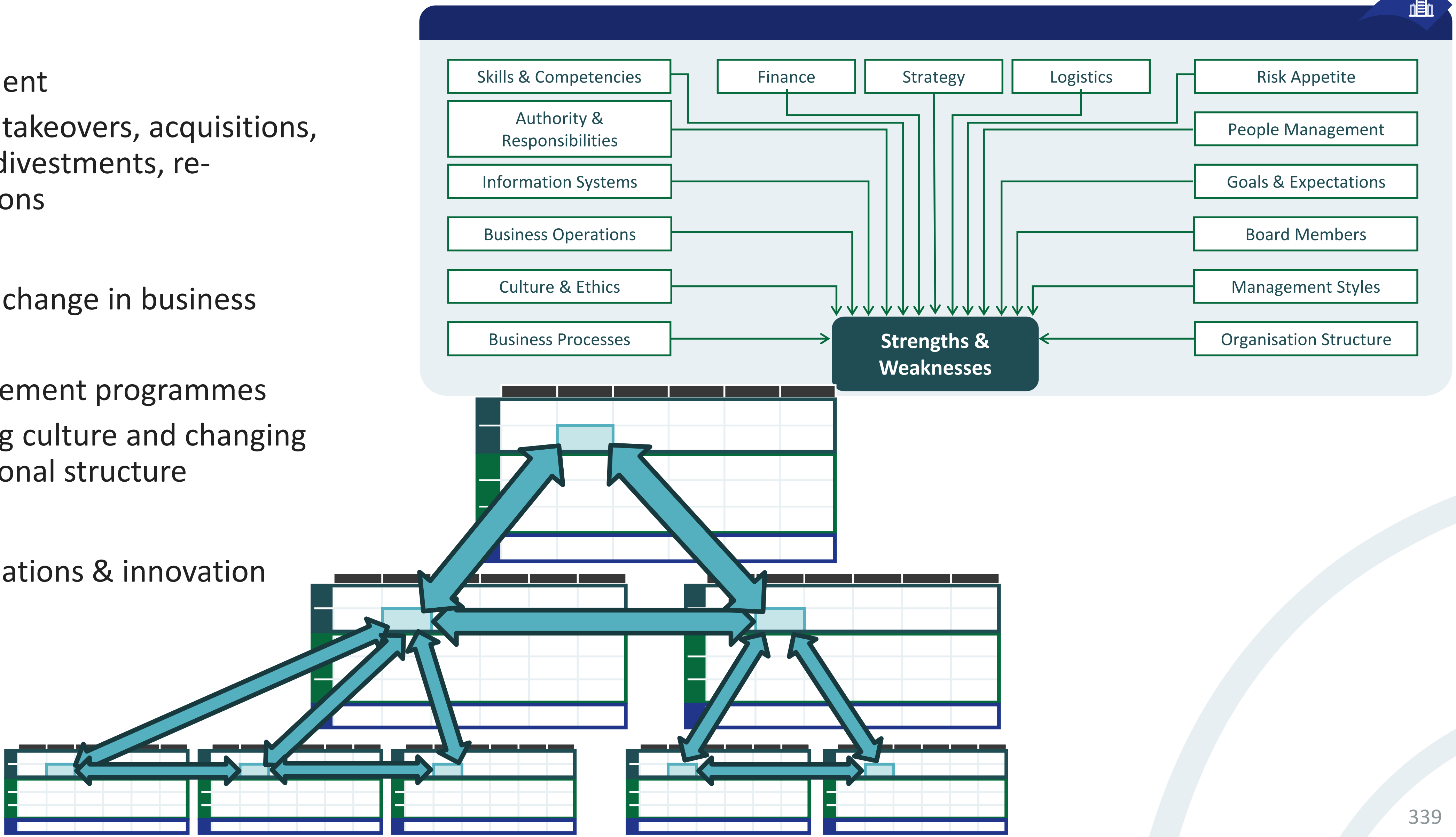
The role of KRIs

The monitoring subsystem requires input that indicates change, the need to change, and ability to change. These indicators are called Key Risk Indicators and can be utilised at any point in the risk management lifecycle

