

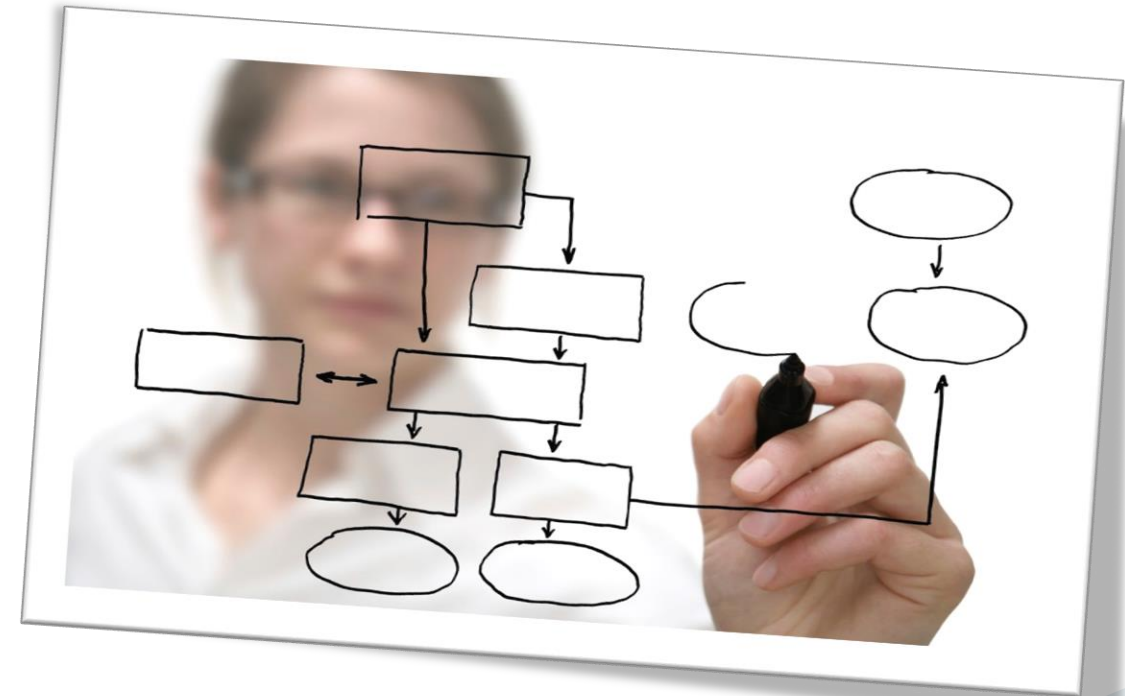
SABSA Foundation

SABSA Chartered Architect
Foundation Level (SCF)
v2.4.3

F1 – Security Strategy & Planning

Foundation Module Approach

- Presentation of concepts
- Workshops to apply techniques
- Peer groups
- Individual analysis



Module F1 – Course Outline

- Section 1 – SABSA Executive Summary
- Section 2 – SABSA Certification Programme
- Section 3 – SABSA Principles & Objectives
- Section 4 – SABSA Framework Overview
- Section 5 – Business Requirements & SABSA Attributes Profile Concept
- Section 6 – SABSA Risk & Opportunity Concept
- Section 7 – SABSA Policy Architecture
- Section 8 – SABSA Architecture Strengthening-Depth Engineering Concepts
- Section 9 – SABSA Governance, Roles & Responsibilities
- Section 10 – SABSA Domain Concepts
- Section 11 – SABSA Time & Performance Management

SABSA Executive Summary

Section 1

What is SABSA?

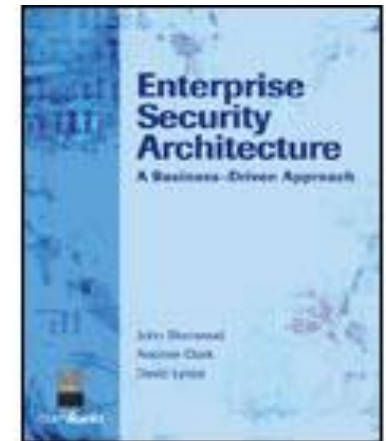
- Sherwood Applied Business Security Architecture
- Methodology for developing business-driven, risk and opportunity focused enterprise security & information assurance architectures, and for delivering security infrastructure solutions that traceably support critical business initiatives
- Comprised of a number of integrated frameworks, models, methods and processes

Applications of SABSA

- Enterprise Security Architecture
- Enterprise Architecture
- Individual solutions-based Architectures
- Risk & Opportunity Management
- Business requirements engineering & solutions traceability
- Information Assurance
- Governance, Compliance & Audit
- Policy Architecture
- Security management
- Service management (including performance, measures & metrics)
- Over-arching decision-making framework for end-to-end solutions
- Seamless security integration & alignment with other frameworks (including TOGAF, ITIL, ISO27000 series, Zachman, DoDAF, CobIT, etc.) and fills the gaps for security architecture and security management left by them

History

- Originally authored by John Sherwood 1995
- First used in global financial messaging 1995
- SABSA Textbook (CMP / Elsevier version) by Sherwood, Clark & Lynas, September 2005
- Adopted as UK MoD Information Assurance Standard 2007
- Certification programme introduced March 2007



Institute Status

- SABSA Institute registered as formal non-profit Community-of-Interest
 - Underwrites free-use status in perpetuity
 - Guarantees protected on-going development
 - Certifies & accredits official SABSA (method, training, certification, services, systems, architects & organisations) to provide confidence & assurance to industry, government & the professional community
 - Board of Trustees appointed 2014 with 9 Trustees from around the world

Growth & Standardisation

- Now used as a standard (formal & de facto) world-wide, including:
 - UK Ministry of Defence
 - Canadian Government
 - The Open Group
 - Incorporation into TOGAF Next Project
 - Security Service Catalog Project
 - ISACA, CISM Study Guides & Examinations
 - IT Governance Institute

Features & Advantages Summary

Feature	Advantage
Business-driven	Value-assured
Risk-focused	Prioritised & proportional responses
Comprehensive	Scalable scope
Modular	Agility - ease of implementation & management
Open Source (protected)	Free use, open source, global standard
Auditable	Demonstrates compliance
Transparent	Two-way traceability

SABSA Certification Programme

Section 2

Certification Roadmap Summary

- Competency-based framework utilises Bloom's Taxonomy of Cognitive Levels
- Three certification levels
 - Foundation (SCF)
 - Training modules F1 and F2
 - Multiple choice (closed book) examinations
 - Practitioner (SCP)
 - Foundation SCF plus:
 - Training module – any **one** Advanced Module from Institute's official curriculum
 - Written (open book) examinations – choose any 2 questions from 5
 - Master (SCM)
 - Practitioner (SCP) plus:
 - Training module – any **one** Advanced Module from Institute's official curriculum
 - Written (open book) examinations – choose any 2 questions from 5
 - Master Thesis

Taxonomy of Cognitive Levels (Foundation)

Competency Level	Skill Demonstrated	Competency Tests
1	Knowledge Observation and recall of information Knowledge of facts Knowledge of major ideas Mastery of subject matter Carry out research to find information	List, define, tell, describe, identify, show, label, collect, examine, tabulate, quote, name, find, identify
2	Comprehension Understand information Grasp meaning Translate knowledge into new context Interpret facts, compare, contrast Order, group, infer causes Predict consequences	Summarise, explain, interpret, contrast, predict, associate, distinguish, estimate, differentiate, discuss, extend



Foundation examination questions test these skills by means of these behaviors



Question Domains / Competency Map

- Foundation level examination questions are evenly distributed throughout the SABSA Competency Map
- There are **six** question domains, directly correlated to the **columns** of the SABSA Matrices:
 1. What (assets) (also includes questions about SABSA as a whole)
 2. Why (risk & motivation factors)
 3. How (process factors)
 4. Who (people factors)
 5. Where (location factors)
 6. When (temporal factors)

F1 Question Domains / Materials Cross-reference

1. What (assets) – F1 sections 3, 4 & 5
2. Why (risk & motivation factors) – F1 sections 6 & 7
3. How (process factors) – F1 section 8
4. Who (people factors) – F1 section 9
5. Where (location factors) – F1 section 10
6. When (temporal factors) – F1 section 11

Foundation Level Examination Format

- There are 2 Foundation level examination modules
 - F1 – SABSA Security Strategy & Planning
 - F2 – SABSA Security Management & Design
- Closed book examination format
- Each consists of 48 questions
- Time limit is 60 minutes per paper
 - 25% (15 extra minutes per module) can be requested by candidates for whom English is not the first language
- Multiple choice question format
 - 4 answer options – A, B, C and D
- Questions randomly selected
 - The question set is unique per examination session
- Each module contains 8 questions from each of the 6 knowledge domains
 - The question order is randomised – domains are not identified

Foundation Modules Success Criteria

- To obtain your SCF credential:
 - You must attain a total score of **no less than 75%** (36 correct answers out of 48) in **BOTH** examination modules
- **AND**
 - You must attain a score of **no less than 60%** in at least **4 out of 6** knowledge domains in **EACH** examination module

Taxonomy of Cognitive Levels (Practitioner)

Competency Level	Skill Demonstrated	Competency Tests
3	Application Use information Use methods, concepts, theories in new situations Solve problems using required skills or knowledge	Apply, demonstrate, calculate, complete, illustrate, show, solve, examine, modify, relate, change, classify, experiment, discover
4	Analysis Seeing patterns Organising of parts Recognition of hidden meanings Identification of components	Analyse, separate, order, connect, classify, arrange, divide, compare, select, infer



Practitioner examination questions test these skills by means of these behaviors



Taxonomy of Cognitive Levels (Master)

Competency Level	Skill Demonstrated	Competency Tests
5	Synthesis Use old ideas to create new ones Generalise from given facts Relate knowledge from several areas Predict, draw conclusions	Combine, integrate, modify, rearrange, substitute, plan, create, build, design, invent, compose, formulate, prepare, generalize, rewrite
6	Evaluation Compare and discriminate between ideas Assess value of theories, presentations Make choices based on reasoned argument Verify value of evidence Recognise subjectivity	Assess, evaluate, decide, rank, grade, test, measure, recommend, convince, select, judge, discriminate, support, conclude



Practitioner examination questions test these skills by means
of these behaviors supplemented by a Masters Thesis



Competency Framework

Knowledge Domains	Detailed Knowledge Elements	Competency Level					
		Knowledge	Comprehension	Application	Analysis	Synthesis	Evaluation
What (Assets)	Detailed K.E. 1.1						
	Detailed K.E. 1.2						
	Detailed K.E. 1. <i>n</i>						
Why (Motivation)	Detailed K.E. 2.1						
	Detailed K.E. 2.2						
	Detailed K.E. 2. <i>n</i>						
How (Process)	Detailed K.E. 3.1						
	Detailed K.E. 3.2						
	Detailed K.E. 3. <i>n</i>						
Who (People)	Detailed K.E. 4.1						
	Detailed K.E. 4. <i>n</i>						
Where (Location)	Detailed K.E. 5.1						
	Detailed K.E. 5.2						
	Detailed K.E. 5. <i>n</i>						
When (Time)	Detailed K.E. 6.1						
	Detailed K.E. 6.2						
	Detailed K.E. 6. <i>n</i>						



Foundation Level



Practitioner Level



Master Level

SABSA® | Certification Roadmap

CERTIFICATION LEVEL	EDUCATION REQUIREMENT		EXAMINATION REQUIREMENT
<div> FOUNDATION LEVEL SCF You need to attend TWO foundation modules...</div>	Module F1 - SABSA Security Strategy & Planning		...and pass multiple choice exams for modules F1 & F2
	Module F2 - SABSA Security Service Management & Design		
You need to be SCF certified before becoming SCP certified			
<div> PRACTITIONER LEVEL SCP You need to attend any ONE advanced module...</div>	Module A1 (5 days) SABSA Advanced Risk Assurance & Governance	Module A4 (5 days) SABSA Advanced Incident, Monitoring & Investigations Architecture	...and pass corresponding advanced written exam for the module you attend
	Module A2 (5 days) SABSA Advanced Architecture Programme Management	Module A5 (5 days) SABSA Advanced Business Continuity & Crisis Management	
	Module A3 (5 days) SABSA Advanced Architectural Design		
You need to be SCP certified before becoming SCM certified			
<div> MASTER LEVEL SCM You need to attend any ONE additional advanced module...</div>	Module A1 (5 days) SABSA Advanced Risk Assurance & Governance	Module A4 (5 days) SABSA Advanced Incident, Monitoring & Investigations Architecture	...and pass additional advanced written exam and write a thesis
	Module A2 (5 days) SABSA Advanced Architecture Programme Management	Module A5 (5 days) SABSA Advanced Business Continuity & Crisis Management	
	Module A3 (5 days) SABSA Advanced Architectural Design		
<div>OR... You need to attend any TWO special seminars...</div>	Seminar S1 (2 days) SABSA Security Architecture for ITIL Environments	Seminar S4 (2 days) SABSA Security Architecture for Cloud Environments	
	Seminar S2 (2 days) SABSA Security Architecture for TOGAF Environments	Seminar S5 (2 days) SABSA for Enterprise Risk Management	
	Seminar S3 (2 days) SABSA Security Architecture for Classified Environments	Seminar S6 (2 days) SABSA for Audit, Compliance & Assurance	

SABSA Principles & Objectives

Section 3

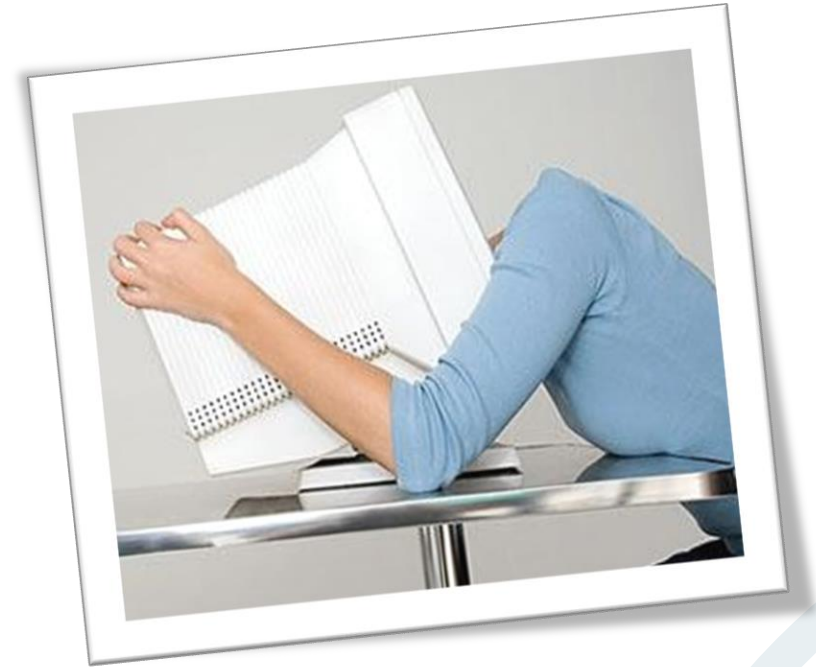
Section 3 Competency Objectives

Competency / Question Domain 1 – What (Assets)

Knowledge Element	Knowledge Competency	Comprehension Competency
Enterprise Security Architecture Framework	Describe the SABSA concept of Enterprise	Articulate the Enterprise concept in terms of business benefit
	Describe the SABSA concept of Security	Articulate the Security concept in terms of business benefit
	Describe the SABSA concept of Architecture	Articulate the Architecture concept in terms of business benefit
	Describe the role of an architectural Framework	Articulate the role of an architectural framework in terms of business benefit
Guiding Principles	List SABSA guiding principles, drivers & constraints	Explain consequences & benefits of SABSA guiding principles, drivers & constraints
Holistic Approach	Identify how SABSA resolves the historical, tactical & silo-ed approach to security	Explain the engineering concept of the 'Complex System' in the SABSA approach to security
Features, Advantages & Benefits	List the 7 primary features & advantages of the SABSA approach to Enterprise Security Architecture	Interpret the features & advantages as benefits to individual stakeholders

Legacy of Security as a Restraint

- ‘Badge, gun & guard-dog’ attitude
- More passwords
- More rules
- More limitations on access
- More firewalls & barriers
- More difficulties
- Can’t get on with the real business



A Bad Reputation

- “The Business Prevention Department”



The Problem of Operational Imbalance



History of Component-based Tactical Solutions

- A tradition of “technically-led”, IT-based, security projects
- No real business alignment
- No long-term strategy
- No real standardization
- No framework within which to design solutions for new problems
- Point solutions for tactical problems



Example – Component Solutions Failing

Threat	Inappropriate or illegal images on corporate machines
Impact	Legal liability & proceedings
Vulnerability	We don't scan for or prevent illegal content
Control	Filter content at the gateway

Example – Component Solutions Fail

- But then this happened...



- Each of these devices (and those to come in future) by-pass the technology-specific gateway content filter
- So the gateway filtering solution no longer solves the problem and we must find (and pay for) a new one each time technology changes
- An architected future-proof solution would have utilised the presentation layer – the issue is '**display** of inappropriate images' and the proper solution could detect them whatever the source of the images (today or in the future)

Tactical Component-led Solutions Cost More

- Continuous re-invention of the wheel
- Operations costs in a diverse environment
- System support - diversity of skills
- User support costs and lost productivity
- Integration difficulties with diverse systems
- Lack of flexibility - no broad vision
- Scaling difficulties
- The COTS dilemma

Why ESA Programmes Fail

- Too much emphasis on technology
 - Not enough attention to solving business problems
- Diverse technical environments
 - Increased total cost of ownership
- Silo approach to security and risk management
 - Lack of understanding of the interactive nature of risks
 - Lack of risk aggregation at the enterprise level
 - Lack of alignment with business strategy

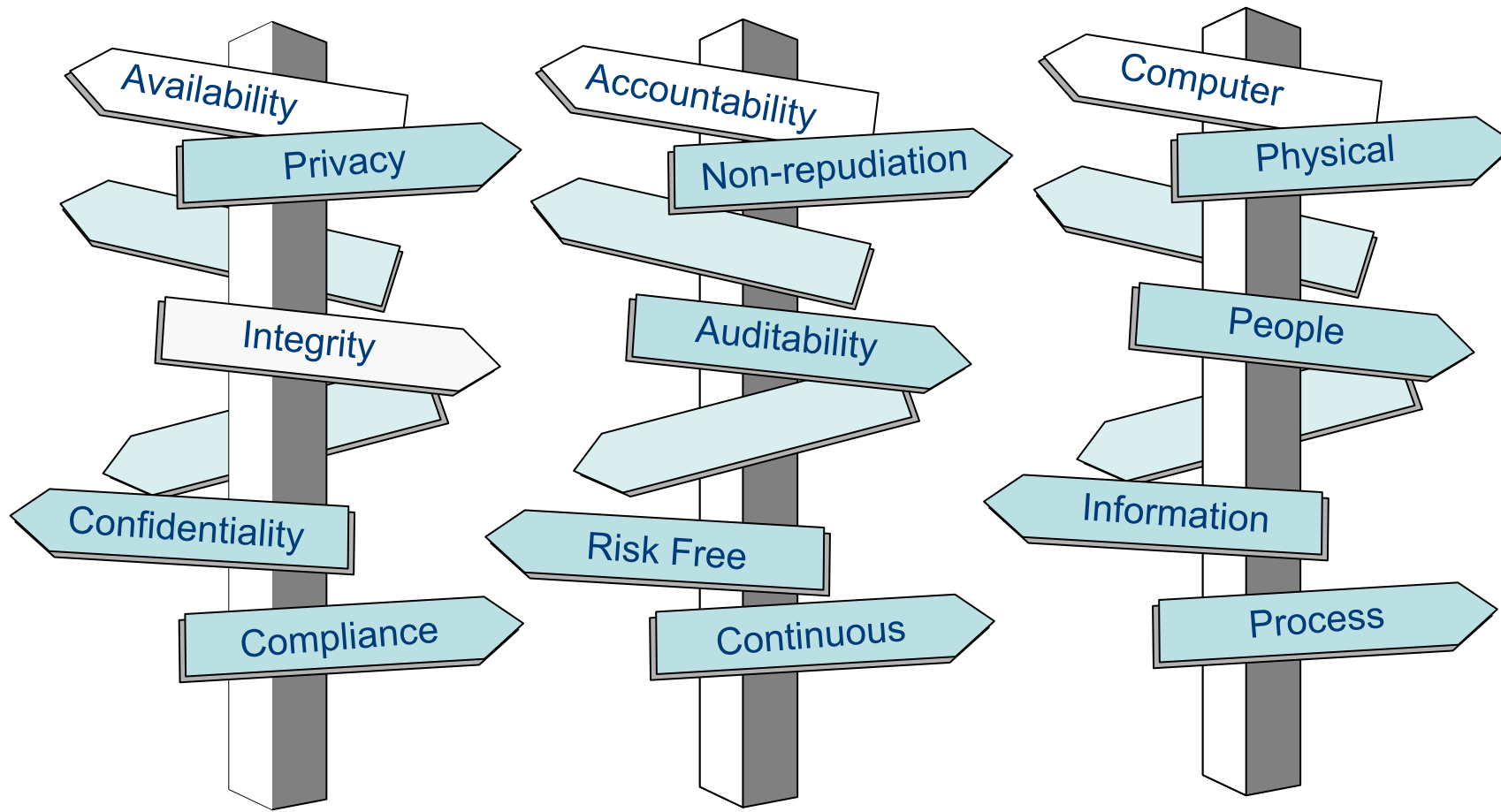
ESA Success Takes More Than Technology

- Good understanding of business needs and risks
- Strategic architectures
- Project Management
- Systems integration
- Security management policies and practices
- Enterprise-wide security culture and infrastructure

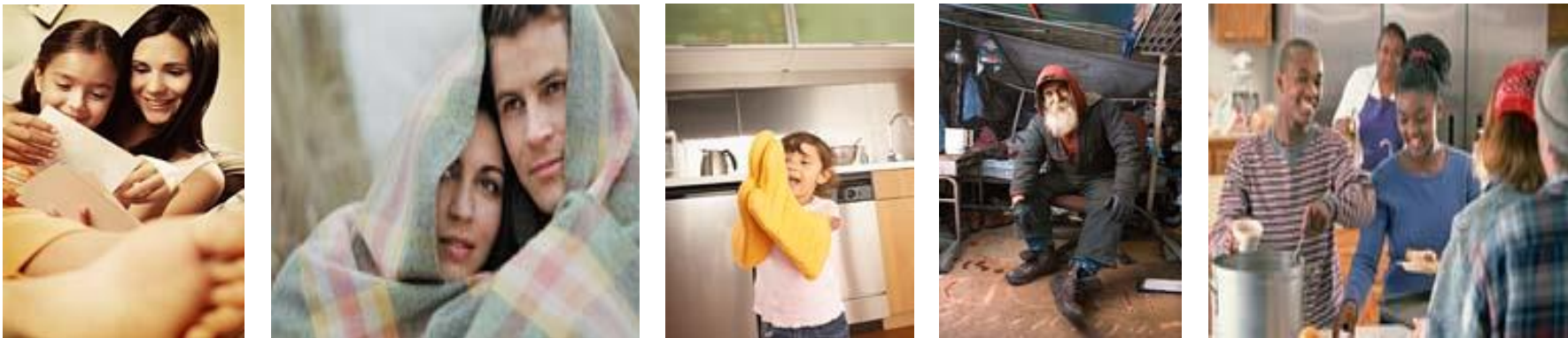
Concept of Security?

- “To provide confidence & assurance”?
 - business can depend upon and trust our technologies
 - business is not exposed to unacceptable risk
 - business can meet its objectives and grasp opportunities
- “To protect business assets”?
 - technology and are our use of it is ‘secure’
 - information and our use of it is ‘secure’
- To support the business objectives!
 - what is our mission?
 - what are our strategic, tactical & operational business objectives?

Security Can Be Difficult To Define



Dynamic Contextual Interpretation



Security is a Property of Something Else

- Security does not exist in isolation
- Relative to a specific business context
- There is no absolute scale
- 'Secure' has no intrinsic meaning
- What do you mean by 'secure'?
- What are you trying to protect (your assets)?
- Against what threats?
- What would be the business impact?
- Does your business have vulnerabilities?
- What is your risk appetite?

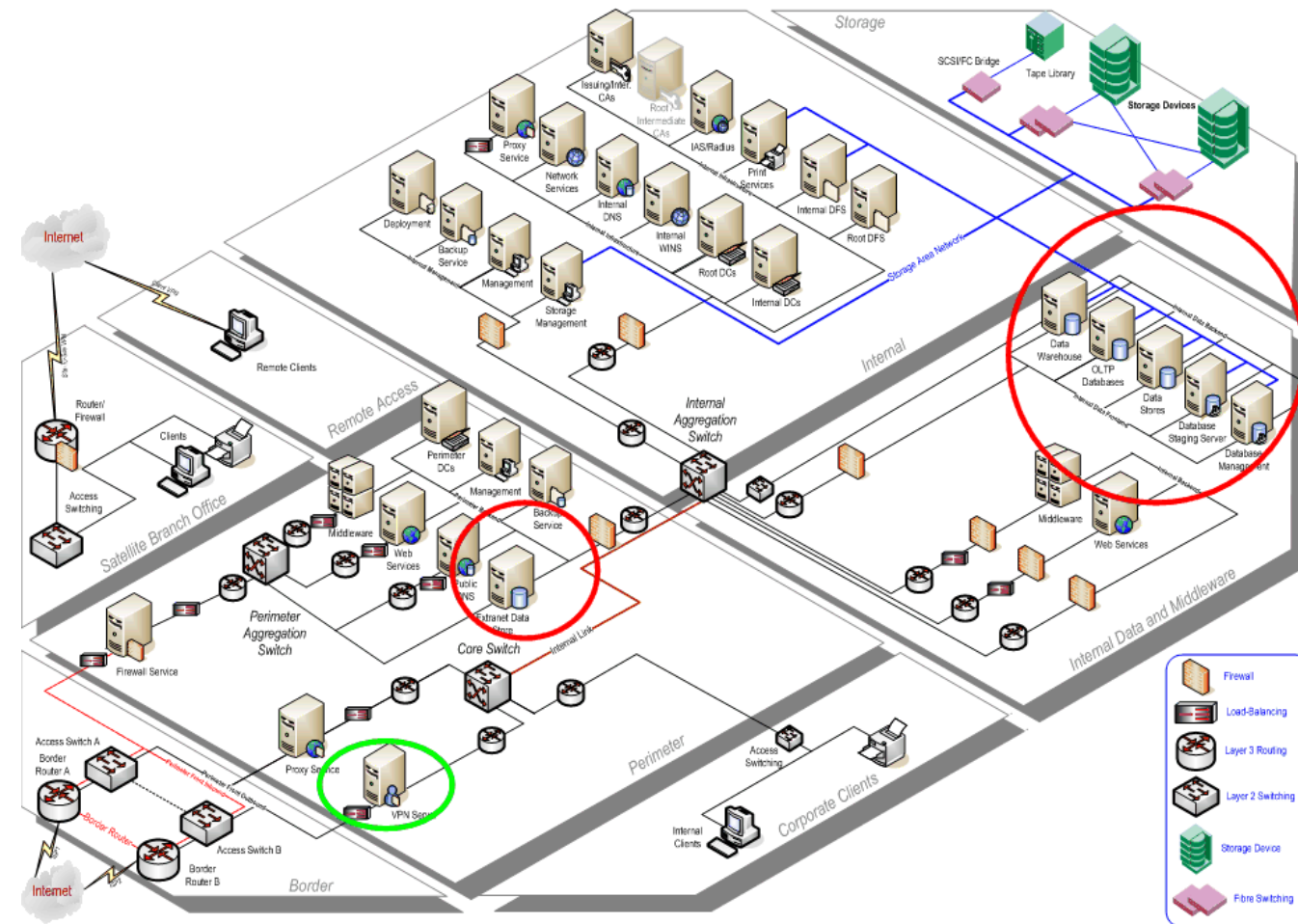
The Real Role of Architected Security

- Restricting security interpretation to only confidentiality, integrity & availability limits our ability to communicate its full purpose & value to the business:
- Enabling business
- Enabling technology
- Enabling change
- Adding value to the core product / service
- Empowering business partners
- Protecting relationships & leveraging trust

Concept of Enterprise

- The treatment of an organisation as a single entity
 - Rather than as a set of cooperating departments
 - Embraces the end-to-end nature of business processes
 - Applies to commercial firms, public services or charitable trusts
- Aims to optimise all parts of the organisation in a coherent way
 - Not just local optimisation
- Delivers improved overall performance
 - Competitiveness
 - Service excellence
 - Diversification of risks for optimal risk management

Concept of Architecture



Architecture Supports Business Strategy

- Every morning in Africa, a Gazelle wakes up. It knows it must run faster than the fastest lion.....or it will be killed.
- Every morning in Africa, a Lion wakes up. It knows it must run faster than the slowest Gazelleor it will die of starvation.
- Is it better to be a Lion or a Gazelle?



Business View – Survival Strategy

When the sun comes up in Africa, it doesn't matter what shape you are:
If you want to survive, what matters is that you'd better be running!

The Importance of a Framework



Architecture Framework

- A consistent set of principles, policies, capabilities and standards that sets the direction and vision for the development and operation of the organisation's business information systems so as to ensure alignment with and support for the business needs

Benefits of an Architecture Framework

- Managing complexity
- Maintaining integrity of design in large complex developments
- Providing a roadmap for all to follow
- Lowering the total cost of ownership
- Good integration of technical and procedural solutions to business problems
- Rational framework for making design decisions & solving new problems
- Attaining an appropriate balance between strategy, tactics & operations
- Resolving conflicting objectives & priorities
- Predictability, flexibility & agility



Architecture: Drivers & Constraints

- The overall business goals for the system(s)
- The functional requirements of the system – what should it do?
- The materials and/or components available for constructing systems
- The environment in which the system will be built and used
- The skills of the people who will build the system
- The skills of the people who will use the system
- The costs incurred and benefits delivered

SABSA Architecture Guiding Principles

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

SABSA Architecture Guiding Principles

- Architecture must meet YOUR unique set of business requirements
- Architecture must provide sufficient flexibility to incorporate choice and change of policy, standards, practices, or legislation
 - ISO 27001, ACSI 33, DSD ISR, HIPAA, ISF Code, CobIT, SOx, PCI, NIST, etc
 - ITIL, TNN, ISO 9000, etc
 - ISO 31000, Basel ii, ISO 27005, etc
 - Balanced scorecards, capability maturity models, ROI, NPV, etc
- When a question is asked starting with “Is this Architecture compatible / compliant with....?” a good Architecture framework will automatically have the answer “Yes”
 - A good architecture provides the roadmap for joining together all of your requirements, whatever they might be, or become
 - It does not replace ITIL or ISO 27001 or NIST etc but rather enables their deployment and effective integration into the corporate culture

Information Security is....as strong as the weakest link



An Architected Complex System



A Layered Framework

- A framework within which many people can work harmoniously and all act toward the goal of a single design authority
- “Achieved through layering techniques and modularisation”



ESA Scope

- True architecture never happens bottom-up
- Enterprise security architecture resolves the business problems caused by a long history of piecemeal implementations
- Business strategy for security is closely linked to the goals of Operational Risk Management
- As part of a business strategy, security must balance with other requirements:
 - Usability, inter-operability, integration, supportability
 - Fast time-to-market, scalability, re-usability
 - Cost effectiveness
- Dealing with conflicting objectives

Architecture Needs a Holistic Approach

- Do we understand all of the requirements?
- Do we have a design philosophy?
- Do we have all of the components?
- Do these components work together?
- Do they form an integrated system?
- Does the system run smoothly?
- Are we assured that it is properly assembled?
- Is the system properly tuned?
- Do we operate the system correctly?
- Do we maintain the system?
- Do we comply with the rules?

Information Security Architecture

- To provide all the links in the chain
- To ensure that security is provided through a fully integrated systems approach
- To ensure that security services are properly managed
- To ensure that security services are properly delivered & supported
- To ensure that security meets the needs of the business

Being a Successful Security Architect

- An architect's skill set differs from that of a plumber
- Broad vision of the business requirements
 - More than just 'security'
- Think in business terms at all times
 - Why are we doing this?
 - What are we trying to achieve for the business?
- Good communication skills
 - You need constantly to explain, to educate, to debate, to sell ideas and to influence key people
- Strength of character
 - Stand up to those who lack understanding of strategic architecture
 - The going can be tough and lonely

SABSA Security Architecture Framework

Features, Advantages & Benefits – Chairman/Board View

Feature	Advantage	Benefit
Business-driven	Value-assured	Protects shareholder value
Risk-focused	Prioritised & proportional	Optimises shareholder risk & aligns with risk appetite
Comprehensive	Scalable scope	Addresses all shareholder concerns
Modular	Agility	Enables flexibility to meet dynamic market & economic conditions
Open Source	Free use, standard	Guarantees perpetuity of return on investment
Auditable	Demonstrates compliance	Demonstrates compliance to regulators & external auditors
Transparent	Two-way traceability	Supports market transparency & disclosure

SABSA Security Architecture Framework

Features, Advantages & Benefits – CEO View

Feature	Advantage	Benefit
Business-driven	Value-assured	Protects corporate reputation
Risk-focused	Prioritised & proportional	Meets corporate governance requirements
Comprehensive	Scalable scope	Meets enterprise –wide requirements
Modular	Agility	Enables fast time to market with business solutions
Open Source	Free use, standard	Provides assurance through industry standard
Auditable	Demonstrates compliance	Ensures a smooth & successful external & regulatory audit process
Transparent	Two-way traceability	Provides a clear view of expenditure and value returned

SABSA Security Architecture Framework

Features, Advantages & Benefits – CFO View

Feature	Advantage	Benefit
Business-driven	Value-assured	Ensures efficient return on investment
Risk-focused	Prioritised & proportional	Improves predictability & consistency
Comprehensive	Scalable scope	Supports scalable, granular budgeting
Modular	Agility	Facilitates effective management of capital & operational costs
Open Source	Free use, standard	Eliminates expensive & on-going license fees
Auditable	Demonstrates compliance	Minimises cost of management time dealing with audit processes
Transparent	Two-way traceability	Enables full auditability for effectiveness of expenditure

SABSA Security Architecture Framework

Features, Advantages & Benefits – COO View

Feature	Advantage	Benefit
Business-driven	Value-assured	Focuses on performance management
Risk-focused	Prioritised & proportional	Enables process improvement
Comprehensive	Scalable scope	Provides end-to-end process coverage
Modular	Agility	Integrates legacy and future environments
Open Source	Free use, standard	Simplifies recruitment and training
Auditable	Demonstrates compliance	Minimises adverse effects of audit findings on performance targets
Transparent	Two-way traceability	Measures efficiency & effectiveness of processes & resources

SABSA Security Architecture Framework

Features, Advantages & Benefits – CRO View

Feature	Advantage	Benefit
Business-driven	Value-assured	Enables flexible fit with industry regulations
Risk-focused	Prioritised & proportional	Supports enterprise risk & opportunity management
Comprehensive	Scalable scope	Enables a fully-integrated risk management strategy
Modular	Agility	Enables incrementally increasing maturity
Open Source	Free use, standard	Provides global acceptability for auditors & regulators
Auditable	Demonstrates compliance	Ensures that compliance risk is effectively managed
Transparent	Two-way traceability	Demonstrates current state, desired state of compliance levels

SABSA Security Architecture Framework

Features, Advantages & Benefits – CIO View

Feature	Advantage	Benefit
Business-driven	Value-assured	Enables a digital transformation-age business
Risk-focused	Prioritised & proportional	Identifies information exploitation opportunities
Comprehensive	Scalable scope	Sustains through-life information architecture
Modular	Agility	Enables technology-neutral information management strategies
Open Source	Free use, standard	Provides a future-proof framework for information management
Auditable	Demonstrates compliance	Facilitates smooth & successful audits of systems & processes
Transparent	Two-way traceability	Encourages fully integrated people-process-technology solutions

SABSA Security Architecture Framework

Features, Advantages & Benefits – CISO View

Feature	Advantage	Benefit
Business-driven	Value-assured	Facilitates alignment of security goals with business goals
Risk-focused	Prioritised & proportional	Facilitates prioritisation of security and risk-control solutions
Comprehensive	Scalable scope	Ensures all business security & control concerns are addressed
Modular	Agility	Enables a project-focused approach to security development
Open Source	Free use, standard	Provides a sustainable framework for security integration
Auditable	Demonstrates compliance	Supports security, risk & opportunity review process
Transparent	Two-way traceability	Provides traceability of business-aligned security implementations

SABSA Security Architecture Framework

Features, Advantages & Benefits – CTO/Architect View

Feature	Advantage	Benefit
Business-driven	Value-assured	Leverages the full power of information technology
Risk-focused	Prioritised & proportional	Manages information system risk
Comprehensive	Scalable scope	Applies at any project size or level of complexity
Modular	Agility	Provides a holistic and integrated architectural approach
Open Source	Free use, standard	Avoids vendor dependence and lock-in
Auditable	Demonstrates compliance	Improves relationship and interactions with auditors and reviewers
Transparent	Two-way traceability	Verifies justification and completeness of technical solutions

SABSA Framework Overview

Section 4

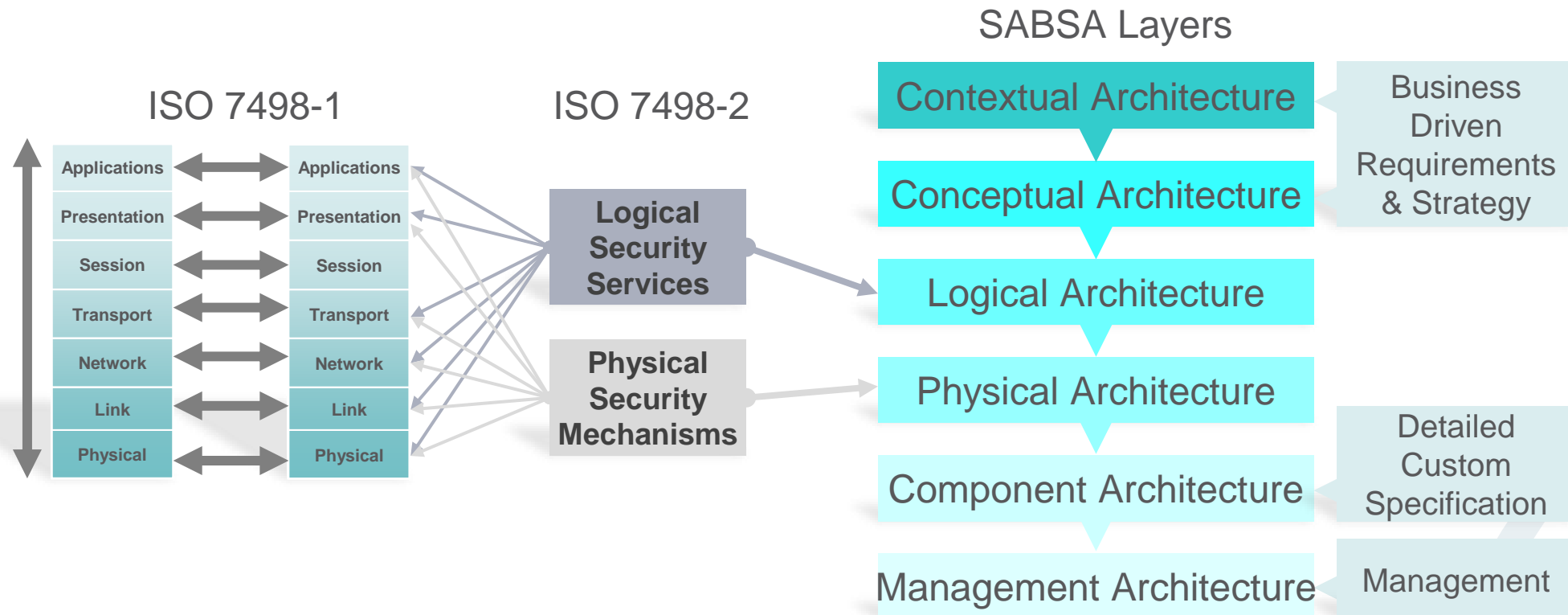
Section 4 Competency Objectives

Competency / Question Domain 1 – What (Assets)

Knowledge Element	Knowledge Competency	Comprehension Competency
The SABSA Matrix	List the 6 views of SABSA Architecture	Differentiate between the 6 Architecture views
	Name the 6 layers of the SABSA Architecture Matrix	Differentiate between the 6 Matrix layers
	Label the 6 columns of the SABSA Matrices	Differentiate between the 6 Matrix columns
	Identify the position of key deliverables in the SABSA Matrices	Interpret the structure of the SABSA Architecture Matrix to contrast the positions of key deliverables
The Traceability Concept	Describe the overlaying of layer 6 to create the Management Matrix	Differentiate between deliverables of the SABSA Architecture Matrix & activities of the SABSA Management Matrix
	Describe the traceability concept and its benefits	Summarise the applications of layer-mapping to provide traceability through architecture layers

SABSA Built to Drive Complex Design Solutions

- SABSA influenced in 1995 by need to enhance ISO 7498-2



SABSA Architecture Views

Business View	Contextual Architecture
Architect's View	Conceptual Architecture
Designer's View	Logical Architecture
Builder's View	Physical Architecture
Tradesman's View	Component Architecture
Manager's View	Management Architecture

Kipling's "Six Honest Serving Men"

I keep six honest serving-men
(They taught me all I knew);
Their names are What and Why
and When
And How and Where and Who.
I send them over land and sea,
I send them east and west;
But after they have worked for me,
I give them all a rest.
I let them rest from nine till five,
For I am busy then,
As well as breakfast, lunch, and
tea,

For they are hungry men.
But different folk have different
views;
I know a person small-
She keeps ten million serving-
men,
Who get no rest at all!
She sends them abroad on her
own affairs,
From the second she opens her
eyes-
One million Hows, two million
Wheres,
And seven million Whys!

Vertical Analysis: Six Honest Serving Security Men

What	<p>What are we trying to do at this layer?</p> <p>The assets, goals & objectives to be protected & enhanced</p>
Why	<p>Why are we doing it?</p> <p>The risk & opportunity motivation at this layer</p>
How	<p>How are we trying to do it?</p> <p>The processes required to achieve security at this layer</p>
Who	<p>Who is involved?</p> <p>The people and organisational aspects of security at this layer</p>
Where	<p>Where are we doing it?</p> <p>The locations where we are applying security at this layer</p>
When	<p>When are we doing it?</p> <p>The time related aspects of security at this layer</p>

The Business View (Contextual Layer)

What	Business Goals & Decisions: Bus. Value; Taxonomy of Bus. Assets, Goals & Objectives, Success Factors, Targets
Why	Business Risks: Opportunities & Threats
How	Business Processes: Business Value Chain; Business Capabilities
Who	Business Governance: Organisational Structure & the Extended Enterprise
Where	Business Geography: Inventory of Buildings, Sites, Territories, Jurisdictions, etc
When	Business Time Dependence: Time dependencies of Business Goals and Value Creation

The Architect's View (Conceptual Layer)

What	Business Value & Knowledge Strategy: Business Attributes Taxonomy & Profile (with integrated performance targets)
Why	Risk Management Strategy & Objectives: Enablement & Control Objectives; Policy Architecture; Risk Categories; Risk Management Strategies; Risk Architecture; Risk Modelling Framework; Assurance Framework
How	Strategies for Process Assurance: Inventory of all Operational Processes (IT, Industrial & manual; Process Mapping Framework; Architectural Strategies for IT used in process support
Who	Security & Risk Governance; Trust Framework: Owners, Custodians and Users; Service Providers & Customers; Trust Modelling Framework
Where	Domain Framework: Security Domain Concepts & Framework
When	Time Management Framework: Through-Life Risk Management Framework; Attribute Performance Targets

The Designer's View (Logical Layer)

What	Information Assets: Inventory of Information Assets; Information Model of the Business
Why	Risk Management Policies: Risk Models; Domain Policies; Assurance Criteria
How	Process Maps & Services: Information Flows; Functional Transformations; Service Oriented Architecture; Services Catalogue; Application Functionality and Services
Who	Trust Relationships: Domain Authorities; Entity Schema; Privilege Profiles; Trust Relationship Models
Where	Domain Maps: Domain Definitions; Inter-domain Associations & Interactions
When	Calendar & Timetable: Start Times, Lifetimes & Deadlines

The Builder's View (Physical Layer)

What	Data Assets: Data Dictionary & Data Storage Devices Inventory
Why	Risk Management Practices: Risk Management Rules & Procedures; Risk Metadata
How	Process Mechanisms: Working Procedures; Application Software; Middleware; Systems; Security Mechanisms; Process Control Points
Who	Human Interface: User Interface to Business Systems; Identity & Access Control Systems
Where	Infrastructure: Workspaces; Host Platforms, Layout of Devices & Networks
When	Processing Schedule: Timing & Sequencing of Processes & Sessions

The Tradesman's View (Component Layer)

What	Component Assets: Products and Tools, including Data Repositories and Processors
Why	Risk Management Components & Standards: Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools
How	Process Components & Standards: Tools and Protocols for Process Delivery; Application Products
Who	Human Entities: Components & Standards: Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists
Where	Locator Components & Standards: Nodes, Addresses and other Locators; Component Configuration
When	Step Timing & Sequencing Tools: Time Schedules, Clocks, Timers, Interrupts

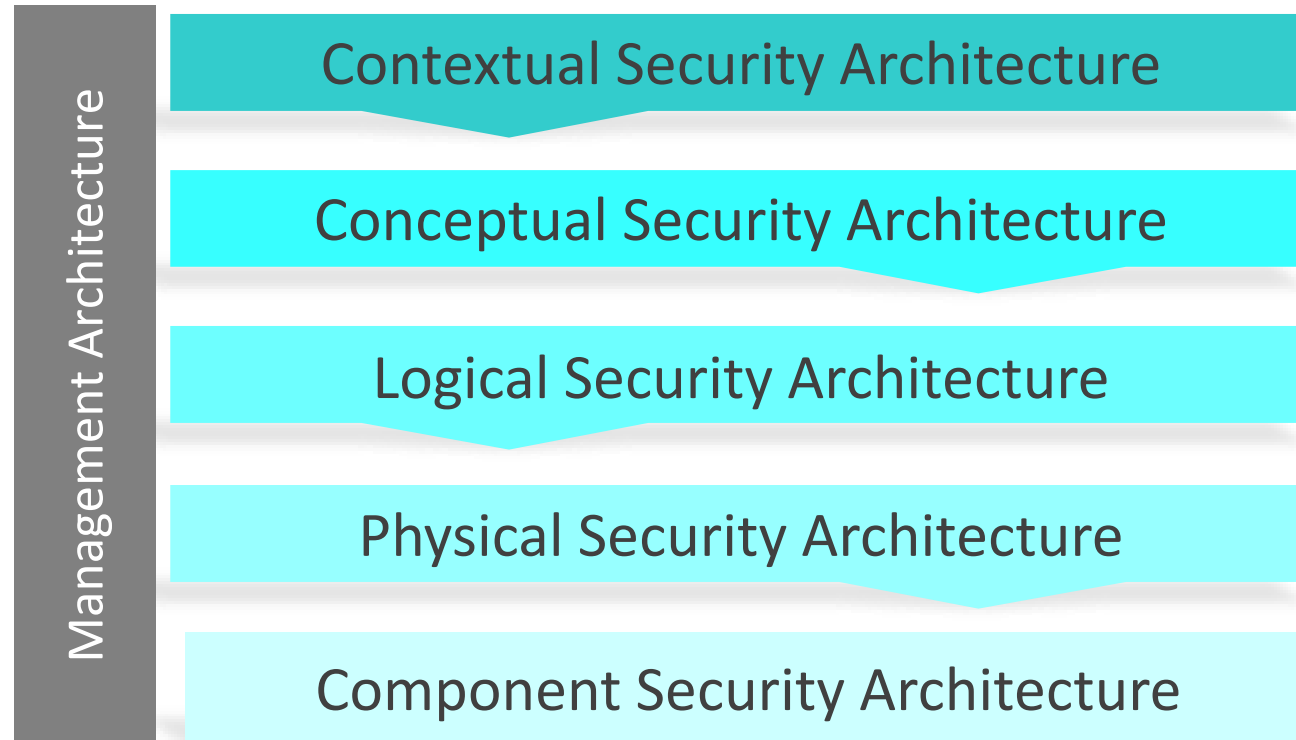
The Manager's View (Management Layer)

What	Delivery and Continuity Management: Assurance of Operational Excellence & Continuity
Why	Operational Risk Management: Risk Assessment, Risk Monitoring & Reporting; Risk Treatment
How	Process Delivery Management: Management & Support of Systems, Applications & Services
Who	Governance, Relationship & Personnel Management: Management & Support of Enterprise-wide and Extended Enterprise Relationships
Where	Environment Management: Management of Buildings, Sites, Platforms & Networks
When	Time & Performance Management: Management of Calendar and Timetable

The SABSA Matrix (see Appendix 1)

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business Goals & Decisions	Business Risk	Business Meta-Processes	Business Governance	Business Geography	Business Time Dependence
Conceptual	Business Value & Knowledge Strategy	Risk Management Strategy & Objectives	Strategies for Process Assurance	Security & Risk Governance; Trust Framework	Domain Framework	Time Management Framework
Logical	Information Assets	Risk Management Policies	Process Maps & Services	Trust Relationships	Domain Maps	Calendar & Timetable
Physical	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	Infrastructure	Processing Schedule
Component	Component Assets	Risk Management Components & Standards	Process Components & Standards	Human Entities: Components & Standards	Locator Components & Standards	Step Timing & Sequencing Components and Standards
Management	Delivery & Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management