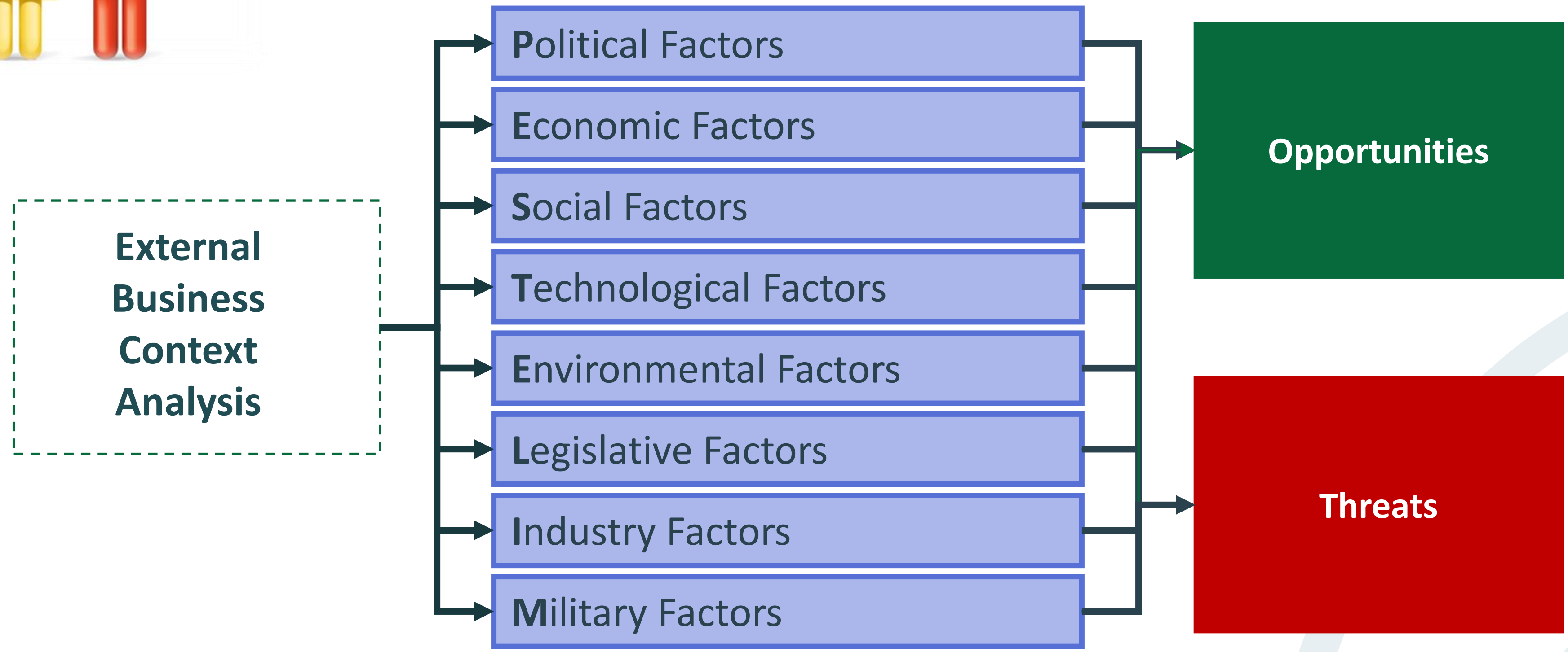


Monitor – Internal Risk Factor KRIs

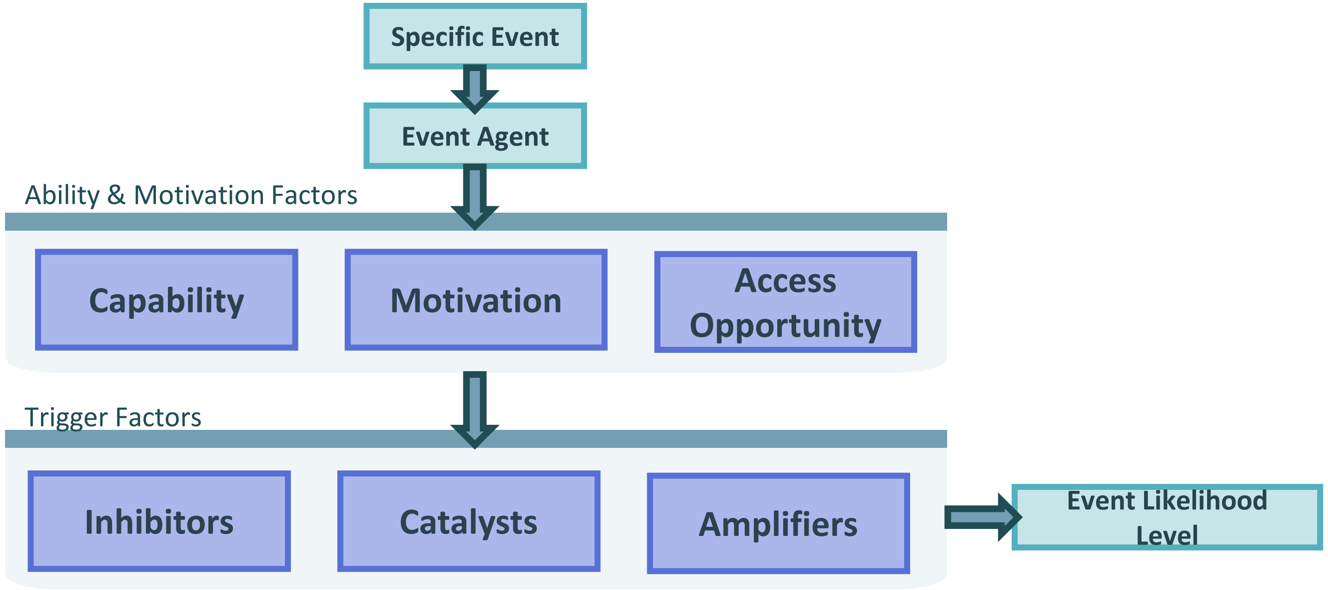
- New management
  - Following takeovers, acquisitions, mergers, divestments, re-organisations
- New targets
  - Following change in business strategy
- Change management programmes
  - Re-aligning culture and changing organisational structure
- New projects
  - Transformations & innovation projects
- New policies



Monitor – External Risk Factor KRIs

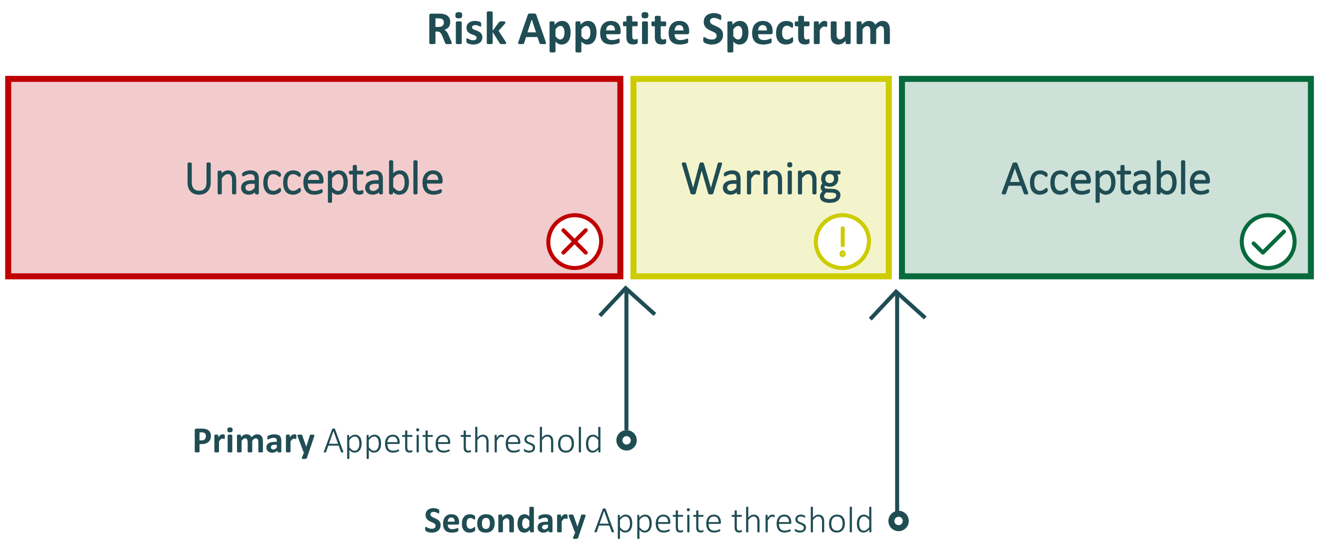


Monitor – External Risk Factor KRIs



Inhibitors	Catalysts (Candidate KRIs)	Amplifiers
Fear of capture	External events that trigger a response	Peer pressure
Fear of failure	Changes in personal circumstances creating a 'need'	Fame
Insufficient access limiting the opportunity	Step changes in level of access increasing the opportunity	Easy access providing high level of opportunity
High level of technical difficulty	Step changes in level of difficulty through new technologies and tools/ demonstrable increased prevalence	Ease of execution because of low level of technical difficulty
High cost of participation	Step changes in level of cost	Low cost of participation
Sensitivity to adverse public opinion	Dramatic changes in public opinion and cultural values	Belief in sympathetic public opinion

Measure – Effect of Controls & Enablers on Targets



- Deploy control A?
- Deploy control B?
- Deploy control A + B?
- Deploy controls from each domain of the multi-tiered controls strategy?

How do we assess the effectiveness of a control/enabler? Which control or combination of controls/enablers causes the residual risk rating to cross a threshold?

Measure – Effect of Controls & Enablers on Targets

The role of actuarial data

Estimated Current State

Unacceptable

Attribute performance criteria removes some subjectivity in initial rating by creating defined impact parameters & thresholds