Management View



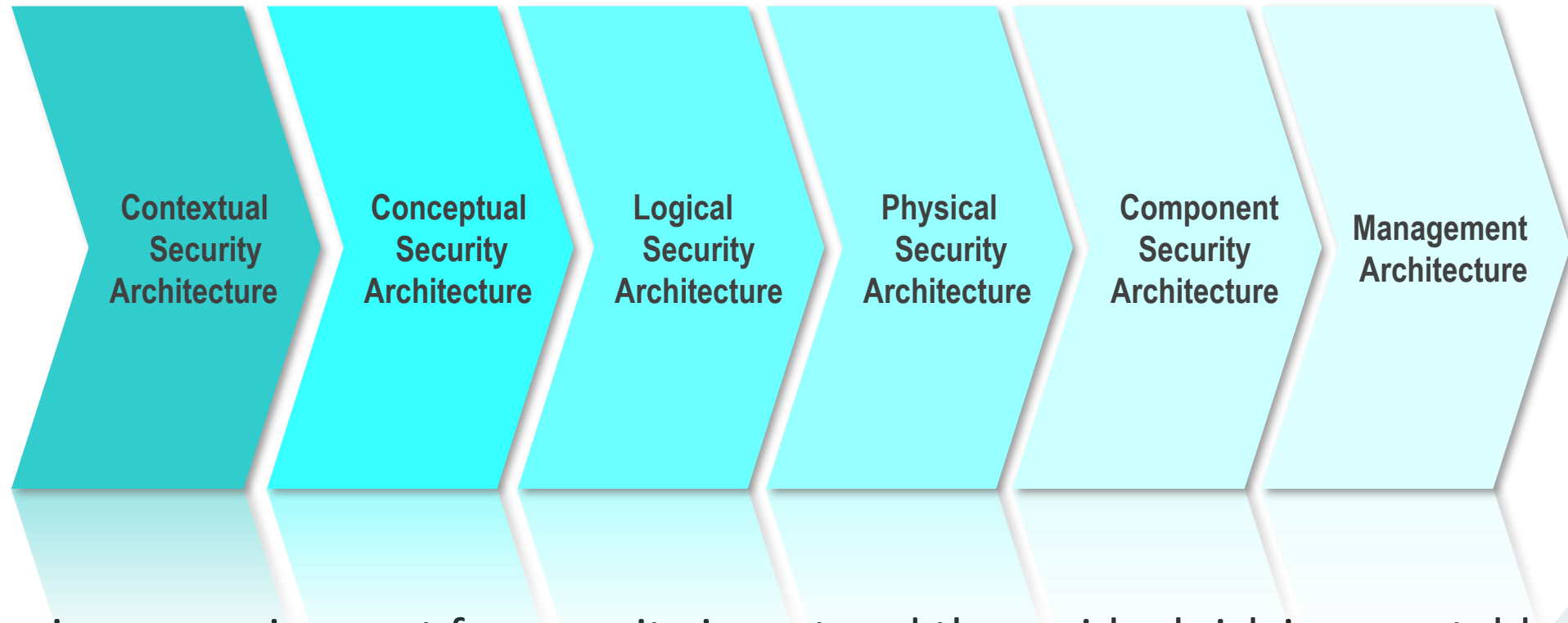
SABSA Management Matrix

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

Inspector's View

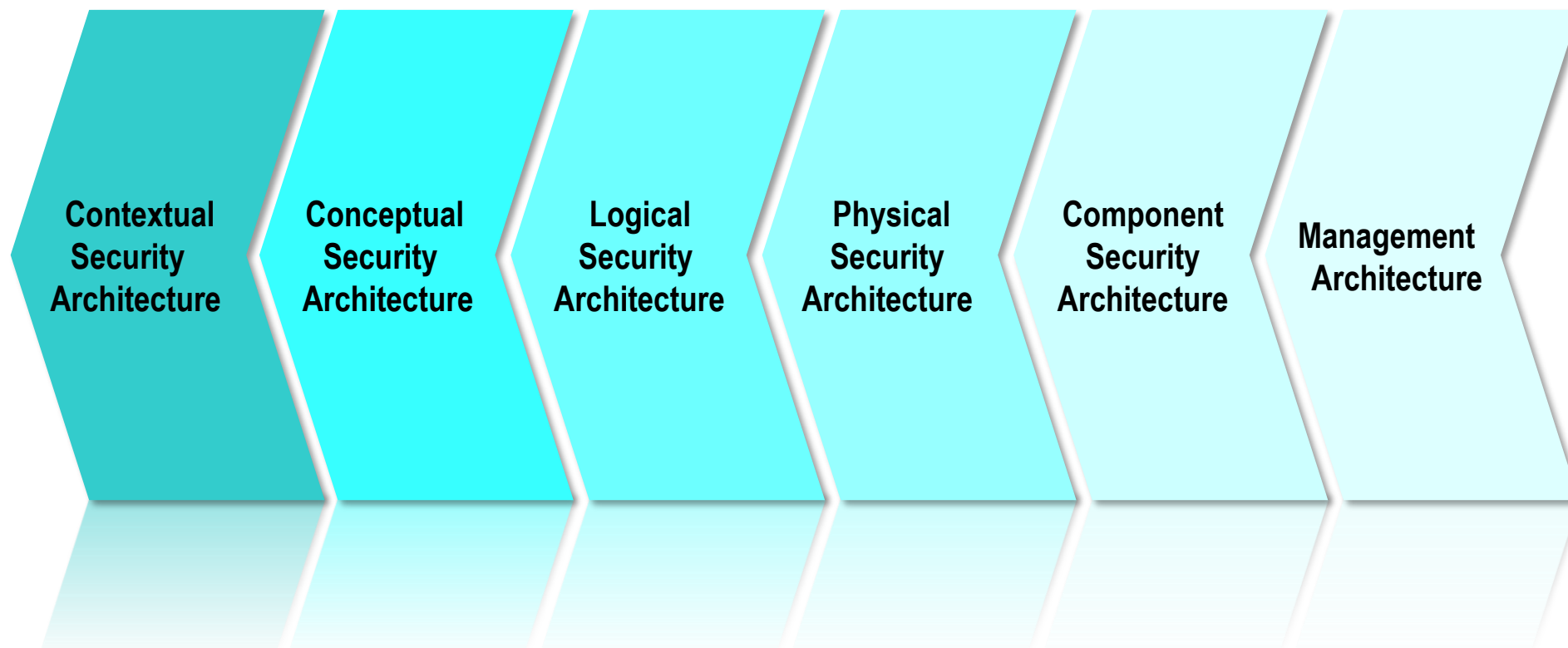
- Provide assurance that the architecture is
 - Complete
 - Robust
 - Fit-for-purpose
 - Consistent
- Integral to and inherent in the architectural development process and the vertical view of operations and management
- SABSA also provides an Assurance Management Framework (see module F2)

Traceability for Completeness



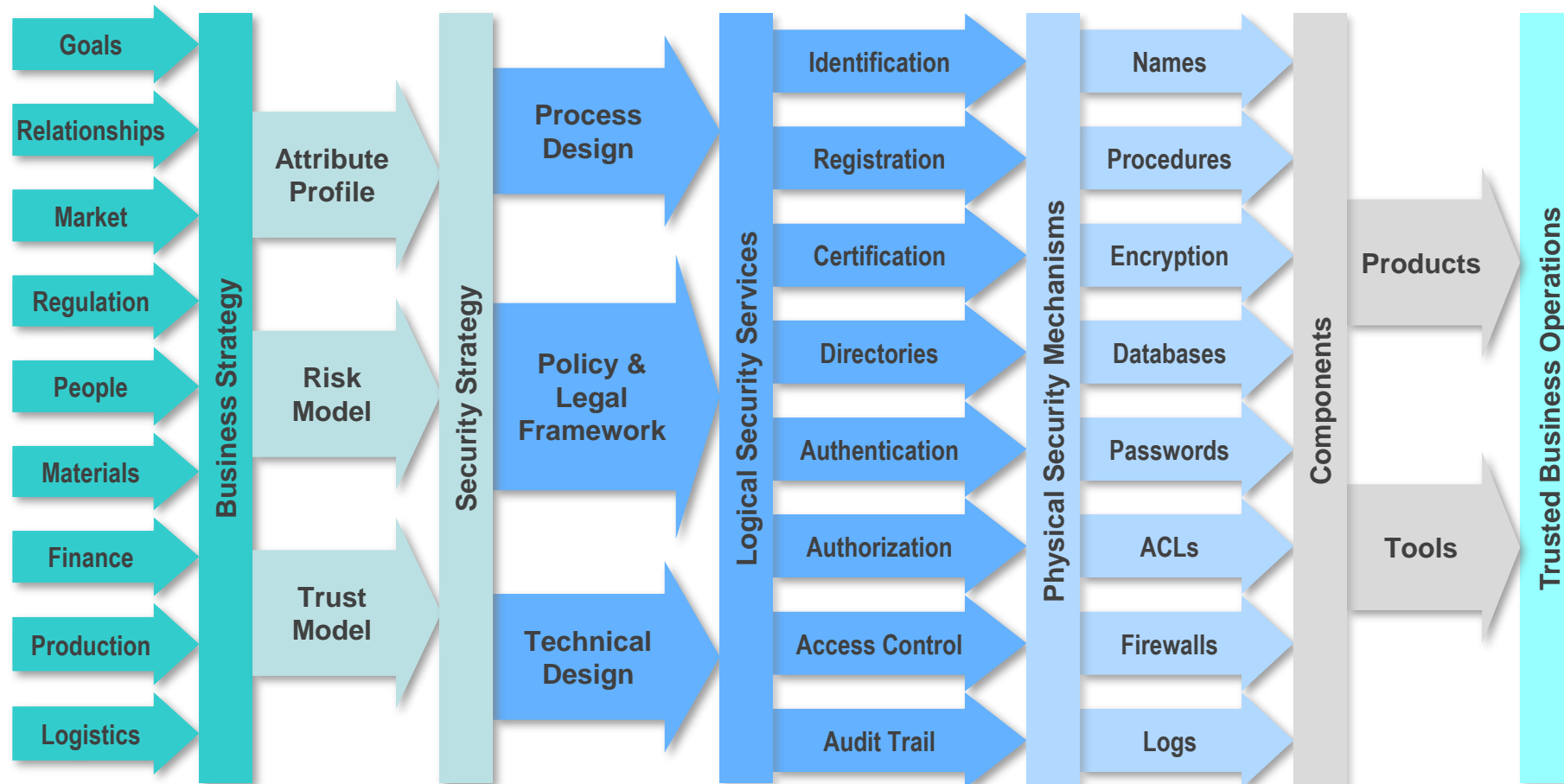
- Every business requirement for security is met and the residual risk is acceptable to the business appetite

Traceability for Justification



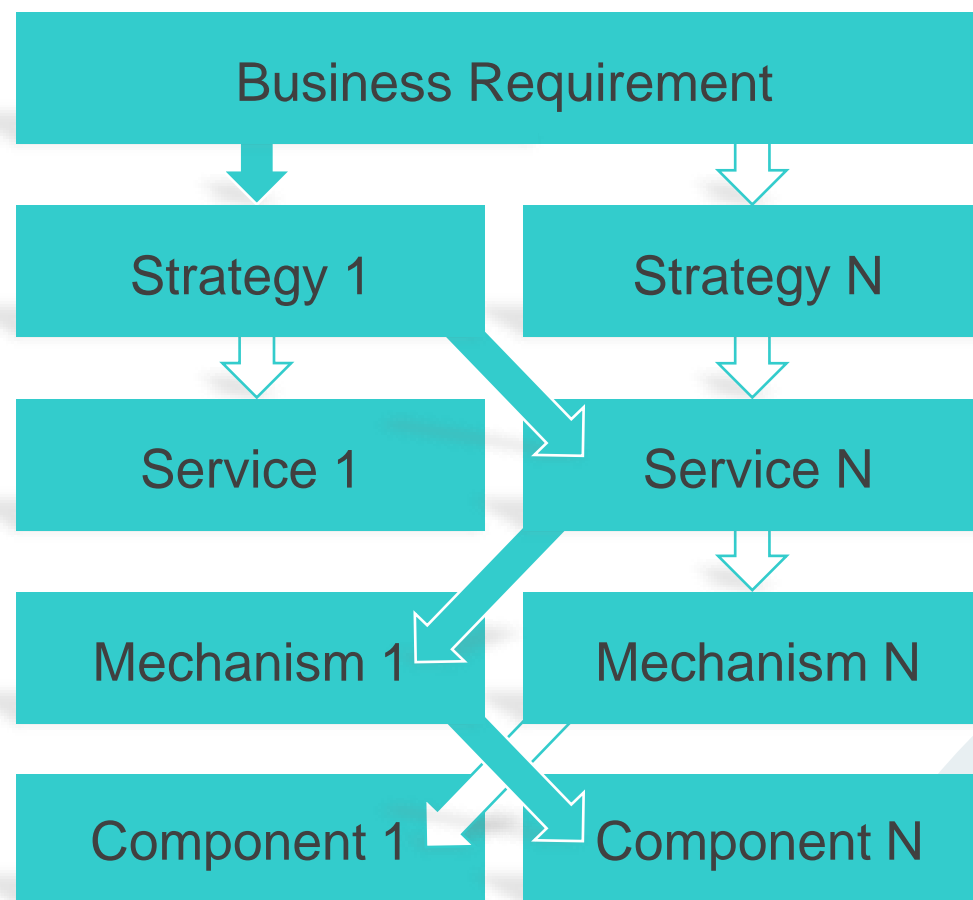
- Every operational or technological security element can be justified by reference to a risk-prioritised business requirement

Layer Mapping for Traceability



Applications of the Traceability Layer Map

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



Appendix F1-1

- SABSA Executive White Paper
 - Soft copy from
 - SABSA website <https://www.sabsa.org>
 - OR <https://www.sabsacourses.com>
- Other Resources
 - Institute Members <https://www.sabsa.org>
 - Annual World Congress <https://www.cosac.net>
 - Regional 'Chapters' and 'SABSA World Days' <https://sabsaworld.org>
 - LinkedIn Groups
 - Global, Francophile, Canadian, Dutch

Business Context & Requirements

Section 5

Scope: Strategy & Planning Phase - Assets

	Architecture Matrix	Management Matrix
Contextual	Business Goals & Decisions	Business Driver Development
	Business Value; Taxonomy of Business Assets, including Goals & Objectives , Success Factors, Targets	Business Benchmarking & Identification of Business Drivers
Conceptual	Business Value & Knowledge Strategy	Proxy Asset Development
	Business Attributes Taxonomy & Profile (with integrated performance targets)	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs

Section 5 Competency Objectives

Competency / Question Domain 1 – What (Assets)

Knowledge Element	Knowledge Competency	Comprehension Competency
The Traceability Concept	Define the traceability flow from business requirements to Attributes	Explain the approach to credible abstraction & mappings between requirements and Attributes
SABSA Attributes	Define SABSA Attributes	Associate Attributes with business drivers
	Describe the rules & features of Attributes	Explain the process of creating Attributes
	Define Attributes Taxonomy & Profile	Differentiate between Attributes Taxonomy & Attributes Profile
	Identify elements of Attributes requiring customisation	Customise Attribute names, definitions, measures & taxonomies
	Describe applications & benefits of the Attributes Profiling technique	Explain approaches to applying the Attributes Profiling technique

Business Driven Architecture

- Being business-driven means never losing sight of the organisation's goals, objectives, success factors and targets, and ensuring that the security strategy demonstrably supports, enhances and protects them
- The contextual architecture captures and presents the full set of relevant requirements for the scope of the assignment
 - Including conflicts in business strategy, risks & priorities
 - At this stage we are confirming that they are complete and we understand them
 - The conceptual layer will later resolve these conflicts by delivering an appropriate, measurable security strategy

Our Business Needs Are Unique

- We use Trust & Confidence mechanisms in **different** ways, in **different** places, and to **differing** degrees
 - Protecting intellectual property
 - Protecting against theft of materials, services or subscriptions
 - Manufacturing and engineering process control and remote process control
 - Supply chain
 - eProcurement, eBanking, eGovernment
 - Operational continuity and stability
 - Competence, reliability & stakeholder confidence
 - Safety critical dependencies
 - National security
 - Sectoral governance, compliance & regulation
 - Organisation, trust relationships and information sharing
 - Management hierarchies
 - Outsourcing, joint ventures, partnerships, divestments, mergers and acquisitions
 - Location dependence
 - Deadlines and performance criteria
 - Business strategy
 - Brand protection

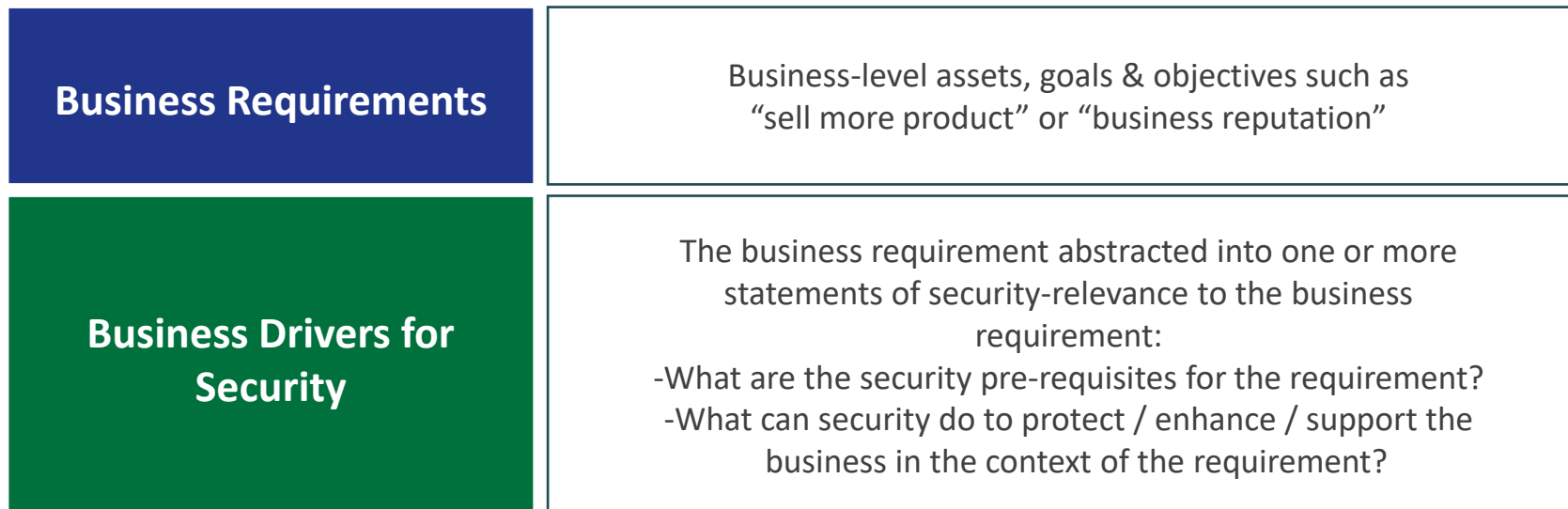


Approach to Traceability

- Good traceability requires small, credible steps, not big jumps
- A flawed approach
 - Stakeholder: “I need to sell more product”
 - Security Architect: “Then you need a firewall”
- A credible approach
 - Collect business drivers, goals and objectives
 - Abstract them in business-language into meaningful business drivers for security
 - Stakeholder: “I need to ship more product”
 - Security Architect: “We can ship more product if security enhances the core product through higher trust levels and ease of use”

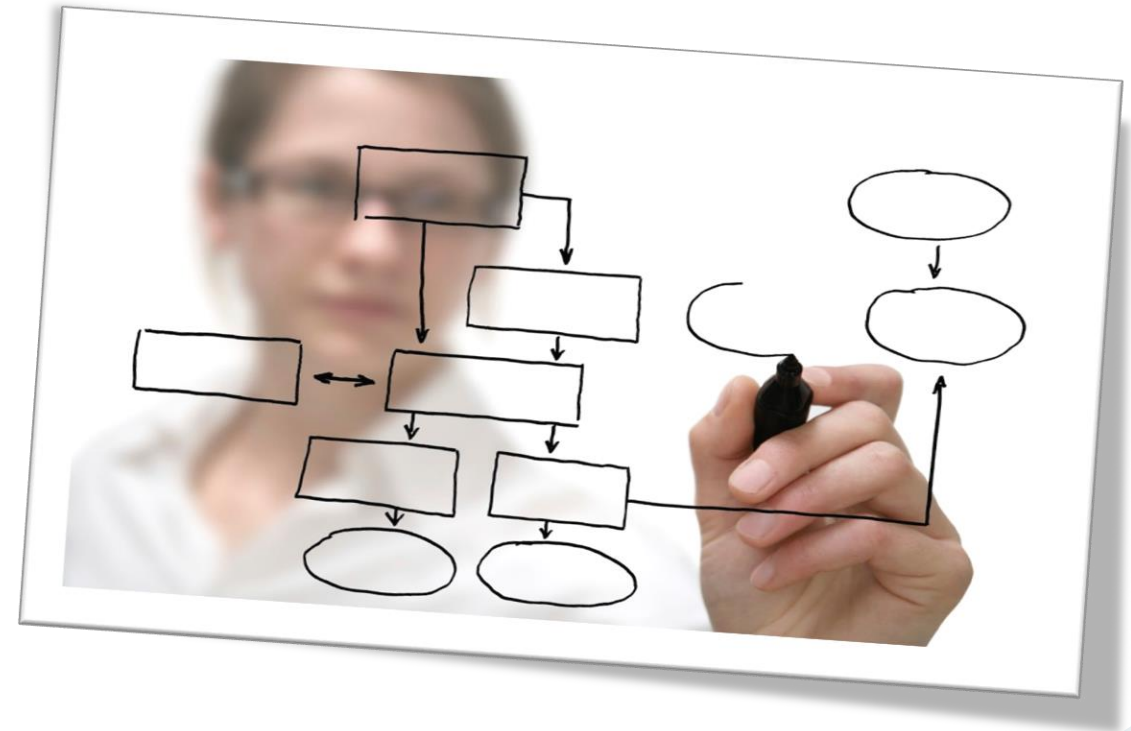
Credible Abstraction is Key

- Meaningful traceability is enabled by credible abstraction from business context (assets, goals & objectives) to a business security context
- Traceability therefore starts by delivering two slightly different sets of requirements:



Workshop F1-1

Engineering Business Drivers for Security



What Are SABSA Business Attributes?

- An Attribute is a conceptual abstraction of a real business requirement (the goals, objectives, drivers, targets, and assets confirmed as part of the business contextual architecture)
- The Attributes Profiling technique enables any unique set of business requirements to be engineered as a standardised and re-usable set of specifications
- The Attributes are modelled into a normalised language that articulates requirements and measures performance in a way that is instinctive to all stakeholders



Two-way Traceability – Drivers to Attributes

Business Driver	Attribute
BD1	Credible, Reputable
BD8	Controlled, Governable
BD17	Access Controlled, Authenticated, Confidential, Identified, Private

Two-way Traceability –Attributes to Drivers

Attribute	Business Driver
Private	BD17
Informed	BD5, BD30, BD31
Non-repudiable	BD3, BD4, BD13, BD14, BD19

Attributes Profiling Rules & Features

- Attributes can be tangible or intangible
- Each attribute requires a meaningful name and detailed definition customised specifically for a particular organisation
- Each attribute requires a measurement approach and metric to be defined during the SABSA Strategy & Planning phase to set performance targets for security
- Attributes must be validated (and preferably created) by senior management & the business stake-holders by report, interview or facilitated workshop
- The performance targets are then used as the basis for reporting and/or SLAs in the SABSA Manage & Measure phase
- Powerful requirements engineering technique
- Populates the vital 'missing link' between business requirements and technology / process design

Definitions: Taxonomy & Profile

- SABSA Business Attributes Taxonomy
 - Name
 - Definition
 - Classification (usually on taxonomy graphic)
- SABSA Business Attributes Profile
 - Taxonomy enhanced with:
 - Measurement approach
 - Metric
 - Performance target

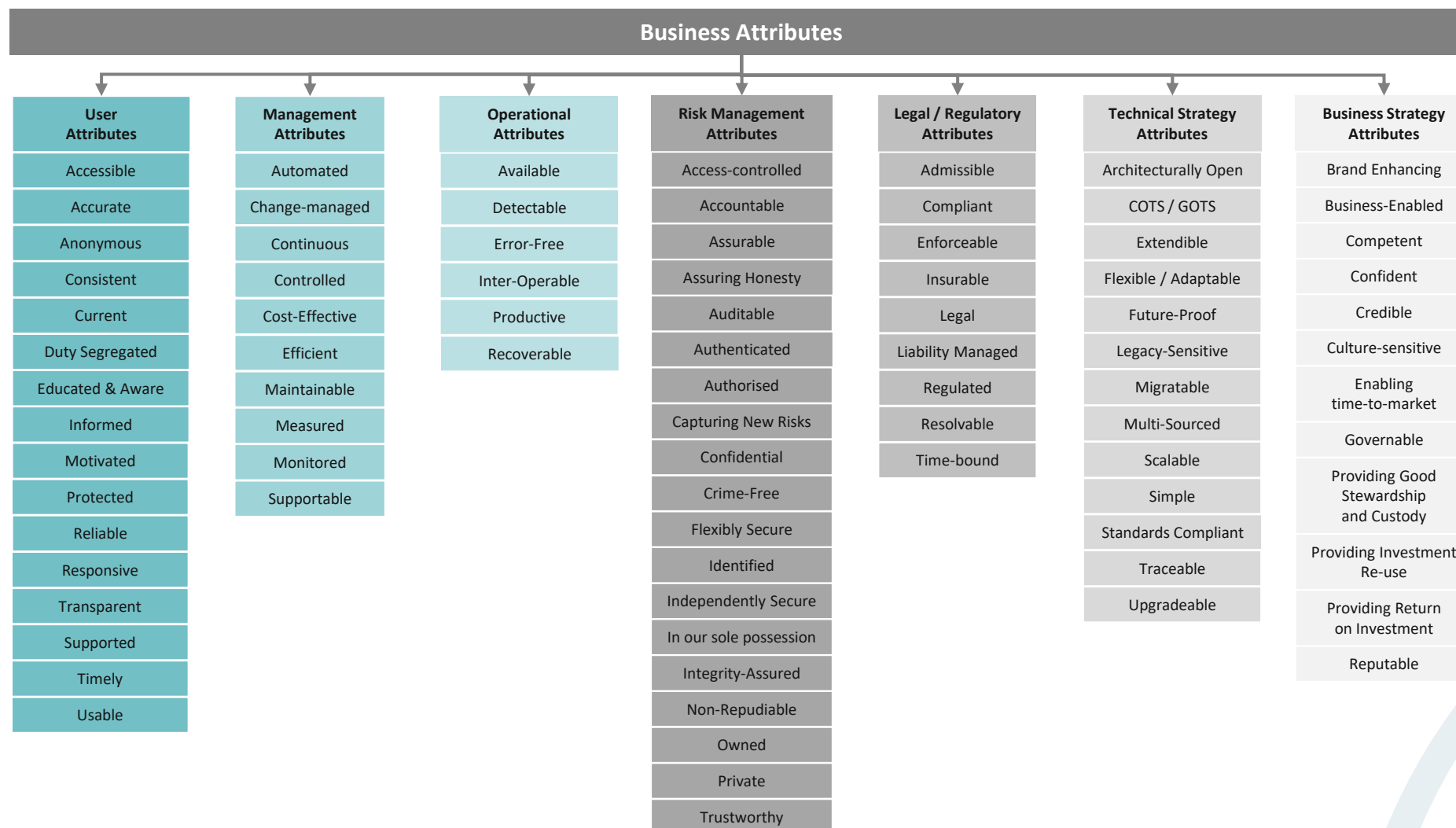
Applications of Attributes Profiling

- Pick-list of desired requirements
- Cross-check for completeness of requirements
- Key to traceability mappings
- Measurement & operations – contracts, SLAs, performance targets
- Return on Investment & Value propositions
- Procurement
- Risk status summary & risk monitoring
- Key to a SABSA integrated compliance tool
- Powerful executive communications

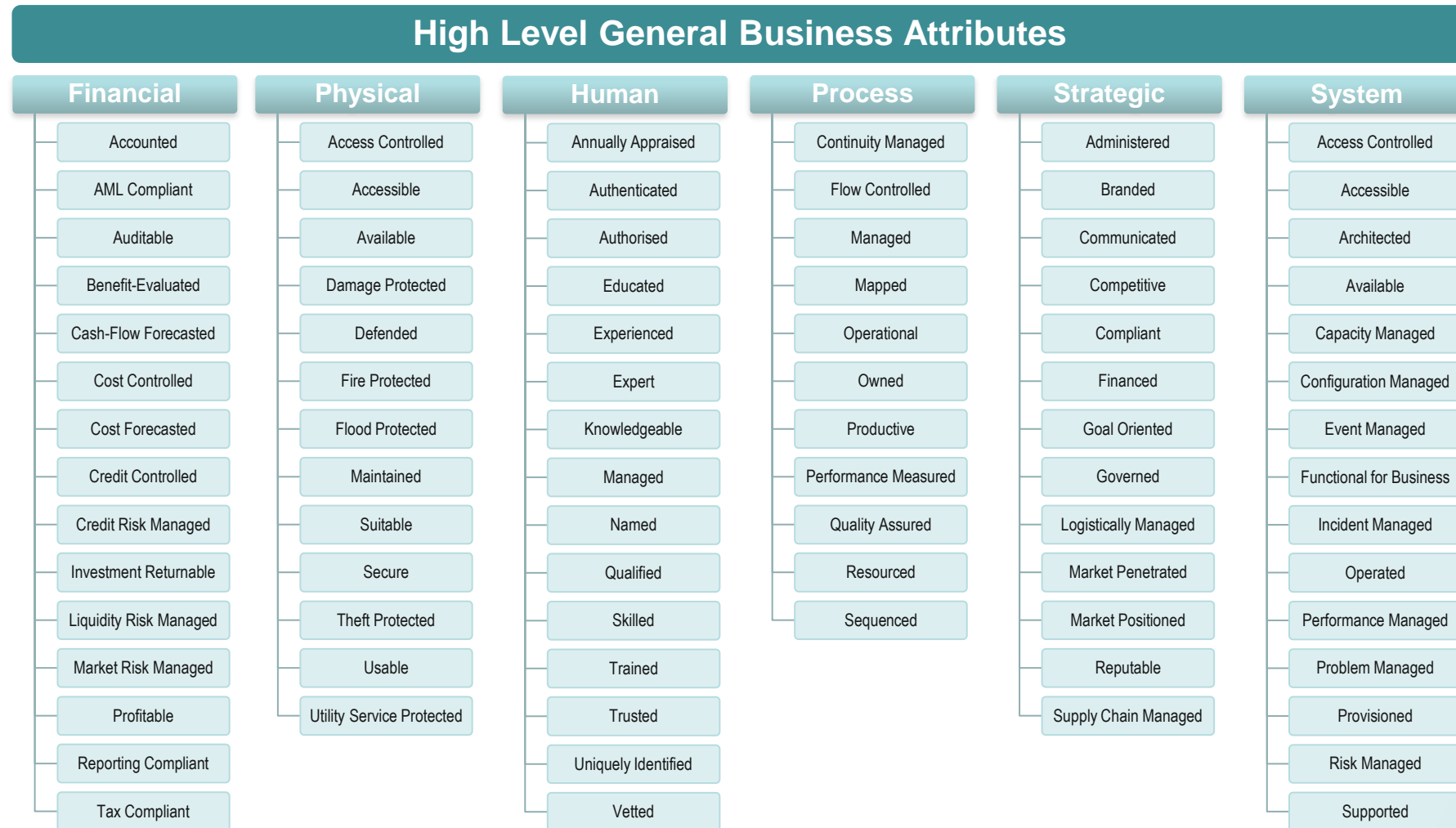
Attributes Customisation

- The Attributes Profile represents the business requirements for security for a specific organisation and should be customised to fully reflect local needs & culture
- Customised attribute names
- Customised attribute definitions
- Customised attribute measures, metrics & performance targets
- Customised classification and taxonomy categories
- Customised business level of application
 - Advanced usage involves multiple domain levels with linkage and aggregated performance

Sample Taxonomy of ICT Attributes

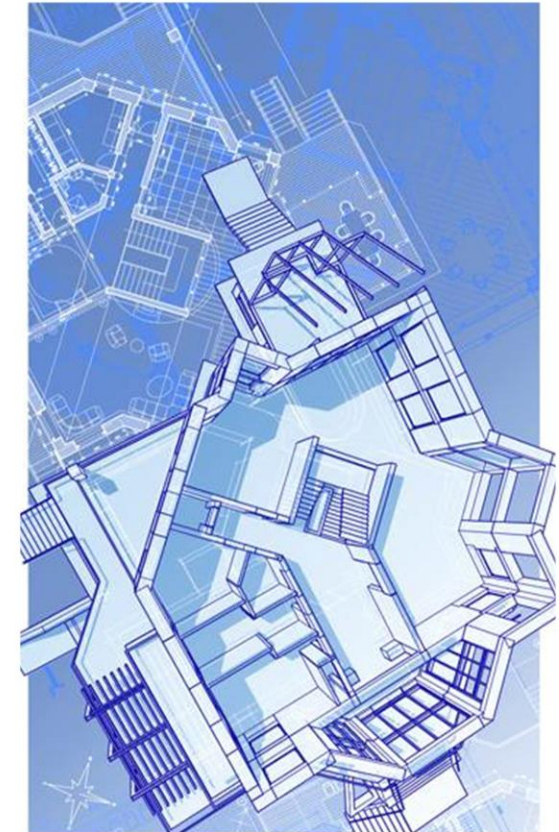


Sample Business-Level Taxonomy



Cultural Importance of the Taxonomy

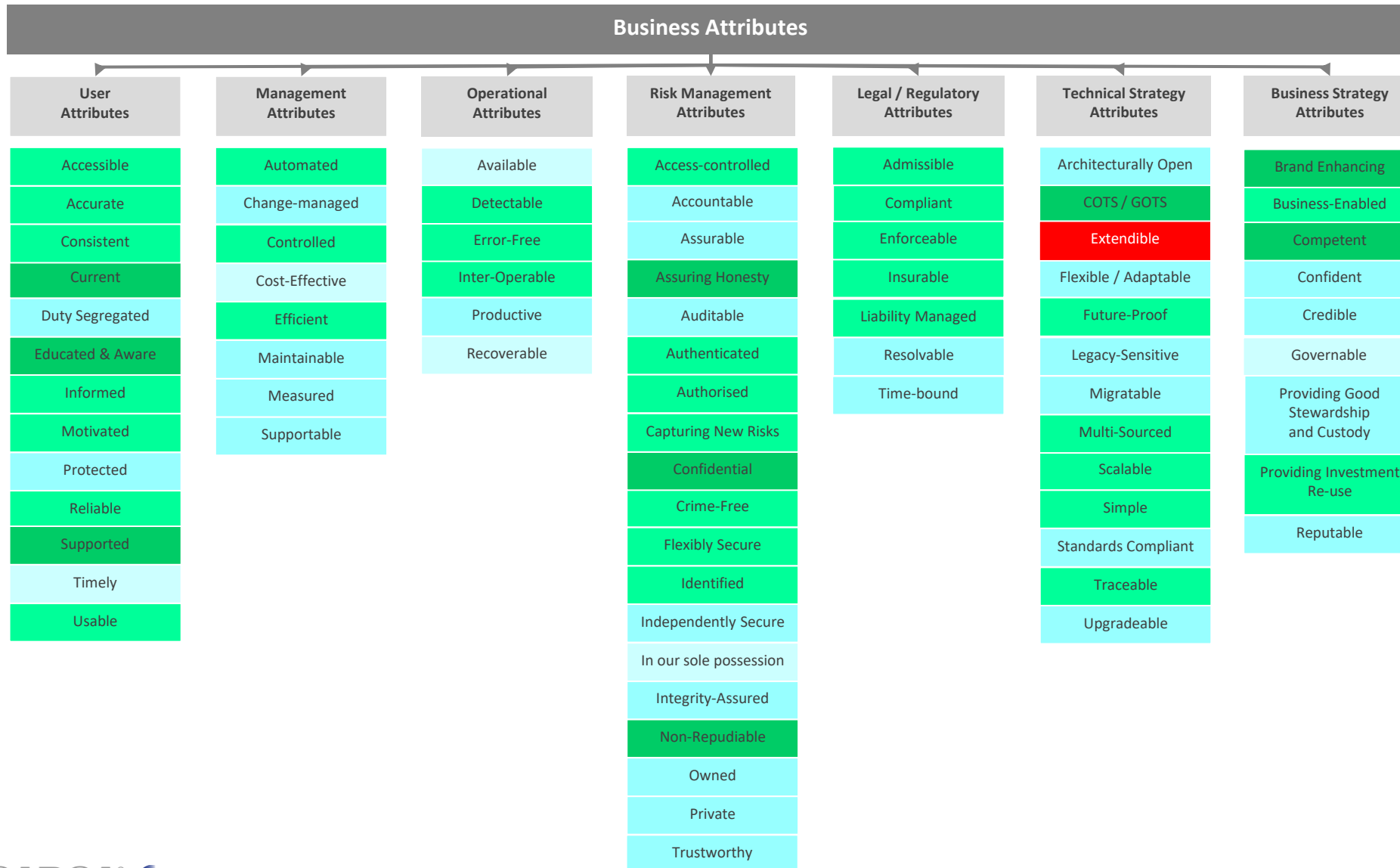
- The Attributes Taxonomy is ‘just a picture’ but a very important one
- It is used to demonstrate that we fully understand the requirements and to gain buy-in and support for developing the solution in the SABSA Design phase
- Analogy:
 - Tell an architect you need a 3-bedroom, 2 bathroom house
 - Almost the first thing the architect does is sketch a picture
 - Tell 100 architects you need a 3-bedroom, 2 bathroom house and they will all draw different pictures
 - Our picture must reflect the desires & culture of the stakeholders to maximise support for our solution strategy



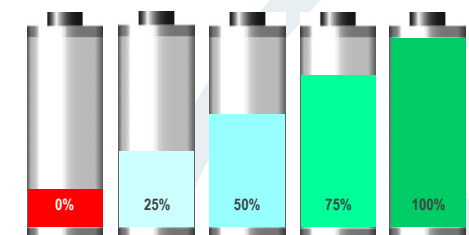
Attributes Case Study - Procurement

- The following example of a tender evaluation process is reproduced with permission from a Bank
- It is the executive presentation that was used to announce and justify the winning vendor
- The example shown is the final competition between two candidates

Attributes Case Study - Procurement



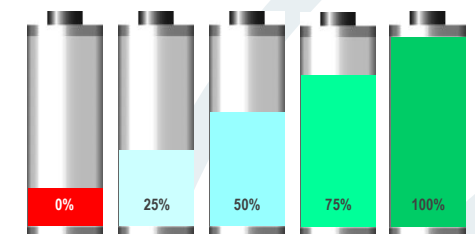
Vendor A



Attributes Case Study - Procurement

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

Vendor B



Attributes Case Study – Risk Management

- The following case study is reproduced with permission from the Australian Electoral Commission and with thanks to Tim Evans, Assistant Commissioner
- All risk rating content has been sanitised

AEC Attributes Taxonomy

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

AEC Attributes Taxonomy

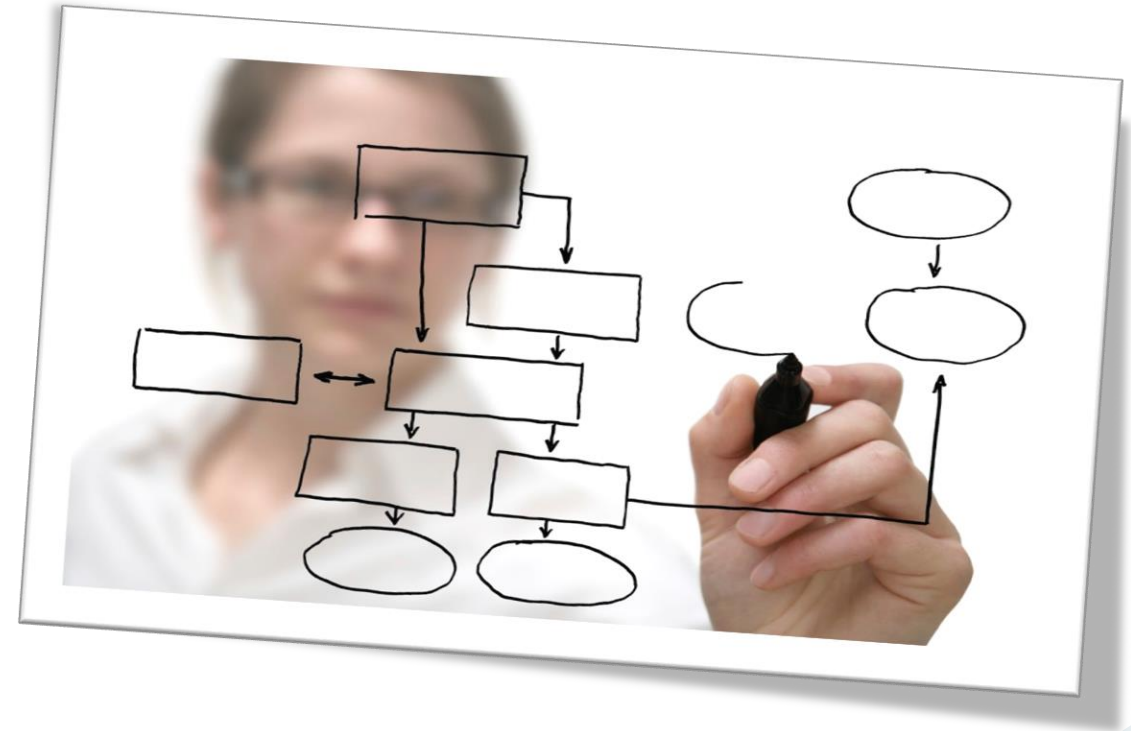
Core Values					
Electors Candidates Scrutineers Media	Impartiality	Integrity	Service	Respect	Transparency
	Secrecy of the Vote	Confidence & Preparation	Privacy	Accessibility & Deliberation	Transparency
				Timeliness of the Result	
Senior Management	Reputation	Governability	Compliance	Financial Viability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

Risk Information in Support of Business Mission

- SABSA Attributes-driven Risk Management database
- Periodic and real-time information
- Acceptable impact metrics / performance targets set for each asset
- Used for vendor evaluation
- Mandated for all IT Projects
- Multi-use by wide variety of stakeholders

Workshop F1-2

Attributes Taxonomy



Sample Questions

Competency Domain 1

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



Competency Domain 1

- At which layer of the SABSA Architecture Matrix is the Attributes Profile delivered?
 - A. Contextual Security Architecture
 - B. Conceptual Security Architecture
 - C. Logical Security Architecture
 - D. Physical Security Architecture

Competency Domain 1

- Which ONE of the following guiding principles for a sound architecture framework is TRUE?
 - A. The architecture framework must not presuppose any particular technical standards or operating culture
 - B. The architecture resulting from use of the framework must meet the set of business requirements dictated by current 'best practice'
 - C. The architecture framework must assume current policy, standards and technologies will remain static over time
 - D. The architecture framework must always be constructed to comply with pre-existing technical solutions

Risk & Opportunity Framework

Section 6

Scope: Strategy & Planning Phase - Motivation

	Architecture Matrix	Management Matrix
Contextual	Business Risk	Business Risk Assessment
	Opportunities & Threats Inventory	Analysis of Internal & External Risk Factors
Conceptual	Risk Management Strategy & Objectives	Developing Risk Objectives
	Enablement & Control Objectives; Policy Architecture; Risk Categories Risk Management Strategies; Risk Model Risk Architecture; Risk Modelling Framework; Assurance Framework	Maintaining Risk Modelling Framework; Risk Analysis on Business Attributes Proxy Assets

Section 6 Competency Objectives

Competency / Question Domain 2 – Why (Motivation)

Knowledge Element	Knowledge Competency	Comprehension Competency
Role of Risk Management in Business & Architecture	Identify drivers for, and objectives, benefits & applications of Architected Risk Management	Summarise how the SABSA process meets the Risk Management objectives & delivers benefits
	Describe the SABSA Balanced Risk Model	Explain how the SABSA Balanced Risk Model enables service & performance excellence
Risk Assessment	Describe the SABSA approach to assessing the elements of Risk	Explain the SABSA approach to measuring risk using attributes
	Describe the role of attributes performance thresholds in removing subjectivity of risk assessments	Explain the application of attributes performance thresholds to determine risk appetite & KRIs, and deliver early warnings for decision-making
Risk Management Process	Describe the SABSA process for compiling business risk management objectives	Distinguish between internal & external context, and explain the SABSA use of SWOT to create business-driven enablement & control objectives
	Show the traceable relationship between attributes and controls & enablers	Associate controls & enablers with business requirements using SABSA traceability concepts
Risk Management Systems	List architectural considerations for creating risk management systems & dashboards	Discuss an approach to creating a SABSA Threat & Opportunity Management system / dashboard

Regulatory Drivers for Operational Risk Management

- Corporate governance
- Sarbanes-Oxley Act (USA)
- Patriot Act (USA)
- Basel II (Banking Industry) (Basel III to come)
- Solvency II (European Insurance Industry)
- Gramm-Leach-Bliley Act (USA)
- HIPAA (Health Insurance Portability and Accountability Act) (USA)
- 21 CFR (Code of Federal Regulations) Part 11 (Pharmaceuticals Industry, USA)
- FAA, CAA and Others (Civil Aviation Industry)
- Data Protection Legislation (EU)
- PCI

Aims, Characteristics & Benefits

- Achieve an appropriate balance between realizing opportunities for gains while minimising losses
- Establish an appropriate infrastructure and culture and apply a logical and systematic method
- Embed into the organisation's philosophy, practices and business processes
- Early warnings & fewer surprises
- Economic & efficient exploitation of opportunities
- Improved planning through provision of information for decision-making
- Accountability assurance & governance

Applications of Risk Management

- Strategic, operational and business planning
- Asset management, resource planning & allocation
- Business interruption and continuity
- Change: organizational, technological and political
- Liability: Design, product, director, public, health & safety
- Environmental, ethics, fraud, security and probity issues
- Compliance & governance
- Procurement & contracting
- Project & Operations management

Risk Analysis Measures Risk Elements

- Identifying and valuing assets
- Identifying threats
- Quantifying business impacts
- Identifying vulnerabilities
- Applying suitable metrics
- Ranking the risks in relative priority order
- Providing a basis for risk management decisions
- Identifying where additional controls are required

Issues With Threat-driven Approach

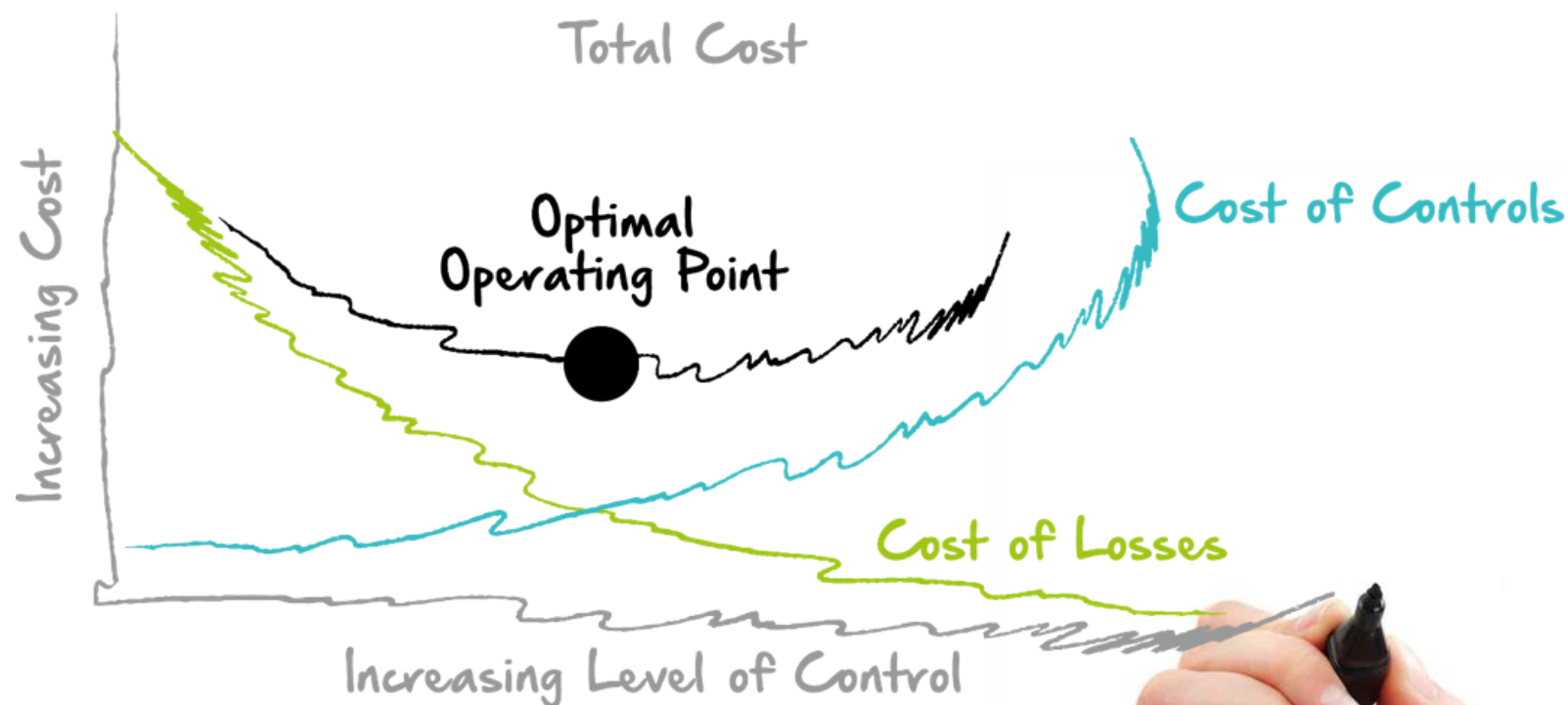
- Quantification requires good actuarial data (which we don't have)
- Statistical data is often not relevant in a dynamic technical environment, the past is usually a poor predictor of the future
- “Scare tactics” ask for investment to treat negatives (like Y2K)
- Technical threats are not well understood by stakeholders
- Impact is a much clearer starting point