Predicted Target State

Warning

Predicted Target State

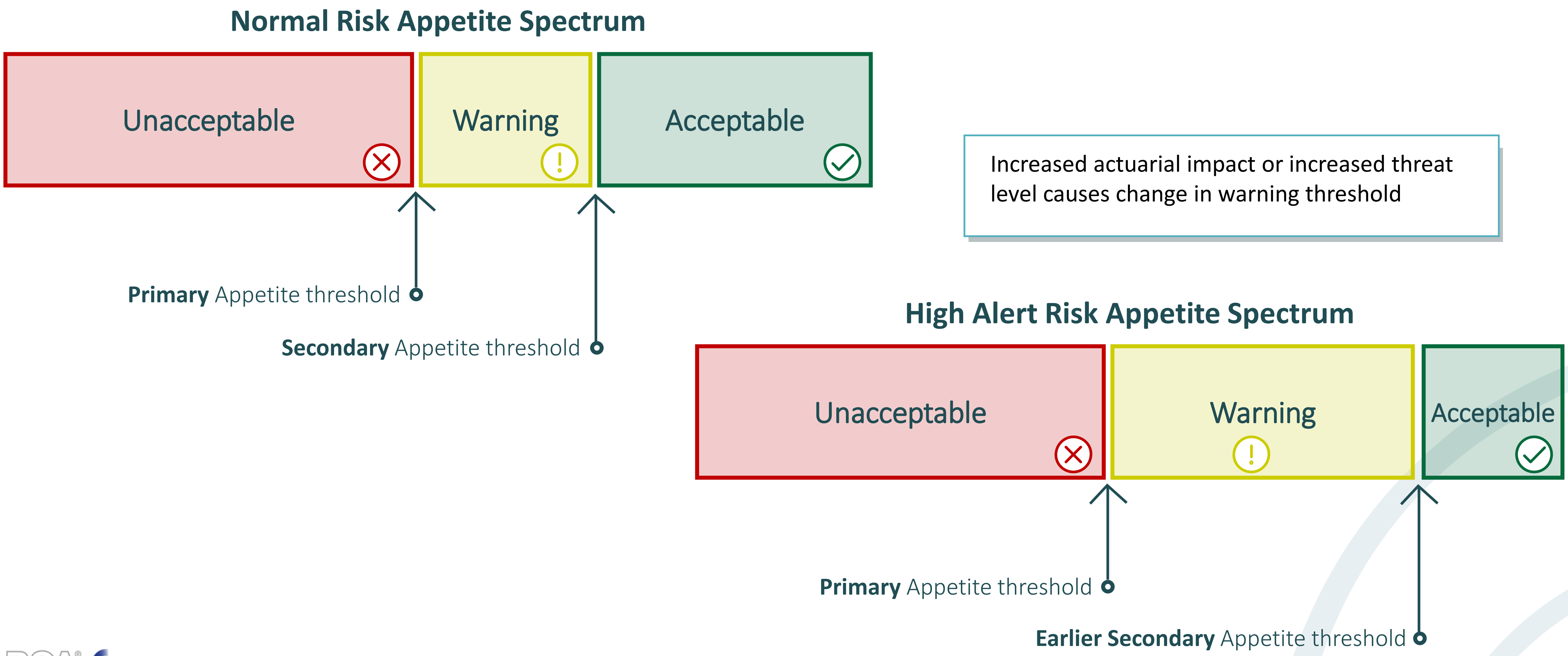
Warning

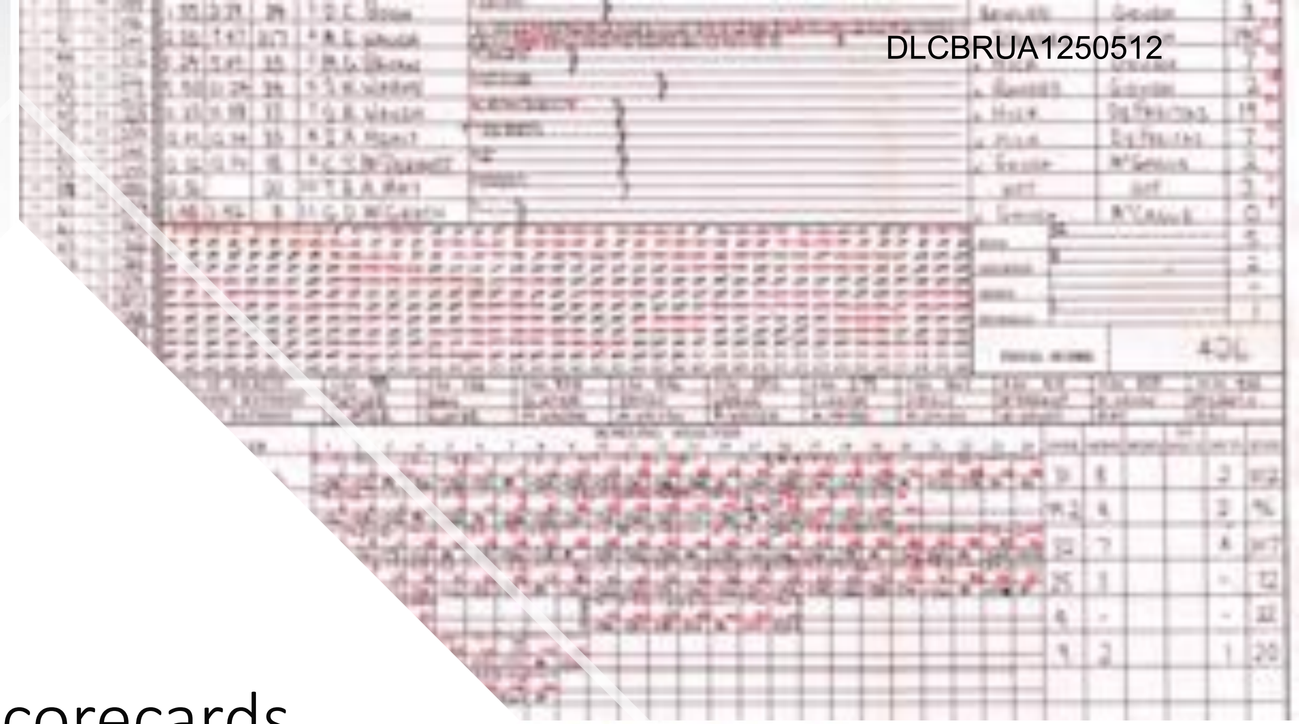
Iteration 1
Informed estimate result of controls deployment
Low process maturity, low confidence in rating

Retain actuarial data & historical rating data
Iteration 20
Validated result of controls deployment
High process maturity, high confidence in rating

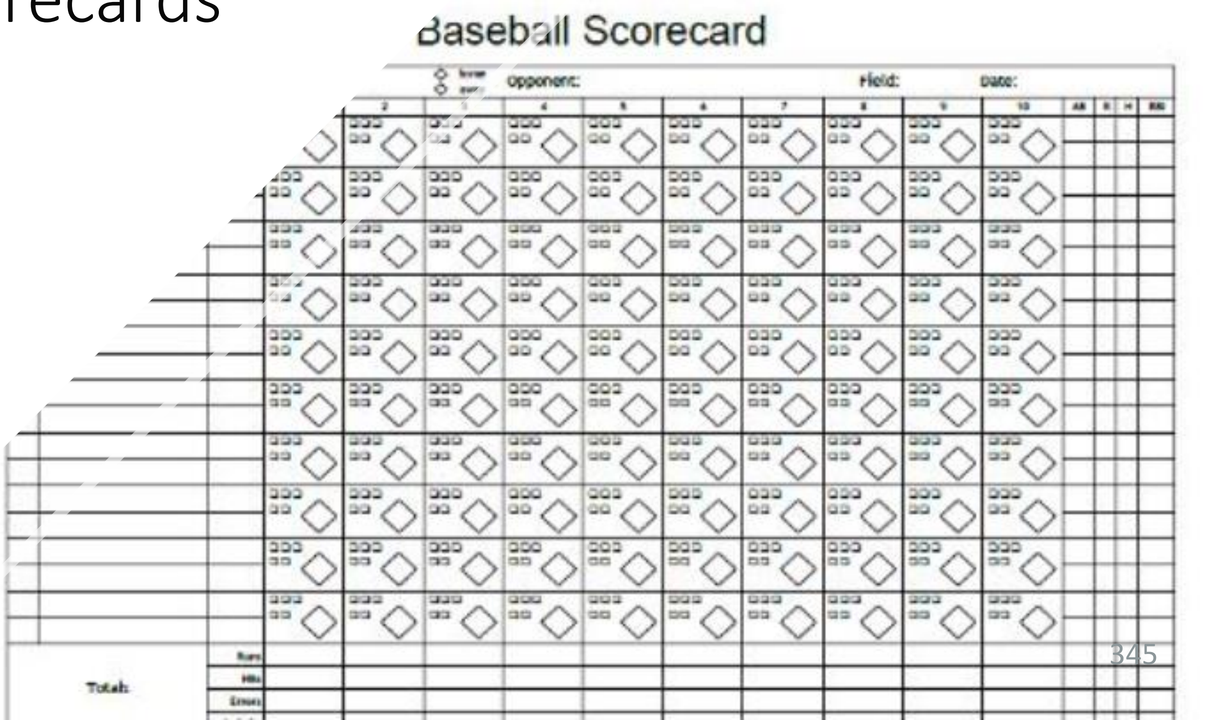
Measure – Effect of Controls & Enablers on Targets