Advantages of the Impact-based Approach

- Much broader view of the business goals - not just the tangible assets
- Provides a good view of business criticality
- Allows priorities to be established
- Focuses attention on “business critical” and “mission critical” risks
- Uses language that is understood by business managers
- Involves the business managers in the process
- Speed, cost, usability

Total Cost of Risk (Cost of Action + Cost of Inaction)



Doing Business Means Taking Risk

- All business, whether it is commercial, government, military or charitable, is based upon exploiting opportunities to further the goals of the enterprise
- With each opportunity come potential threats, and thus risk is implicit in doing business, whatever the nature of that business
- To do business is to take risks
- However, the level of residual risk must be acceptable within the risk appetite of the organisation (but can never be zero)

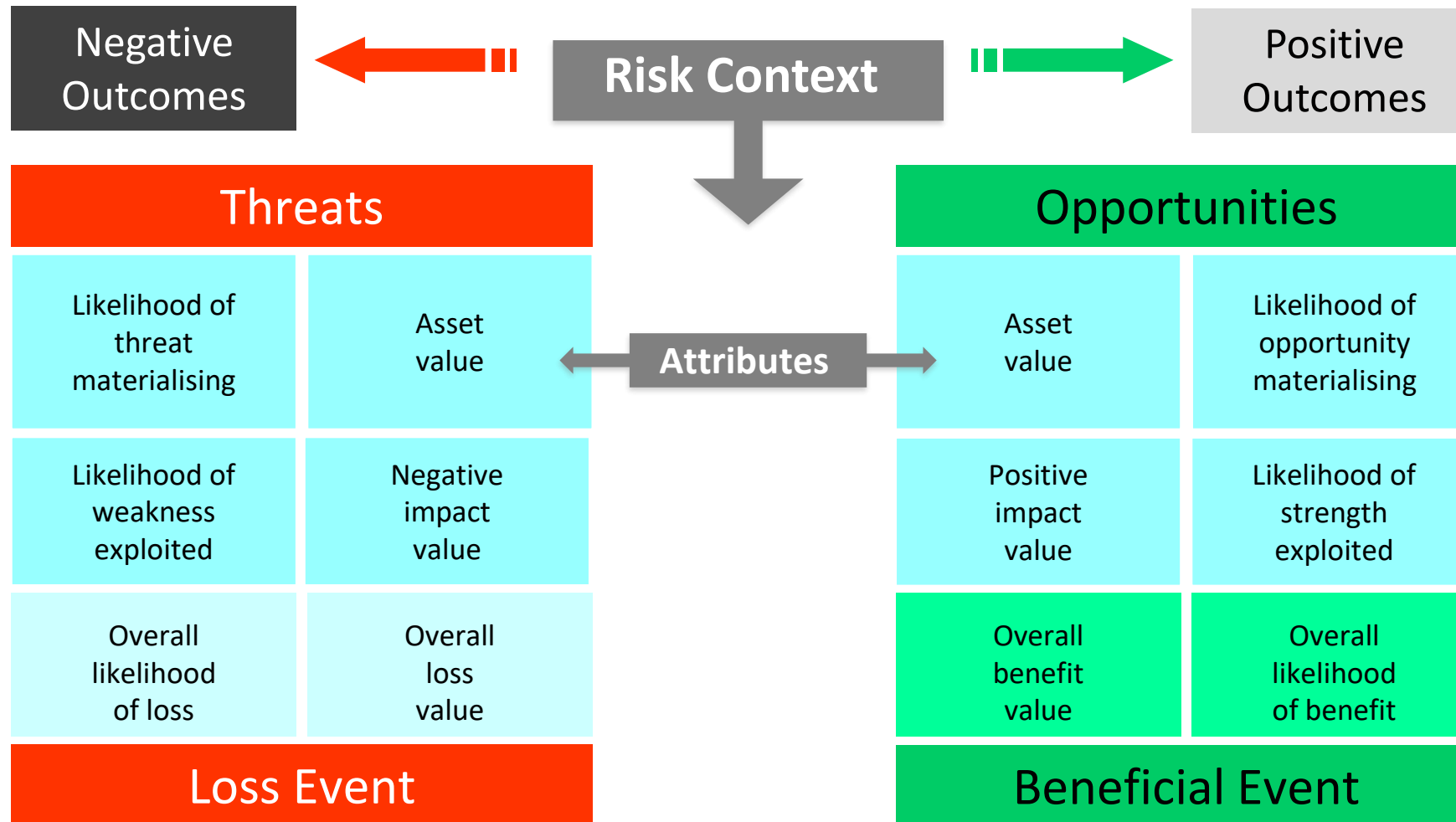
Perceptions & Characteristics of Risk

- Uncertain event(s) and outcome(s)
- Measured by:
 - Severity: potential magnitude of impact
 - Frequency: probability of event
- Outcome has Impact on business objectives
 - Positive impact: opportunity
 - Negative impact: threat
- Human Perception
 - Psychological association with loss – people have a tendency to take risk to recover perceived losses
 - Psychological association with gain – people have a tendency to be risk averse to protect perceived gains

SABSA Operational Risk Opportunities

- In a sense no-one 'chooses' to take operational risk in the same way that they 'choose' to take financial risk or strategic risk
- Operational risk is generally seen as being all downside risk
 - Operational risk is perceived as 'things that can go wrong'
- Despite this negative view, operational risk-taking is needed to realise business opportunities, either financial or strategic
- In the SABSA world operational risk can also be an upside risk
 - Business enablement is achieved through excellence in operational processes, people and technical systems
 - SABSA is a framework for achieving this excellence

SABSA Balanced Risk Model



SABSA Approach to Impact

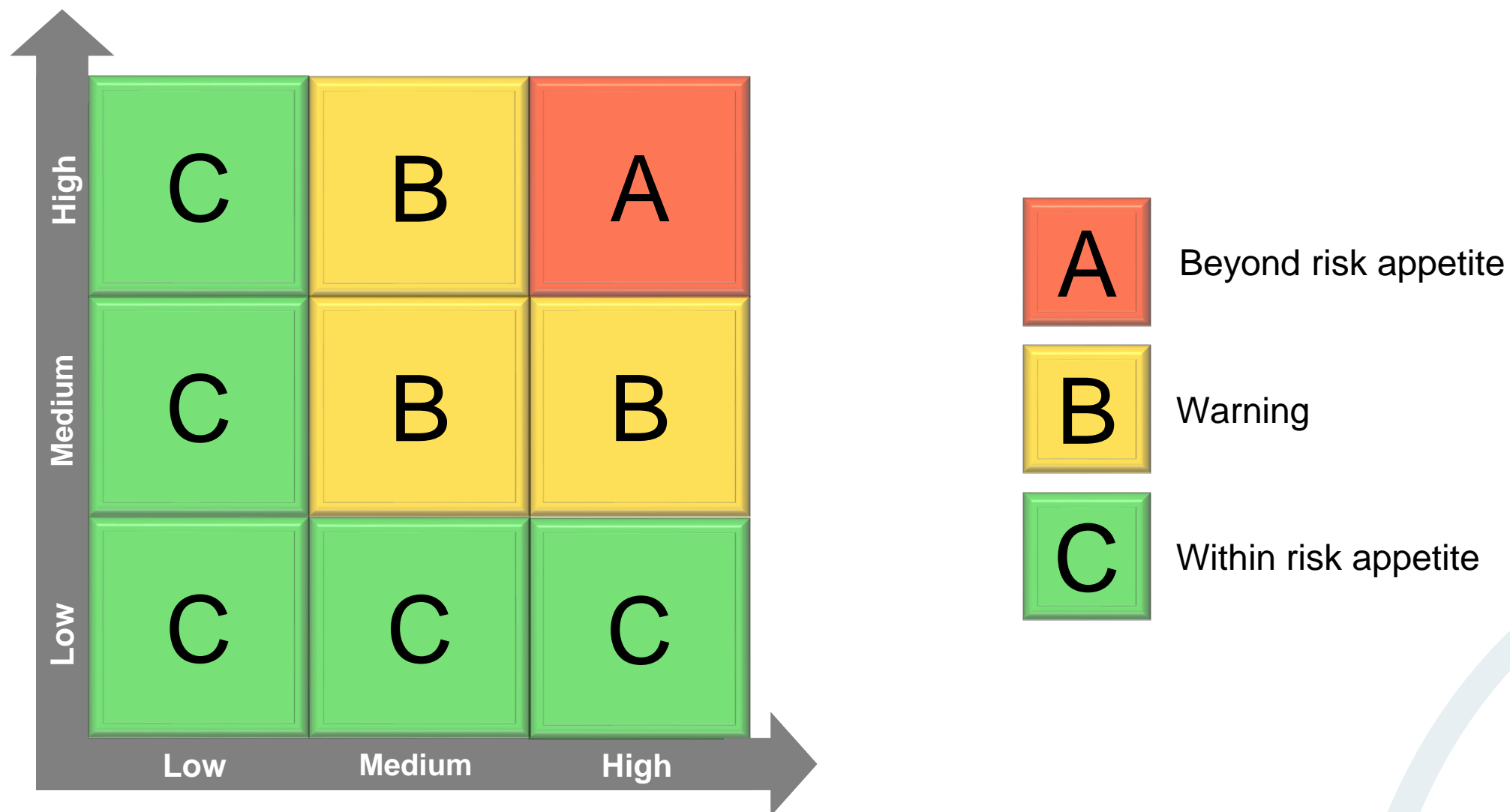
- Impact is expressed as positive or negative consequences of potential events upon Attributes
- Negative impact expressed as
 - Reduction in Attribute performance
 - Failure to meet Attribute performance target
- Positive impact expressed as
 - Increase in Attribute performance
 - Increase in Attribute performance threshold to higher target



Attributes Determine Risk Thresholds

- Performance target on an attribute provides the threshold for 'acceptable risk'
 - The attribute target is by definition a business goal / objective
 - Failure to meet it must therefore be an unacceptable outcome
 - This parameter is a key element of enabling risk assessment to be less subjective
- Early warnings are provided by the introduction of a second risk / performance threshold
 - Engineers would normally define the first threshold crossed as the primary
 - In SABSA however, we must define the early warning as secondary because 'primary' is the threshold that:
 - Exists in every scenario
 - Is the most important / has greatest consequence

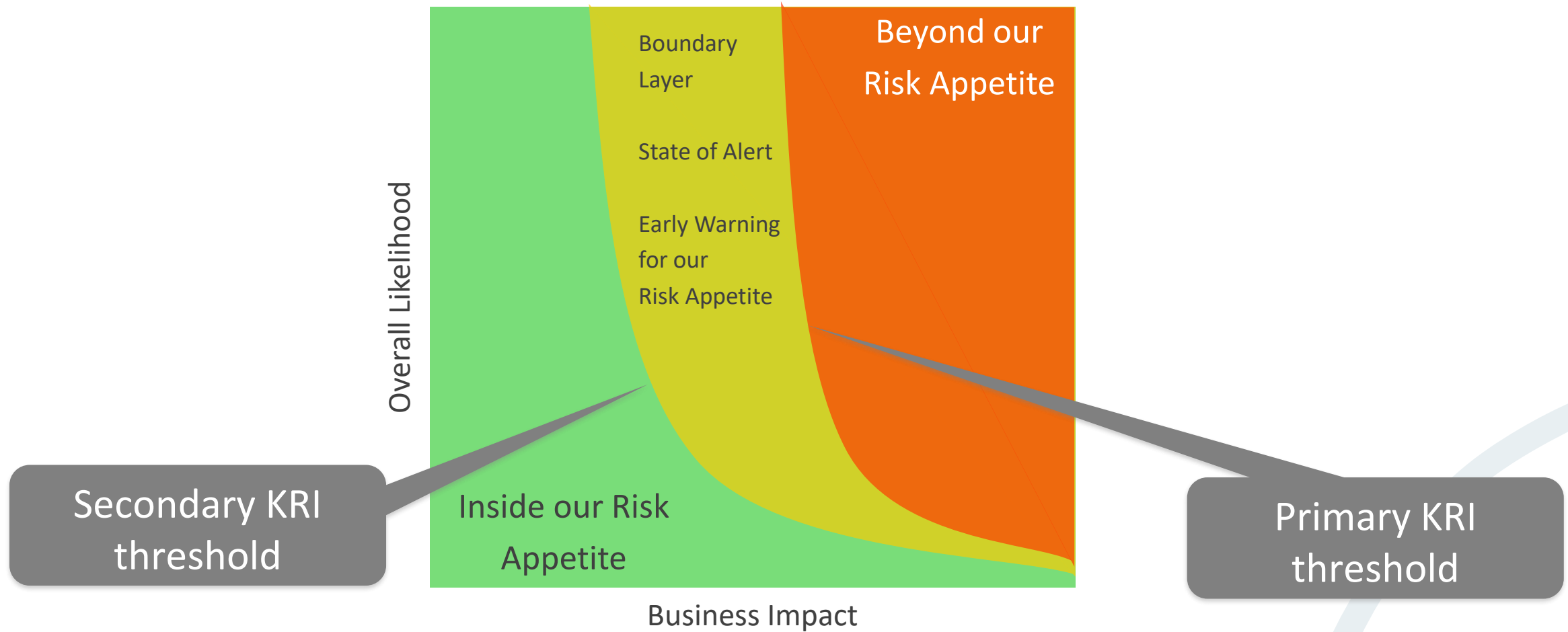
Qualitative Risk Assessment Thresholds



SABSA Key Risk Indicator Thresholds

- Business Attribute performance targets
 - Primary performance target is **Amber** / **Red** KRI threshold
- Set a secondary, lower, performance target
 - Defines **Green** / **Amber** boundary
 - Provides early warning that KRI is approaching
 - Prompts management intervention to prevent reaching the Red zone – i.e. exceeding risk appetite

SABSA Risk Appetite Thresholds



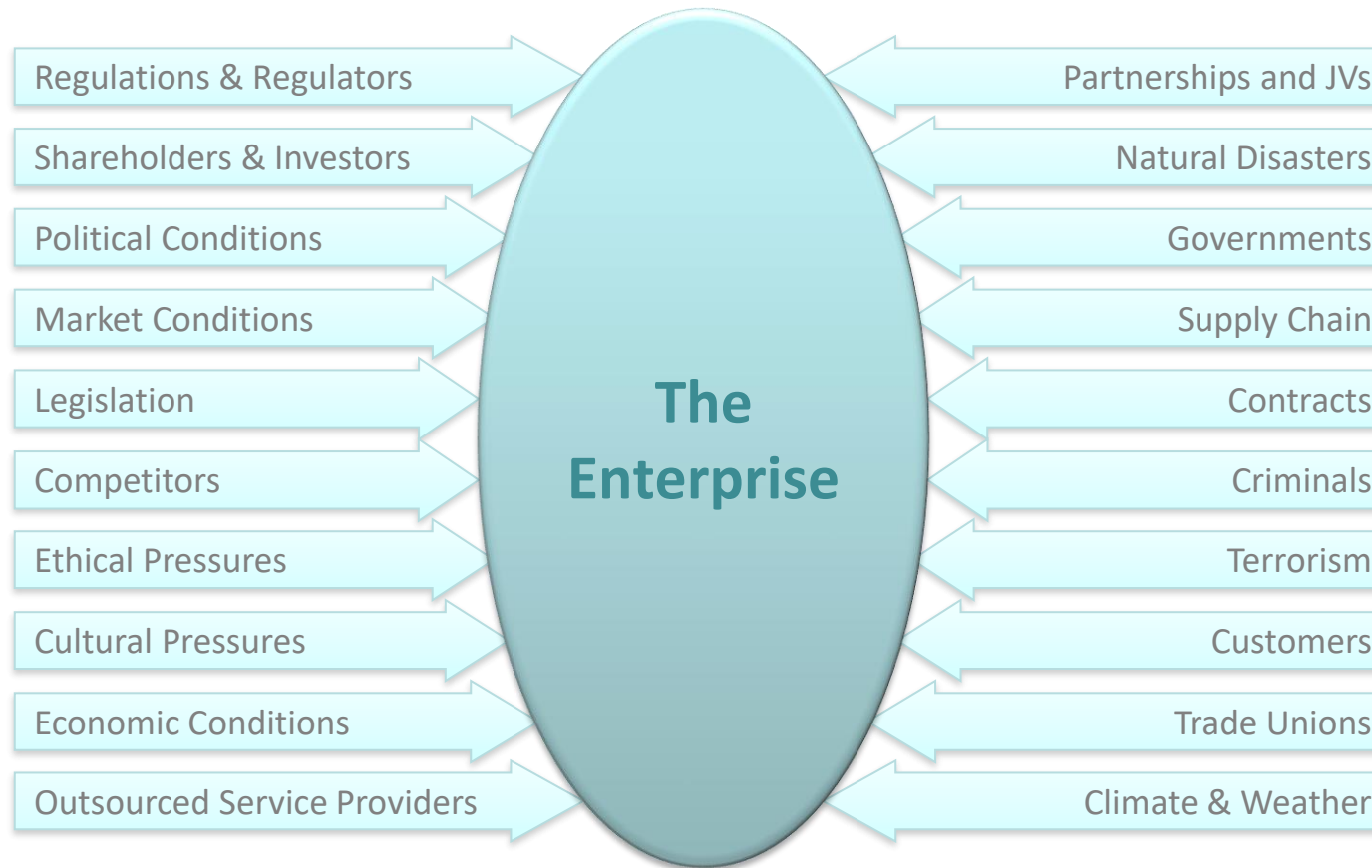
Examples of Key Risk Indicators (KRIs)

Events Monitored to Detect Crossing of Risk Thresholds

- Level of financial risk exposure
- Various financial accounting ratios (such as 'debtor days')
- Throughput capacity of a manufacturing or production facility
- Staffing levels
- Staff overtime levels
- Staff sickness and attendance levels
- Price of crude oil
- Level of traffic on an internet site
- Level of 'churn' in customer accounts
- Level of experience of staff working on a project

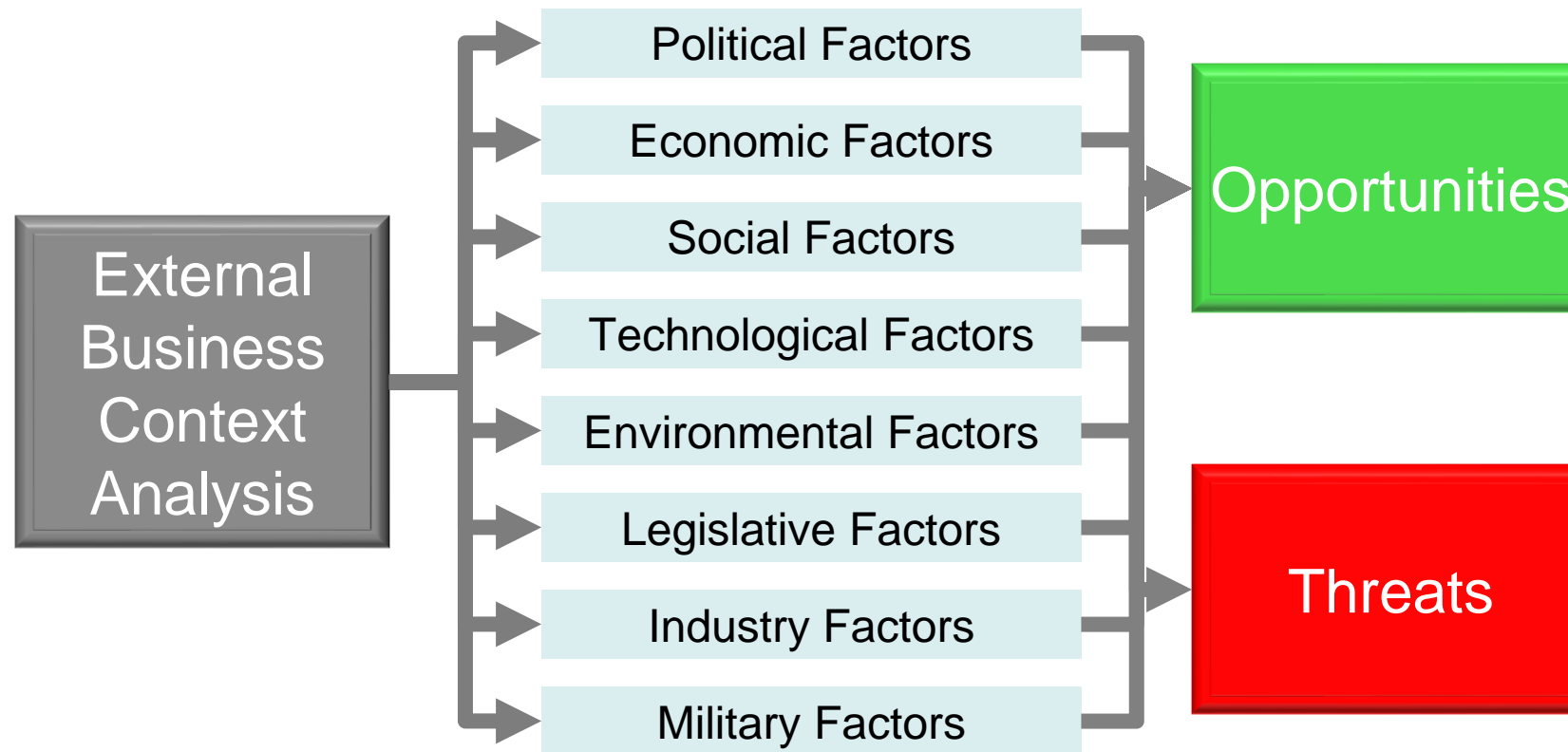
Compiling SABSA Risk Management Objectives

Taxonomy for Analysis of Threats & Opportunities (External)



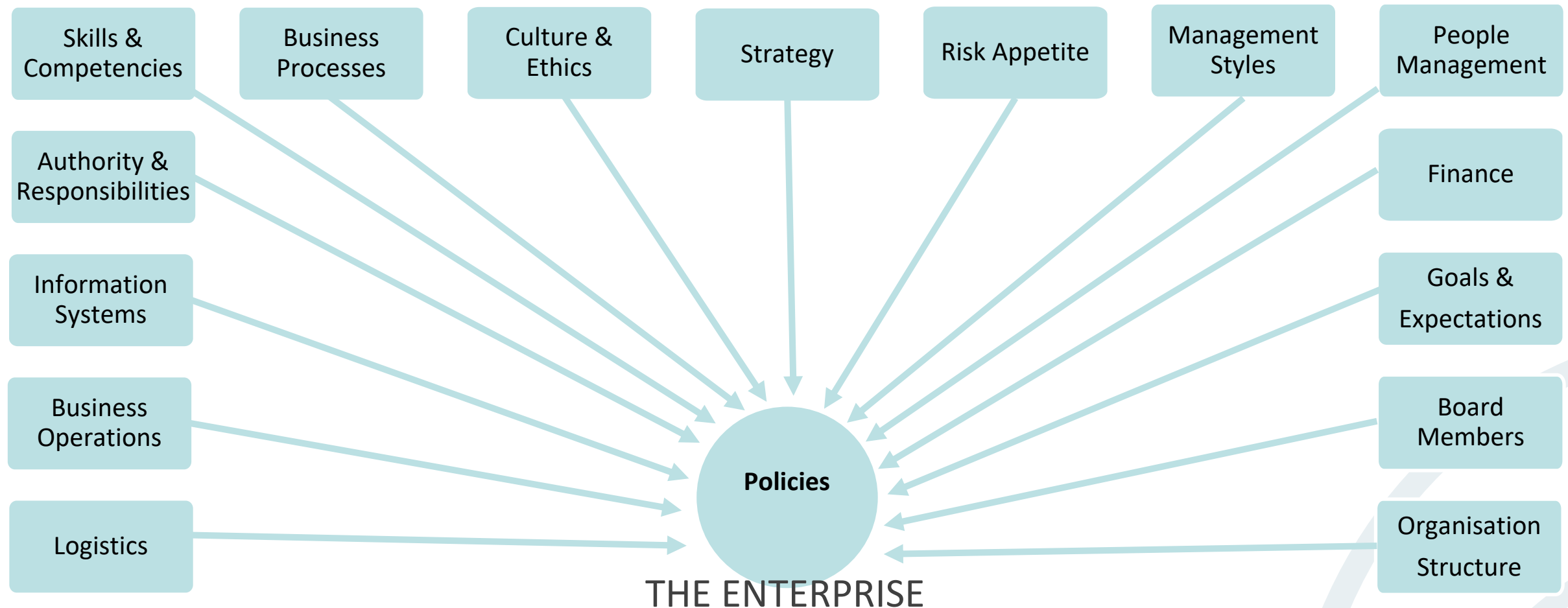
SABSA External Risk Factors Analysis

PESTELIM Analysis



Compiling SABSA Risk Management Objectives

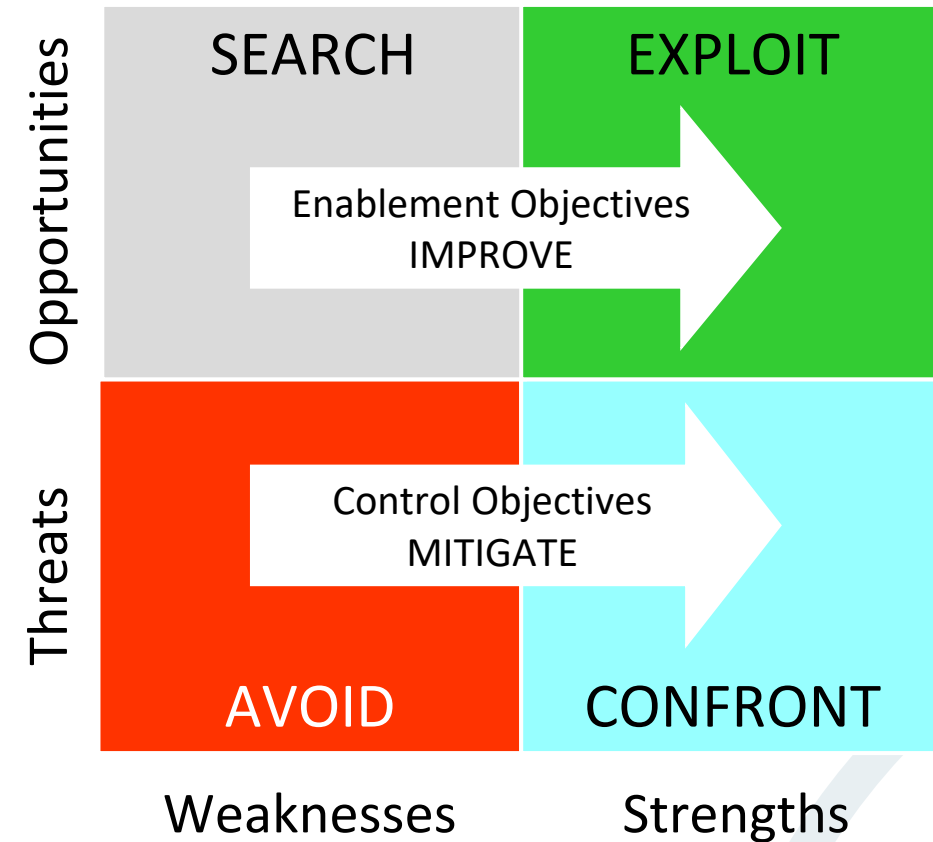
Taxonomy for Analysis of Strengths & Weaknesses (Internal)



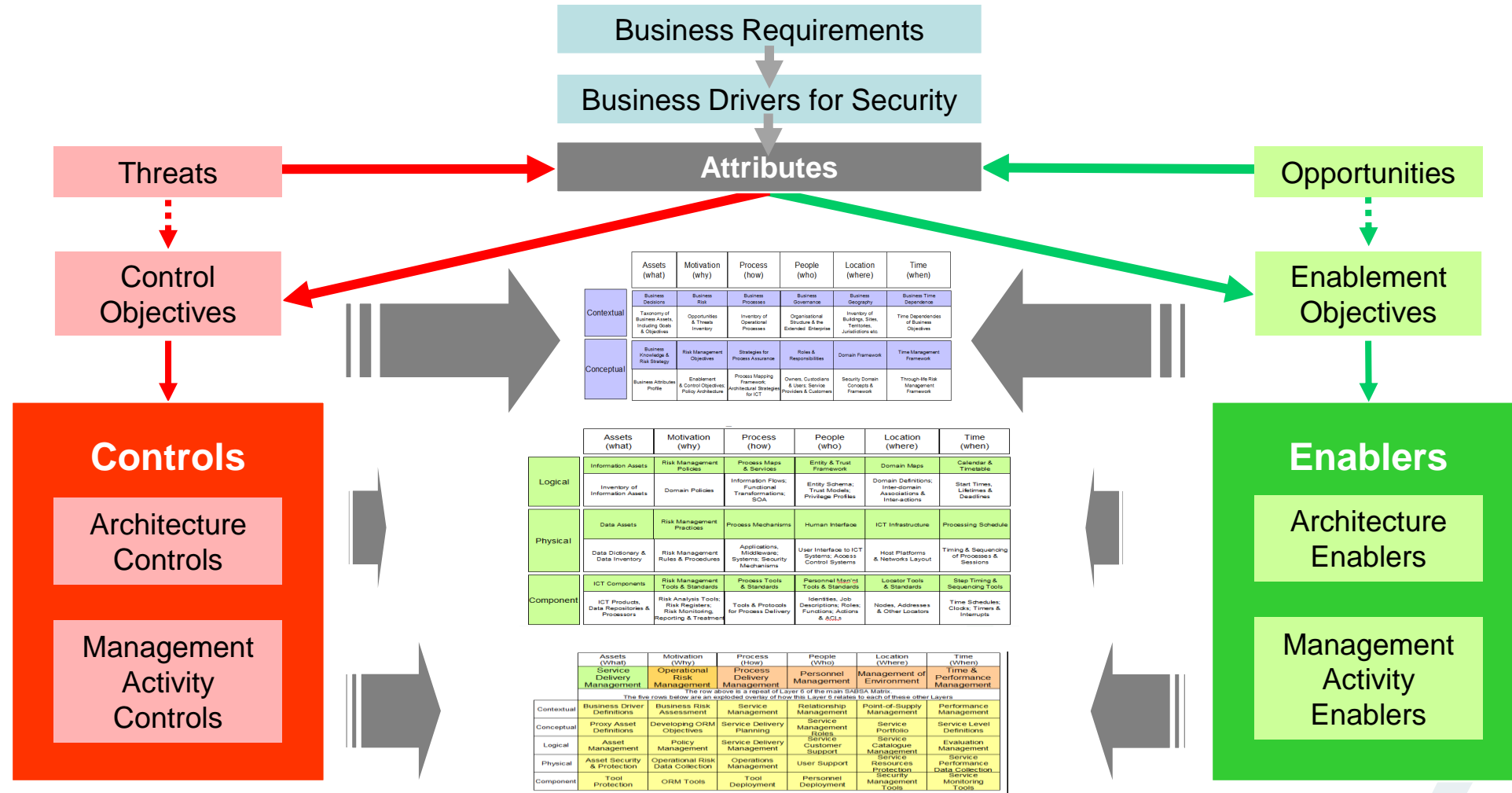
SWOT Analysis in SABSA Strategy & Planning

SWOT Methodology

- Step 1: Analyse threats and opportunities (external)
- Step 2: Analyse strengths/weaknesses (internal)
- Step 3: Use strengths to exploit opportunities and to confront threats
- Step 4: Mitigate weaknesses that might be exploited by threats and convert them to strengths
- Step 5: Search for ways of improving weaknesses that might hinder the exploitation of opportunities
- Step 6: Where you cannot mitigate a weakness to a threat, avoid that type of business



SABSA Controls & Enablers Derivation



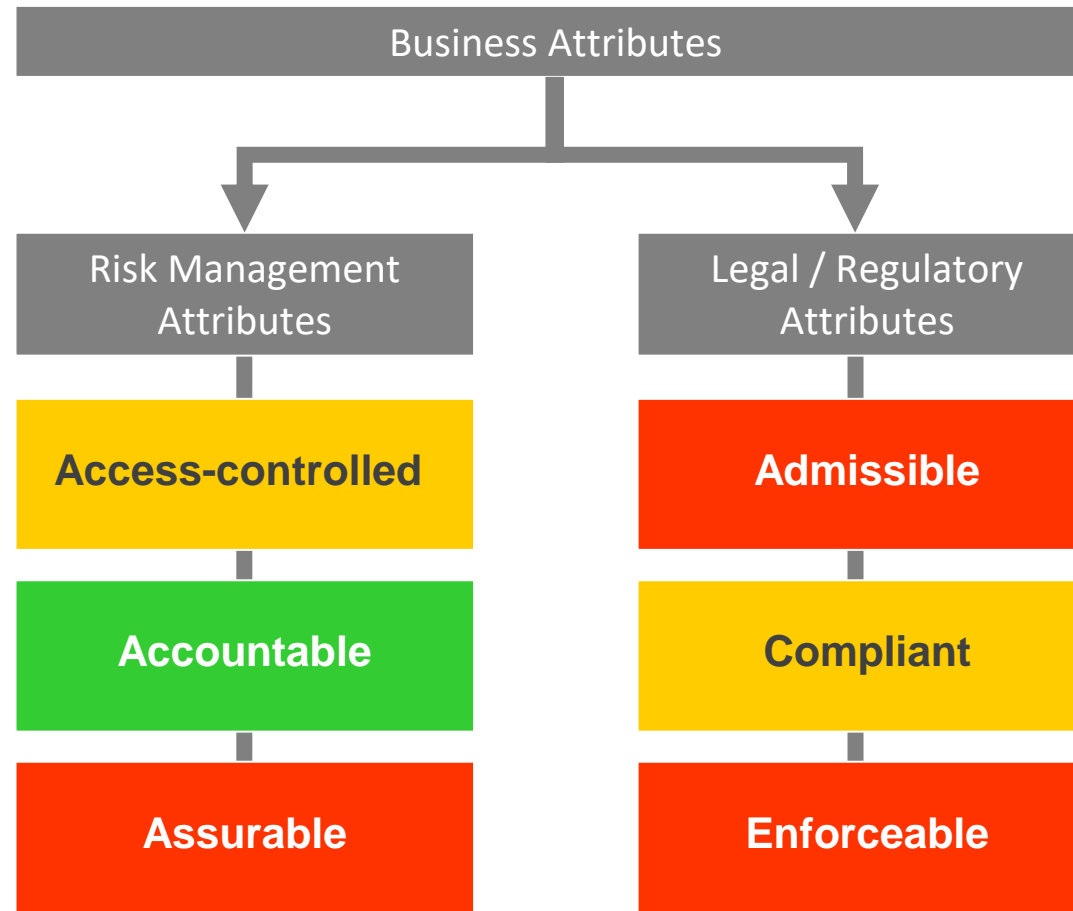
SABSA Risk Management Tools

- Risk register
 - Contains details of all risks identified during risk assessment
 - Primary repository of risk information
 - Used for risk tracking and future risk assessment / risk control initiatives
- Risk treatments plan
 - Planned remedial actions
 - Cross-referenced in the risk register

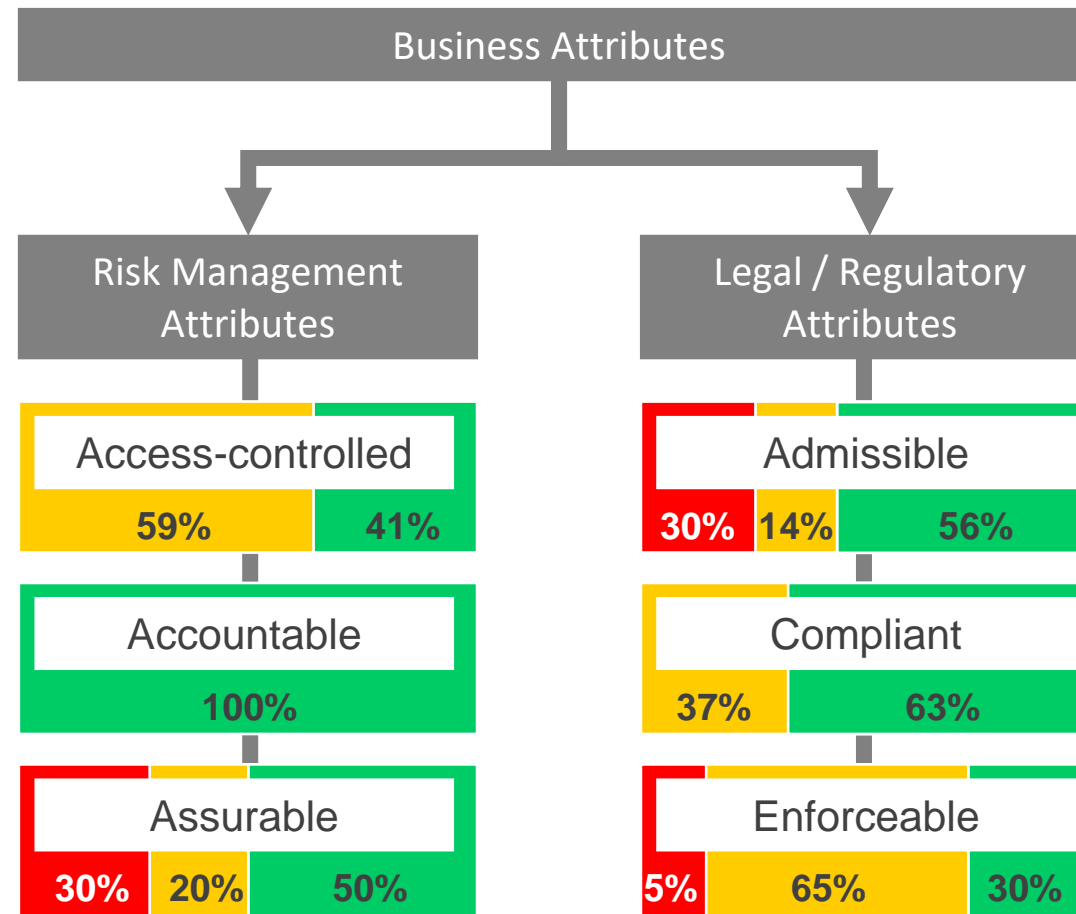
Dynamic Risk Dashboards

- Real-time updating of the risk register
 - Automated feeds from business applications
 - Automated calculation and display of Key Risk Indicators (KRIs)
 - Traffic light reporting
 - Integration of information across the entire enterprise
 - Single corporate version of the truth
 - Forecasting problems rather than viewing history

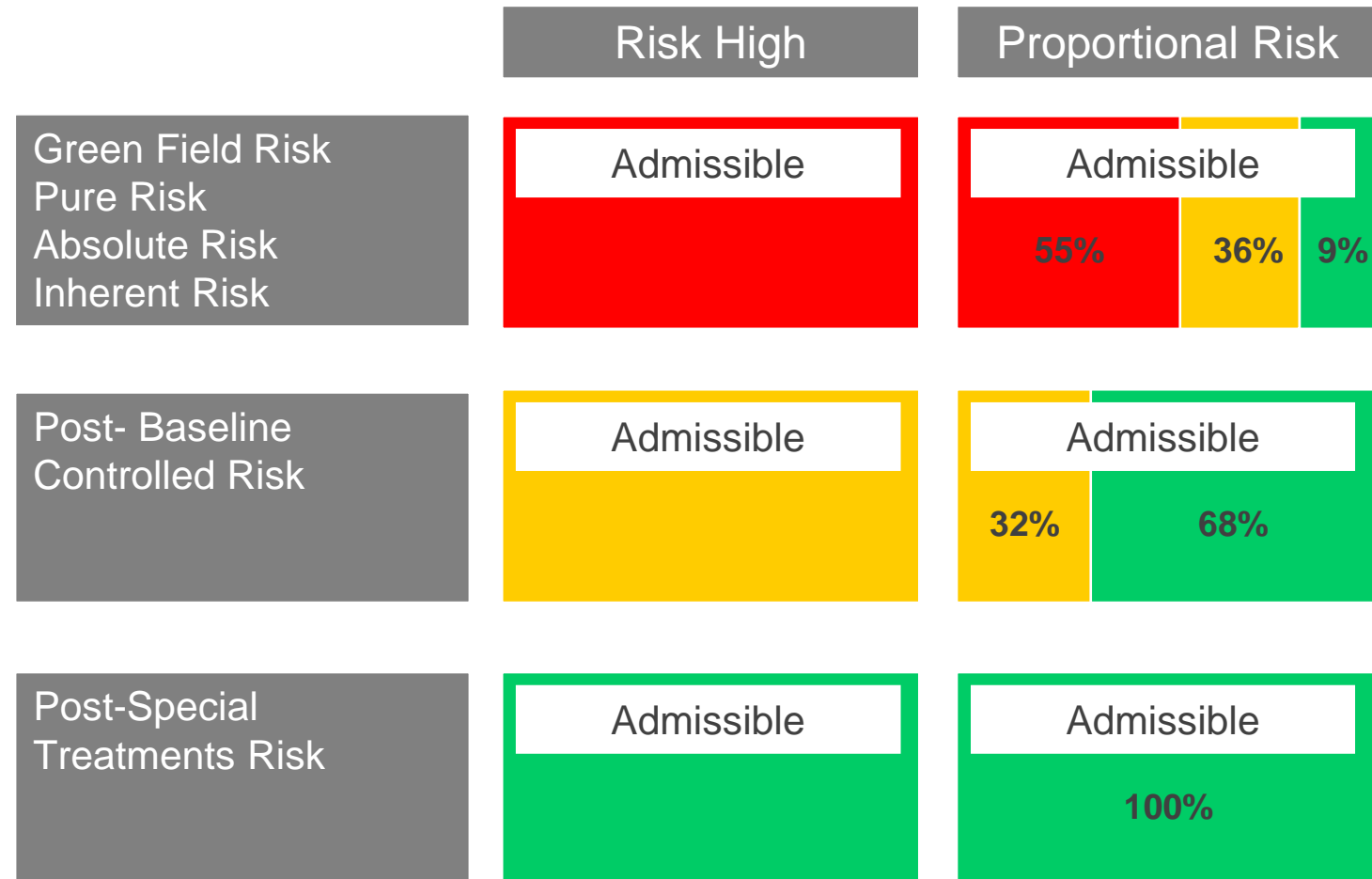
Risk-High Dashboard



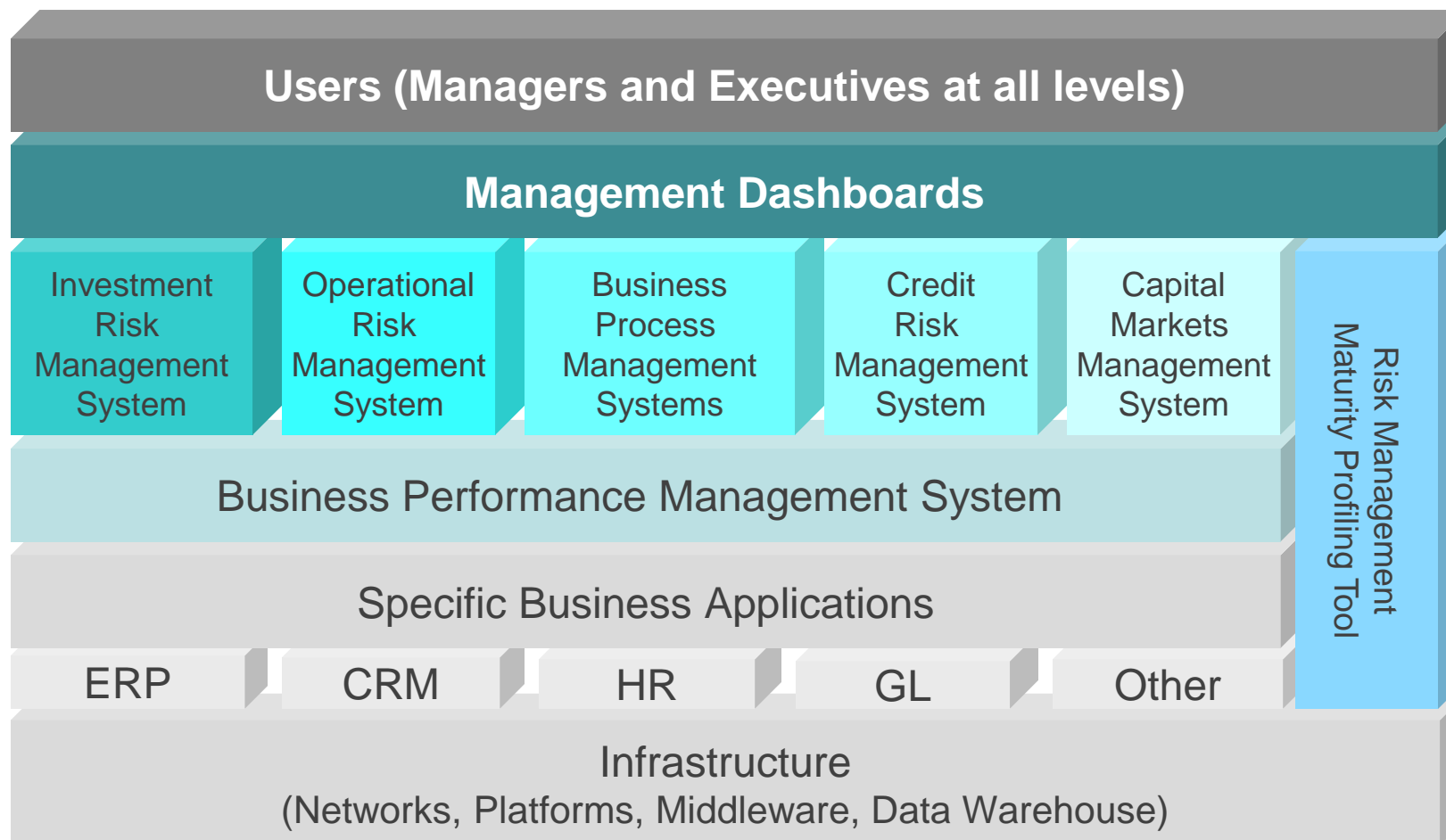
Proportional Risk Dashboard

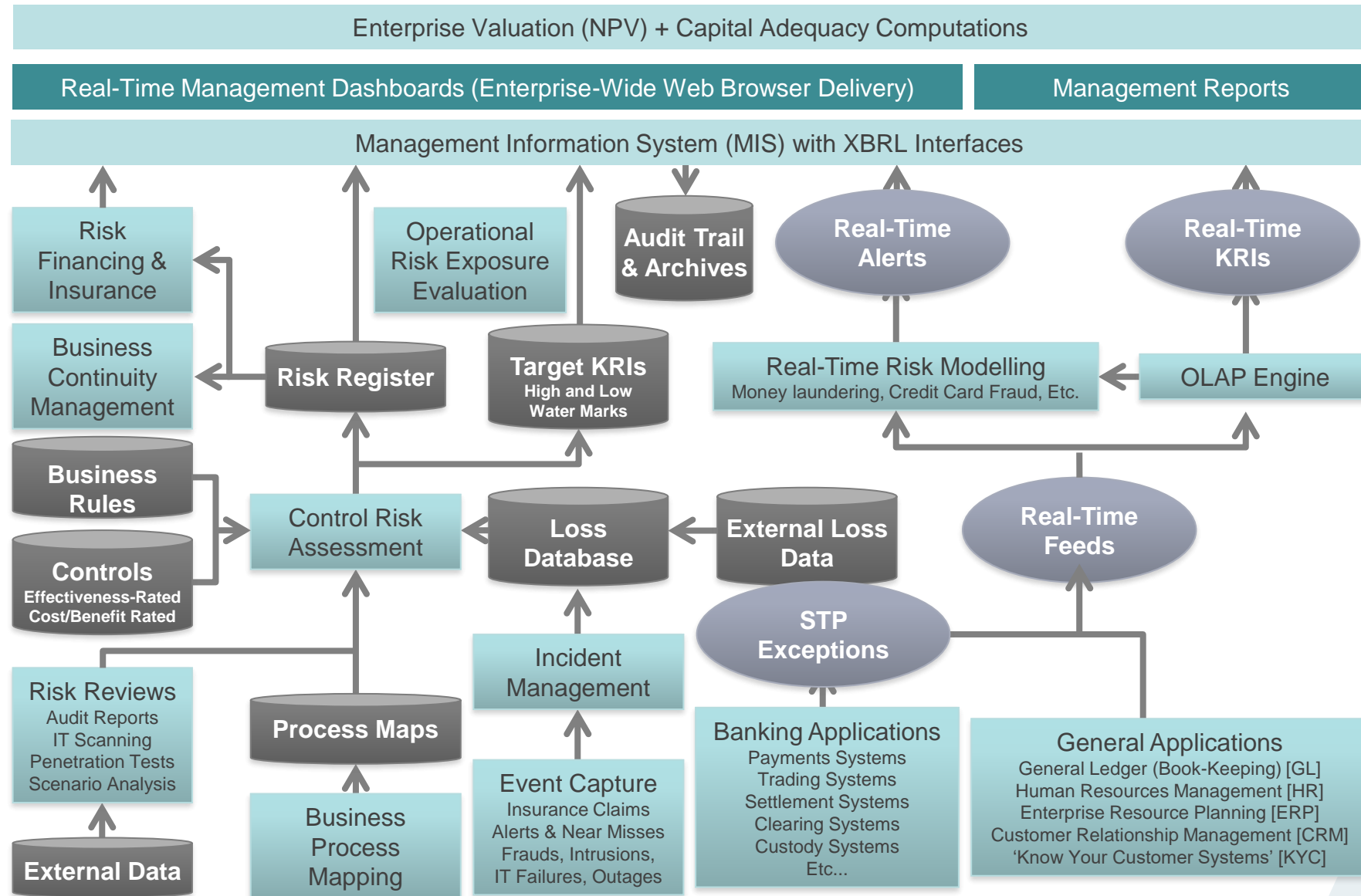


Progressive Treatments Risk Dashboard



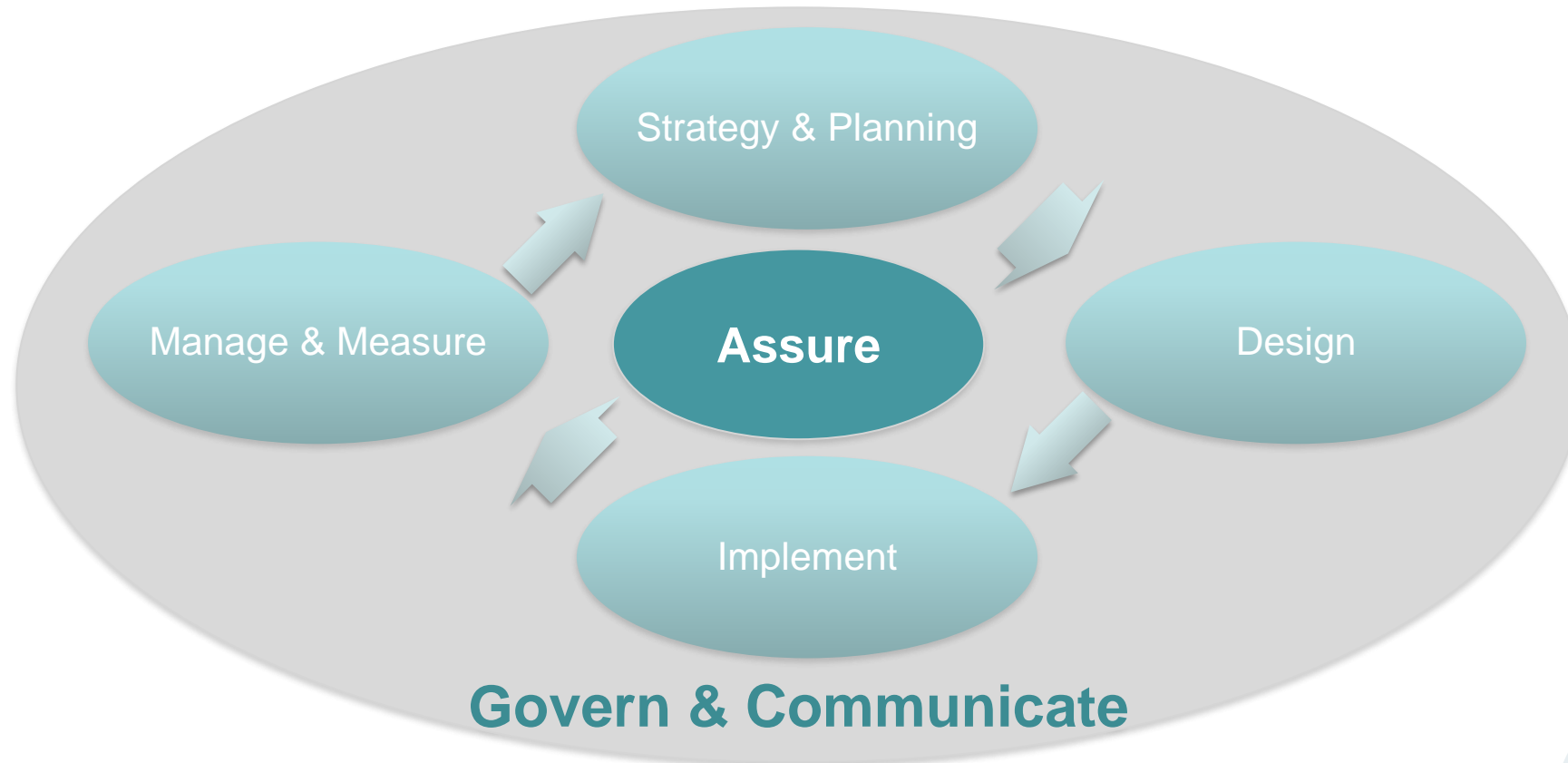
Integrated, Automated Enterprise Risk Management: Overall Solution Architecture





SABSA Risk Management Process

The SABSA RMP is the subject of Advanced Module A1
'Risk, Assurance & Governance'



Policy Architecture

Section 7

Section 7 Competency Objectives

Competency / Question Domain 2 – Why (Motivation)

Knowledge Element	Knowledge Competency	Comprehension Competency
Policy Framework	<p>Identify drivers for, and objectives, benefits & applications of, the SABSA Policy Framework</p> <p>Describe the SABSA Policy Framework & identify each of its layers and components</p>	<p>Summarise how the Policy Framework approach is applied to meet objectives & deliver benefits</p> <p>Differentiate between layers of the Policy Framework and summarise the population of each</p>
Policy Domain Concept	<p>Describe the SABSA Policy Domain concept</p> <p>Identify & describe Policy Domain inter-actions in terms of Risk Appetite Distribution and Risk Performance Aggregation</p>	<p>Discuss the rules, features, functions and objectives of Policy Domains</p> <p>Explain the SABSA approach to ownership, responsibility, conflict resolution, exception authorisation, and systemic risk management, in both hierarchical and peer relationships between policy domains</p>
Policy Domain Model	<p>Identify issues with multi-dimensional Policy Domain Architectures</p> <p>Describe the use of the Policy Framework & Policy Domain concepts to create an Enterprise Policy Domain Model</p>	<p>Explain the SABSA approach to modelling multi-dimensional domain policies</p> <p>Construct a SABSA Enterprise Policy Domain Model</p>

Real-world Issues & SABSA Objectives

Drivers for a SABSA Approach

Issue	SABSA Objective
Policy-driven business	Business-driven policy
Business-inhibiting	Business-enabling
Reactive & unpopular	Proactive & welcomed
Pushed by security, audit & compliance check-lists	Proportional, prioritized & traceable to business needs
Complex & conflicted	Simplified & hierarchical
High maintenance & Cost of ownership	Multi-layered architecture for ease of use & maintenance
Policy authority does not understand or support policy	Policy authority has clear risk ownership & vested interest

What is Policy?

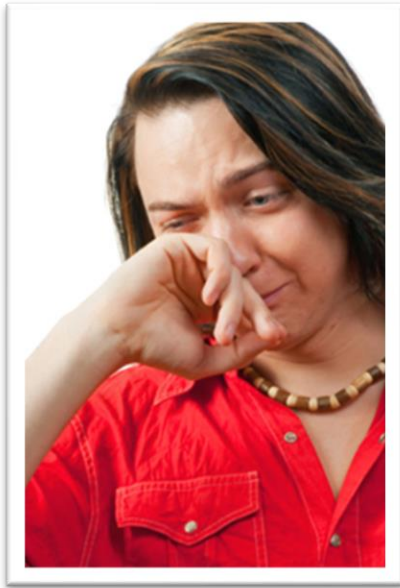


- A Definition (according to Oxford English Dictionary)
 - A course or principle of action adopted or proposed by an organisation or individual
- Policy Architecture
 - Policy Architecture is the discipline of embedding an organisation's intended objectives into a structured set of documents that direct, influence and motivate the organisation's resources and capabilities (people, systems, processes) to best meet the objectives
 - Policy articulates the organisation's approach to realising opportunity for gain (enablement objectives) while minimising loss (control objectives) according to stakeholder Risk Appetite
 - Policy is an important element of Governance and (like the objectives it contains) is a dynamic, living, breathing entity that exists at a range of levels

Psychology of Workplace Motivation

Frederick Herzberg (1959)

- Dissatisfiers (pain / demotivates)



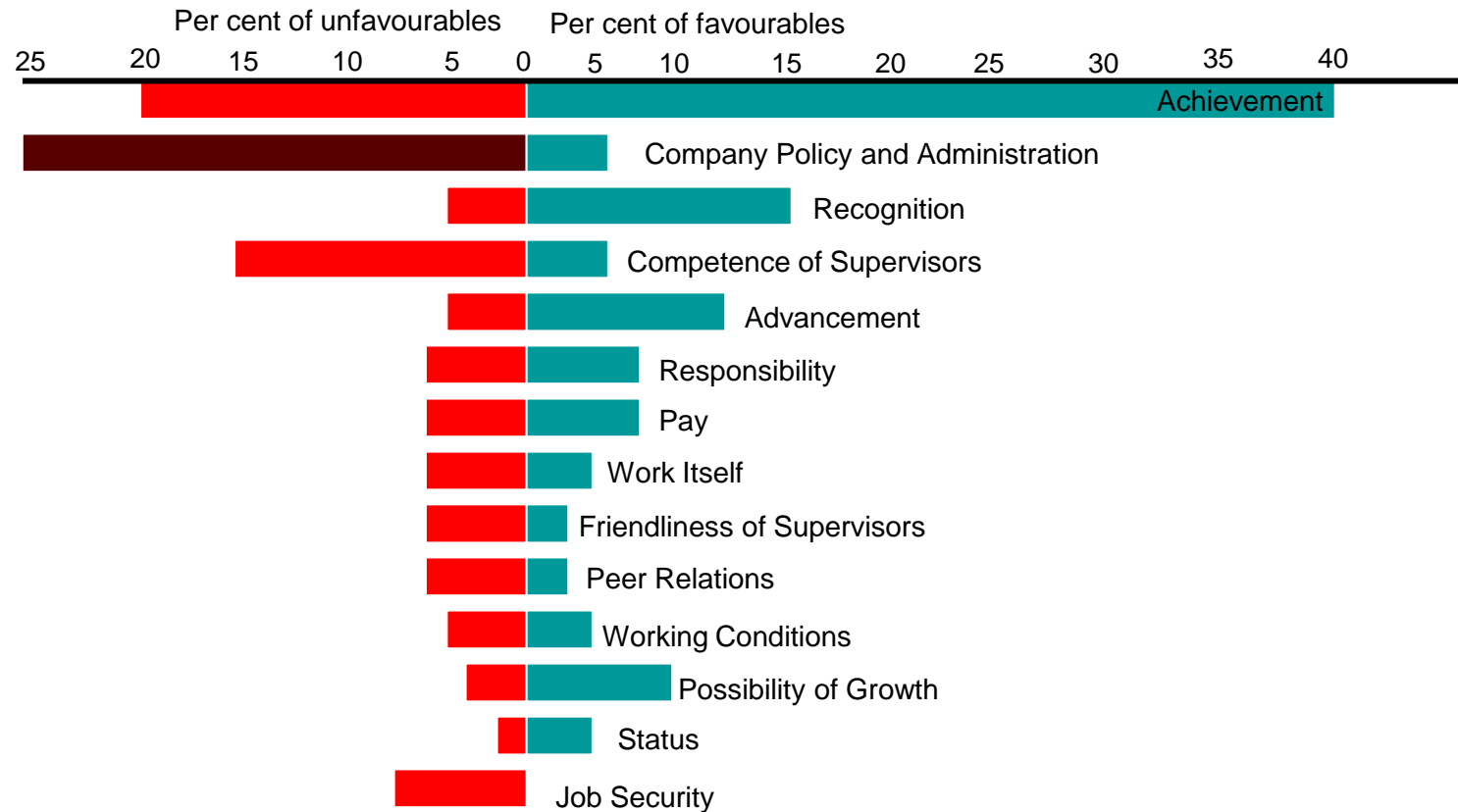
- Satisfiers (pleasure / motivates)



- So what is consistently the greatest cause of dissatisfaction (demotivation/pain) in the workplace?

Psychology of Workplace Motivation

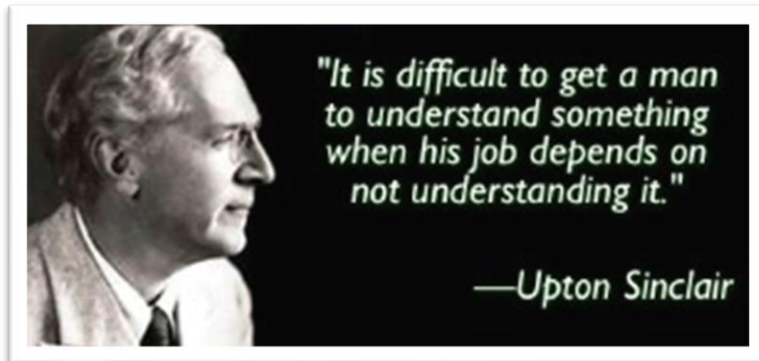
M. Scott Myers (Texas Instruments)



Policy: The Single Biggest Demotivator

Vested Interest Makes Things Happen

- It is impossible / unsustainable to try to make humans do something they do not want to do or to stop them doing something they do want to do
- Policy should leverage vested interest to motivate, engage and empower



Psychology of Influence & Motivation

Policy Structure & Content

- Address your message only to the group of people whose opinion or behaviour you seek to influence, do not attempt to make your communication a 'catch-all' for everyone
- Speak only in the language, concepts and terminology used by the group whose opinion or behaviour you wish to influence
- Address only those issues that are of interest to the group whose opinion or behaviour you wish to influence
- Prioritise your material, presenting the most important messages first
- Scientific approach of logical argument does not necessarily work with senior executives
 - Consider the effect in our case study of 7 different proposal summaries tuned to the vested interest of each Stakeholder

Security Domain Definition

Vested Interest Through Risk Ownership

- A security domain is a set of elements subject to a common security policy defined and owned by a single security policy authority
- Every domain has a Policy Authority – the owner of risk TO that domain
 - CFO owns risk TO the Finance Domain
 - CTO owns risk TO the Technology Domain



Domain
(policy)

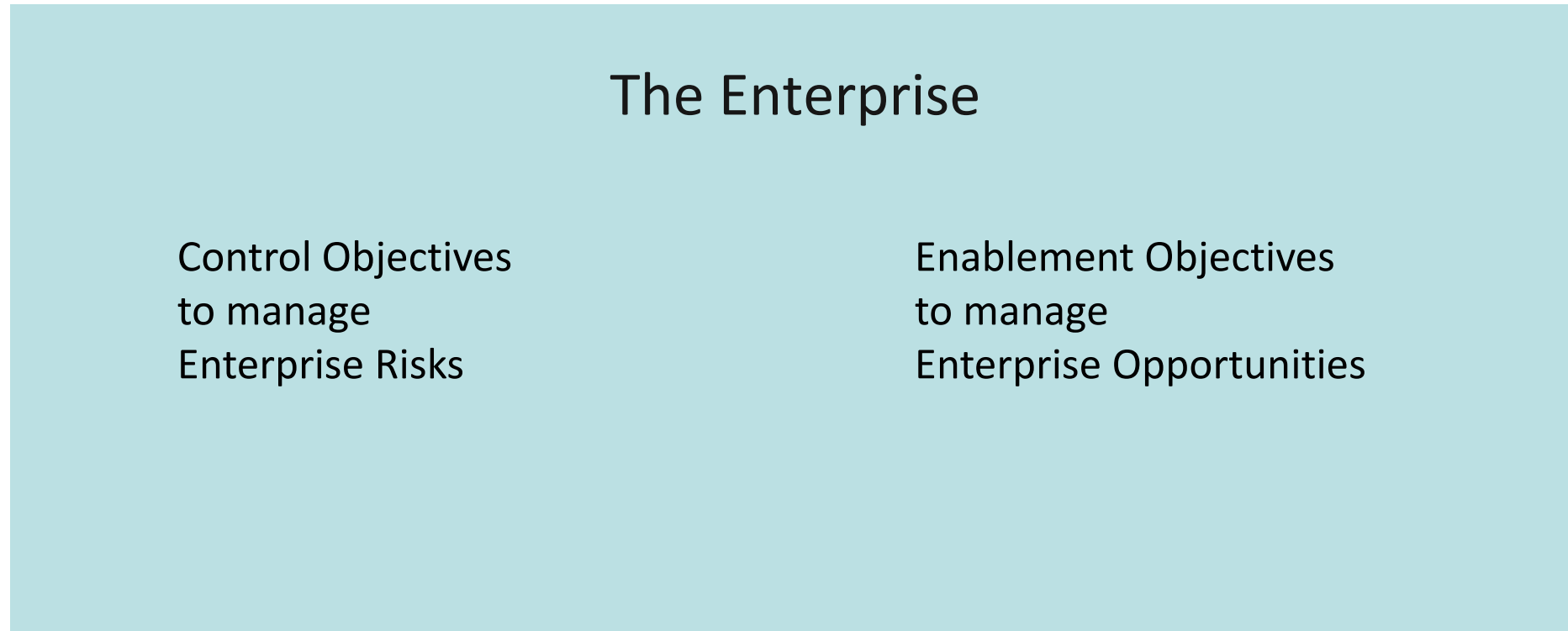
Domain Risk Accountability & Responsibility

Vested Interest Through Risk Ownership

- Each Policy Authority in the SABSA Policy Framework is accountable for the risks and opportunities to their own domain-level assets (attributes), goals & objectives
 - They are unquestionably the primary subject matter expert
 - They know more about risks to their domain than anyone else
 - They have vested interest in their own critical success factors
 - Therefore they issue and sign policy for their own domain
- However, they may then delegate responsibility for complying with their policy and achieving their performance target

Domain Levels

Contextual Domain – The Enterprise



- Who owns the risk TO The Enterprise as a whole? (CEO)

Domain Risk Accountability & Responsibility

The Risk Appetite Distribution & Policy Delegation Issue

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

- But how does the King check the horseshoe nails?

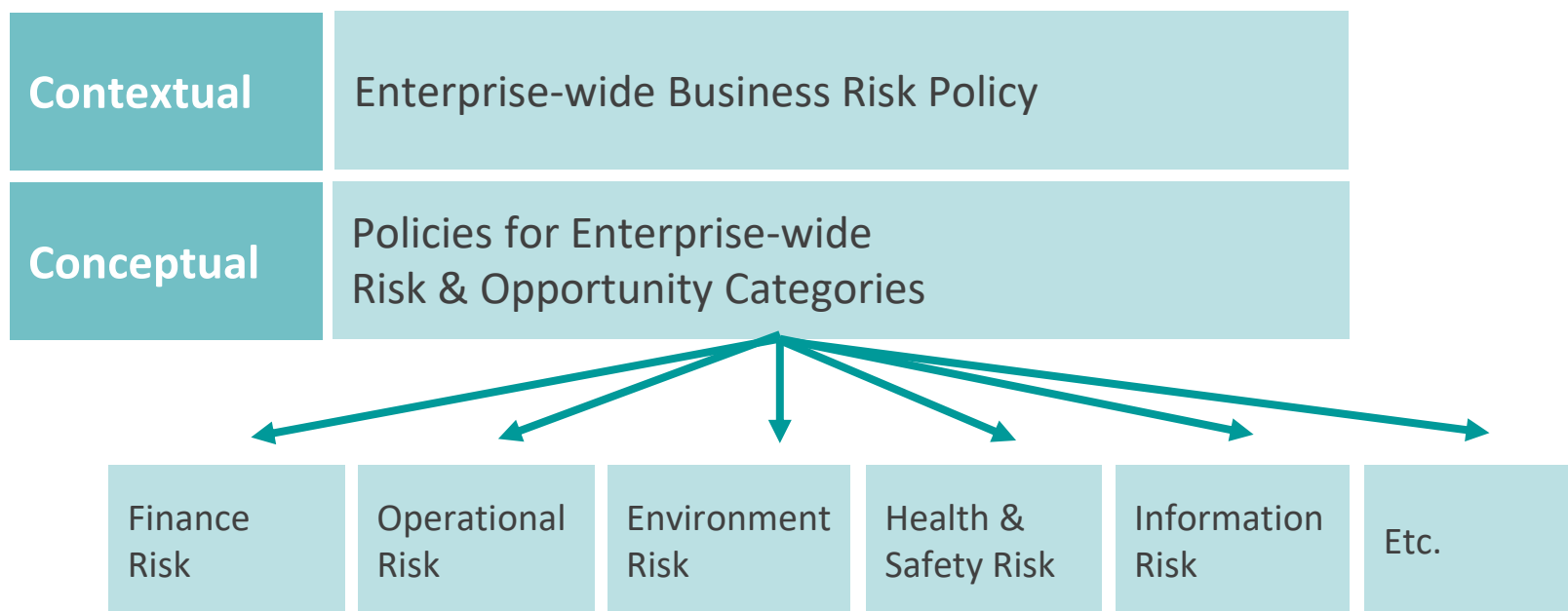
Risk Appetite Distribution & Policy Delegation

Accountability & Responsibility Embedded in Domain Architecture

- Although he is Accountable for the Risk & Opportunity performance of his Domain, the Domain Policy Authority (in this case the CEO) cannot possibly do everything himself
- He distributes risk appetite and risk management responsibility to lower level subdomains each of which is responsible for managing a subset of the overall risk and opportunity
- The Policy Authorities for these lower level subdomains are subject matter experts who from a risk reporting perspective report to him
- They therefore set policy for their own domain in the context of meeting the risk and opportunity performance levels of their superdomain authority:
 - Their policy must comply with, meet the needs of, and be authorised by, their super domain authority

Domain Levels

Conceptual Domains – Enterprise Risk Dimensions, Concepts & Strategies



- These Conceptual Domains are NOT Departments
- They are Enterprise-wide Policies covering Risk dimensions, types or categories (subdomains of Enterprise Risk)

Domain Levels – Conceptual Risk Domains



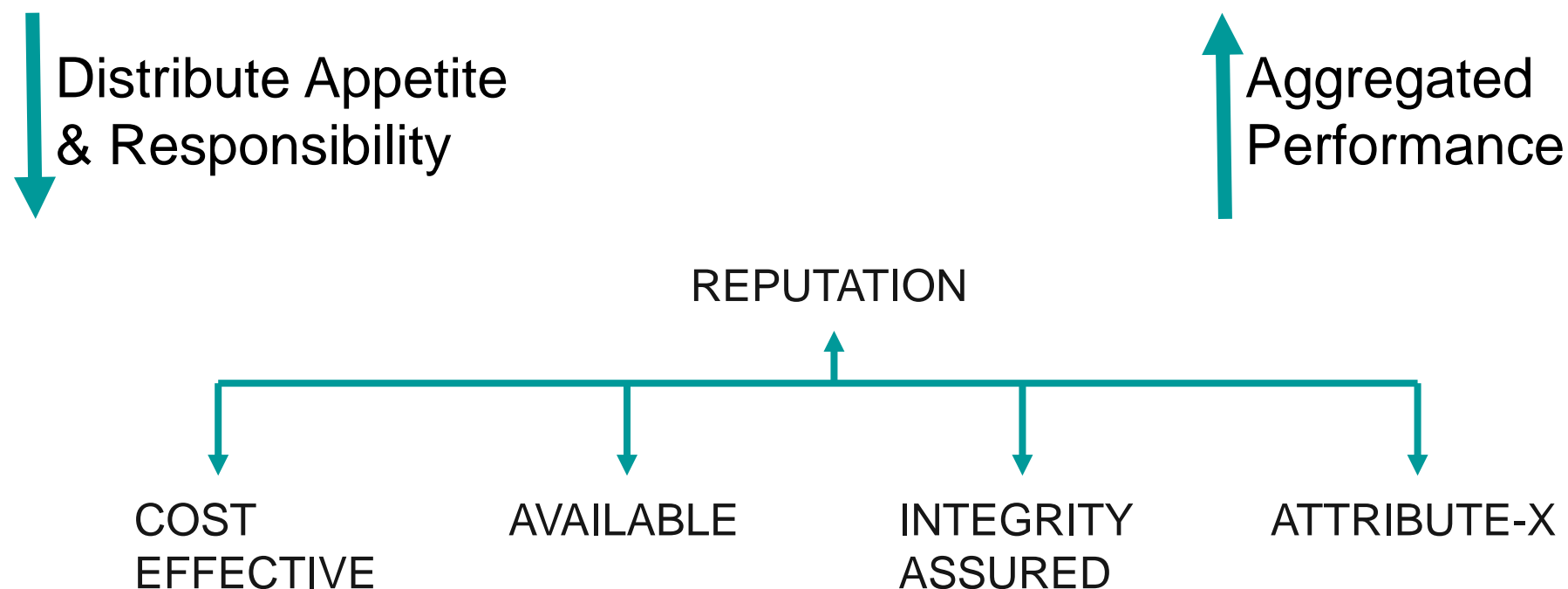
Risk Appetite Distribution & Policy Delegation

The Role of Attributes in Domain Architecture

- Attributes are a representation of the ‘things that matter most’ to any Stakeholder
- The first rule of Attributes is that they must be measurable
- The performance targets represent the appetite thresholds for Risk and Opportunity
- The Attributes can be Domain-specific
 - Reputation is owned in the Enterprise Risk Domain
 - Cost-effective is owned in the Finance Risk Domain
- The Attributes in any domain articulate the performance targets of that domain in relation to the requirements of its Superdomain
 - The performance of Subdomain Attributes contribute to and systemically impact those of the Superdomain

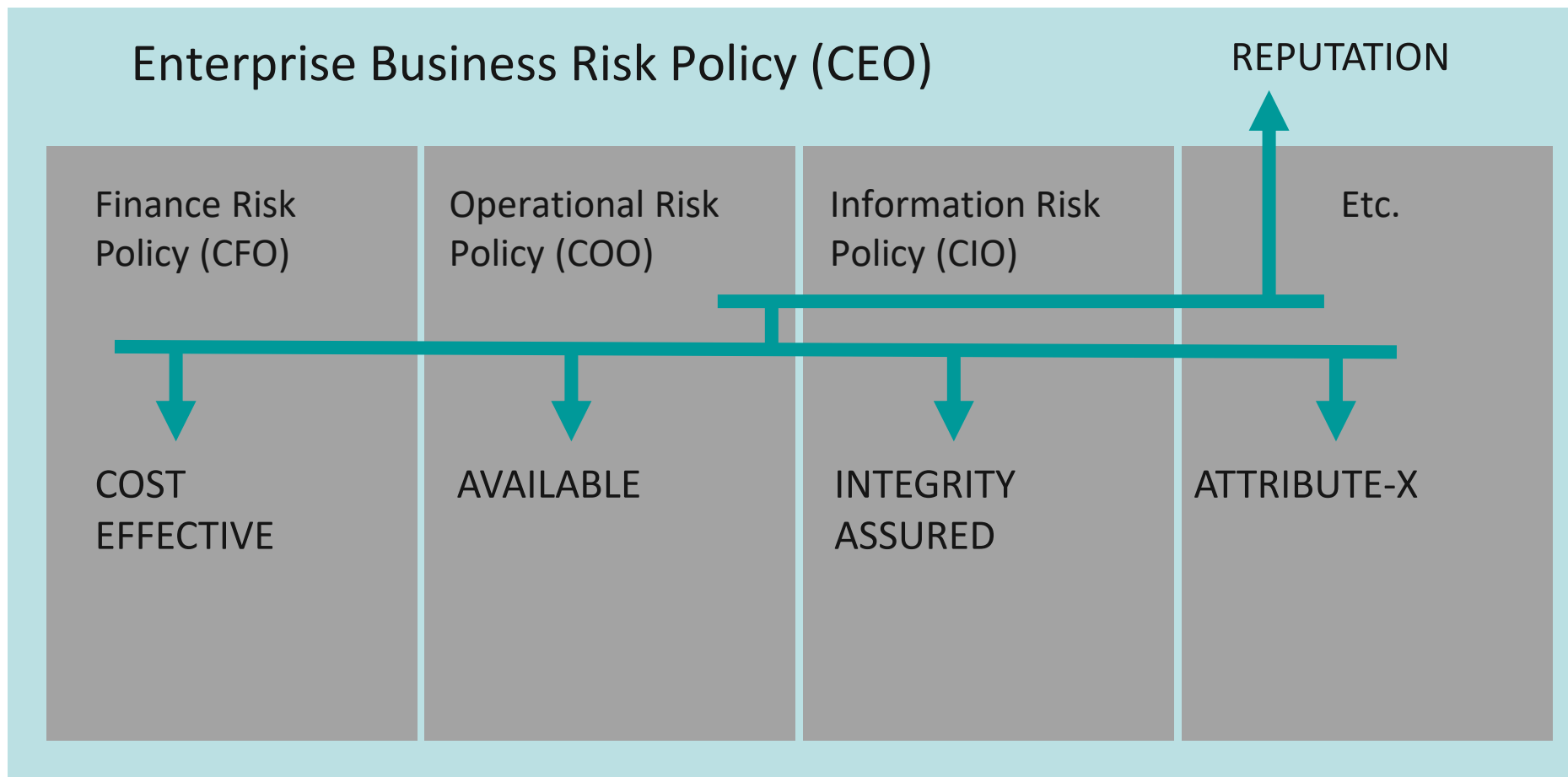
Risk Appetite Distribution & Policy Delegation

Multi-tiered Attributes in Domain Architecture



Risk Appetite Distribution & Policy Delegation

Multi-tiered Attributes in Domain Architecture



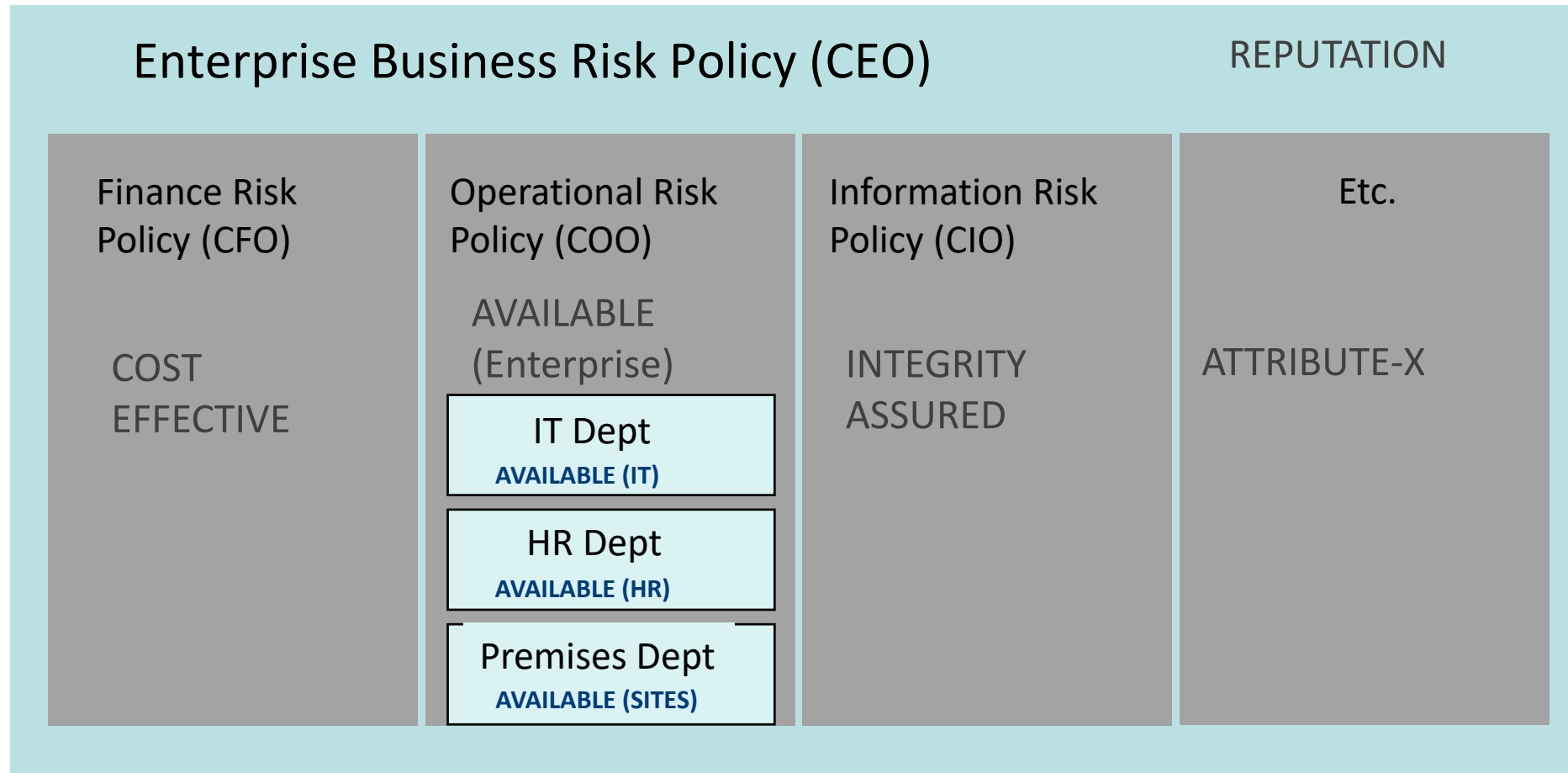
Domain Levels

Logical Domains

- A Logical Domain is:
 - A line of business
 - A logical classification (such as for information sensitivity)
 - A community of users such as a Department
- The Conceptual domains delegate some specialised part of their Enterprise Risk category to be managed by the subject matter experts of the Logical domains
- Logical domains interpret Enterprise Policy in more granular local terms (requirements for Security Services to secure Business information)
- The responsibility to manage risk takes the form of:
 - A compliance relationship
 - A service-provider or custodian relationship

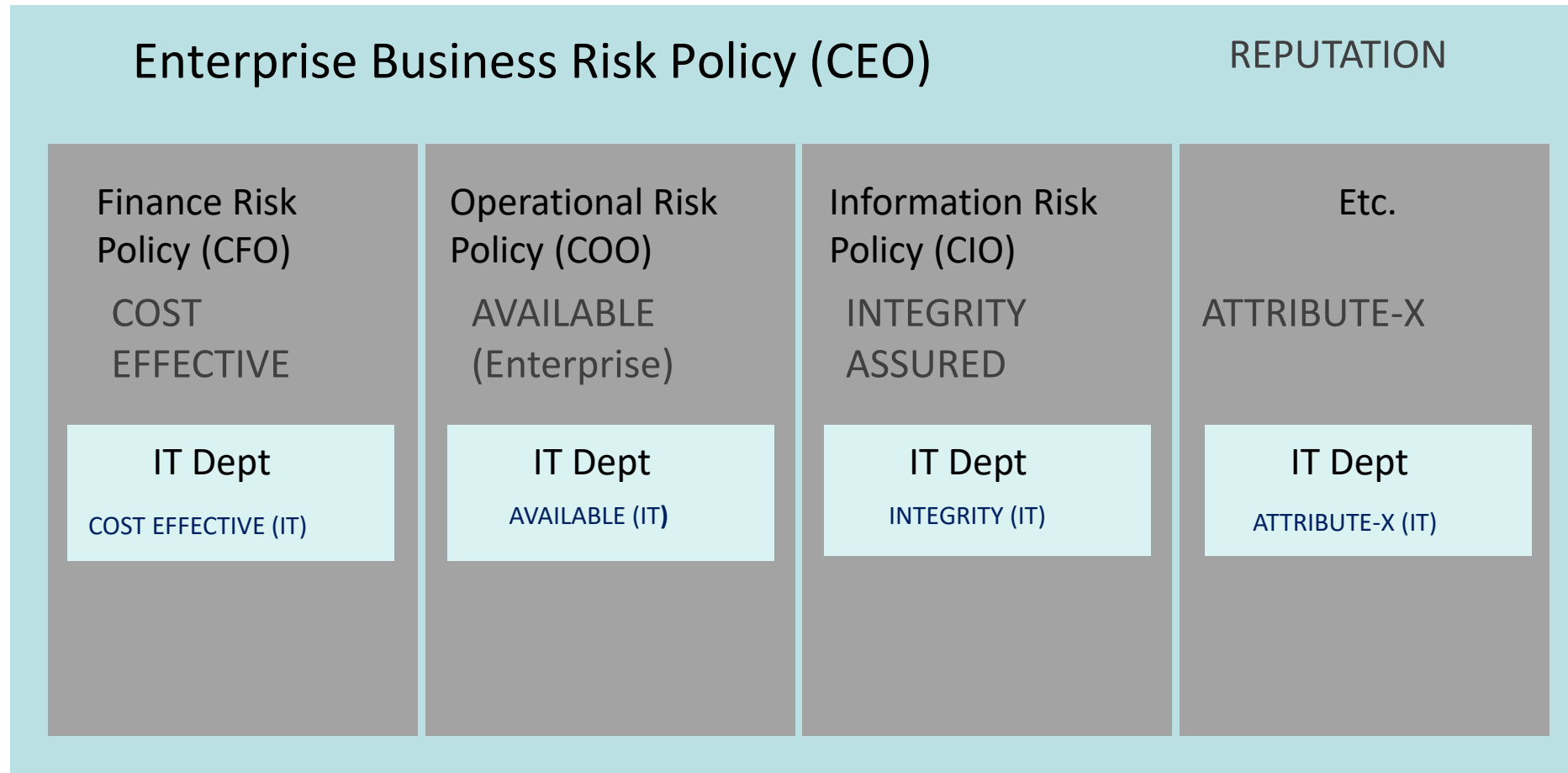
Risk Appetite Distribution & Policy Delegation

Enterprise Risk Distribution to Logical Domains



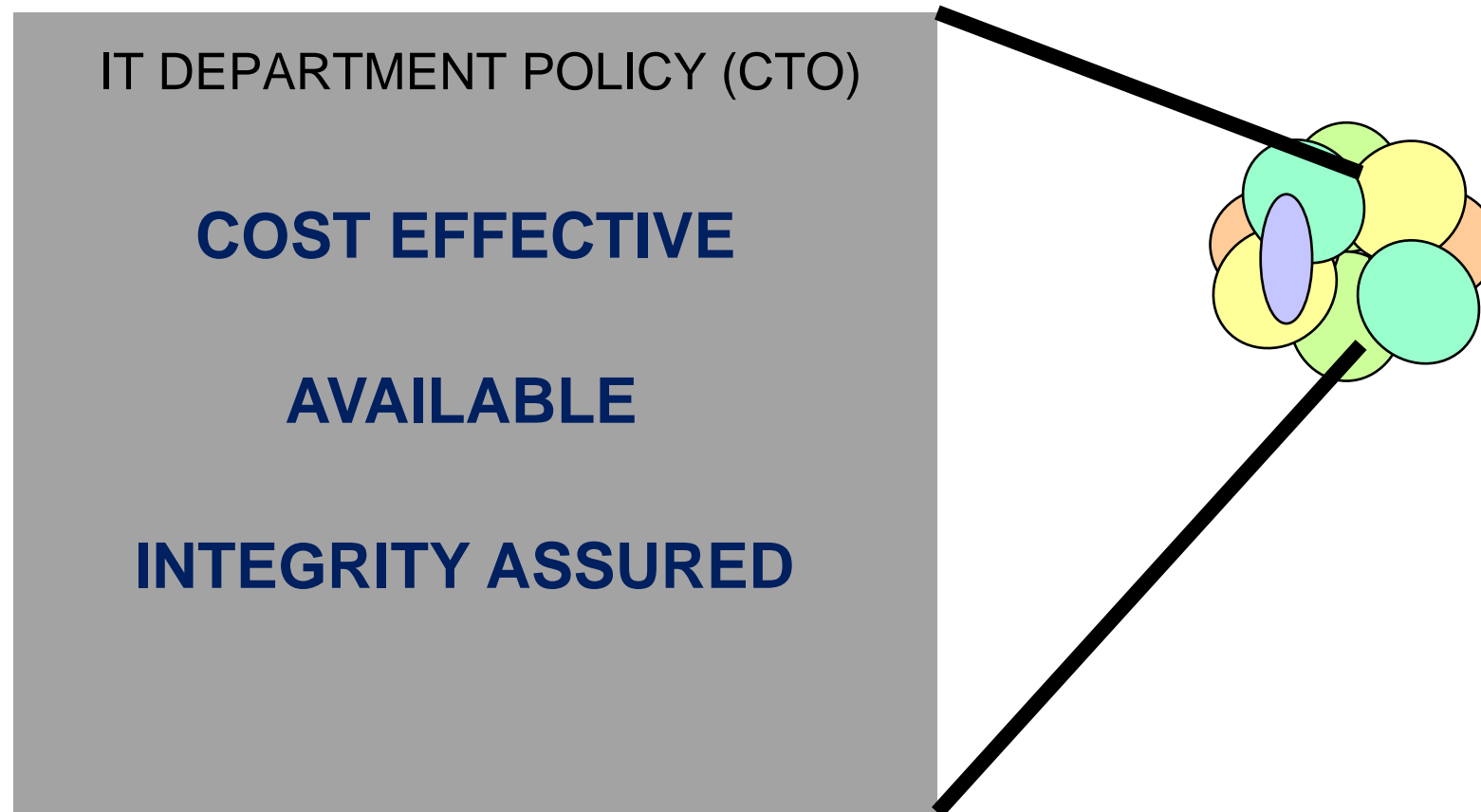
Risk Appetite Distribution & Policy Delegation

Enterprise Risk Distribution to Logical Domains



SABSA Policy Framework

Logical Domain Policy Defined to Serve Diverse Business Needs

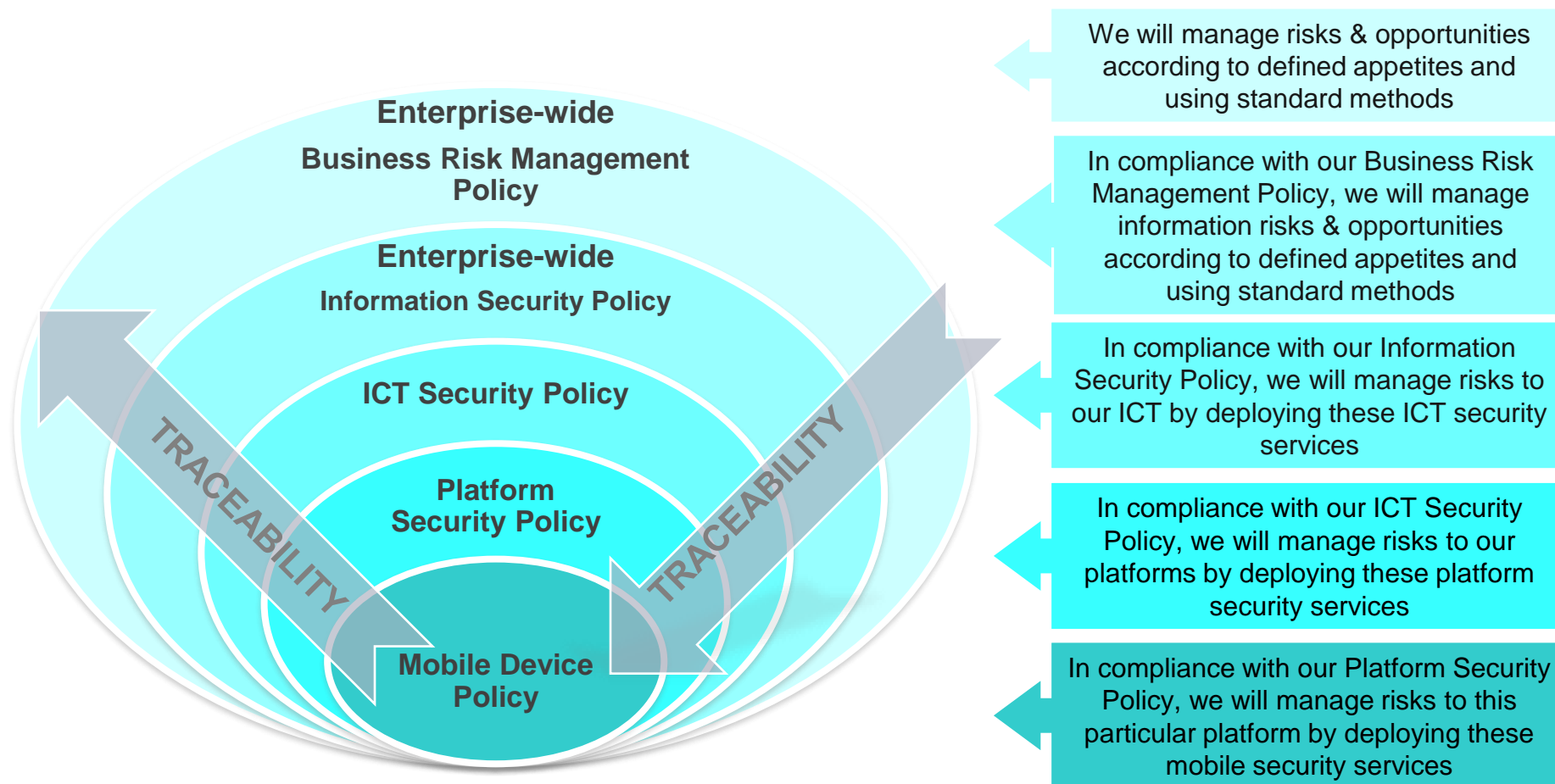


Domain Levels

Physical Domains

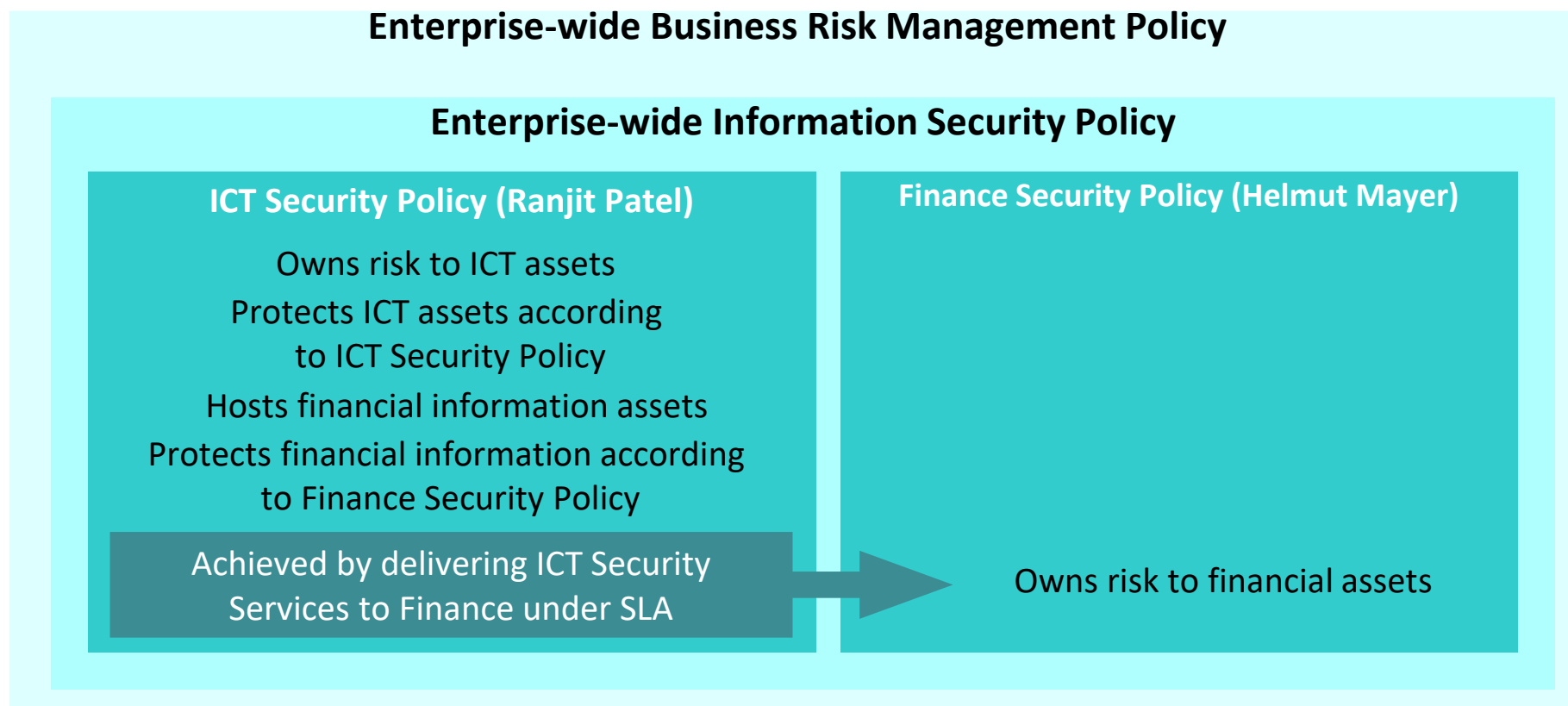
- A physical domain is a set of physical elements (in a specific physical location or technology layer) subject to a common security policy defined and owned by a single security policy authority
 - Territory, site, building, platform, network, system classification, etc.
- Physical Domains (such as Infrastructure) serve the needs of the Logical Domains (Business units)
 - A compliance relationship
 - A service-provider or custodian relationship

Vertical Traceable Distribution



Inter-domain Policy Relationships

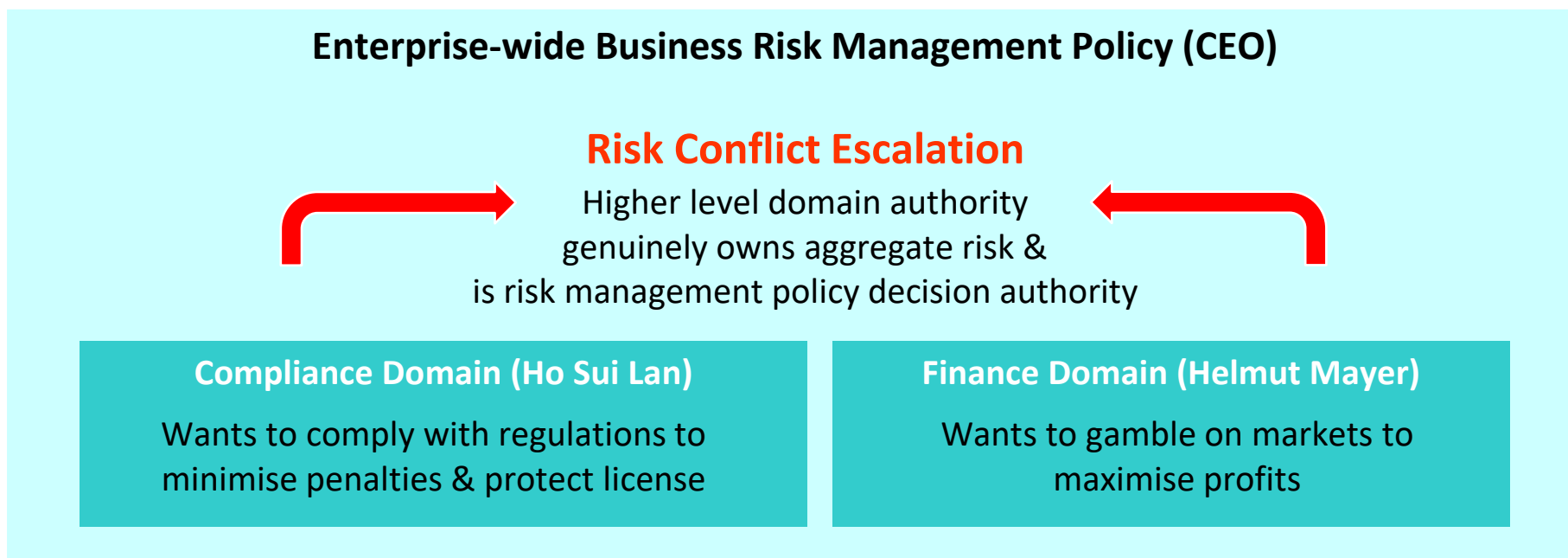
Peer Domain – Risk Ownership & Responsibility



The Policy Authorities share a common requirements language - Attributes

Inter-domain Policy Relationships

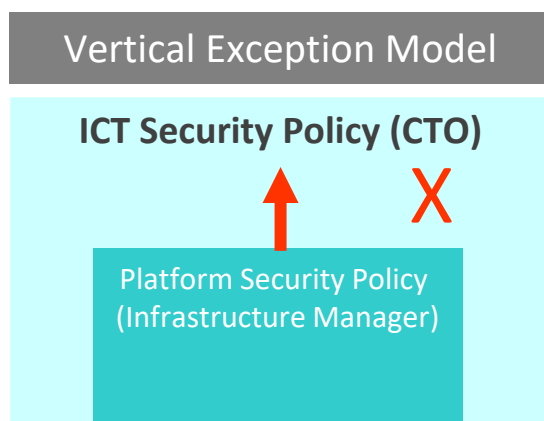
Peer Domain – Risk Conflict Resolution



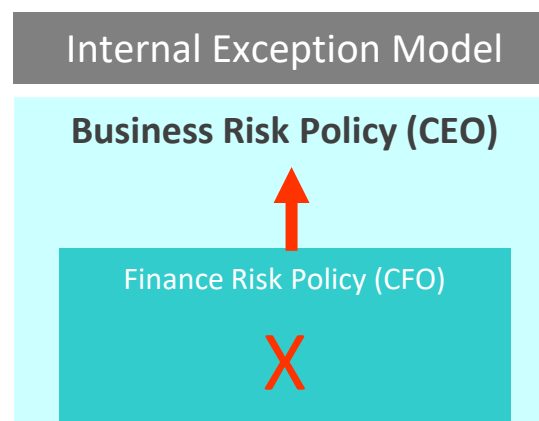
To avoid conflict of interest a single individual should not normally be the policy authority at more than one domain level simultaneously

Domain Policy Waivers & Exemptions

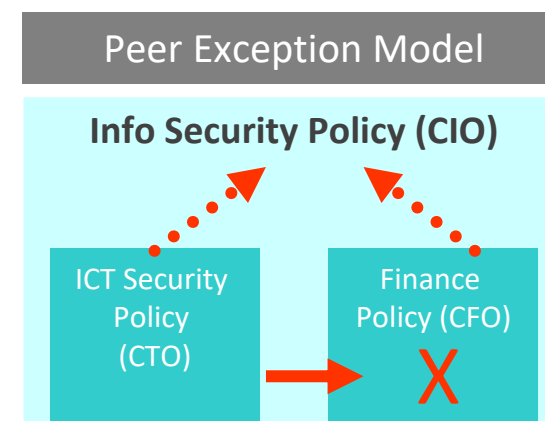
- Formal waivers & exceptions provide a mechanism to avoid policy violation
- Waivers & exceptions are based upon business case
- What are the criteria for allowing a waiver?