Creation of dynamic appetite thresholds





Report Scorecards



Domain Lens

An authority's view through complexity

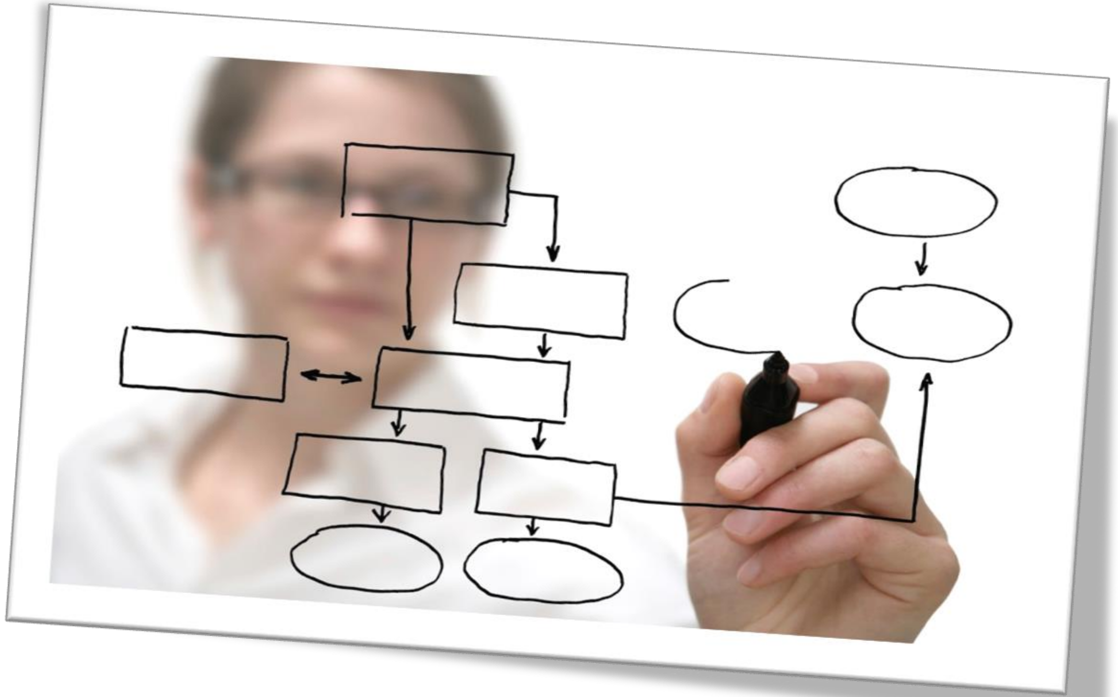
- Apply a lens to Enterprise complexity to view it in the most appropriate way for the stakeholder authority(ies) who are consumers of the Domain Architecture
- Consider the explicit and implicit domain traceability – Domains to represent:
  - Sets of assets or objectives
  - Risk types or categories
  - Capabilities or processes
  - Organisational units
  - Geographical or logical locations, or jurisdictions
  - Performance criteria or deadlines
- Consider the choice of Attributes Taxonomy
  - Already validated
  - Stakeholders already engaged
  - Emotional connection has been established
  - Common language enables collaborative modelling through varying perspectives

Report – Attribute-based Scorecards

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

Workshop A1-10

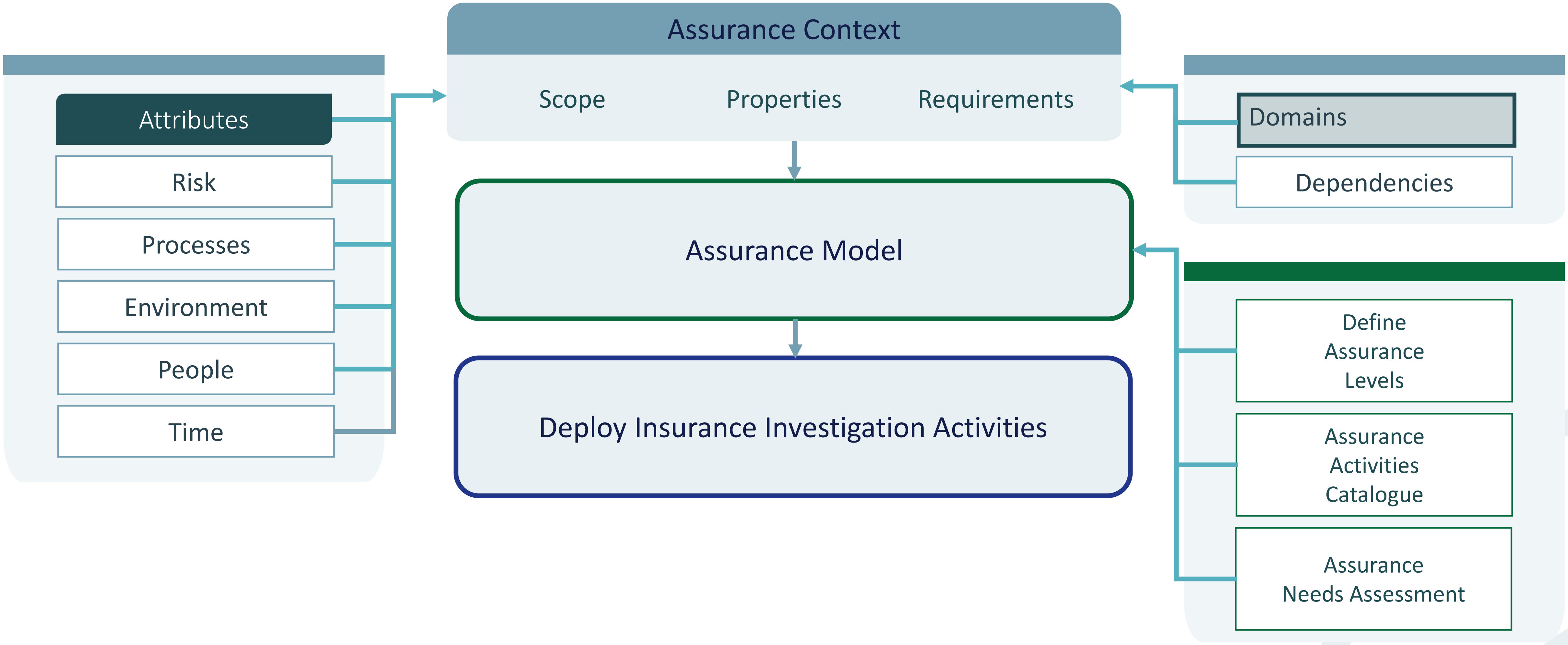
Risk Management



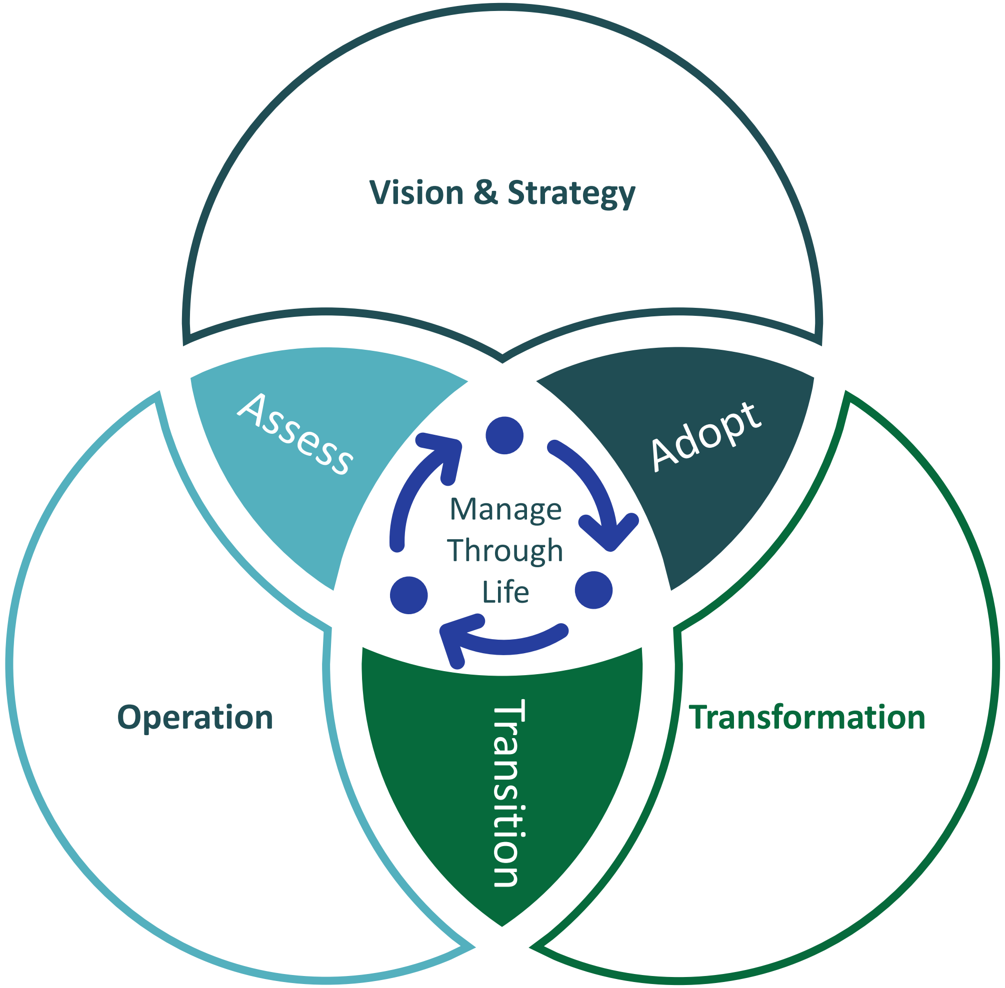
Risk Assurance

Section 13

Refresh - SABSA Assurance Framework



Refresh – Assurance is Required Through-life



DLCBRUA1250512

Refresh – SABSA Architecture Assurance

The SABSA Assurance Framework assures SABSA artefacts & processes

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Contextual	Enterprise Vision	Enterprise Risk	Enterprise Value Chain	Enterprise Governance	Enterprise Geography	Enterprise Time Dependence
Conceptual	Attributes Framework	Risk & Policy Frameworks	Process Framework	Governance & trust Frameworks		
Logical	Information	Policy	Information Processing & Services			
Physical	Data	Practices & Procedures	Data Comms & Mechanisms	Data & System		
Component	Products & Tools	Risk Standards	Protocol Standards			
Management	Delivery & Continuity	Risk Management	Process Management			

	What (Asset Perspective)	Why (Risk Perspective)	How (Process Perspective)	Who (People Perspective)	Where (Location Perspective)	When (Temporal Perspective)
Management	Delivery and Continuity	Risk Management	Process Management	Governance, Management	Environment Management	Time 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

	What	Why	How	Who	Where	When
Contextual	Analyse Requirements	Assess Risks	Manage Value Chain	Manage Relationships	Manage Facilities	Manage Time
Conceptual	Define Requirements	Define Risk Objectives	Manage Processes	Define Trust Relationships	Define Domains	Define Time Framework
Logical	Manage Information	Manage Policy	Manage Services	Manage Roles	Manage Domains	Manage Time Model
Physical	Manage Data	Manage Practices	Manage Mechanisms	Manage Access	Manage Infrastructure	Manage Processing Schedule
Component	Manage Configuration	Manage Standards	Manage Protocols	Manage Entities	Manage Addressing	Manage Timing

Refresh - Assurance Requirements & Target Properties

Provide confirmation, trust & confidence that architecture:

- Is business-driven
- Is traceable – that each artefact & process meets its explicit & implicit requirements
- Delivers the required capabilities to the defined performance level
- Operates within risk appetite
- Delivers the business benefits for which it was commissioned
- Is complete
- Is of adequate quality
- Is resilient & robust
- Is governable & is being governed properly
- Is manageable & is being managed properly
- Functions as intended
- Is fit-for-purpose
- Etc.