Request for exception to super domain policy authorised by super domain policy authority



Request for exception to own policy authorised by super domain policy authority (due to vertical systemic risk impact)

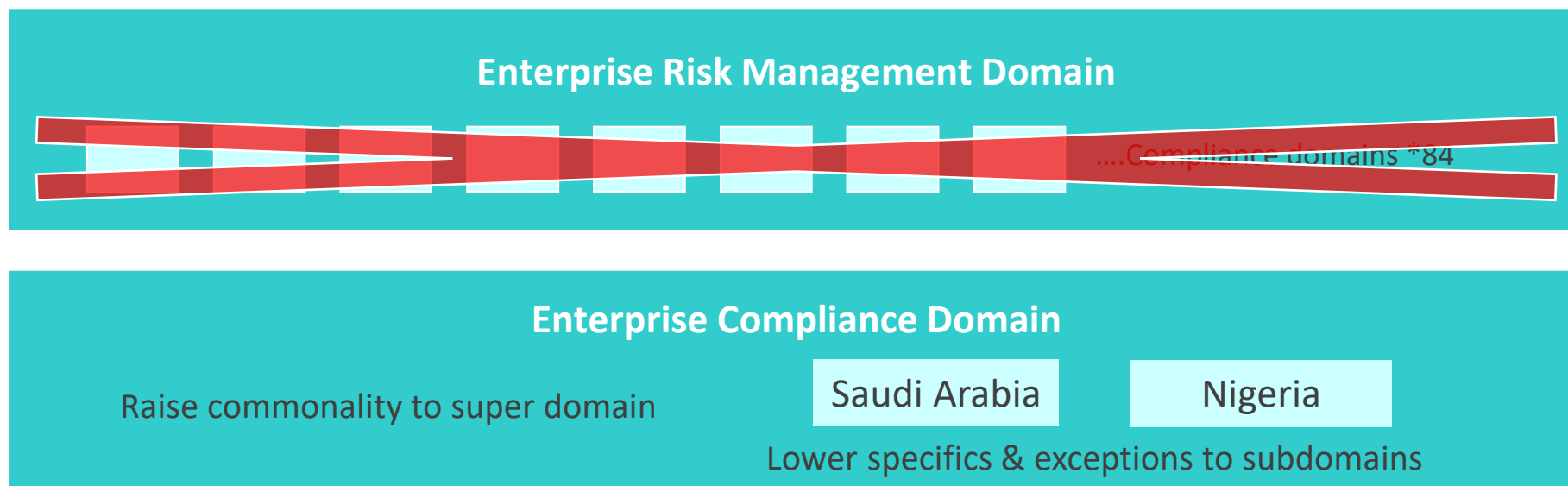


Request for exception to peer policy authorised by peer policy authority (with conflict resolution by super domain policy authority)

SABSA Policy Framework

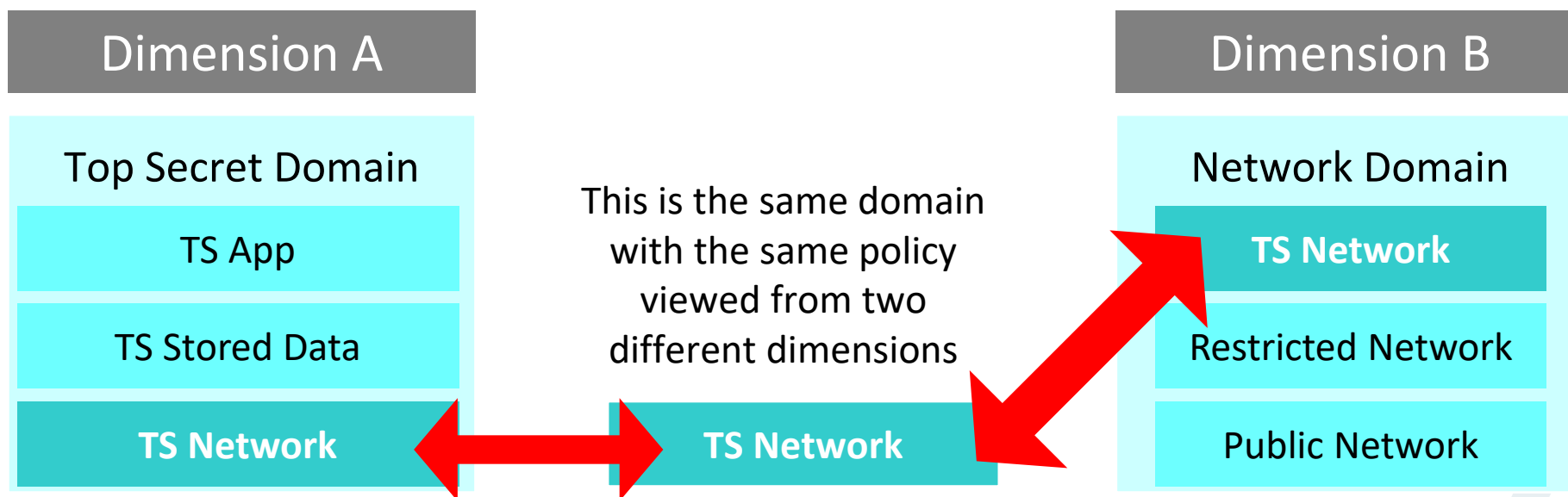
Commonality Moves Up – Exceptions Move Down

- Following the conventions of multi-layer architecture
- Example: IBFS operates in 84 countries but we don't want to maintain 84 separate policies



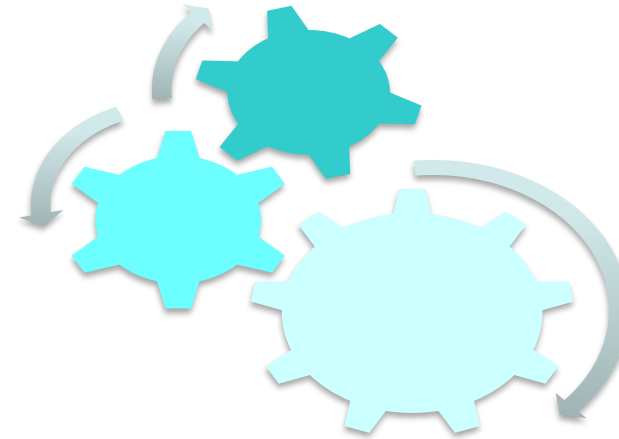
Multi-dimensional Policy

- Domains (and therefore policies) of many types can exist in multiple dimensions
 - Logical community domains by business unit and/or geography
 - Logical information domains by classification
 - Physical infrastructure domains (technology layer domains)



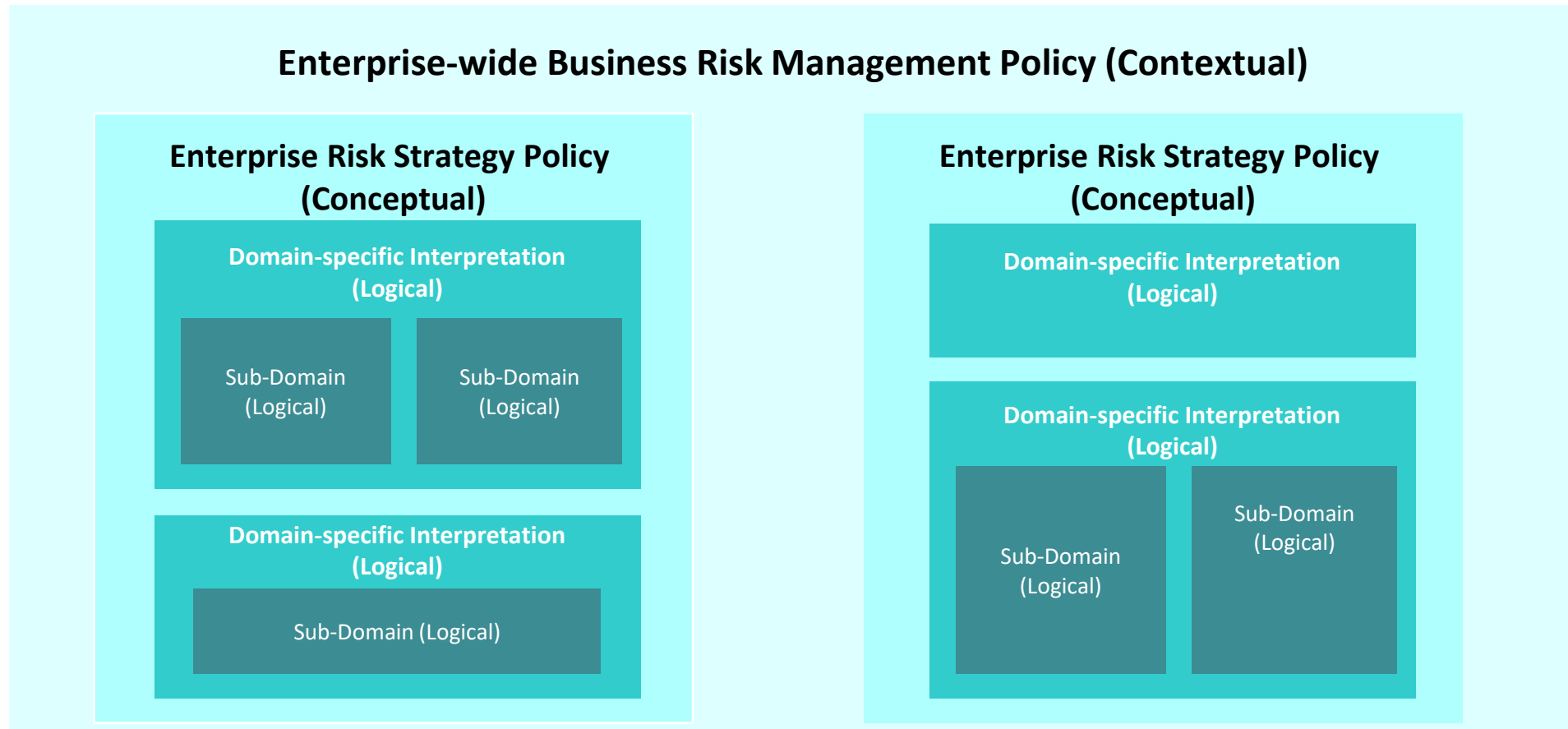
Multi-dimensional Policy – Domain Diagram

- The complexity of the real world means that multiple dimensions will almost always exist
- Multi-dimensional domain diagrams are complex and often confusing
- Guidance is to draw domain diagrams with single views
 - Specific views of the overall policy architecture for specific stakeholders (possibly including a compounded view of inter-sections)
 - According to the SABSA “rules of influencing opinion”



SABSA Policy Framework

Enterprise Domain Model Delivering All Concepts in this Section



SABSA Policy Framework

Policy has Multiple Iterations & Interpretations

- Policy terminology can be very varied
- The generic word “Policy” has many interpretations at multiple levels of documentation
 - Policy
 - Standards
 - Procedures
 - Guidelines
 - Operating Instructions
 - Standard Operating Procedures
 - Etc
- There is currently no Universal standard

SABSA Policy Framework

Policy has Multiple Iterations & Interpretations

- The security policy is determined by the business requirements for information management and information systems, following an assessment of the possible operational risks & opportunities
- Security policy is a statement of business requirements for security, translated into a logical structure that can be consistently applied, monitored and measured (using Attributes)
- The security policy states what logical services are required but as far as possible avoids any reference to particular physical mechanisms that will deliver the services
- Security policy documentation exists at a number of different levels, and hence it is useful to conceive of a hierarchically layered security policy architecture

SABSA Policy Framework

Overview of the Six-layer Policy Framework

Enterprise Policy	Contextual Policy (Business View)	Over-arching Business Risk Management Policy (Enterprise Wide)
	Conceptual Policy (Architect's View)	Policies for each Enterprise Risk Strategy (Enterprise Wide)
Domain Policy	Logical Policy (Designer's View)	Domain Policy for each Risk Strategy (Domain Level)
	Physical Policy (Builder's View)	Procedures & Practices for each Risk Strategy (Domain Level)
	Component Policy (Tradesman's View)	Detailed Standards and Rules for each Risk Strategy (Domain Level)
	Management Policy (Manager's View)	Detailed Security Implementation & Operation Guides (Domain Level)

SABSA Policy Framework

Overview of the Six-layer Policy Framework

Contextual	Enterprise-wide Business Risk Policy					
Conceptual	Policies for Enterprise-wide Risk & Opportunity Categories					
	Finance Risk	Operational Risk	Environment Risk	Health & Safety Risk	Information Risk	Etc.
Logical	Policies for Logical Domains	Policies for Logical Domains	Policies for Logical Domains	Policies for Logical Domains	Policies for Logical Domains	Policies for Logical Domains
Physical	Procedures for Physical Domains	Procedures for Physical Domains	Procedures for Physical Domains	Procedures for Physical Domains	Procedures for Physical Domains	Procedures for Physical Domains
Component	Standards for Nodes, Addresses, Components	Standards for Nodes, Addresses, Components	Standards for Nodes, Addresses, Components	Standards for Nodes, Addresses, Components	Standards for Nodes, Addresses, Components	Standards for Nodes, Addresses, Components

Policy Iterations in the Lower Layers

Example: Policy Architecture for Authentication

- Policy Statement (Logical Layer - Services):
 - When you enter my domain you must be authenticated to strength XYZ
- Procedure (Physical Layer – Mechanisms):
 - In this domain we will use Digital Certificate mechanisms
 - The procedure for using Digital Certificates is ABC
- Standard (Component Layer):
 - We will use X.509 standard certificates configured in the form OPQ
- Execution Instruction (Management Layer):
 - To execute procedure ABC execute application E; select menu option F; at the prompt take sub-option G

Enterprise Domain Decomposition

Enterprise Architecture Viewed Top-down Using SABSA

Contextual	Enterprise Domains (The Enterprise and Extended Enterprise)	Business Management Activities to Manage the Enterprise
Conceptual	Domains of Business Risk & Opportunity (Operations, Finance, Health & Safety)	
Logical	Logical Domains (Business Lines, Departments, Information Classifications)	
Physical	Physical Domains (Buildings, Networks, Devices, System Classifications)	
Component	Nodes, Addresses, Component Locations	

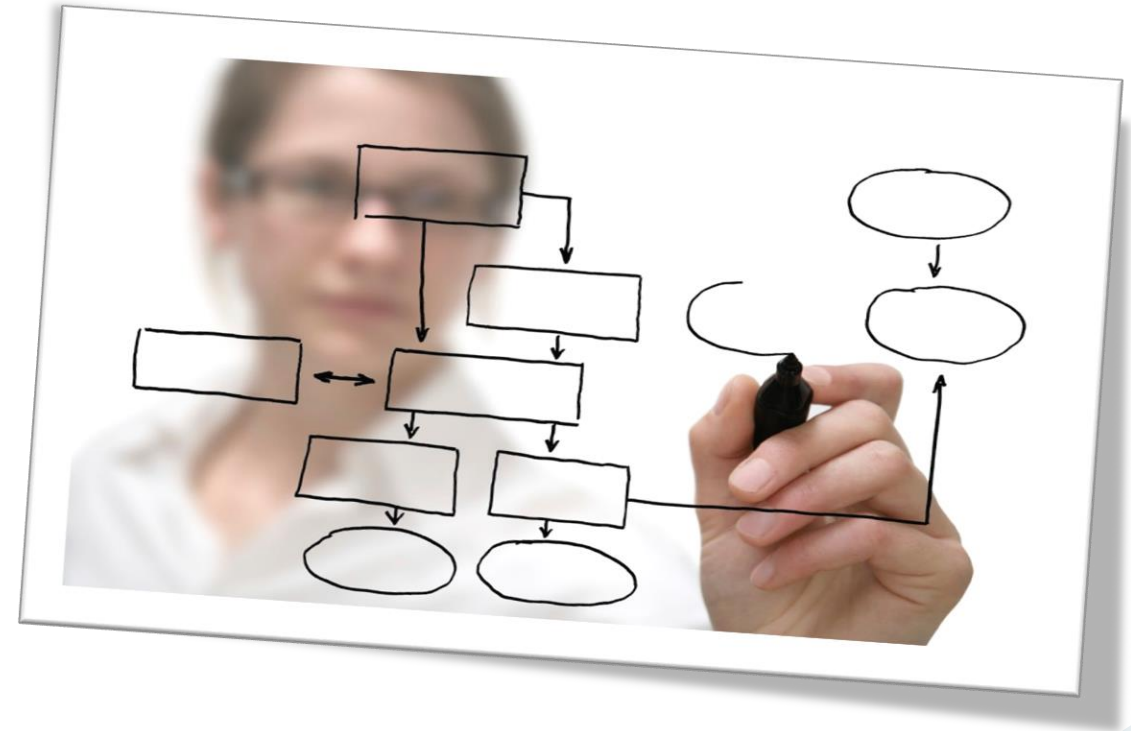
Enterprise Domain Decomposition

Security Policy Architecture Viewed Top-down Using SABSA



Workshop F1-3

Risk Management & Policy Architecture



Sample Questions

Competency Domain 2

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



Competency Domain 2

- Which ONE of the following types of policy applies at the Conceptual Layer of SABSA Policy Architecture?
 - A. Enterprise-wide Business Risk Management Policy
 - B. Enterprise-wide Information Security Policy
 - C. Domain-level Applications Security Policy
 - D. Domain-level Network Security Policy

Competency Domain 2

- Which ONE of the following statements about SABSA Policy Architecture is FALSE?
 - A. Procedures are Physical Layer representations of policy but executing procedures is a Management Layer activity
 - B. Technical standards are the Logical Layer representations of domain policy
 - C. Logical Layer policy states the security services required in a domain
 - D. Policy above the Logical Layer in the SABSA Architecture Matrix applies enterprise-wide

Architectural Strategies

Section 8

Scope: Strategy & Planning Phase - Process

	Architecture Matrix	Management Matrix
Contextual	Business Meta-Processes	Capability Management
	Business Value Chain; Business Capabilities	Managing Processes and Capabilities for Providing Value to Stakeholders
Conceptual	Strategies for Process Assurance	Delivery Planning
	Inventory of all Operational Processes (IT, industrial, & manual); Process Mapping Framework; Architectural Strategies for IT used in process support	SLA Planning; BCP; Financial Planning; Transition Planning. Planning and Maintaining the Inventory of Processes and Services Catalogue

Section 8 Competency Objectives

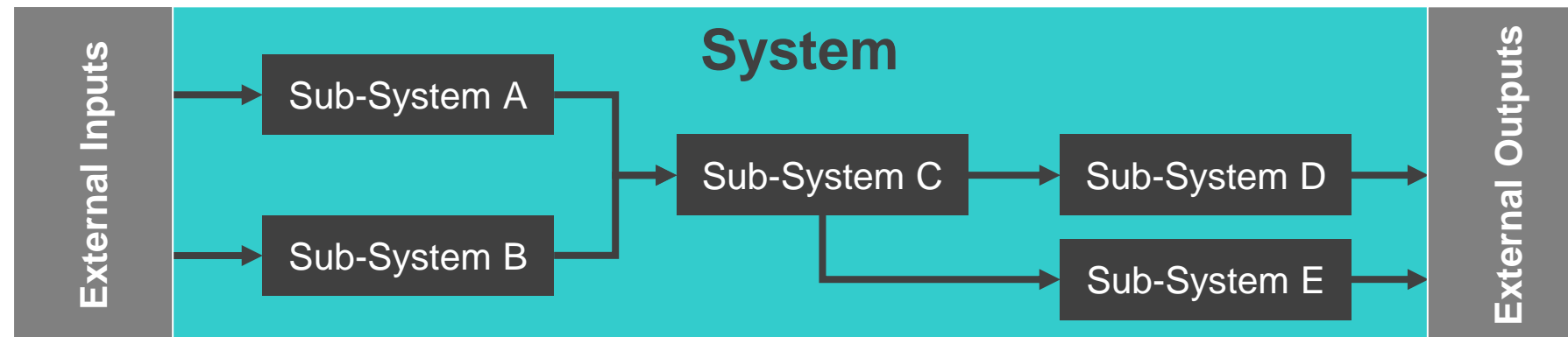
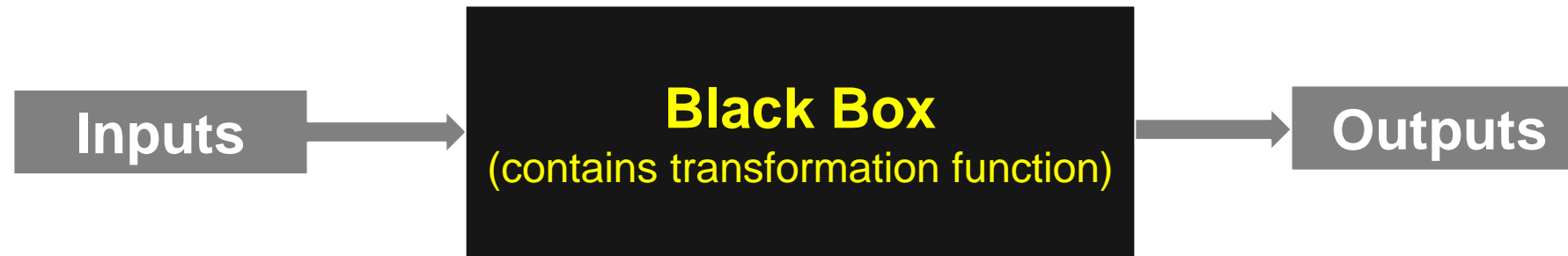
Competency / Question Domain 3 – How (Process)

Knowledge Element	Knowledge Competency	Comprehension Competency
Systems Engineering	List the objectives of systems engineering in SABSA Security Architecture	Interpret systems objectives, environment & performance in a SABSA context
	List the subsystems of a Control System	Sequence & explain the relationships between subsystems in a control feedback loop
Integrated Compliance Framework	Describe the concept of an Integrated Compliance Framework	Discuss possible applications and deployments of an Integrated Compliance Framework in a SABSA-based control system
Control Strategies	Describe the use of control strategies within SABSA Architecture	Explain the principles and objectives of control heatmaps and strength-in-depth models
SABSA Multi-tiered Control Strategy	Describe the SABSA Multi-tiered Control Strategy for defence-in-depth & identify its control capabilities	Sequence the control capabilities of the multi-tiered control strategy model and explain its association with, and application in, risk management

The Role of Systems Engineering

- Systems engineering is “A rational approach to decision-making related to the solution of complex problems in engineering planning, design and operation.” (*Boardman, 1990*)
- Managing complexity
- Top-down decomposition
- Structured thinking
- Peer review
- Communication & documented preservation of ideas

The Role of Systems Engineering



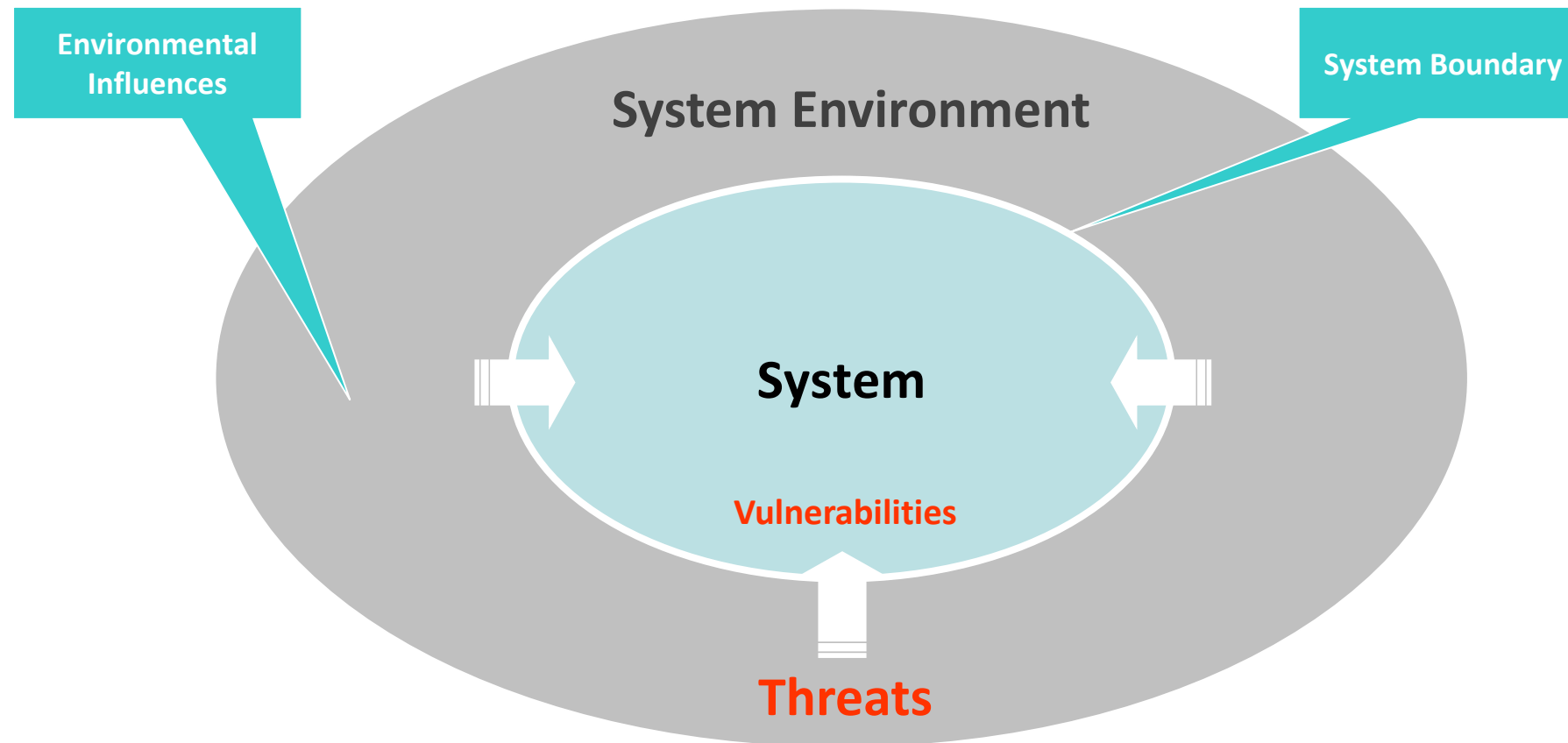
Total System Objectives

- System objectives are expressed as the 'Business Requirements' that the system should satisfy
- In formulating these requirements it is of prime importance that proper consideration is given to how the performance of the system will be measured so as to demonstrate the extent to which it is satisfying those requirements
- If performance against objectives is not measured we cannot manage the solution adequately
- Starting only with technical objectives is a common fault
- Incorrect objectives lead to poor solutions

Performance of a Security System

- Very widest interpretation of 'performance' - meaning 'fulfilling all of the system objectives'
- Obvious measurable performance attributes such as 'throughput', 'latency', 'response time', 'percentage up-time', etc
- In this security interpretation many other attributes are also included that would not normally be associated with the concept of performance
 - maintaining the confidentiality of business information
 - protecting its integrity
 - holding users accountable for their actions

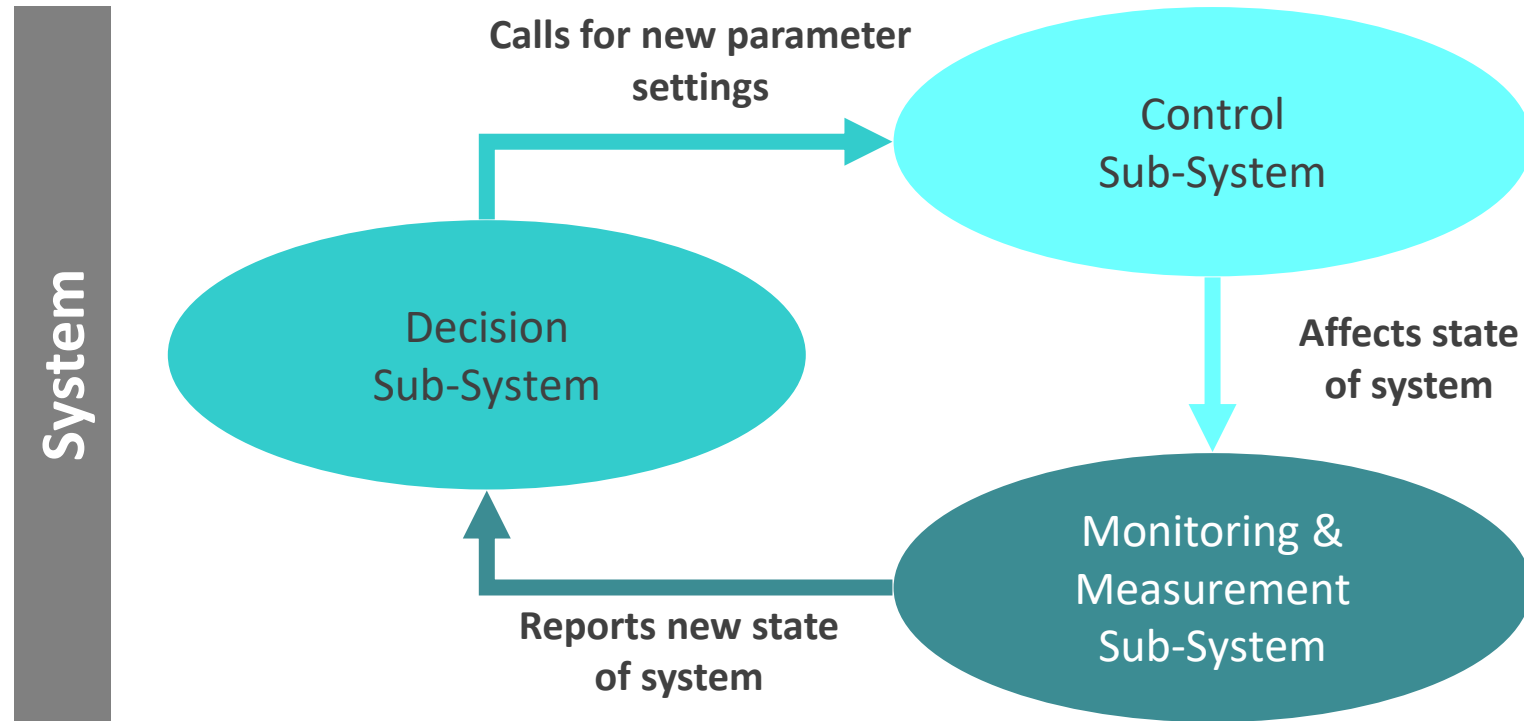
Taking Account of the Threat Environment



The Control System Concept

- The control sub-system – that exerts control
- The monitoring and measurement sub-system – measures the state of the system, which in turn is affected by the actions of the control sub-system
- The decision sub-system – that makes decisions based upon the measurements provided by the measurement sub-system.

Feedback Control Loop System



Boiled Frog Syndrome

- ‘Traditional’ Information Security Risk Management approaches do not cater well for a dynamically changing environment

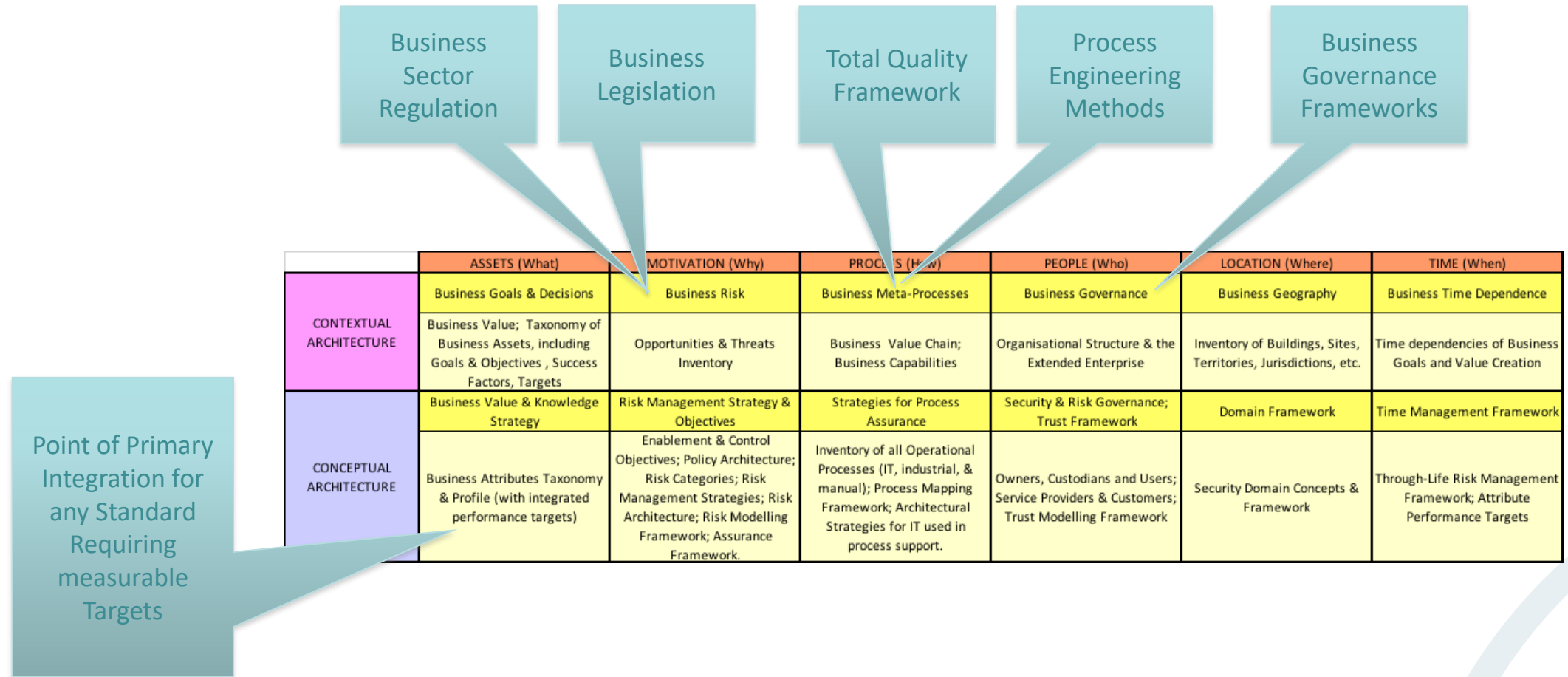


“Boiled Frog” courtesy of Nealon & Clark at
COSAC 2003 www.cosac.net

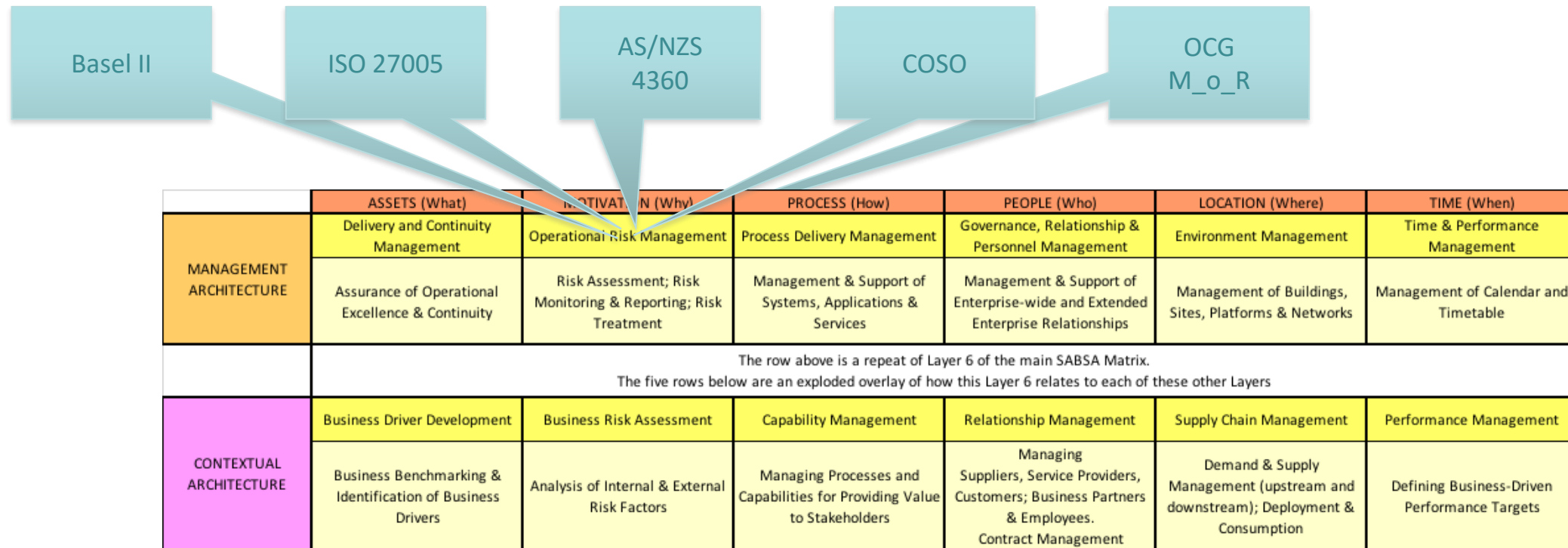
Alignment, Integration & Compliance Strategy

- Understand what needs to be aligned, to what purpose, and where is it positioned within the SABSA framework
- Business model or business process framework
- Legislation, regulation or governance frameworks
- Risk management methods, assurance framework or audit approach
- IT Architecture framework or method
- Controls framework, library or standard
- Performance management & reporting framework
- Etc.