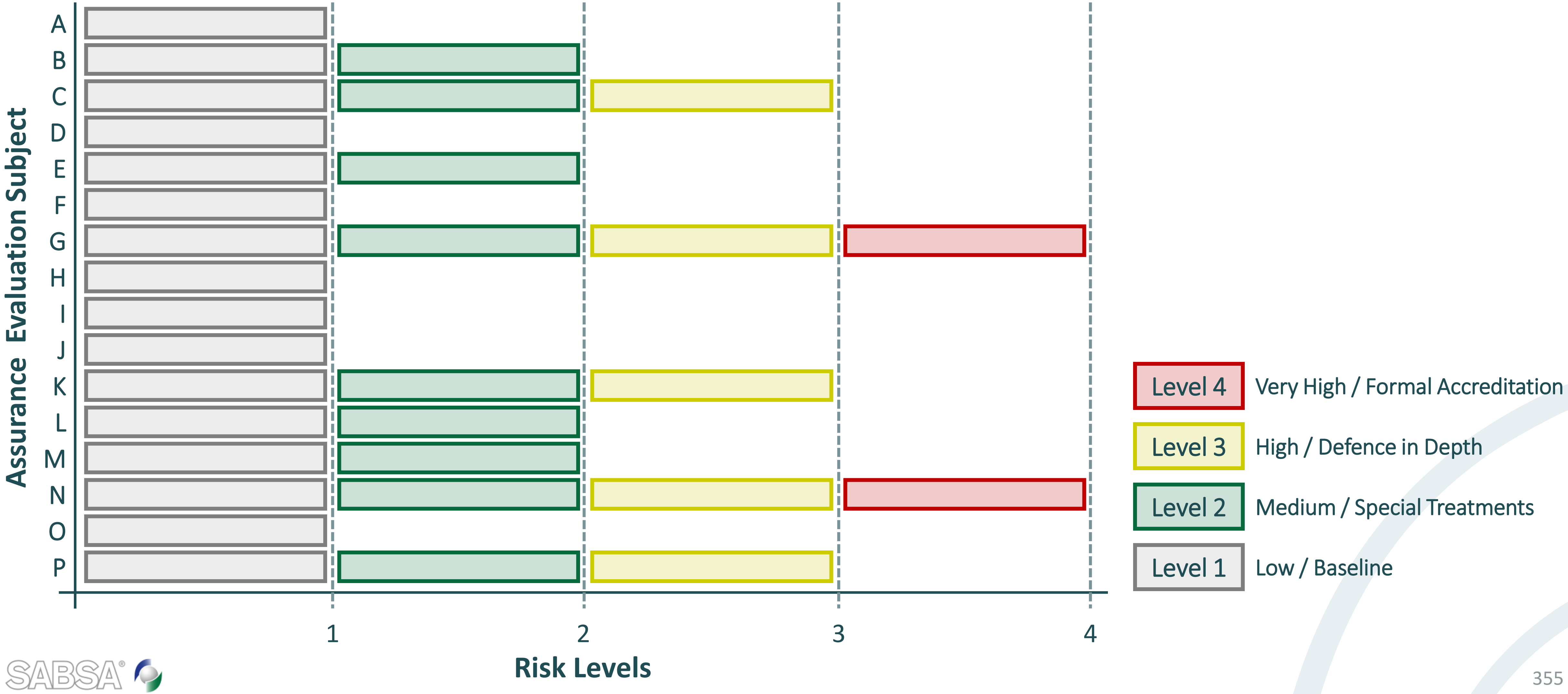
Refresh – The Need for Assurance Levels

The degree of assurance required is contextual & variable

Scope	Investigations can involve varied volumes of artefacts & processes
Depth	Investigations can involve varied levels of granularity and detail
Diligence	The degree of rigour to be applied in the investigation has varied levels of structure and formality