Strategy & Planning Phase Alignment



Risk Management Method Alignment



Performance & Reporting Methods

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	Assurance of Operational Excellence & Continuity	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Management & Support of Enterprise-wide and Extended Enterprise Relationships	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable
	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 ARCHITECTURE	Business Driver Development	Business Risk Assessment	Capability Management	Relationship Management	Supply Chain Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Processes and Capabilities for Providing Value to Stakeholders	Managing Suppliers, Service Providers, Customers; Business Partners & Employees. Contract Management	Demand & Supply Management (upstream and downstream); Deployment & Consumption	Defining Business-Driven Performance Targets
CONCEPTUAL ARCHITECTURE	Proxy Asset Development	Developing Risk Objectives	Delivery Planning	Role Management	Business Portfolio Management	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Maintaining Risk Modelling Framework; Risk Analysis on Business Attributes Profile	SLA Planning; BCP; Financial Planning; Transition Planning. Planning and Maintaining the Inventory of Processes and Services Catalogue	Maintaining Trust Modelling Framework; Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Business Footprint: Points of Supply and Access	Managing Performance Criteria and Targets; Abstracting Attribute Performance Targets
LOGICAL ARCHITECTURE	Logical Asset Management	Policy Management	Delivery Management	Enterprise-wide User Management	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management	Risk Modelling; Management of Policy Development & Maintenance. Policy Publication & Compliance Management	SLA Management; Supply Chain Management; BCM; Financial Management; Transition Management	Trust Modelling; Identity & Access Management; Management of User Privileges, Account Administration & Provisioning	Configuration (CMDB) Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
PHYSICAL ARCHITECTURE	Physical Asset Management	Risk Data Management	Operations Management	User Support	Resources Management	Performance Data Collection
	Change Management; Platform & Data Storage Management	Risk Procedure Management; Risk Metadata Management	Job, Incident, Event, and Disaster Recovery Management	Service Desk, Problem, and Request Management	Physical & Environmental Security Management; Real Estate and Facilities Management	Business Systems Monitoring Procedure Management
COMPONENT ARCHITECTURE	Component Management	Risk Management Components	Component Deployment	Personnel Component Management	Component Environment Management	Monitoring Components
	Product & Component Standards Management	Risk Analysis, Monitoring & Reporting Components, Systems and Standards Management	Product & Component Selection, Procurement. Project and Standards Management	Recruitment, Disciplinary, Training & Awareness Delivery. Component and Standards Management	Physical and Environmental Security Component and Standards Management	Analysis, Monitoring & Reporting Component and Standards Management

Capability
Maturity
Models

Financial Models
ROI/NPV/IRR

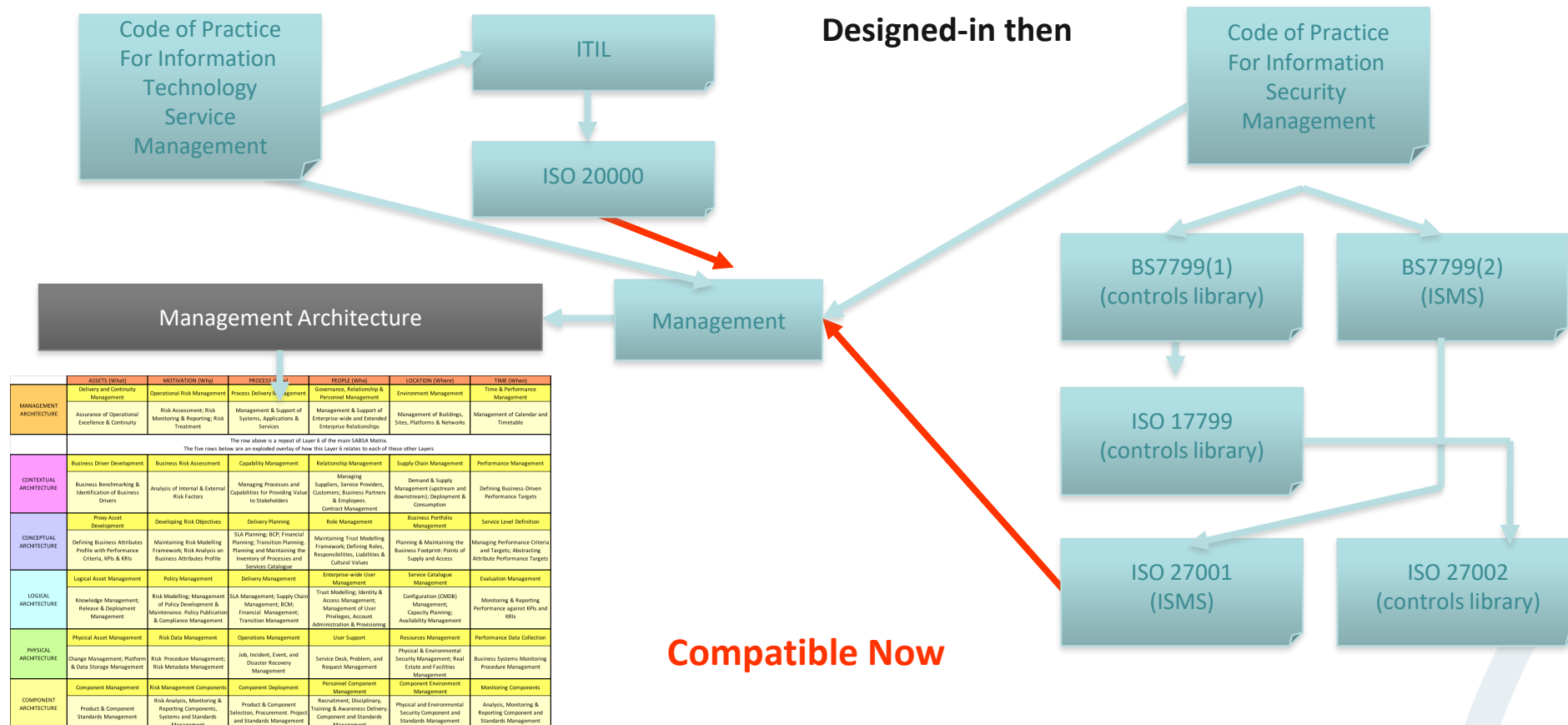
Balanced
Score
Cards

SABSA as a Compliance Framework

- Compliance audits (e.g. against ISO27001)
 - Start with demonstrating that you understand your business requirement
 - Then prove that you have deployed the appropriate controls and control systems
- Contextual layer assesses and communicates the business requirement in the context of overall business risk
- Conceptual layer sets out the strategy for treating risk and meeting the control and enablement objectives
- SABSA lower layers engineer the deployment of controls (both technical and operational) in the best place, at the best time, with the best use of investment
- The aim is to provide the framework for compliance with multiple standards simultaneously

Built to Integrate Management Practices

- SABSA Management designed to comply with, integrate, and enable management best practice of the day



Control Objectives Libraries & Standards

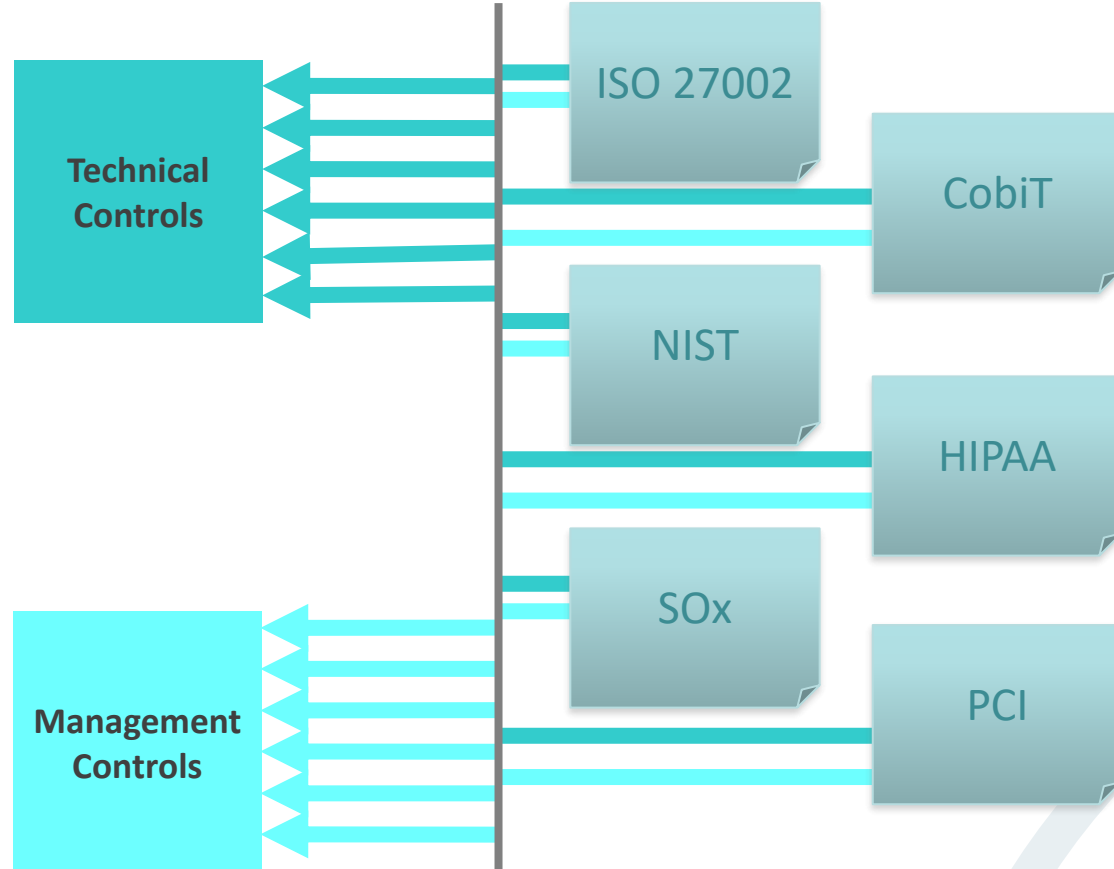
	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Goals & Decisions	Business Risk	Business Meta-Processes	Business Governance	Business Geography	Business Time Dependence
	Business Value; Taxonomy of Business Assets, including Goals & Objectives, Success Factors, Targets	Opportunities & Threats Inventory	Business Value Chain; Business Capabilities	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of Business Goals and Value Creation
CONCEPTUAL ARCHITECTURE	Business Value & Knowledge Strategy	Risk Management Strategy & Objectives	Strategies for Process Assurance	Security & Risk Governance; Trust Framework	Domain Framework	Time Management Framework
	Business Attributes Taxonomy & Profile (with integrated performance targets)	Enablement & Control Objectives; Policy Architecture; Risk Categories; Risk Management Strategies; Risk Architecture; Risk Modelling Framework; Assurance Framework.	Inventory of all Operational Processes (IT, industrial, & manual); Process Mapping Framework; Architectural Strategies for IT used in process support.	Owners, Custodians and Users; Service Providers & Customers; Trust Modelling Framework	Security Domain Concepts & Framework	Through-Life Risk Management Framework; Attribute Performance Targets



Controls Frameworks & Libraries

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

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	Assurance of Operational Excellence & Continuity	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Management & Support of Enterprise-wide and Extended Enterprise Relationships	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable
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 ARCHITECTURE	Business Driver Development	Business Risk Assessment	Capability Management	Relationship Management	Supply Chain Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Processes and Capabilities for Providing Value to Stakeholders	Managing Suppliers, Service Providers, Customers; Business Partners & Employees; Contract Management	Demand & Supply Management (Upstream and downstream); Deployment & Consumption	Defining Business-Driven Performance Targets
CONCEPTUAL ARCHITECTURE	Proxy Asset Development	Developing Risk Objectives	Delivery Planning	Role Management	Business Portfolio Management	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Maintaining Risk Modelling Framework; Risk Analysis on Business Attributes Profile	SLA Planning; RCP; Financial Planning; Transition Planning and Maintaining the Inventory of Processes and Services Catalogue	Maintaining Trust Modelling Framework; Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Business Footprint; Points of Supply and Access	Managing Performance Criteria and Targets; Abstracting Attribute Performance Targets
LOGICAL ARCHITECTURE	Logical Asset Management	Policy Management	Delivery Management	Enterprise-wide User Management	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management	Risk Modelling; Management of Policy Development & Maintenance; Policy Publication & Compliance Management	SLA Management; Supply Chain Management; BCM; Financial Management; Transition Management	Trust Modelling; Identity & Access Management; Management of User Privileges, Account Administration & Provisioning	Configuration (CMDB) Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
PHYSICAL ARCHITECTURE	Physical Asset Management	Risk Data Management	Operations Management	User Support	Resources Management	Performance Data Collection
	Change Management; Platform & Data Storage Management	Risk Procedure Management; Risk Metadata Management	Job, Incident, Event, and Disaster Recovery Management	Service Desk, Problem, and Request Management	Physical & Environmental Security Management; Real Estate and Facilities Management	Business Systems Monitoring Procedure Management
COMPONENT ARCHITECTURE	Component Management	Risk Management Components	Component Deployment	Personnel Component Management	Component Environment Management	Monitoring Components
	Product & Component Standards Management	Risk Analysis, Monitoring & Reporting Components, Systems and Standards Management	Product & Component Selection, Procurement, Project and Standards Management	Recruitment, Disciplinary, Training & Awareness Delivery, Component and Standards Management	Physical and Environmental Security Component and Standards Management	Analysis, Monitoring & Reporting Component and Standards Management



SABSA BAP – The Key to Integrated Compliance

ISO/SEC 2700x - Commented version


AB.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 employment²⁰ should reflect the organization's security policy in addition to clarifying and stating ²⁰²¹:

- [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 agreement²² 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, ISO 27000 committee

Sample Attributes Mapped to ISF Control Objectives

Authenticated

SM41. Standards & Procedures. To provide a coherent framework of information security solutions.

IP12. Standards & Procedures. To provide personnel running the installation with a clear statement of disciplines they are expected to follow.

IP44. Access Privileges. To provide authorized users with access that is sufficient but not excessive.

IP45. Sign-on Process. To ensure users follow a rigorous process before gaining access to information.

IP46. User Authentication. To ensure users are identified and authenticated before gaining access to the system.

Sample Attributes Mapped to CobIT Control Objectives

Accurate

AI1. Identify solutions

AI2. Acquire and maintain application software

AI3. Acquire and maintain technology architecture

AI4. Develop and maintain IT procedures

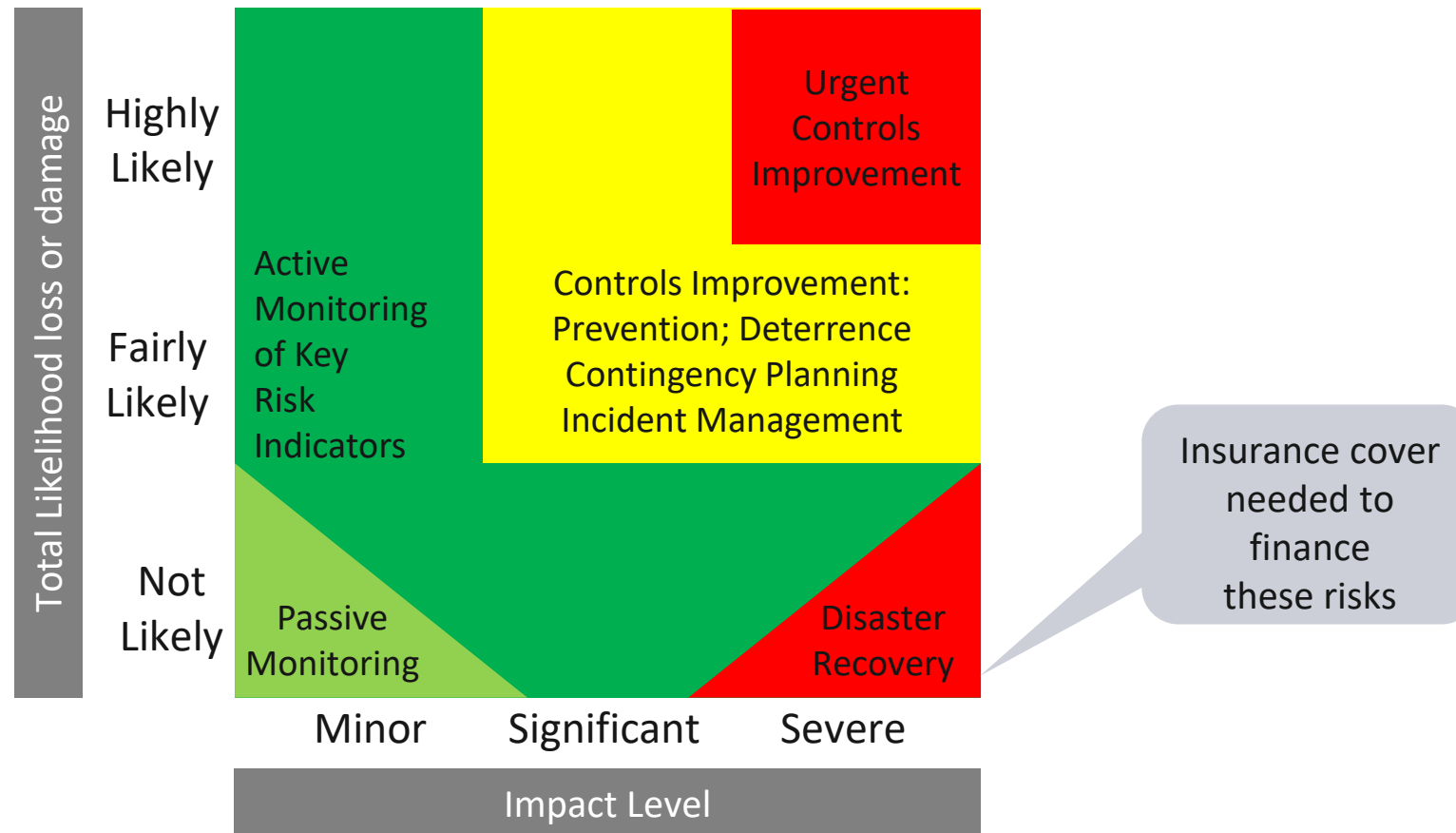
AI5. Install and accredit systems

DS1. Define service levels

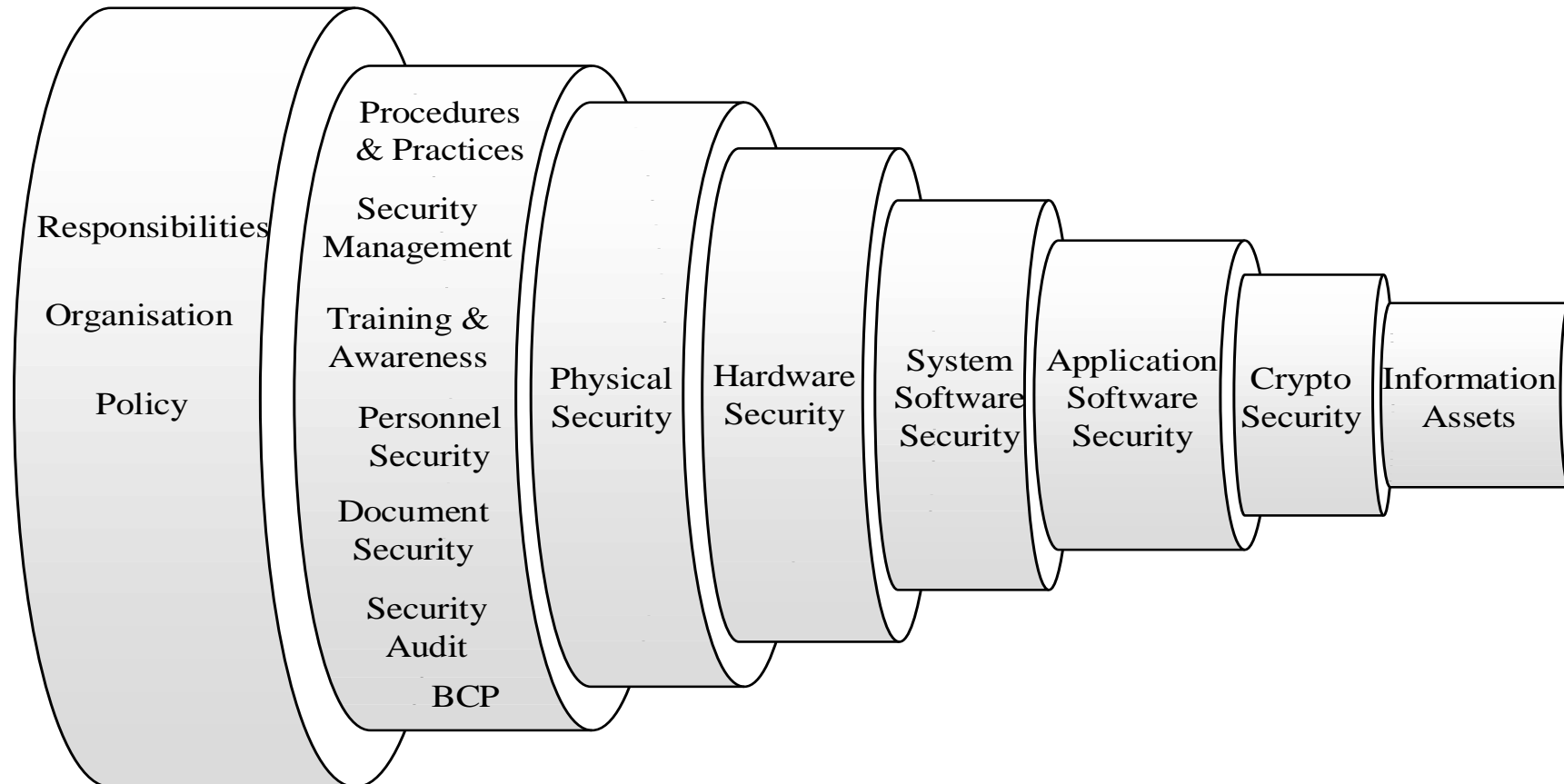
DS3. Manage performance and capacity

DS11. Manage data

Control Strategy Heat Map



Generic Defence in Depth Layering

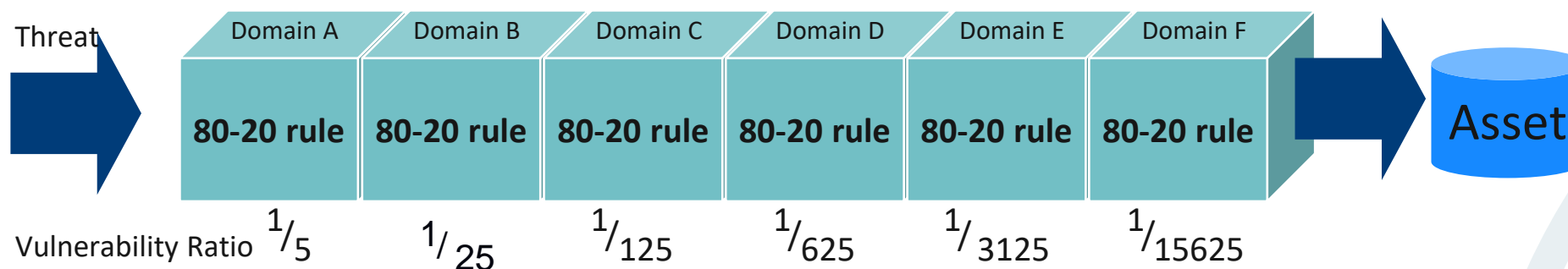


Strength-in-Depth Controls Models

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

SABSA Defence-in-Depth Principles

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



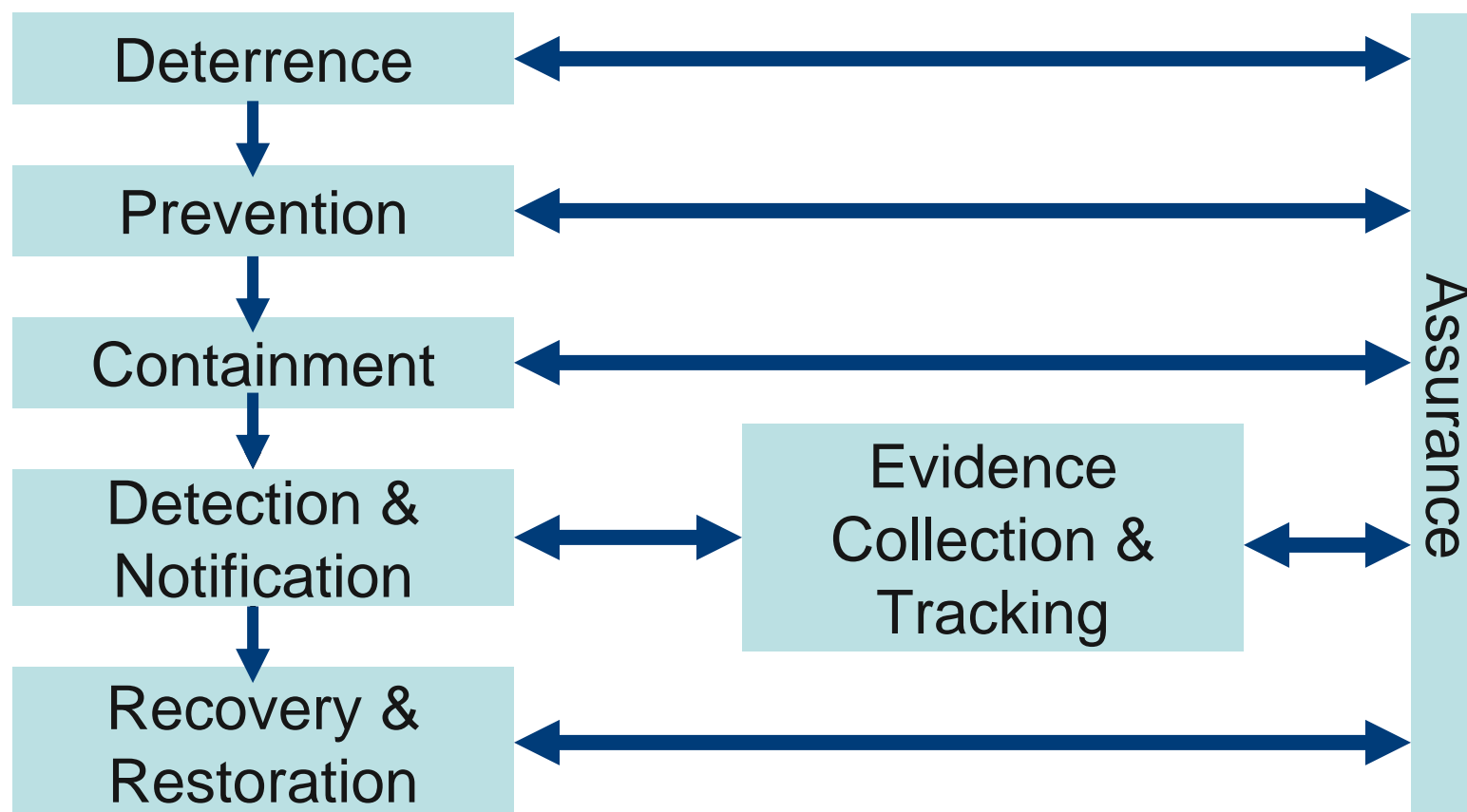
Multi-tiered Controls Strategy - Capabilities

Prioritised, Proportional & Balanced Investment

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



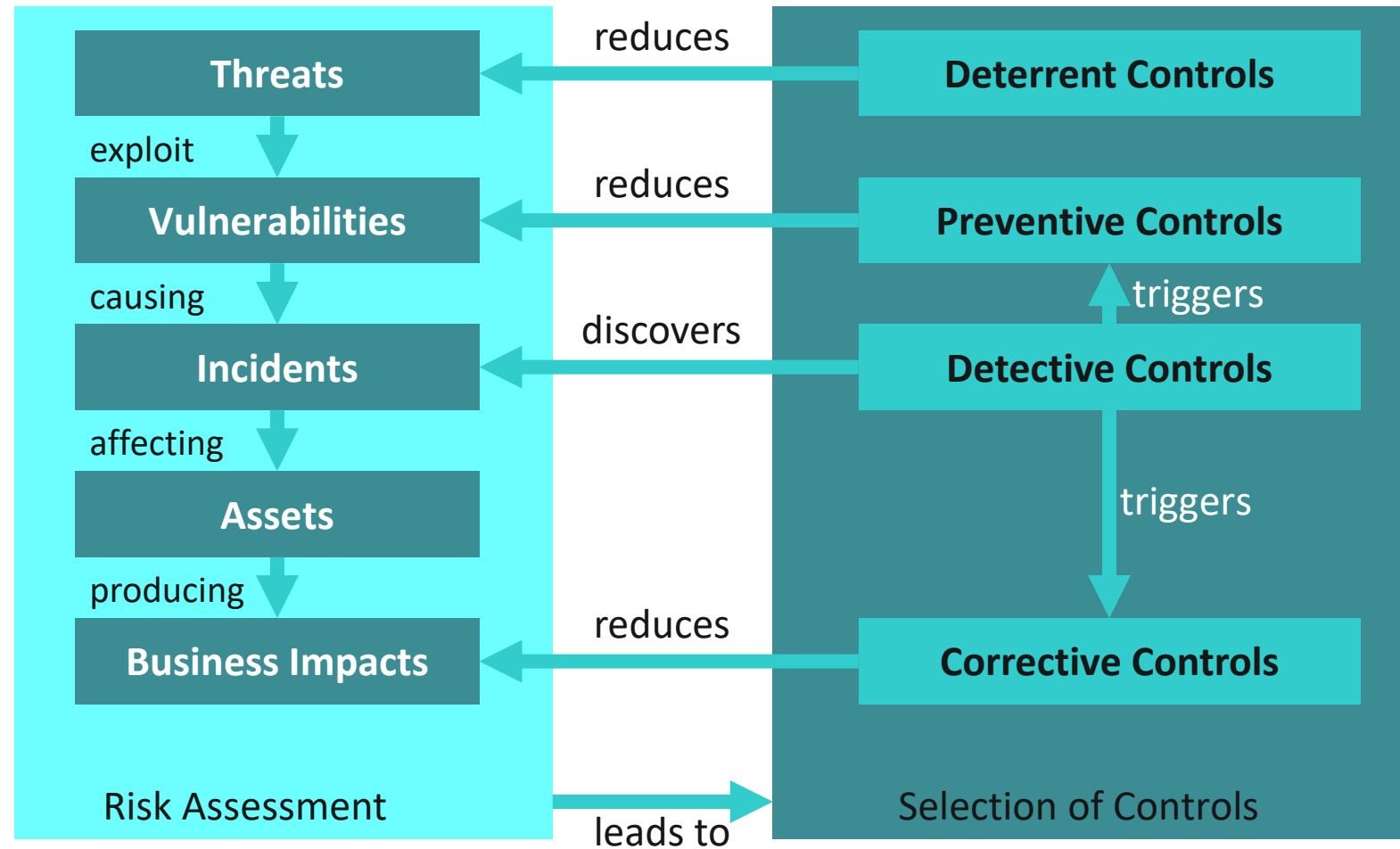
SABSA Multi-tiered Control Strategy



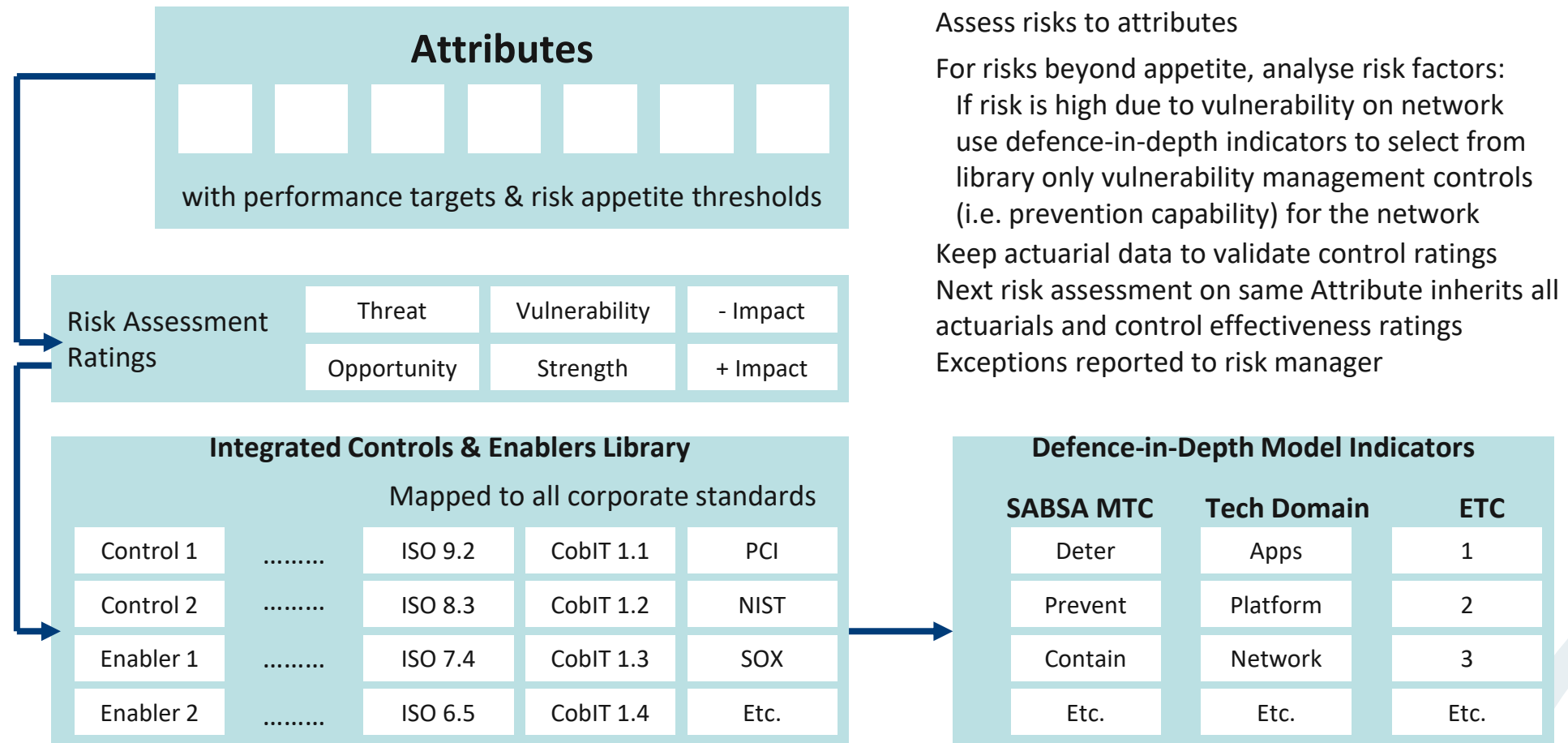
Application of Multi-tiered Controls in Risk

- The multi-tiered controls strategy is 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-tier Control



Application of Multi-tiered Control Strategy



Sample Questions

Competency Domain 3

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



Competency Domain 3

- Of the sequence of capabilities in the SABSA Multi-tiered Control Strategy defence-in-depth model which ONE of the following appears EARLIEST?
 - A. Containment
 - B. Prevention
 - C. Recovery and Restoration
 - D. Detection and Notification

Competency Domain 3

- Which ONE of the following is of LEAST benefit to the Security Architect when applying to security the engineering concept of the Single Integrated Complex System?
 - A. It enables a checklist approach
 - B. It designs in the ability to deal with rapid or frequent change
 - C. It ensures that requirements for properly delivered and supported security services are included within the scope of the architecture
 - D. It provides assurance that security components and processes are designed, procured and managed to work together with other security components and processes as an integrated security architecture

Role & Responsibility Concepts

Section 9

Scope: Strategy & Planning Phase - People

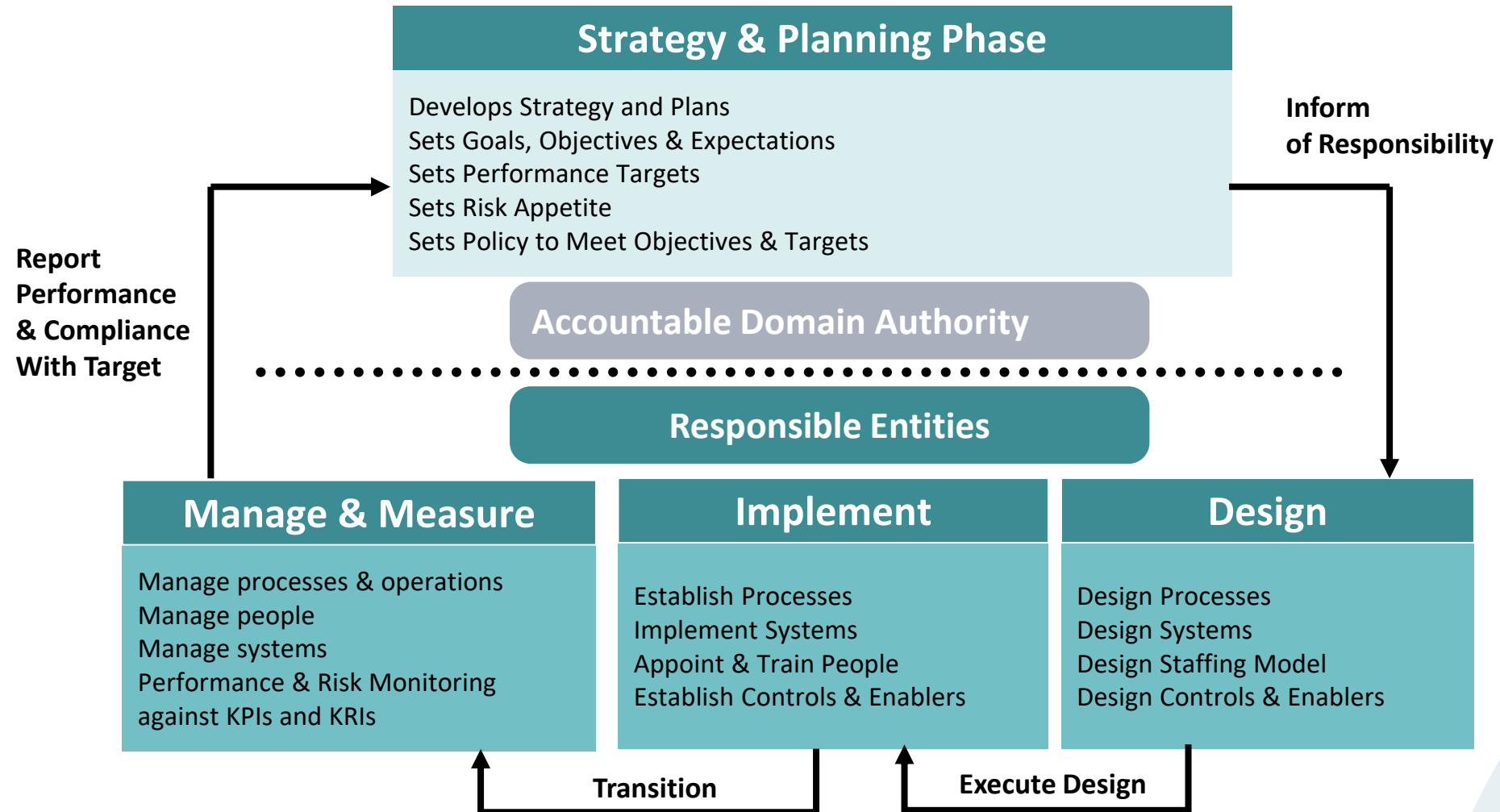
	Architecture Matrix	Management Matrix
Contextual	Business Governance	Relationship Management
	Organisational Structure & the Extended Enterprise	Managing Suppliers, Service Providers, Customers; Business Partners & Employees. Contract Management
Conceptual	Roles & Responsibilities	Role Management
	Owners, Custodians and Users; Service Providers & Customers; Trust Modelling Framework	Maintaining Trust Modelling Framework; Defining Roles, Responsibilities, Liabilities & Cultural Values

Section 9 Competency Objectives

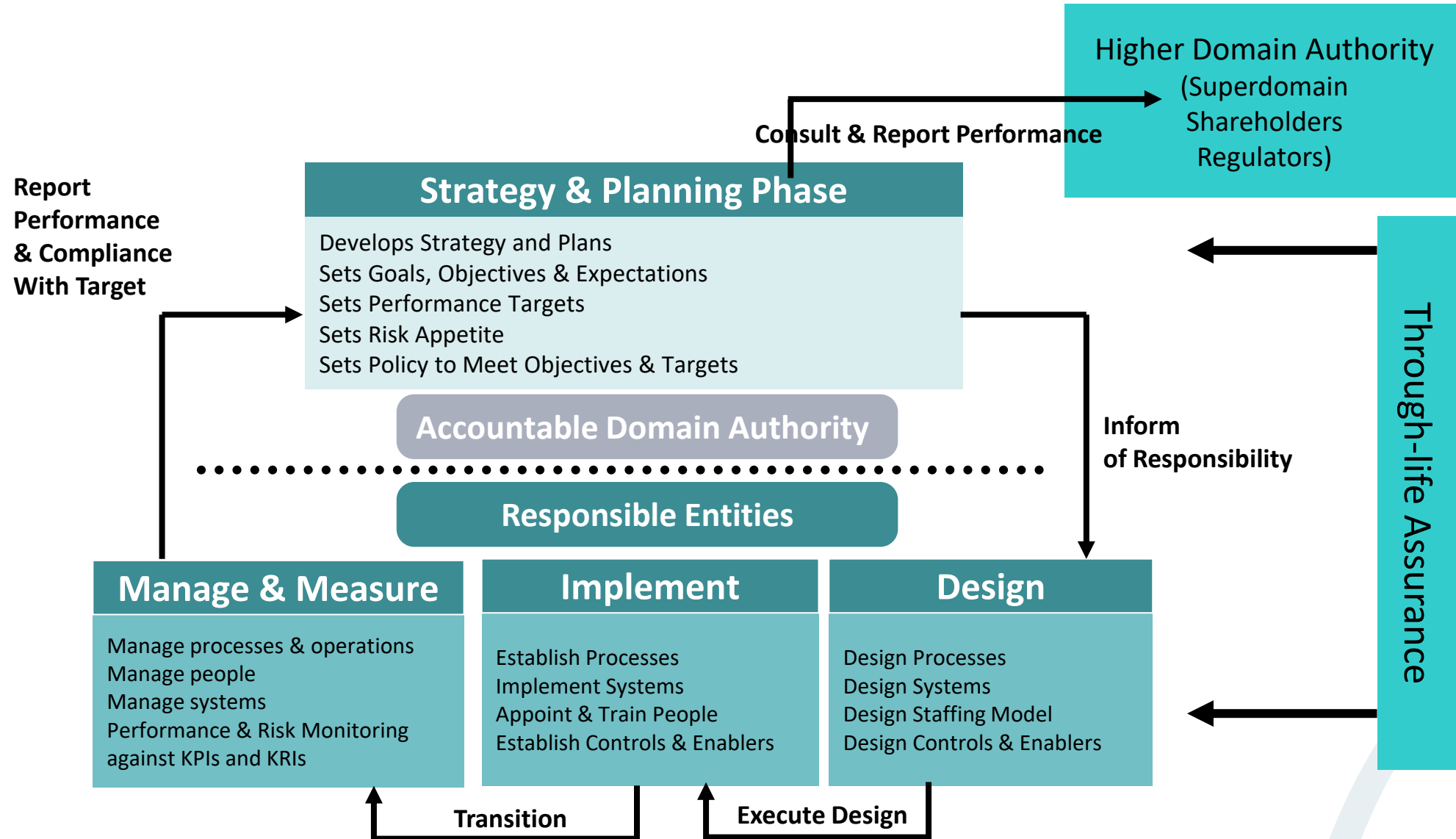
Competency / Question Domain 4 – Who (People)

Knowledge Element	Knowledge Competency	Comprehension Competency
SABSA Governance Model	Identify & label the phases & activities of the SABSA Governance Model	Associate the SABSA Governance Model activities with specific roles & responsibilities within an Enterprise Domain Model
SABSA Role & Responsibilities Model	List & define the roles & responsibilities in a SABSA RACI model	Differentiate between the SABSA roles & responsibilities in and between domains, and overlay a RACI on an Enterprise Domain model
	Define the concept of ownership in the SABSA roles & responsibilities model	Distinguish between ownership of attributes, ownership of liability & ownership of risk impact
	Define the roles of Trustees & Custodians in the SABSA roles & responsibilities model	Distinguish between the roles & responsibilities of Trustees and Custodians
	Define the roles of Service Providers & Customers in the SABSA roles & responsibilities model	Distinguish between the roles & responsibilities of Service Providers & Customers
	Define the roles of Compliance & Audit in the SABSA roles & responsibilities model	Distinguish between the roles & responsibilities of Compliance & Audit
Aggregated Roles & Responsibilities	Describe how SABSA approaches contribute to risk aggregation & reporting	Differentiate between risk appetite distribution & risk performance aggregation in a domain model

SABSA Governance Model



SABSA Governance Model



RACI Modelling

- All roles must be clearly defined so that the right decisions are made quickly by the right people
- **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

Service Desk RACI Example

Service Desk Activities	1 st Level	2 nd Level	3 rd 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 process (chasing 2 nd & 3 rd level support)	A	R	R	R	I	R	
Communicate status updates to customer	R	C	C	A	C	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

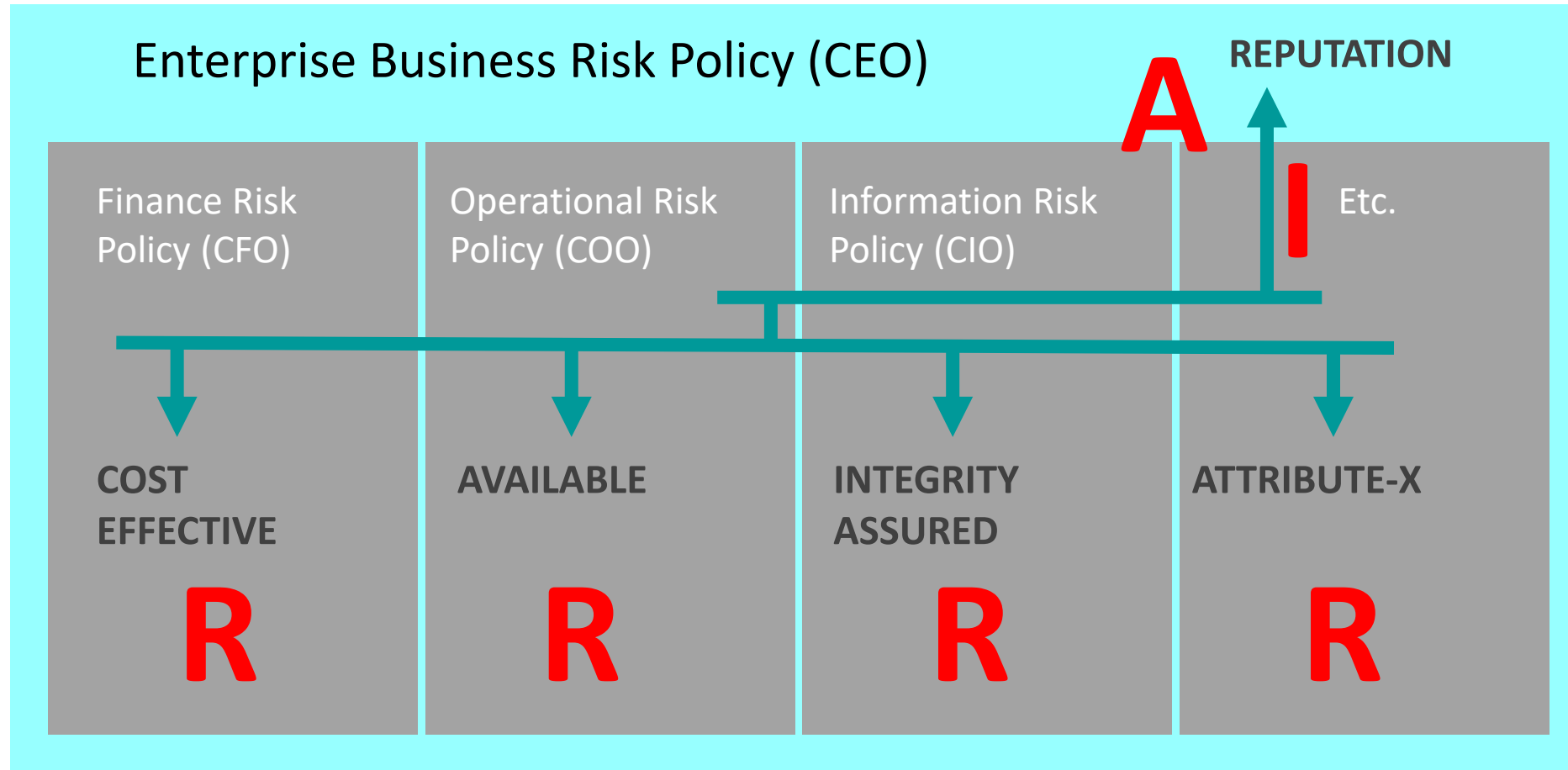
Ownership is Multi-faceted

- Ownership of:
 - Asset / attribute
 - Impact
 - Liability
- Ownership type is specific to position in:
 - Governance model
 - Domain model



Governance Roles & Responsibilities

RAI Indicators in Domain Architecture



Governing Domain Systemic Risk

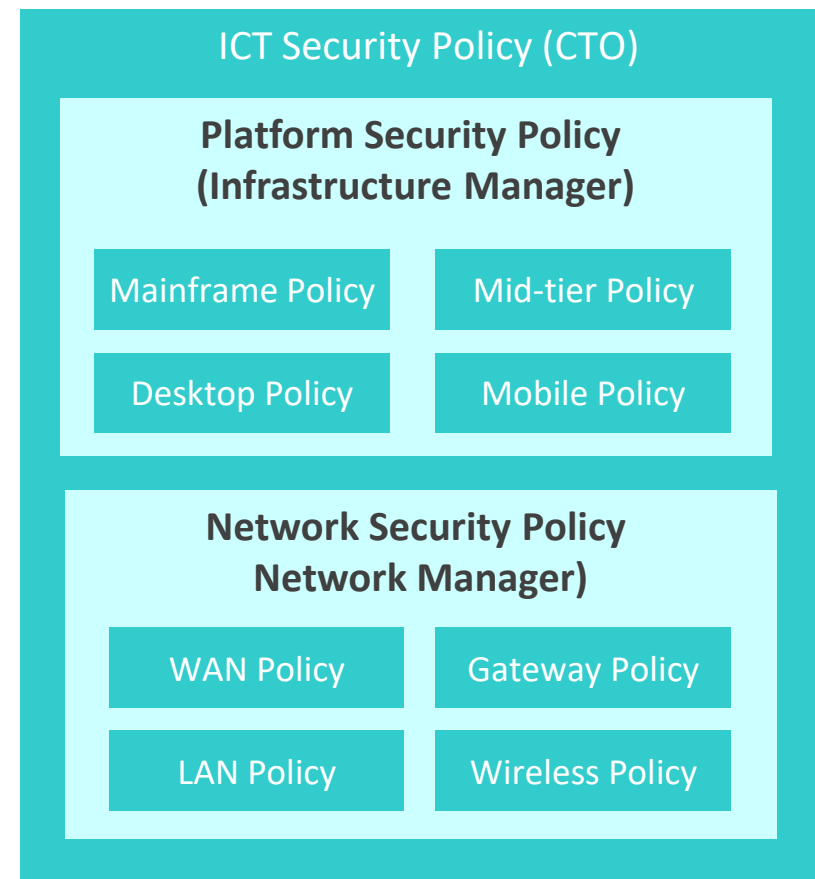
The Need for Vertical & Lateral Consultation & Reporting

- Although we have given each Policy Authority in the SABSA Policy Framework accountability for managing risks to their own domain-level assets, goals & objectives they must be accountable TO someone else
- Therefore they set their policy in the context of, and must consult & report risk performance to:
 - Their superdomain authority policy & performance requirements
 - Their peer domain requirements
- The superdomain always authorises the subdomain policy because the subdomain exists in the first place as a risk responsibility delegation of some part of the superdomain risk

Vertical Domain Systemic Risk

The Need for Vertical Consultation & Reporting

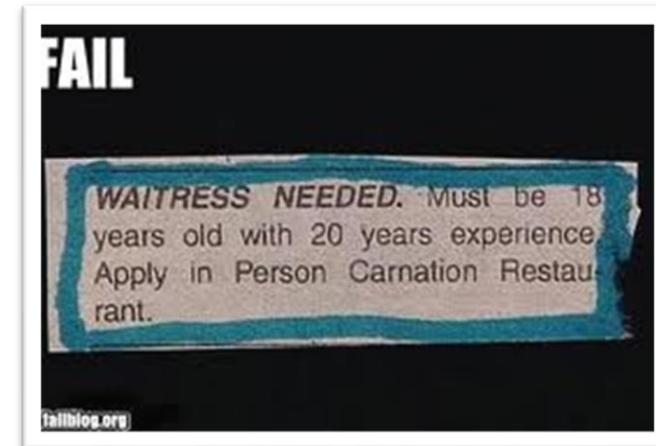
- The CTO has a delivery commitment to the 'business', expressed through a high-level SLA
- If the CTO's SLA is to be met, all the sub-domains must be bound by contributory OLAs
- For example, there must be a Network OLA that is met
- For the Network OLA to be met, the WAN OLA must be met
- For the WAN OLA to be met, the third-party bandwidth supplier UPC must be met
- There is a hierarchical, back-to-back SLA chain
- Failure to meet a lower SLA cascades upwards (domino effect) causing failures at higher levels
- This is known as 'systemic risk' and it has implications for risk aggregation



The Need to Close the Feedback Loop

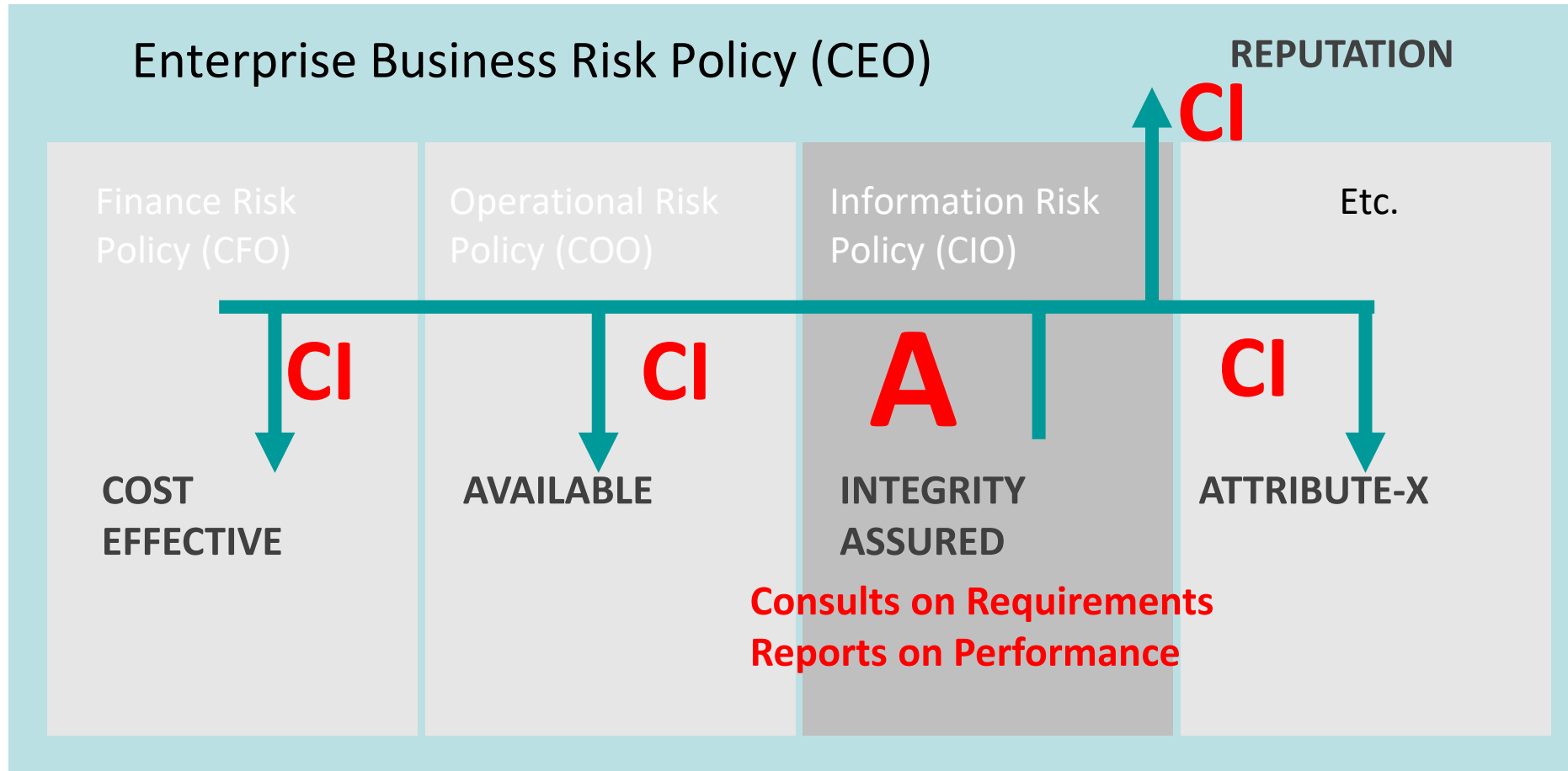
The Failure of Performance Reporting

- 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



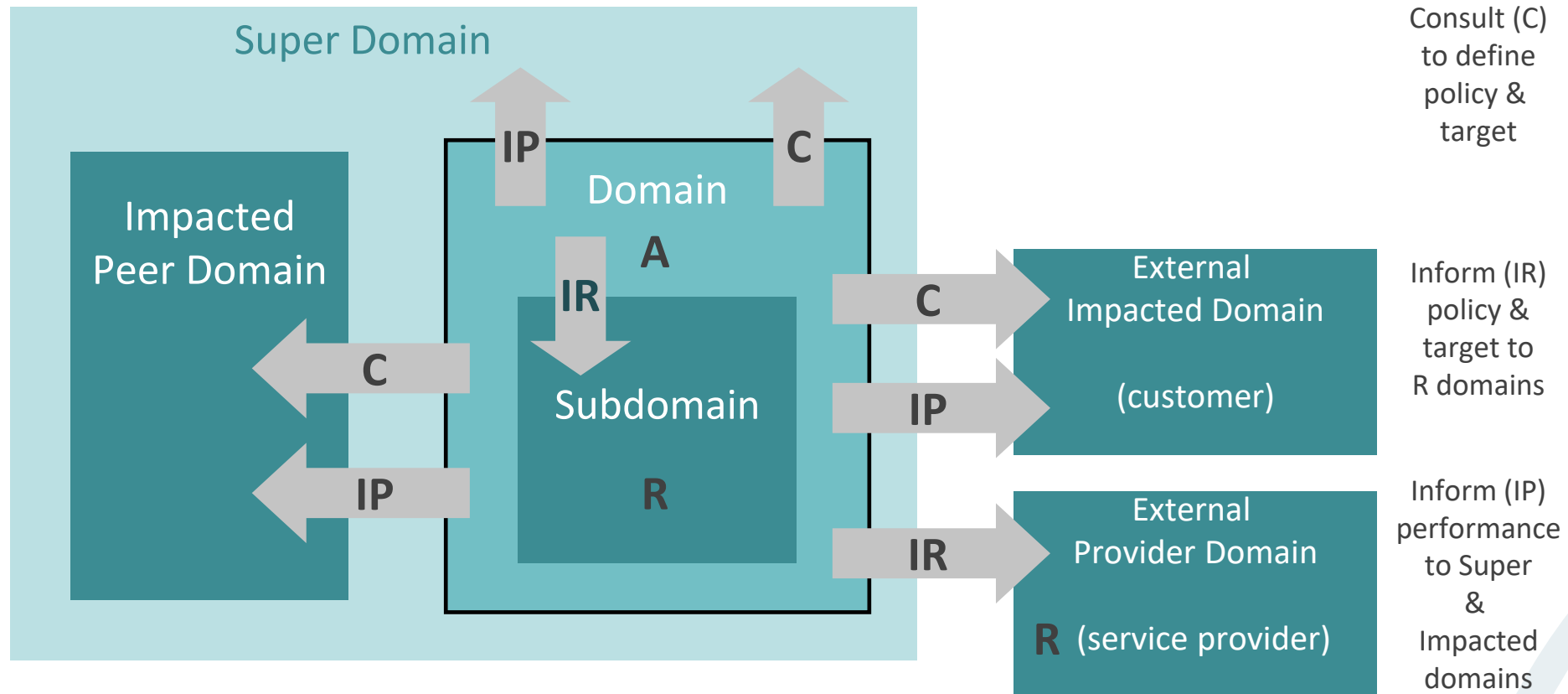
Governance Roles & Responsibilities

C Indicators in Domain Architecture



SABSA Governance Model

Governance Model Overlaid on Domains and RACI



Owner Role

- **Definition:**

- The Owner is the domain policy authority who sets goals, risk appetite, and performance targets for the assets (attributes) in a specific domain

- **Role:**

- Accountable for the performance of the assets (attributes) in a specific domain

- **Governance Model:**

- Strategy & Planning phase

- **Policy Role:**

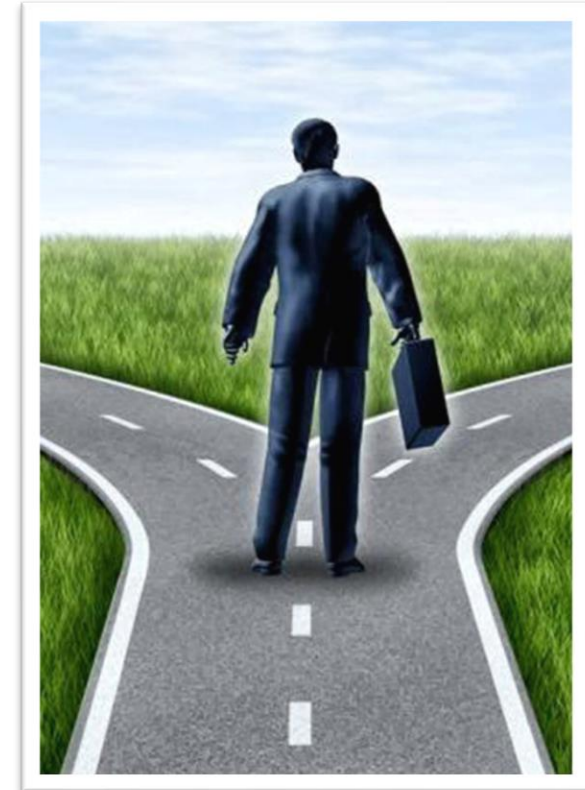
- Sets policy for the domain

- **Risk Management Communications Role:**

- Consults: super domain authority on risk appetite
- Consults: lateral or external impacted domain authorities
- Informs: risk performance to super domain authority (or externally if enterprise domain authority)
- Informs: policy & performance targets to subdomains & service providers

Owner Responsibility Delegation

- Sometimes the risk owner is:
 - Unqualified or inexperienced
 - Vulnerable
 - Not in a position to make the best decision for self-preservation
- Risk Owner Responsibility Delegations
 - Responsible for evaluating the risk on behalf of the owner
 - Responsible for mitigating the risk on behalf of the owner
 - It's a big responsibility
 - Responsible
 - Liability doesn't transfer from Owner



Delegated Authority Role - Trustee

- **Definition:**

- The Delegated Authority (often called the steward or trustee) is appointed by a domain owner as a subject matter expert to be responsible for the assets (attributes) in a specific domain. Policy authority is delegated to the steward or trustee

- **Role:**

- Responsible for the performance of the assets (attributes) in a specific domain

- **Governance Model:**

- Strategy & Planning phase (acts as domain authority)

- **Policy Role:**

- Sets policy for the domain on behalf of the domain authority

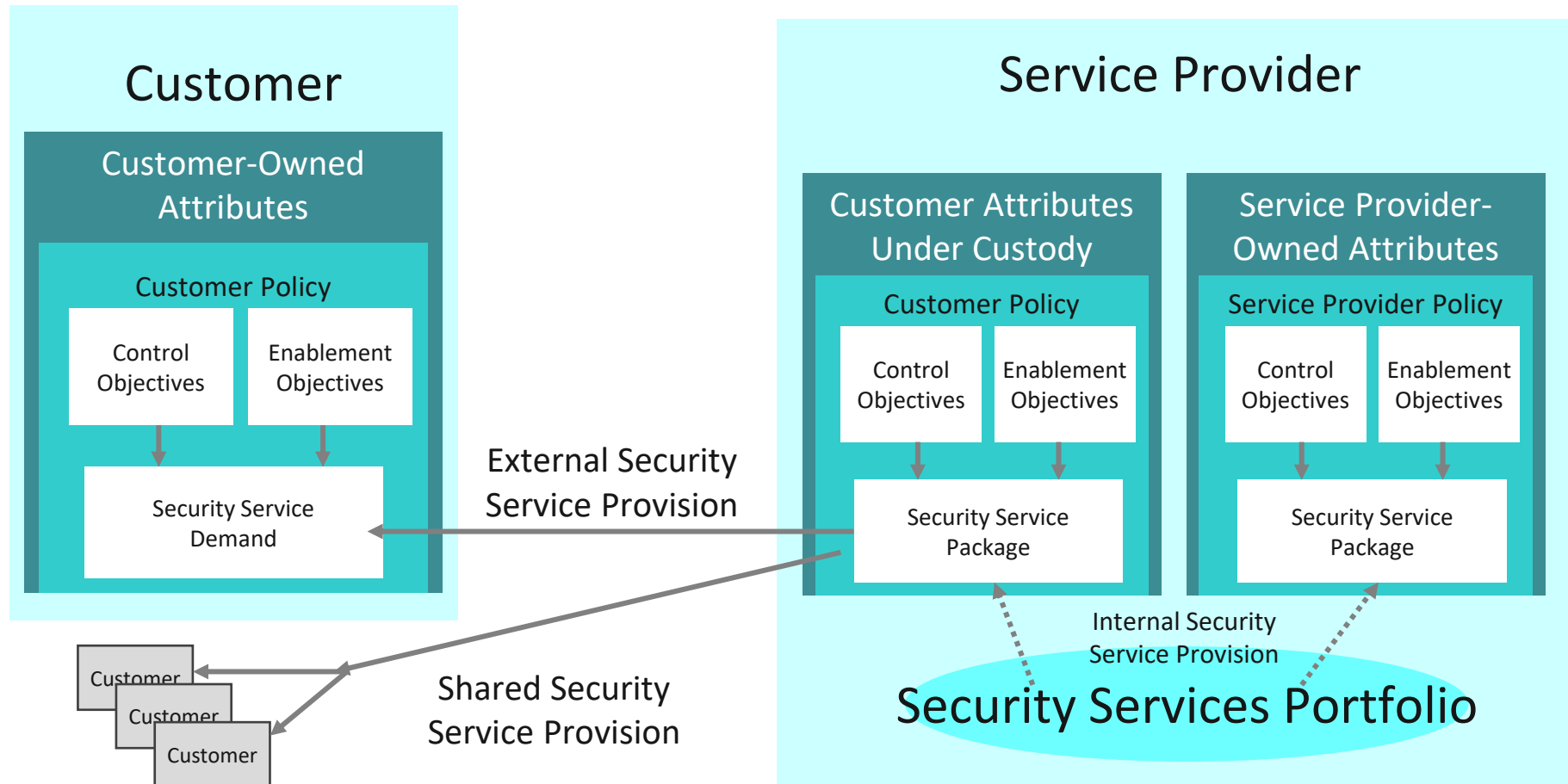
- **Risk Management Communications Role:**

- Consults: super domain authority & domain owner on risk appetite
- Consults: lateral or external impacted domain authorities
- Informs: risk performance to super domain authority (or externally if enterprise domain authority) & domain owner
- Informs: policy & performance targets to subdomains & service providers

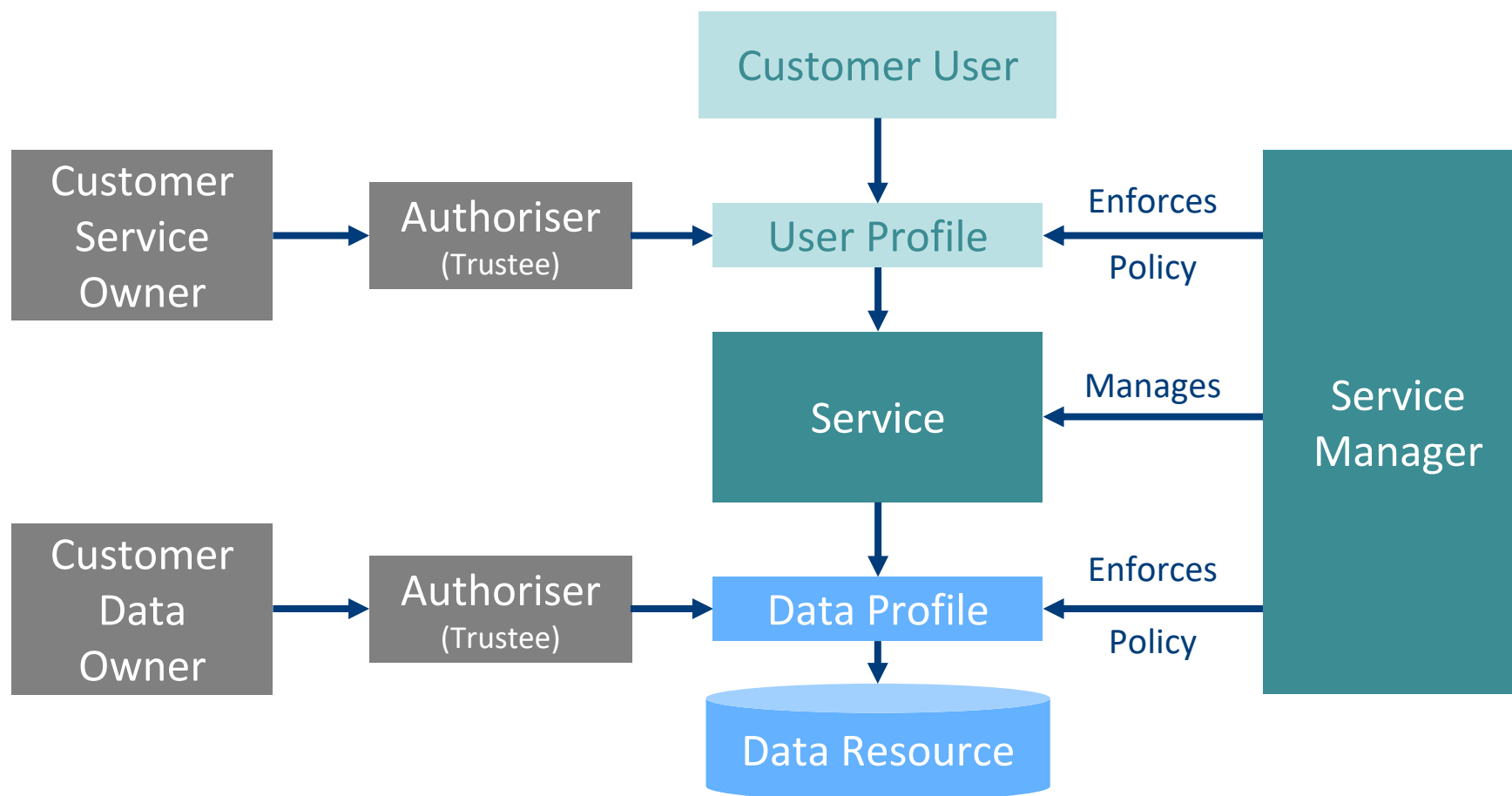
Delegated Responsibility Role - Custodian

- **Definition:**
 - The Custodian is appointed by a domain owner as a subject matter expert or service provider to be responsible for the assets (attributes) in a specific domain. Unlike trustees, policy authority is not delegated to the custodian
- **Role:**
 - Responsible for the performance of the assets (attributes) in a specific domain
- **Governance Model:**
 - Design, Implement and Manage & Measure phases
- **Policy Role:**
 - Complies with policy & SLA for the domain assets on behalf of the domain authority
- **Risk Management Communications Role:**
 - Informed by: domain authority on risk appetite, policy & performance target
 - Informs: risk performance to domain authority

Service Provider Custodian Role



Security Service Manager As Custodian



Assurance Role - Compliance

- **Definition:**

- The Compliance Role is appointed by a domain owner as a subject matter expert to provide a compliance checking service and to report on the degree to which the risk appetite & policy of the owner is being met by responsible and custodial parties

- **Role:**

- Responsible for checking the performance of the assets (attributes) in a specific domain on behalf of the owner

- **Governance Model:**

- Design, Implement and Manage & Measure phases

- **Policy Role:**

- Reports on policy compliance

- **Risk Management Communications Role:**

- Informed by: domain authority on risk appetite, policy & performance target
- Informs: domain authority on policy compliance

Assurance Role - Audit

- **Definition:**

- The Auditor role is appointed by a super domain authority as a subject matter expert to provide an audit service reporting independently on the degree to which the risk appetite & policy of the super domain authority is being met by subdomain authorities

- **Role:**

- Responsible for auditing the performance of the assets (attributes) in a specific subdomain on behalf of the owner of a super domain

- **Governance Model:**

- Design, Implement and Manage & Measure phases

- **Policy Role:**

- Reports on policy compliance and policy & procedure weaknesses

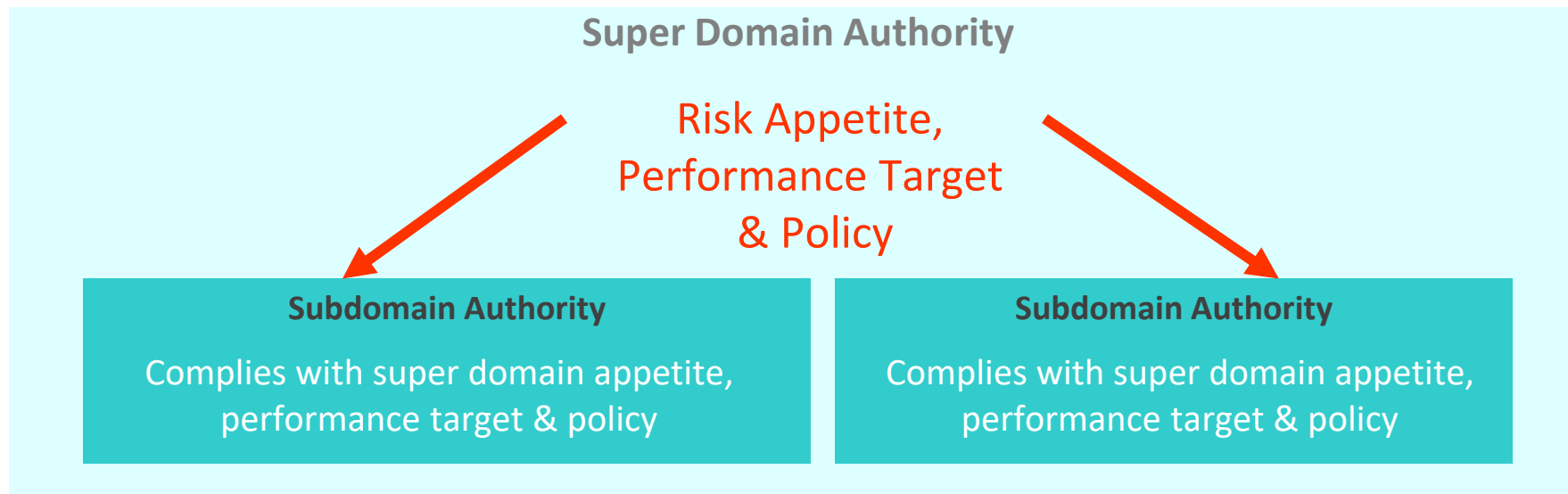
- **Risk Management Communications Role:**

- Informed by: super domain authority on risk appetite, policy & performance target
- Informs: super domain authority on policy compliance

SABSA-Extended RACI Considerations

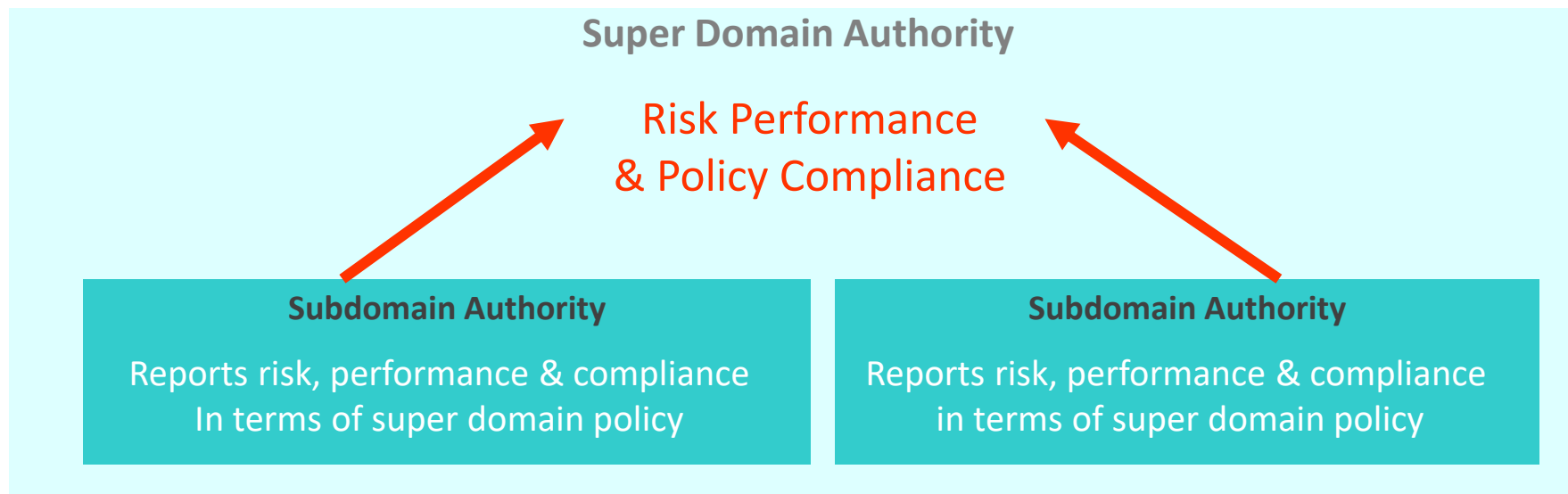
- Many advanced SABSA users extend the standard RACI matrix with additional roles to formally establish and record specialist or security & risk-relevant responsibilities
- Examples include:
 - Ownership (of attribute, of liability, of risk impact)
 - Delegations (trustees & custodians)
 - Assurance (monitor, compliance & audit)
 - Communications (inform, support)
 - Validation & sign-off (review, verify, sign-off)

Roles & Responsibilities in Risk Aggregation



Risk appetite and policy is communicated and distributed top-down in a SABSA domain model

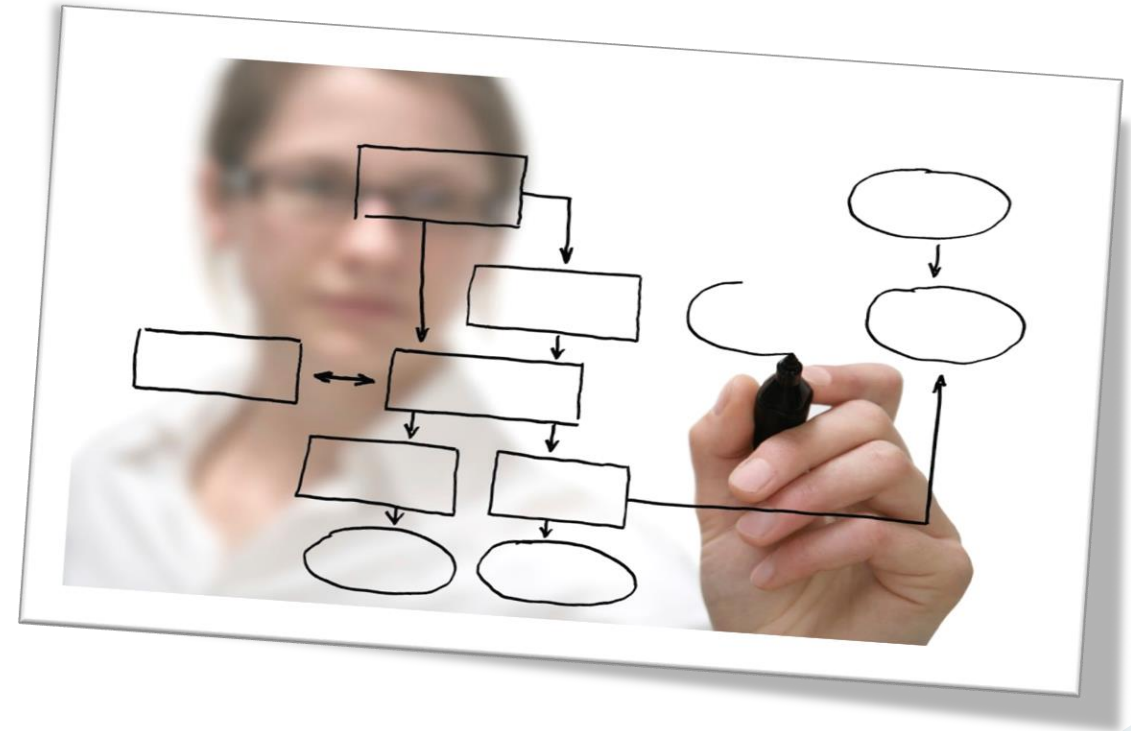
Roles & Responsibilities in Risk Aggregation



Risk performance and policy compliance is communicated and aggregated bottom-up in a SABSA domain model

Workshop F1-4

Roles & Responsibilities



Sample Questions

Competency Domain 4

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



Competency Domain 4

- In the SABSA Corporate Governance Model, which ONE of the following statements is TRUE?
 - A. During the Implement Phase, internal controls are reported to external authorities such as regulators
 - B. During the Strategy & Planning Phase, Domain Authorities design risk management processes
 - C. During the Manage & Measure Phase, Line Management monitors performance against Key Risk Indicator thresholds
 - D. During the Design Phase, staff review risk appetite

Competency Domain 4

- Which ONE of the following is the LEAST applicable ending to the sentence “The SABSA architecture concept aids corporate governance and efficient management by...?”
 - A. Delivering economies of scale and standardization through an enterprise blueprint and roadmap
 - B. Distributing policies, principles and design rules top-down from defined business requirements
 - C. Enabling projects to design and deliver tactical solutions independently of business goals and policies
 - D. Enabling integration of many risk management components under a single holistic framework

Domain Concepts

Section 10

Scope: Strategy & Planning Phase - Location

	Architecture Matrix	Management Matrix
Contextual	Business Geography	Supply Chain Management
	Inventory of Buildings, Sites, Territories, Jurisdictions etc.	Demand & Supply Management (upstream and downstream); Deployment & Consumption
Conceptual	Domain Framework	Business Portfolio Management
	Security Domain Concepts & Framework	Planning & Maintaining the Business Footprint: Points of Supply and Access

Section 10 Competency Objectives

Competency / Question Domain 5 – Where (Location)

Knowledge Element	Knowledge Competency	Comprehension Competency
SABSA Domain Model Concept & Framework	List the benefits of SABSA Domain Models	Explain the applications of Domain Models
	Define Domain types	Distinguish between super domains, subdomains, peer domains, and between logical & physical domains
	Describe the roles of Registration & Credentials Issuing (Certification) Authorities in Domain Models Define Isolated, Independent, Combined & Multi-tiered Domain Models	Differentiate between Registration & Credentials Issuing (Certification) authorities Distinguish between Isolated, Independent, Combined & Multi-tiered Domain Models in resolving segregation & information sharing issues
	Identify Inter-domain policy associations	Interpret Inter-domain policy associations in the context of risk interactions & systemic risk

The Issue

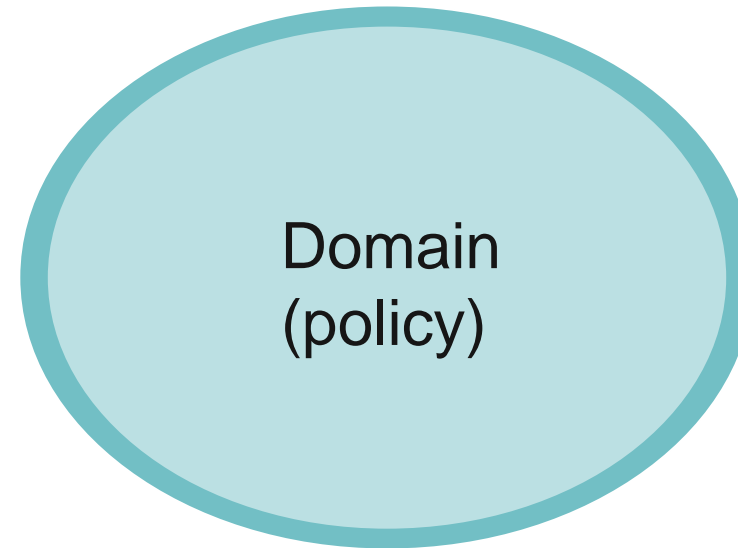
- Consider an electronic transaction:
 - Originated by a human customer who connects to a supplier
 - The customer and supplier are in different physical locations
 - The customer and supplier represent two different organisations
 - They use two different 'ends' of an application on different hardware platforms on different corporate networks
 - The people are in different legal and compliance jurisdictions
 - The technologies are in different legal and compliance jurisdictions
 - They are connected together, possibly through a third party, across the internet and the transaction is routed (possibly randomly) through multiple ISPs, themselves in multiple jurisdictions & using multiple technologies
- Question: under whose policy does the transaction take place?
- This policy 'web' is extremely complex and difficult to govern

Benefits & Applications of Domain Models

- The location embodiment (scope) of policy
- Reduces complexity & delivers clarity
- Controls resource segregation & enables information-sharing
- Key to analysing & implementing risk management roles & responsibilities
- Strategic concept that associates people with technology with policy
- Enables allocation of ownership & responsibility to manage assets
- Provides agility to integrate (and dis-integrate) business units and technologies efficiently and rapidly for divestment & acquisition
- Forms the location basis for Security Service Oriented Architecture (SOA)

Security Domain Definition

- A security domain is a set of elements subject to a common security policy defined and owned by a single security policy authority



Domain Registration Authority

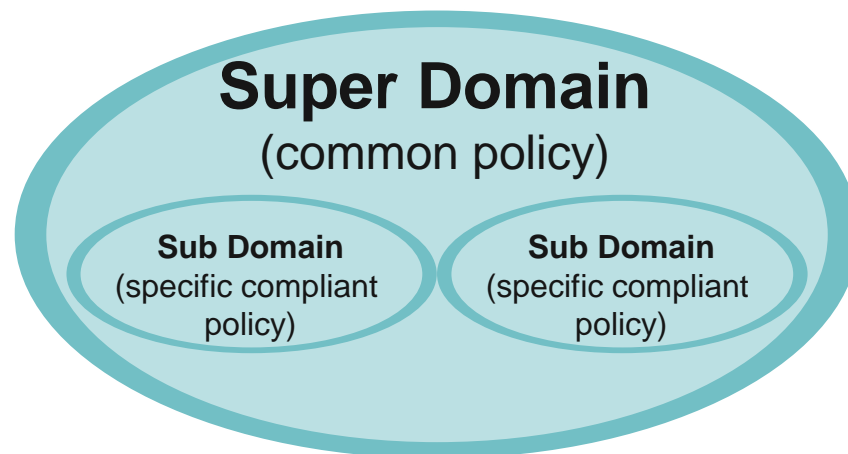
- Setting policy for the domain
- Establishing authentic identity of applicant
- Verifying credentials of applicant
- Establishing right to be registered
- Agreement to security policy and practices
- Authorisation of the applicant to participate
- Does the RA trust the applicant?
- Set operating practices and procedures
- Discipline and revoke registrations

Domain Certification Authority

- Setting credentials issuing (certification) policy and practices (CPS)
- Checking registration and authorisations
- Receiving and certifying public keys
- Authenticating credentials requests
- Publishing credentials and CRLs
- Providing a chain of trust through hierarchical certifications
- Monitoring compliance with policy
- Disciplining and revoking credentials

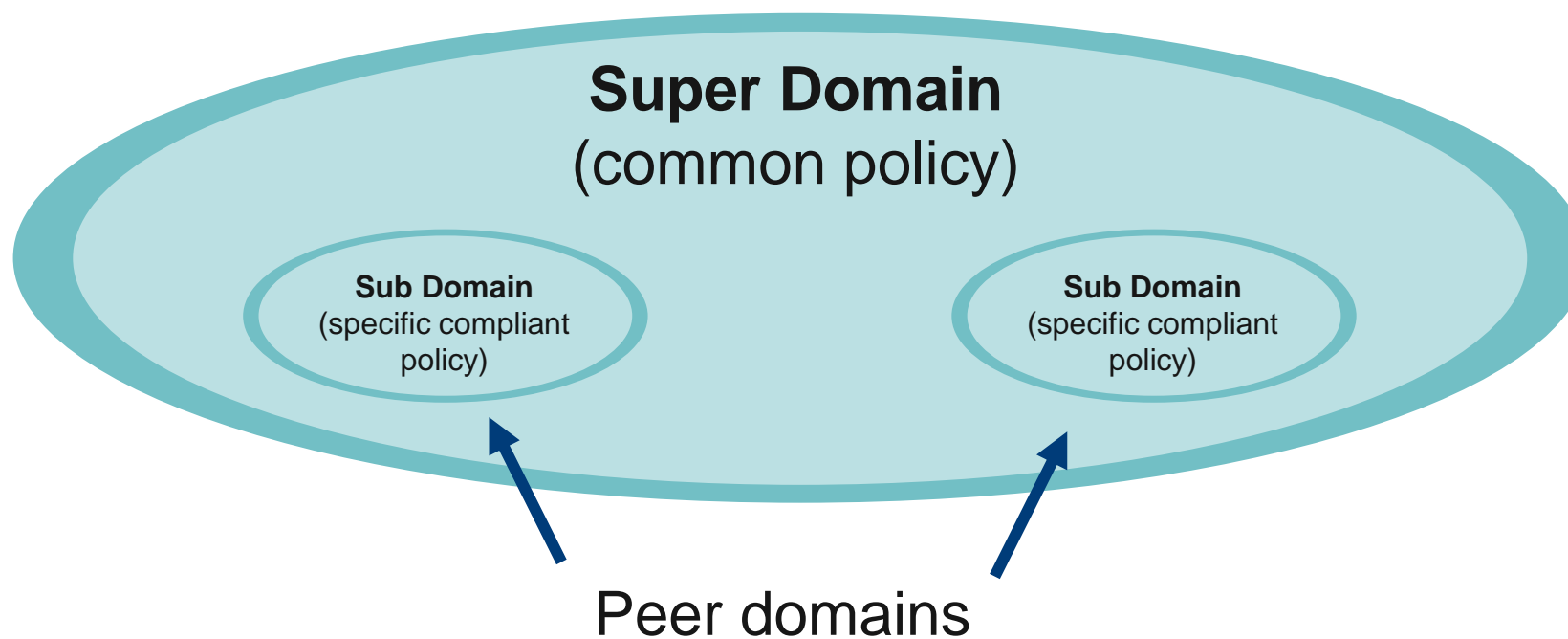
Super Domain & Subdomain Definitions

- A subdomain is a set of elements subject to a security policy defined and owned by a single security policy authority, that is derived from, and complies with, the policy of a higher authority
- A super domain is a set of elements subject to a common security policy defined and owned by a single security policy authority, that contains one or more compliant subdomains, each with their own specific interpretation of the super domain policy



Peer Domain Definition

- Peer domains are subdomains sharing a common super domain policy with which they must comply

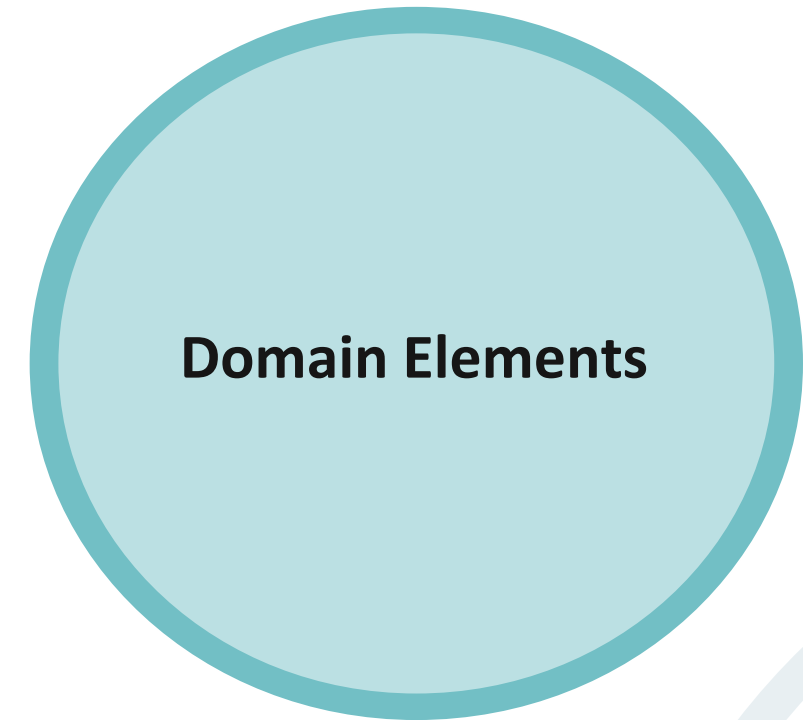


Logical & Physical Security Domains

- A **logical** domain is a set of logical elements (virtual or without specific physical location) subject to a common security policy defined and owned by a single security policy authority
 - Line of business, community of users, information classification, application, etc.
- Logical domains are segregated logically
 - Logical access control services
- A **physical** domain is a set of physical elements (in a specific physical location or technology layer) subject to a common security policy defined and owned by a single security policy authority
 - Territory, site, building, platform, network, etc.
- Physical domains are segregated physically
 - Borders, fences, doors, firewalls, etc.

The Isolated Domain Model

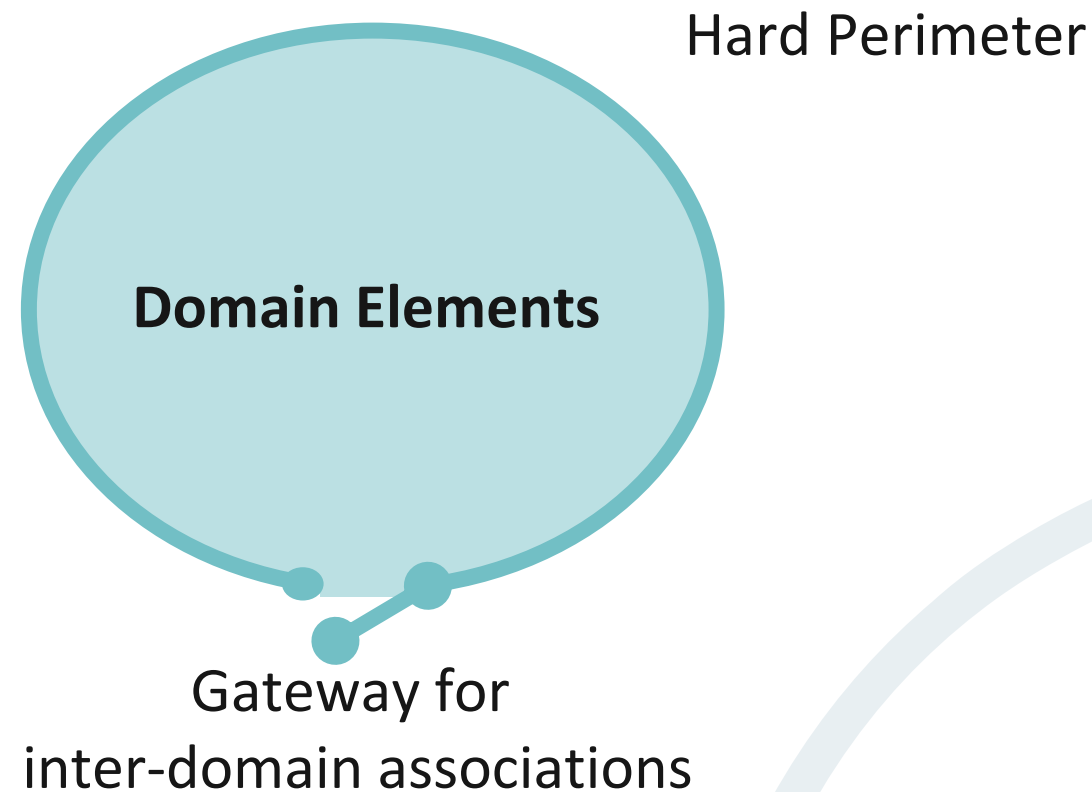
- Each isolated domain should enforce its own self-contained security policy
- The boundary of each domain must be explicit
- Trust within the domain is constant due to common registration



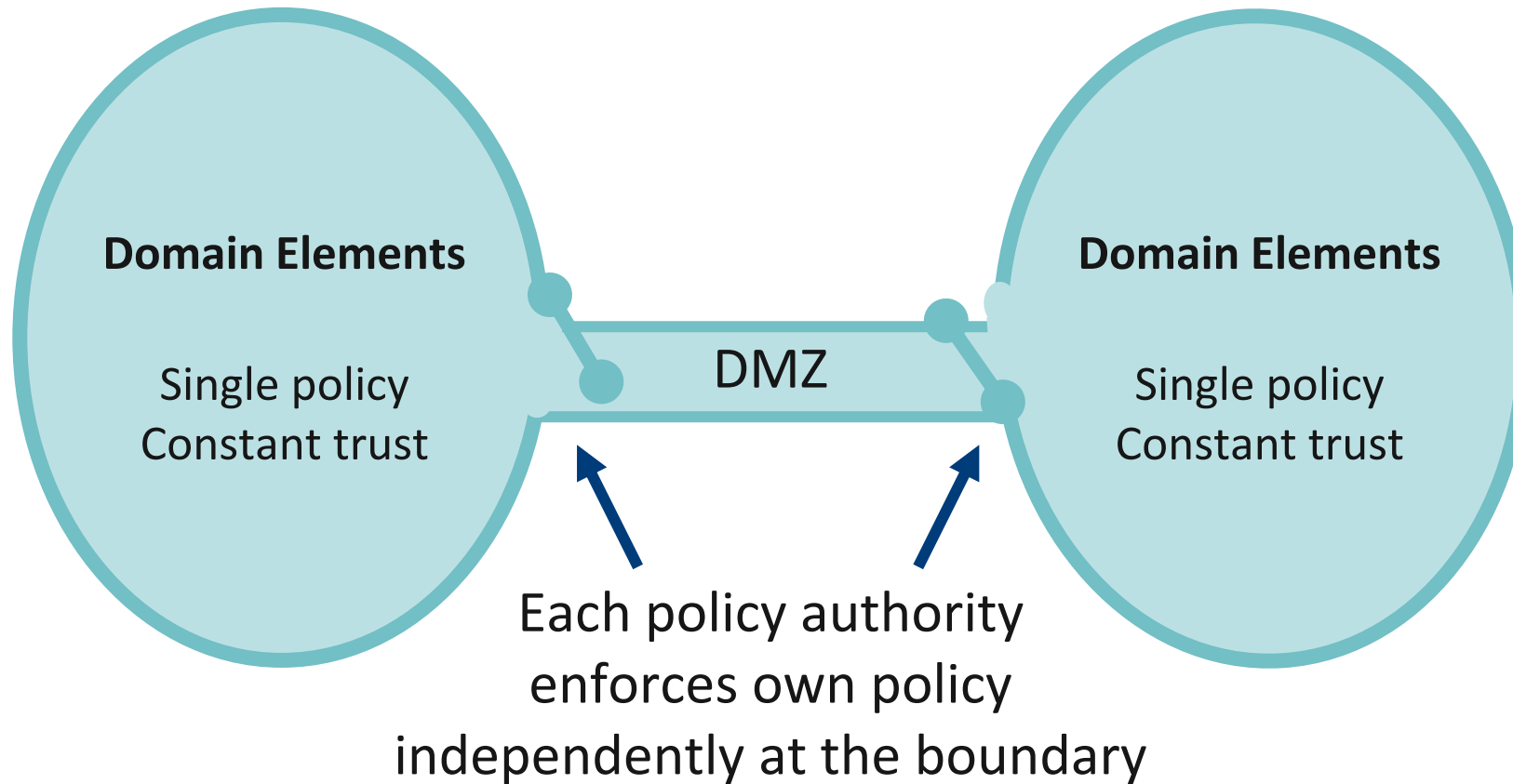
No inter-domain associations

The Independent Domain Model

- Each domain should enforce its own security policy, independently of other domains
- The boundary of each domain must be explicit
- Trust within a domain is constant due to common registration
- Trust between domains is not constant



Inter-domain Boundary Control

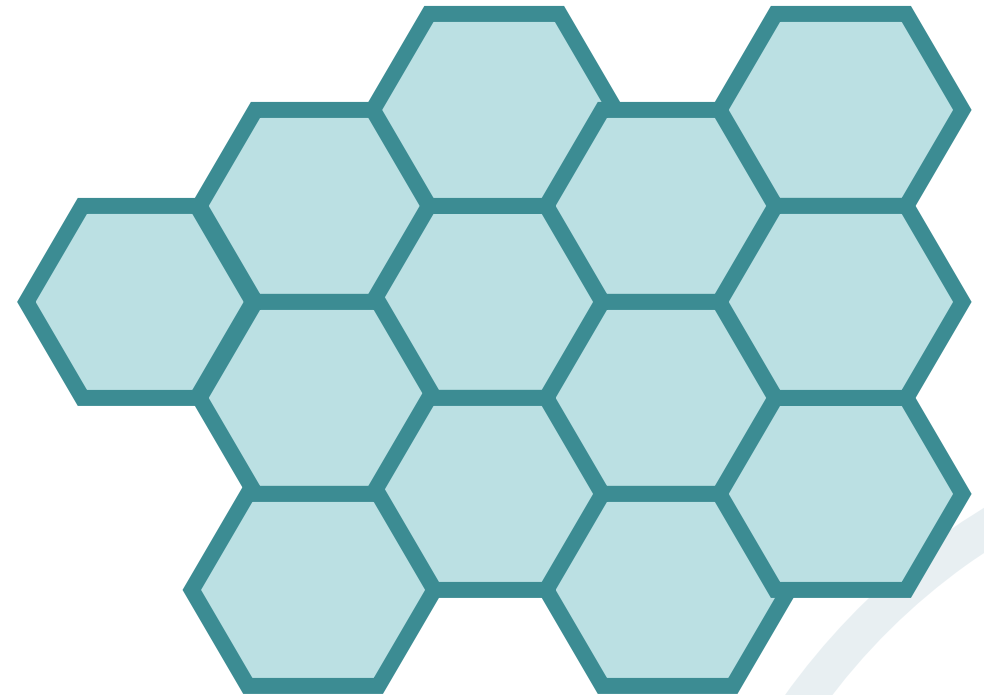


Variable Trust Issue

- Trust is not binary, it is a continuum
- Who do we trust and how much:
 - customers
 - partners
 - agents / brokers
 - suppliers
 - service providers
 - shareholders
 - regulators
 - competitors
 - the public

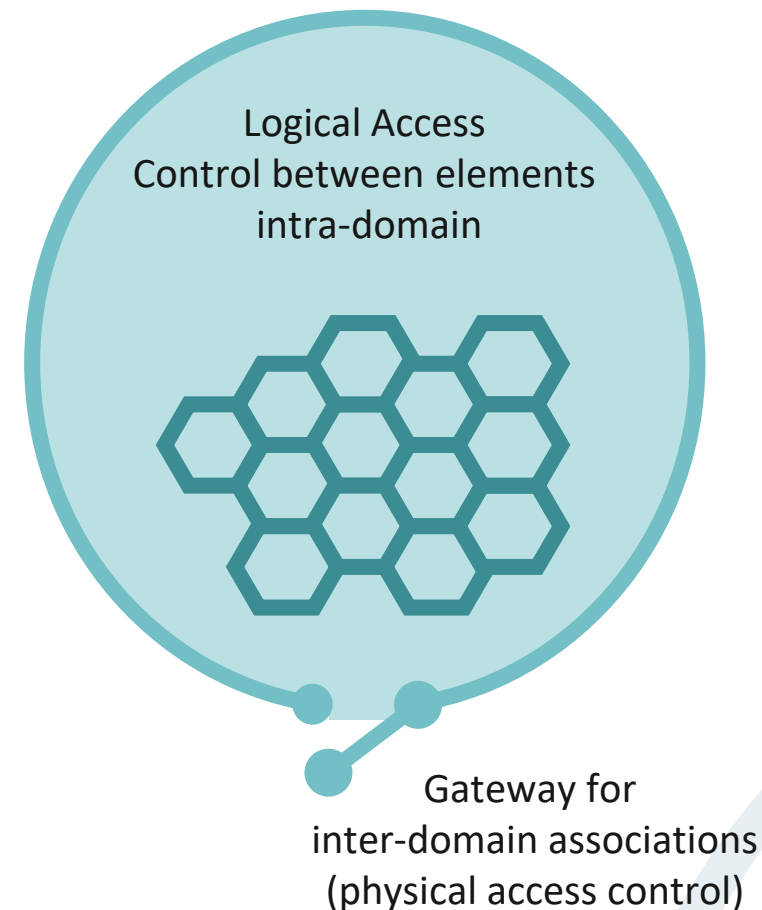
Honeycomb Domain Model

- Many cells
- Each cell has its own perimeter
- Access granted cell by cell
- Access to one cell does not imply access to any other cell
- Each cell has an independent access policy
- Who can enter
- What they can do
- Logical access control system