Refresh – Assessing Assurance Needs

Example – Assurance levels driven by risk standard



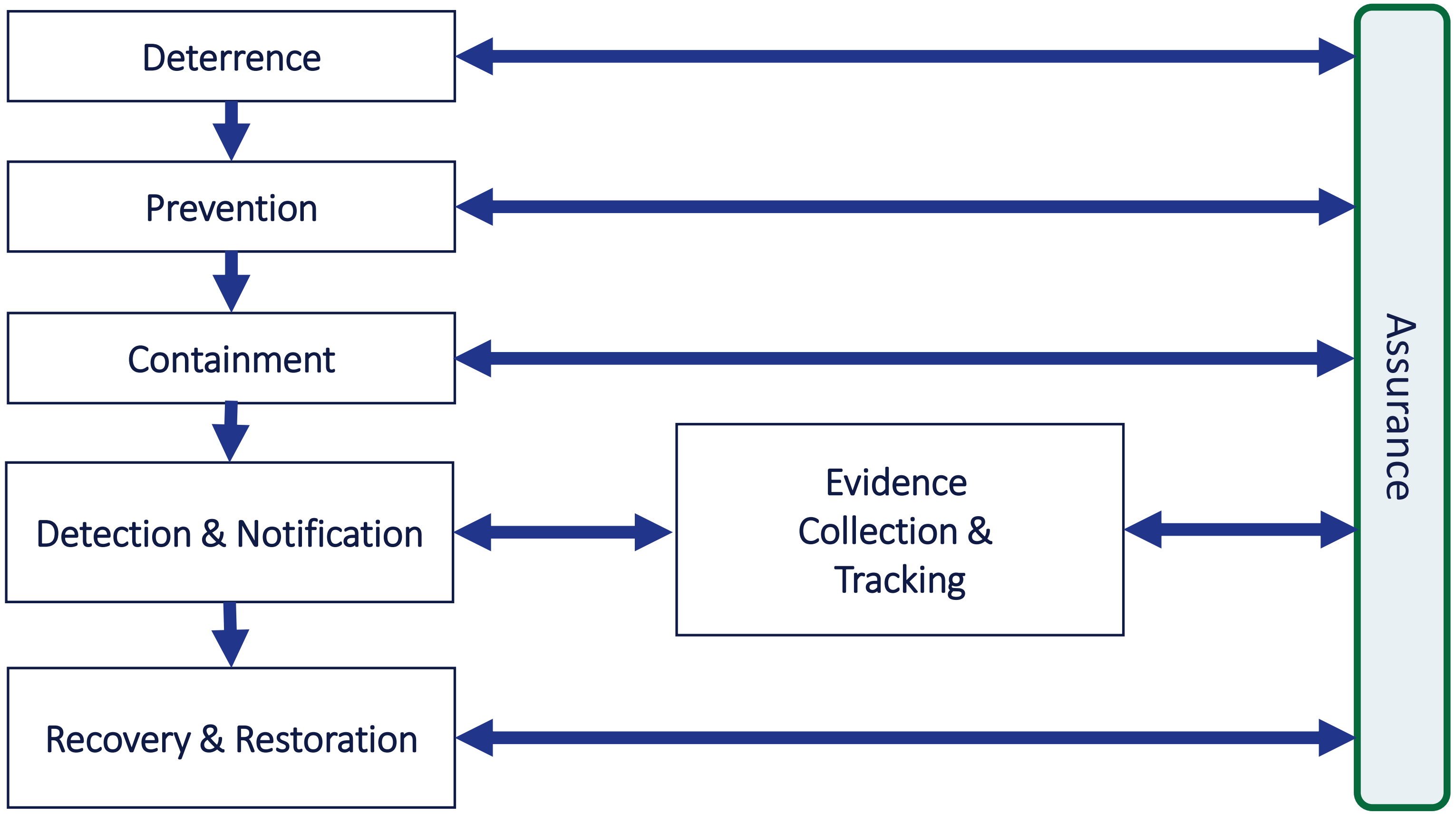
Assurance Levels Influences

Multiple influences determine assurance levels appropriate to context

Criticality	AND/OR Dependency	Inherent Risk	Residual Risk	Maturity	Freq of Change
Negligible	Or	Low	Low	5	Very Infrequent
Marginal	And	Medium	Medium	4	Infrequent
Critical		High	High	3	Frequent
Catastrophic		Very High	Very High	2	Very Frequent
				1	

Assurance Level Required
Low
Medium
High
Very High

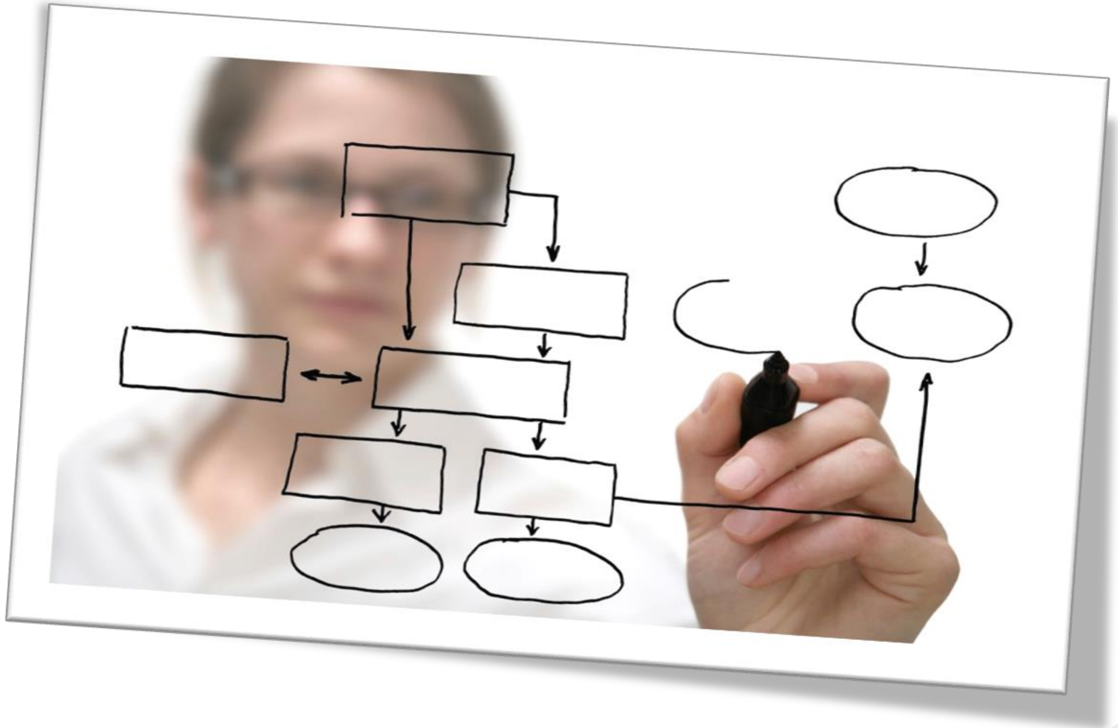
Refresh – Assurance of Defence-in-Depth Capability



SABSA®

Workshop A1-11

Assurance



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

SABSA Advanced A1 – Risk, Assurance & Governance

Thank You!

The SABSA Institute C.I.C