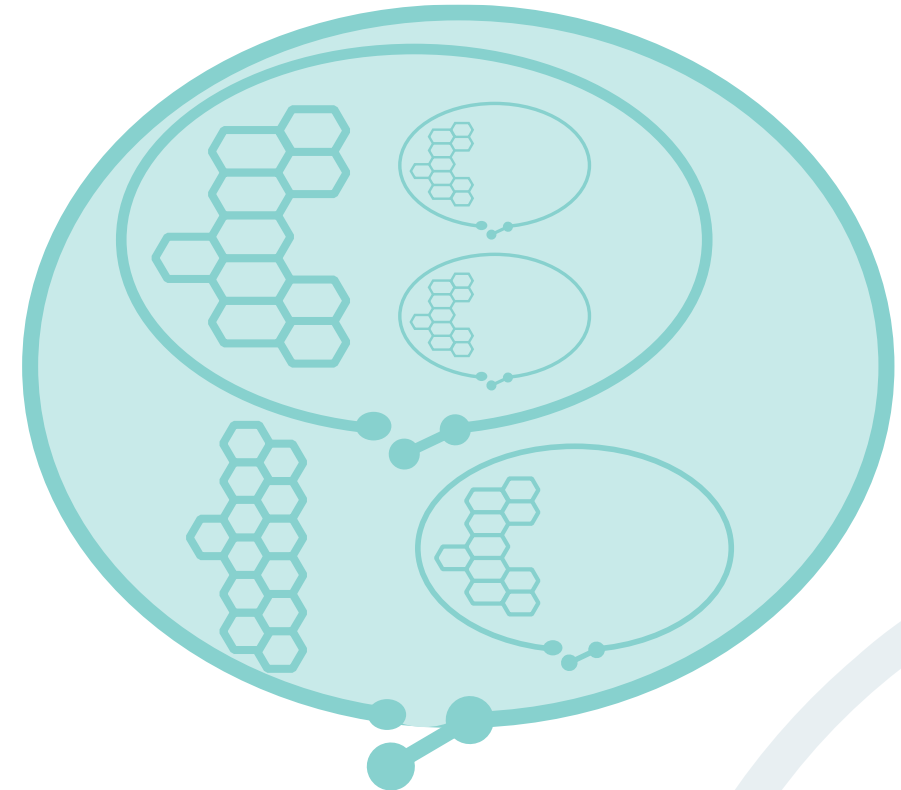
Combined Domain Model

- Combines Independent Domain (or Isolated Domain) with Honeycomb Domain
- Resolves 'binary' gateway issue
- Resolves 'variable trust' issue
- Provides degree of strength-in-depth (combined logical and physical controls)
- Common in classified systems
 - Security clearance gets user through gateway into domain but with no access to resources
 - Access permissions to resources applied as logical honeycomb

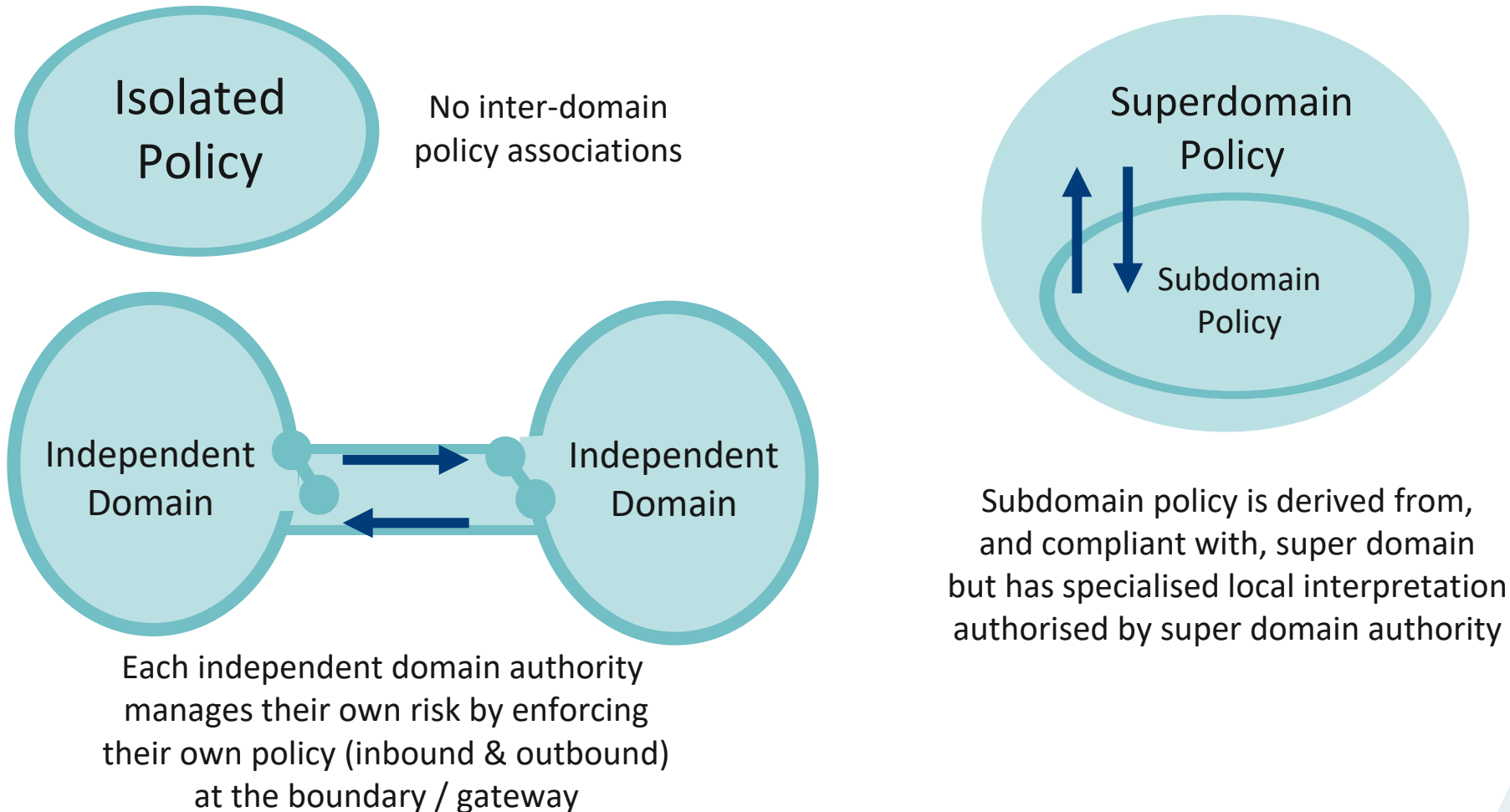


Multi-tiered Security Domain Model

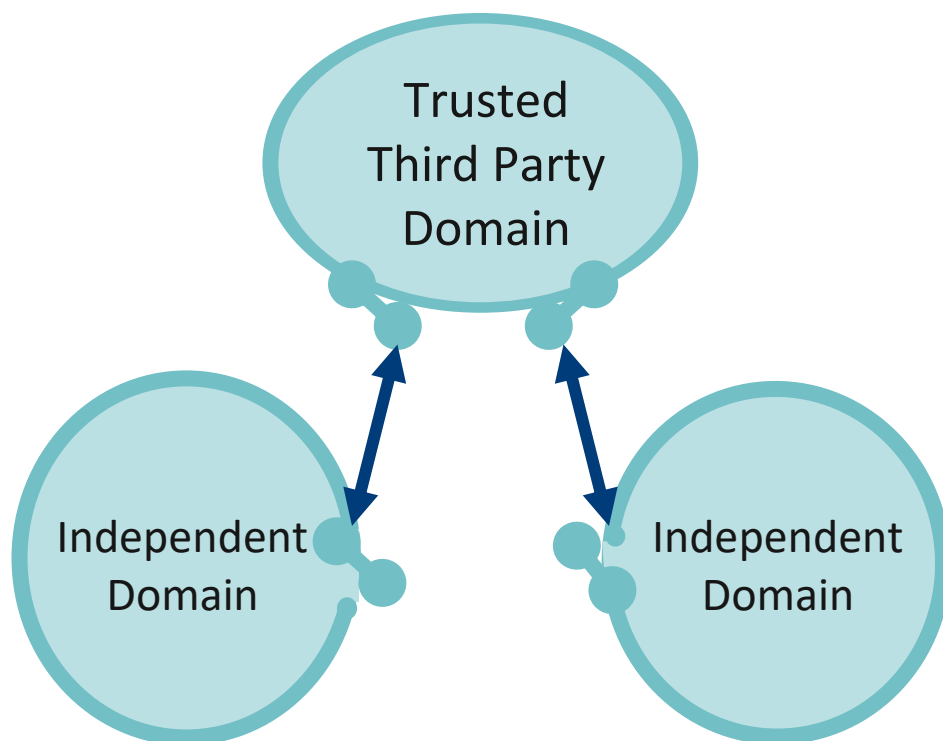
- A layered model of domains
- Access to domains is successive
- At each boundary - a new policy
- Overall - are you registered?
- Overall - are you authenticated?
- At each domain boundary- are you authorised?



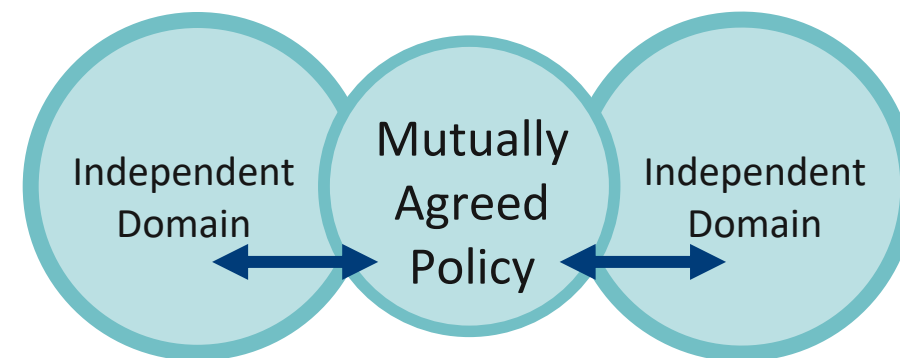
Simple Inter-domain Policy Associations



Complex Inter-domain Policy Associations



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

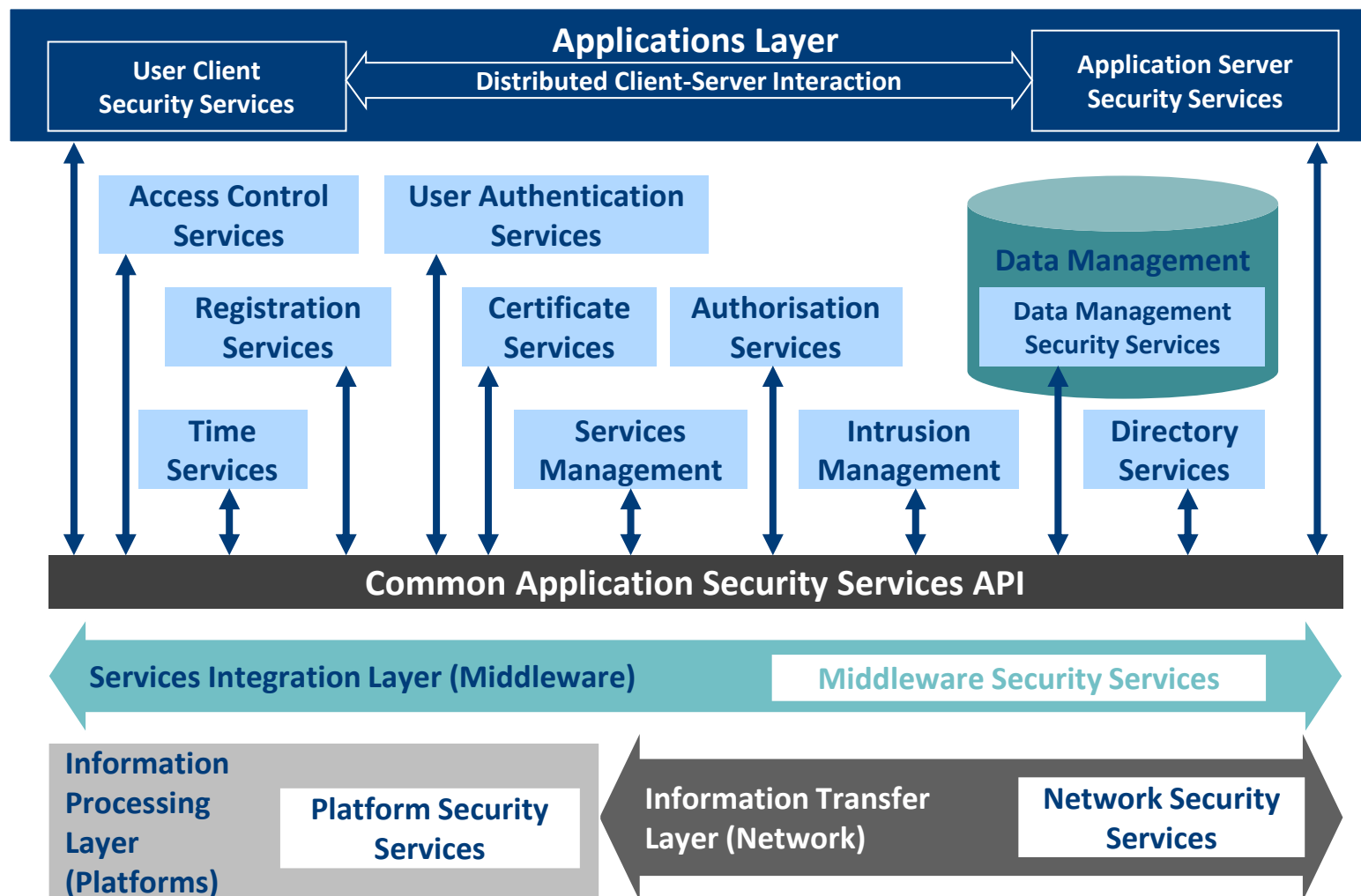


The two independent domain authorities
act collectively to agree / negotiate a
common policy for a shared domain.
Challenging: the common policy must contain
every possible circumstance and/or
very specific risk conflict resolution
processes & procedures

Infrastructure Layer Domains

- Each layer of infrastructure in an architecture is an independent domain
 - Different policy / registration authorities
 - Different technology-specific interpretations of policy
- Rules of Independent Domains apply
 - The boundary of each domain must be explicit
 - Trust within a domain is constant due to common registration
 - Trust between domains is not constant
 - Each domain should enforce its own security policy, independently of other domains
- Security services are deployed in each technical domain to meet the policy, control & enablement objectives of that domain
 - E.g. Network security services exist to protect the network from damage and enable network service excellence – they do not and cannot secure other domains such as the application domains

Security Services in Infrastructure Domains



Domain Complexity

- Most environments comprise a complex web of multiple security domains
 - A single Physical Domain hosts multiple Logical Domains
 - A single Logical Domain operates on multiple Physical Domains
 - In a structure that also combines Super Domains, Subdomains & Peer Domains with multiple different types of domain associations between them
- Involves a diversity of risk types, interactions & strategies

Diverse Risk Domains

Generic Risk Categories

- Economic & financial risk
- Facilities & Environment Risk
- Health & Safety Risk
- Information Security Risk
- Control Frameworks Risk
- Legal & Regulatory Compliance Risk
- Corporate Governance Risk
- Reputation Risk
- Strategic Risk
- Processing and Behavioural Risk
- Technology Risk
- Project Management Risk
- Criminal and Illicit Acts Risk
- Human Resources Risk
- Supplier Risk
- Management Information Risk
- Ethics Risk
- Geo-political Risk
- Cultural Risk
- Climate Risk

Risk Domain Interaction

- 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



Nightclub Finance Risk

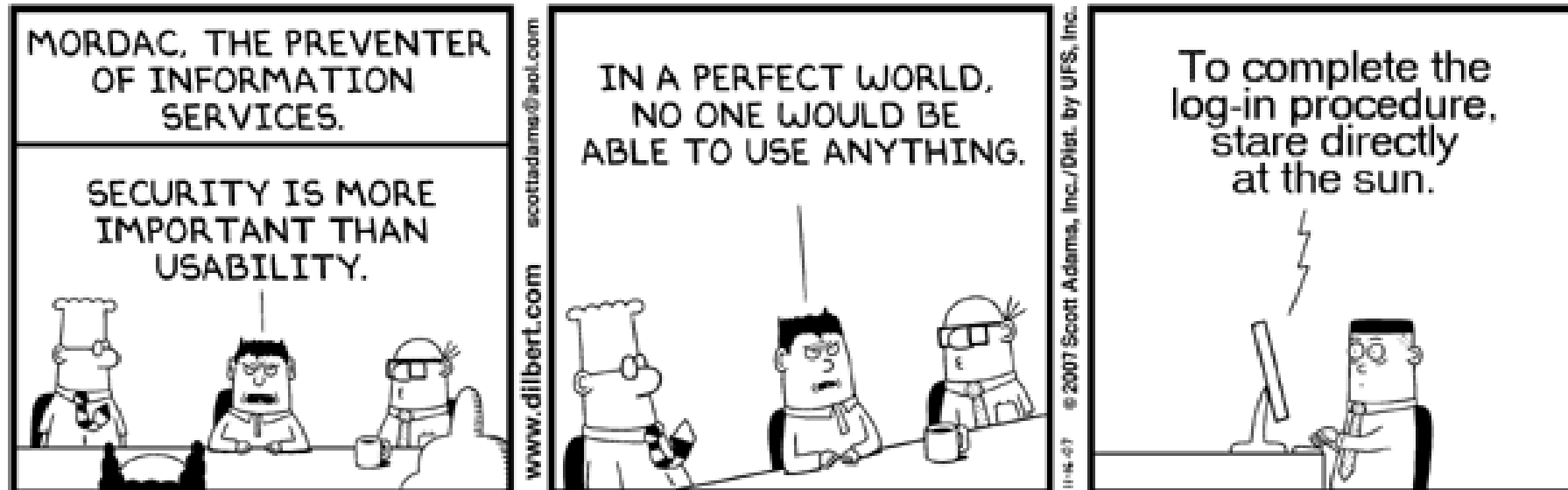
versus

Nightclub Health & Safety Risk



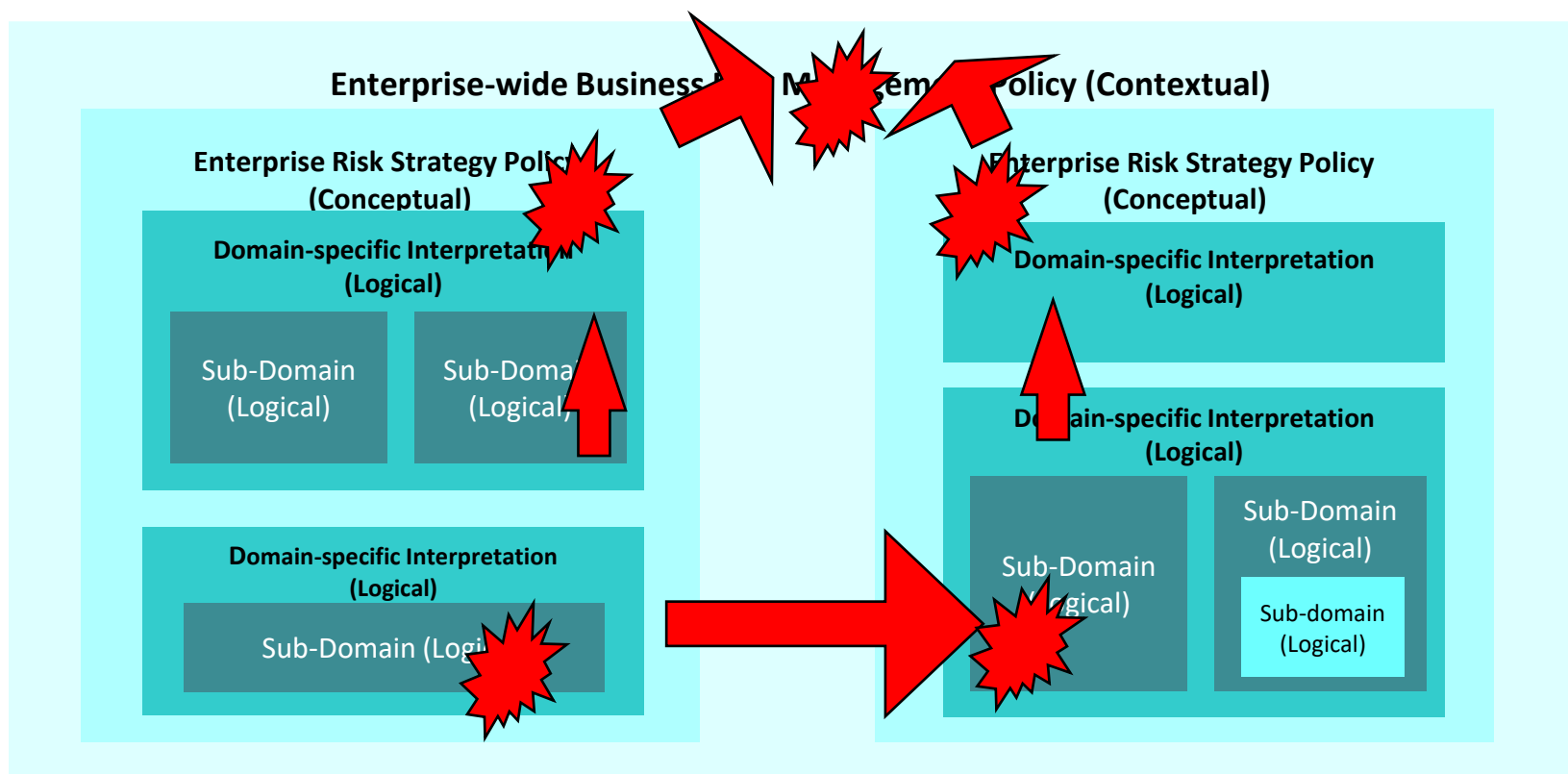
Appendix F1-2

- Risk Domain Interactions – Mapping to ICT

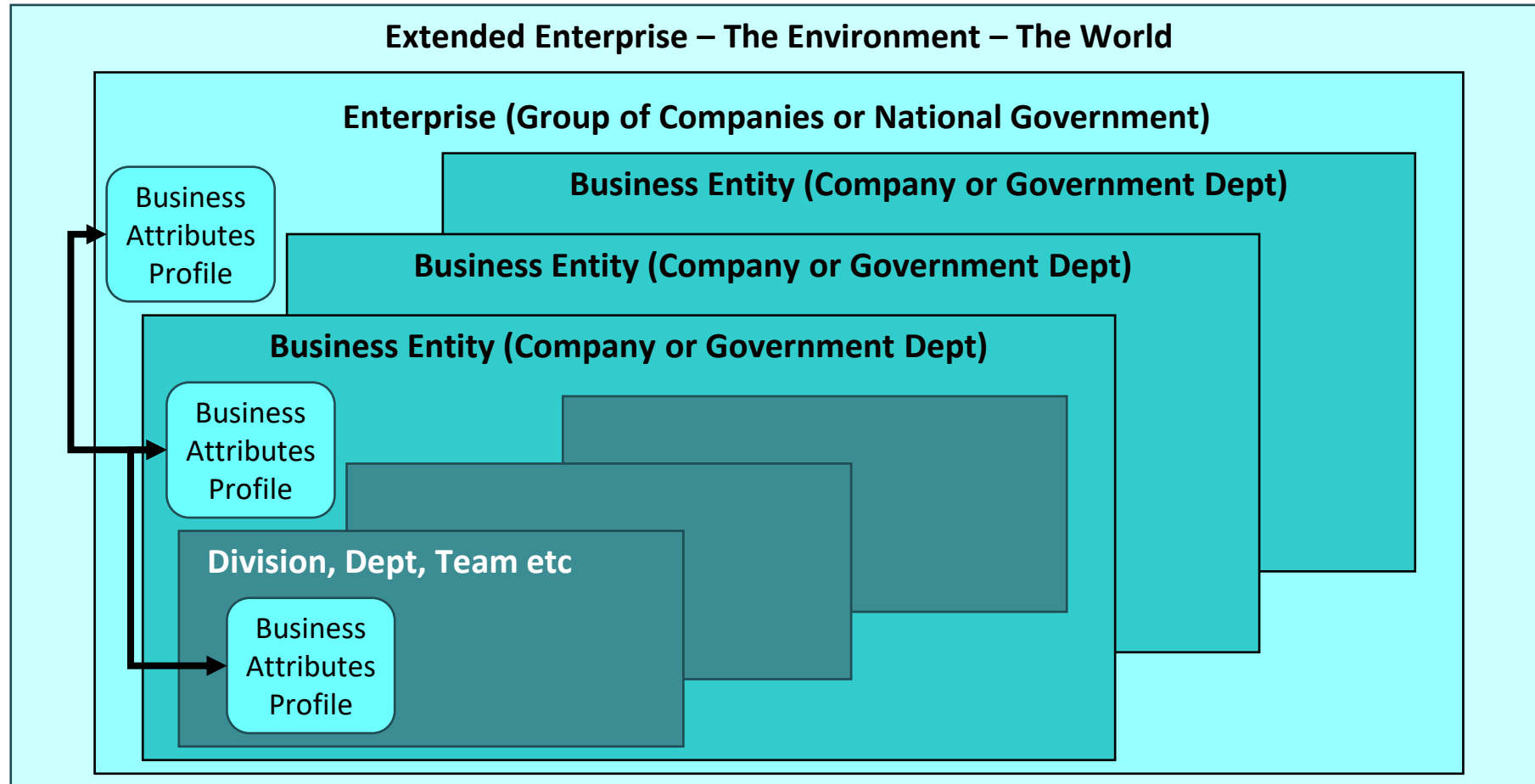


Inter-domain / Systemic Risk

A risk in any domain can have consequences for any other domain in any location on the domain model



Enterprise Domain Risk Perspectives



Sample Questions

Competency Domain 5

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



Competency Domain 5

- Which ONE of the following statements is NOT a rule of SABSA security domains?
 - A. Each domain must enforce its own security policy independently of other domains
 - B. The boundary of each domain must be explicit
 - C. Trust within a single domain is constant
 - D. Trust between domains is constant

Competency Domain 5

- Which one of the following is NOT a benefit of Domain Modelling?
 - A. Reduces complexity and delivers clarity
 - B. Controls resource segregation
 - C. Reorganises businesses
 - D. Enables information sharing

Time & Performance Management Concepts

Section 11

Scope: Strategy & Planning Phase - Time

	Architecture Matrix	Management Matrix
Contextual	Business Time Dependence	Performance Management
	Time Dependencies of Business Goals & Value Creation	Defining Business-Driven Performance Targets
Conceptual	Time Management Framework	Service Level Definition
	Through-life Risk Management Framework; Attribute Performance Targets	Managing Performance Criteria and Targets; Abstracting Attribute Performance Targets

Section 11 Competency Objectives

Competency / Question Domain 6 – When (Time)

Knowledge Element	Knowledge Competency	Comprehension Competency
The SABSA Lifecycle	List in order the 4 phases of the SABSA Lifecycle & identify the relationship between lifecycle and strategic, tactical & operational approaches	Associate lifecycle phases with architecture layers & their deliverables, and align the SABSA & Deming lifecycles
Through-life Risk Management	Describe Through-life characteristics	Summarise lifecycle perspectives of risk
	List the objectives describe the structure of the SABSA Risk Management Process	Explain the relationship & alignment between the SABSA RMP and the SABSA Matrices
Process Improvement Framework	List the domains and process areas of the SABSA SMP & its objectives	Differentiate between levels of the SABSA SMP
Performance Management Framework	Describe the process of defining Business-Driven performance targets	Contrast the 5 measurement categories of the SABSA PMF and explain approaches to obtaining measures & formatting metrics
Through-life Architecture Vitality Framework	Define Architectural Vitality	Explain the SABSA Vitality Framework

Temporal Business Context

- Business deadlines
- Business performance
- Dynamic market & economic conditions
- Time-to-market with business solutions
- Time to execute business re-organisations
- Divestment, acquisitions, partnership, outsourcing, etc.
- Predictability of time-to-market with technical solutions
- Prioritisation & timeliness of risk treatments
- Timeliness of information-sharing for decision making
- Core business process timeliness & sequencing
- Operational continuity

Temporal Strategies & Concepts

- Service Development Lifecycle
- Through-life Risk Management Framework
- Process Improvement Framework
- Performance Management Framework
- Through-life Architecture Vitality Framework

The Problem of Operational Imbalance

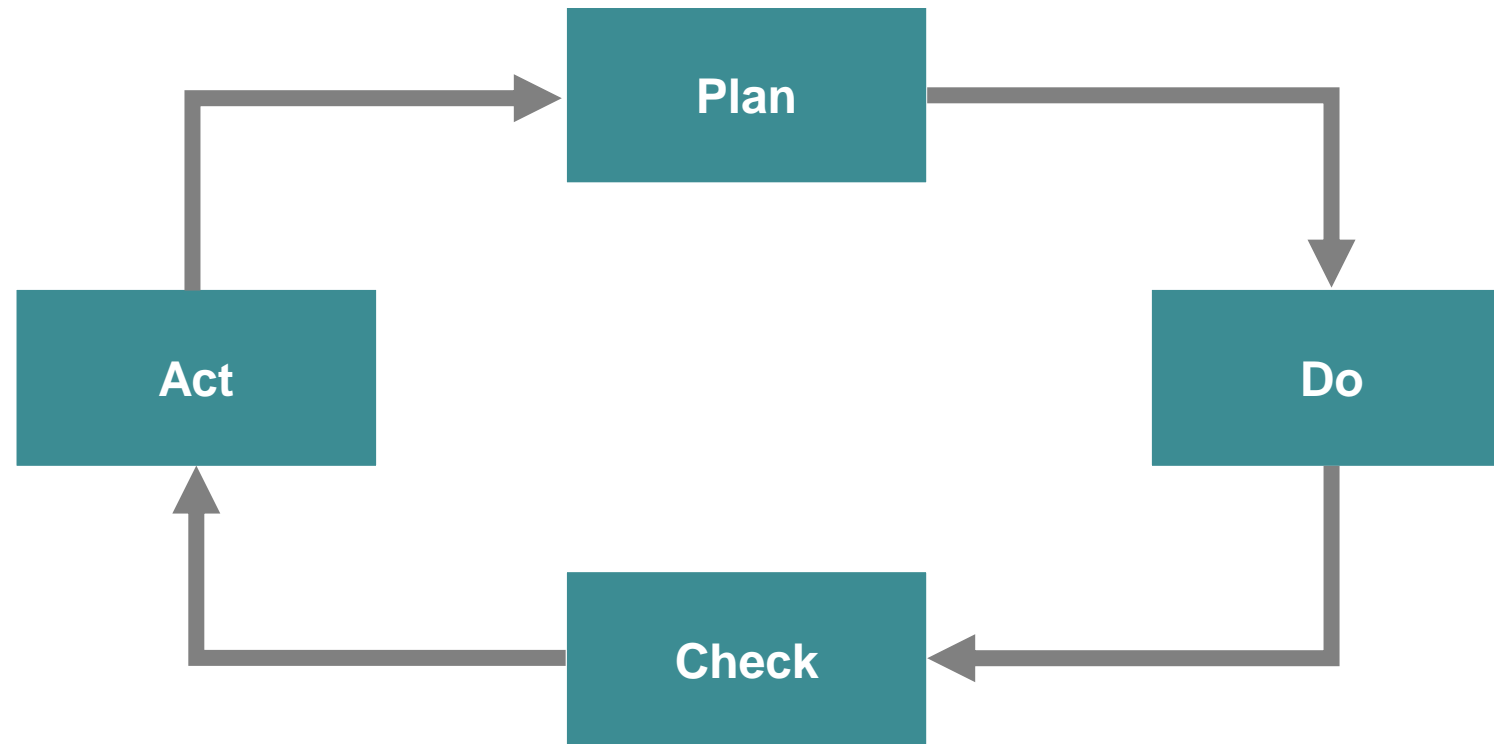


Properties of Strategic Lifecycle

- Strategy
 - Setting out long-term goals and plans for reaching those goals
 - Might have a beginning but never ends
 - Strategic organisations are in state of constant change
- Tactics
 - Setting medium-term goals and plans to achieve those goals
 - Have both a defined beginning and an end (they 'go live')
 - Projects are tactical initiatives towards strategic goals
 - Alternatively, they address an immediate problem
- Operations
 - Deals with the day-to-day job of keeping the business running
 - Based upon repetitive procedures that make up business processes
 - Developed through tactical projects, which in turn were driven by strategies

Feedback Loop Lifecycles

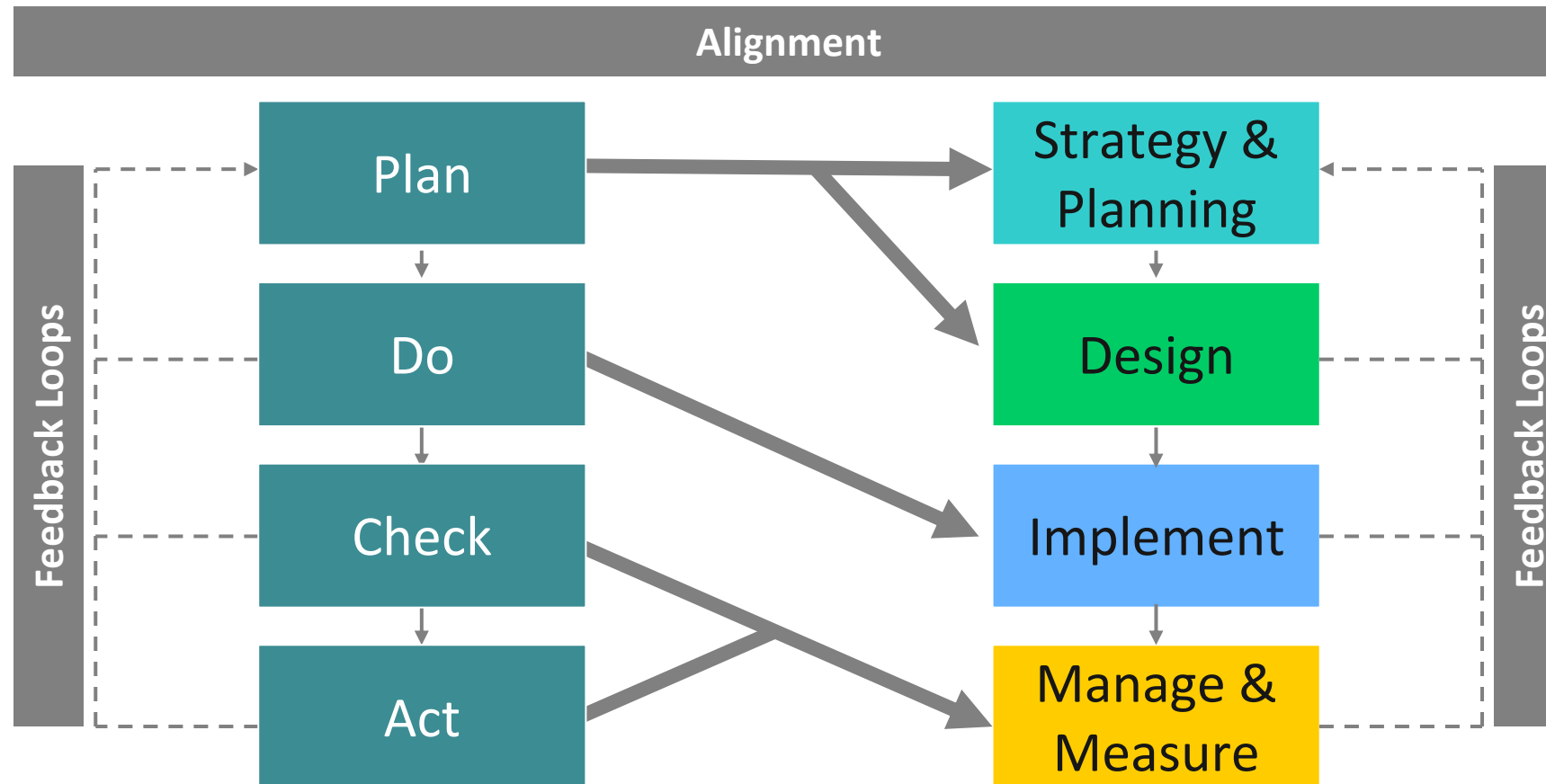
- Deming lifecycle (used in ITIL® & ISO 27000 etc.)



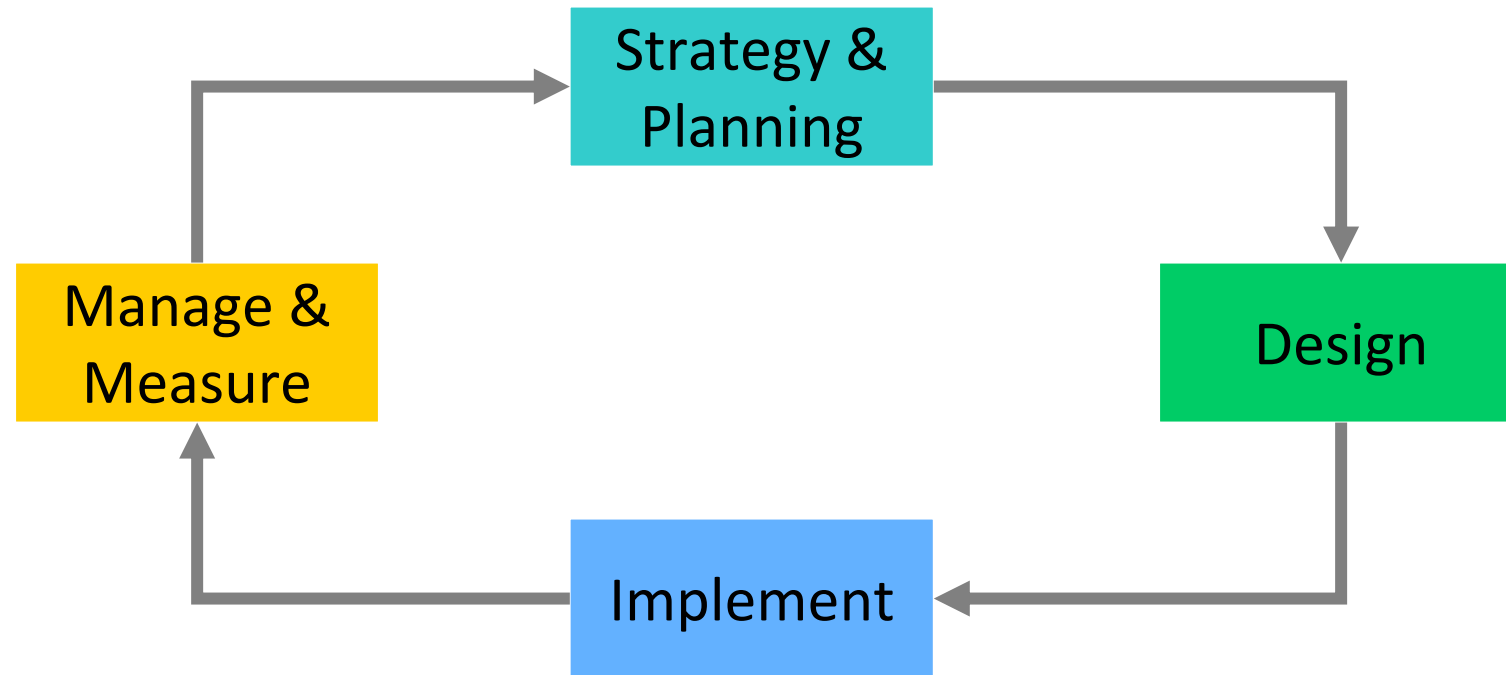
SABSA Lifecycle Principles

- Strongly business-driven
 - Regards it as mandatory that security demonstrably supports the business mission
- Splits “Plan” into two to gain more granular traceability from business need to technical implementation and security management process
 - Strategy & Planning
 - Design
- “If you cannot measure you cannot manage”
 - Considers “Check” and “Act” to be mutually inclusive & inherent to post-implementation operations
- Merges these two elements into
 - Manage & Measure
- The SABSA view is mutually compatible with Deming’s “plan, do , check, act”

Lifecycle Alignment – Deming to SABSA



SABSA Development Lifecycle



Architecture Strategy & Planning Phase

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Goals & Decisions	Business Risk	Business Meta-Processes	Business Governance	Business Geography	Business Time Dependence
	Business Value; Taxonomy of Business Assets, including Goals & Objectives , Success Factors, Targets	Opportunities & Threats Inventory	Business Value Chain; Business Capabilities	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of Business Goals and Value Creation
CONCEPTUAL ARCHITECTURE	Business Value & Knowledge Strategy	Risk Management Strategy & Objectives	Strategies for Process Assurance	Security & Risk Governance; Trust Framework	Domain Framework	Time Management Framework
	Business Attributes Taxonomy & Profile (with integrated performance targets)	Enablement & Control Objectives; Policy Architecture; Risk Categories; Risk Management Strategies; Risk Architecture; Risk Modelling Framework; Assurance Framework.	Inventory of all Operational Processes (IT, industrial, & manual); Process Mapping Framework; Architectural Strategies for IT used in process support.	Owners, Custodians and Users; Service Providers & Customers; Trust Modelling Framework	Security Domain Concepts & Framework	Through-Life Risk Management Framework; Attribute Performance Targets

Architecture Design Phase

	Assets (what)	Motivation (why)	Process (how)	People (who)	Location (where)	Time (when)
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Trust Relationships	Domain Maps	Calendar & Timetable
	Inventory of Information Assets; Information Model of the Business	Risk Models; Domain Policies; Assurance Criteria (populated Assurance Framework).	Information Flows; Functional Transformations; Service Oriented Architecture; Services Catalogue; Application Functionality and Services	Domain Authorities; Entity Schema; Privilege Profiles; Trust Relationship Models	Domain Définitions; Inter-domain Associations & Interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	Infrastructure	Processing Schedule
	Data Dictionary & Data Storage Devices Inventory	Risk Management Rules & Procedures; Risk Metadata	Working Procedures; Application Software; Middleware; Systems; Security Mechanisms; Process Control Points	User Interface to Business Systems; Identity & Access Control Systems	Workspaces; Host Platforms, Layout of Devices & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	Component Assets	Risk Management Components & Standards	Process Components & Standards	Human Entities: Components & Standards	Locator Components & Standards	Step Timing & Sequencing Components and Standards
	Products and Tools, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery; Application Products	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators; Component Configuration	Time Schedules; Clocks, Timers & Interrupts

Implementation Phase & Approach

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

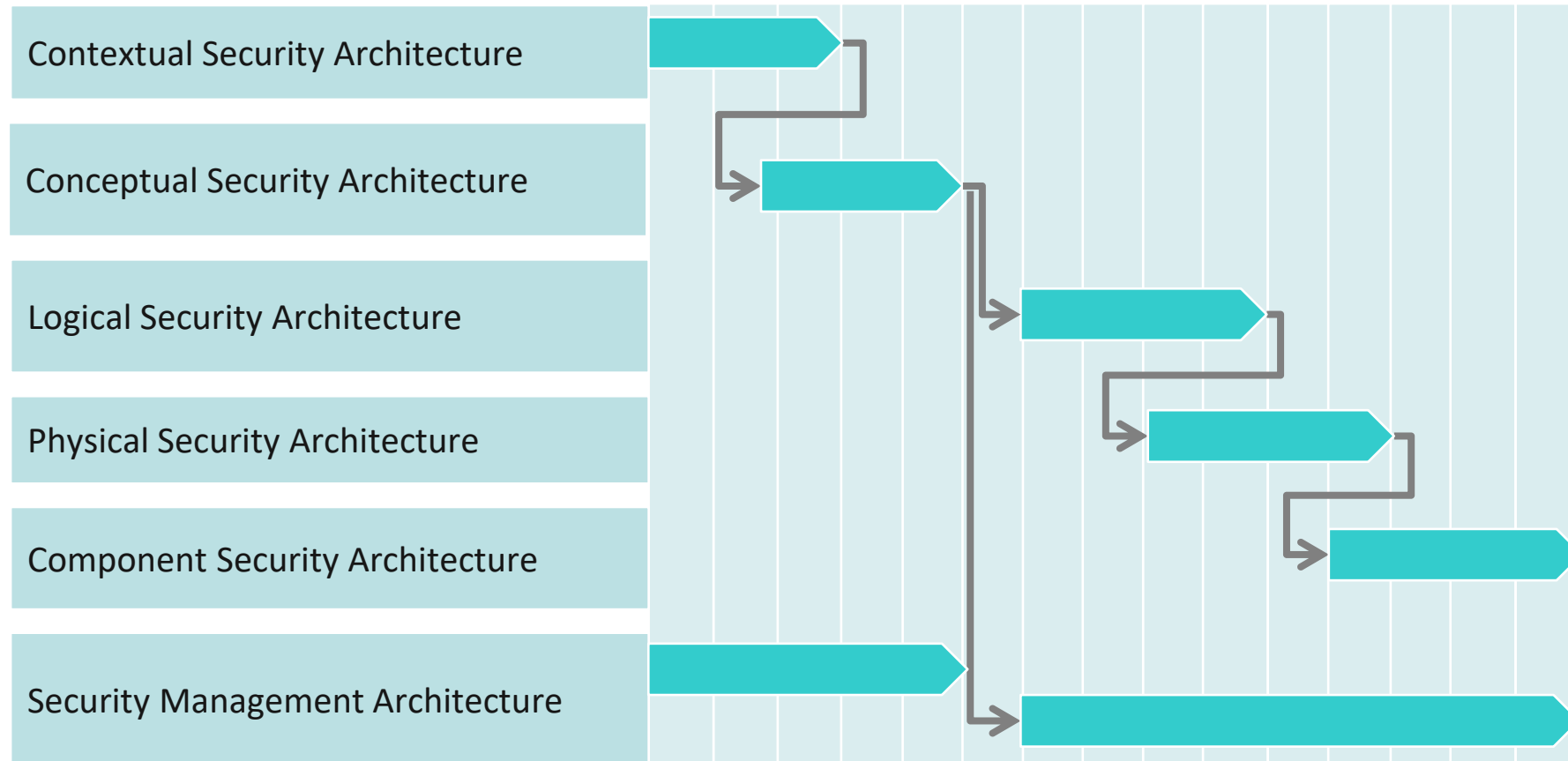
Manage & Measure Phase – Lifecycle Overlay

- SABSA Architecture traceably abstracts from pure Business Context to:
 - Pure technical deployment in the Component layer
 - Pure management in the Management layer
- The Management layer defines all aspects of security management and constructs the means to manage and incorporate change by being presented vertically across the other layers:
 - Strategy (Context & Concept Layers)
 - Tactics (Logical, Physical, & Component Layers)
 - Operations (Security Management Matrix)

Manage & Measure Phase – Management Matrix

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	Assurance of Operational Excellence & Continuity	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Management & Support of Enterprise-wide and Extended Enterprise Relationships	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable
	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 ARCHITECTURE	Business Driver Development	Business Risk Assessment	Capability Management	Relationship Management	Supply Chain Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Processes and Capabilities for Providing Value to Stakeholders	Managing Suppliers, Service Providers, Customers; Business Partners & Employees. Contract Management	Demand & Supply Management (upstream and downstream); Deployment & Consumption	Defining Business-Driven Performance Targets
CONCEPTUAL ARCHITECTURE	Proxy Asset Development	Developing Risk Objectives	Delivery Planning	Role Management	Business Portfolio Management	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Maintaining Risk Modelling Framework; Risk Analysis on Business Attributes Profile	SLA Planning; BCP; Financial Planning; Transition Planning. Planning and Maintaining the Inventory of Processes and Services Catalogue	Maintaining Trust Modelling Framework; Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Business Footprint: Points of Supply and Access	Managing Performance Criteria and Targets; Abstracting Attribute Performance Targets
LOGICAL ARCHITECTURE	Logical Asset Management	Policy Management	Delivery Management	Enterprise-wide User Management	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management	Risk Modelling; Management of Policy Development & Maintenance. Policy Publication & Compliance Management	SLA Management; Supply Chain Management; BCM; Financial Management; Transition Management	Trust Modelling; Identity & Access Management; Management of User Privileges, Account Administration & Provisioning	Configuration (CMDB) Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
PHYSICAL ARCHITECTURE	Physical Asset Management	Risk Data Management	Operations Management	User Support	Resources Management	Performance Data Collection
	Change Management; Platform & Data Storage Management	Risk Procedure Management; Risk Metadata Management	Job, Incident, Event, and Disaster Recovery Management	Service Desk, Problem, and Request Management	Physical & Environmental Security Management; Real Estate and Facilities Management	Business Systems Monitoring Procedure Management
COMPONENT ARCHITECTURE	Component Management	Risk Management Components	Component Deployment	Personnel Component Management	Component Environment Management	Monitoring Components
	Product & Component Standards Management	Risk Analysis, Monitoring & Reporting Components, Systems and Standards Management	Product & Component Selection, Procurement. Project and Standards Management	Recruitment, Disciplinary, Training & Awareness Delivery. Component and Standards Management	Physical and Environmental Security Component and Standards Management	Analysis, Monitoring & Reporting Component and Standards Management

SABSA Development Process



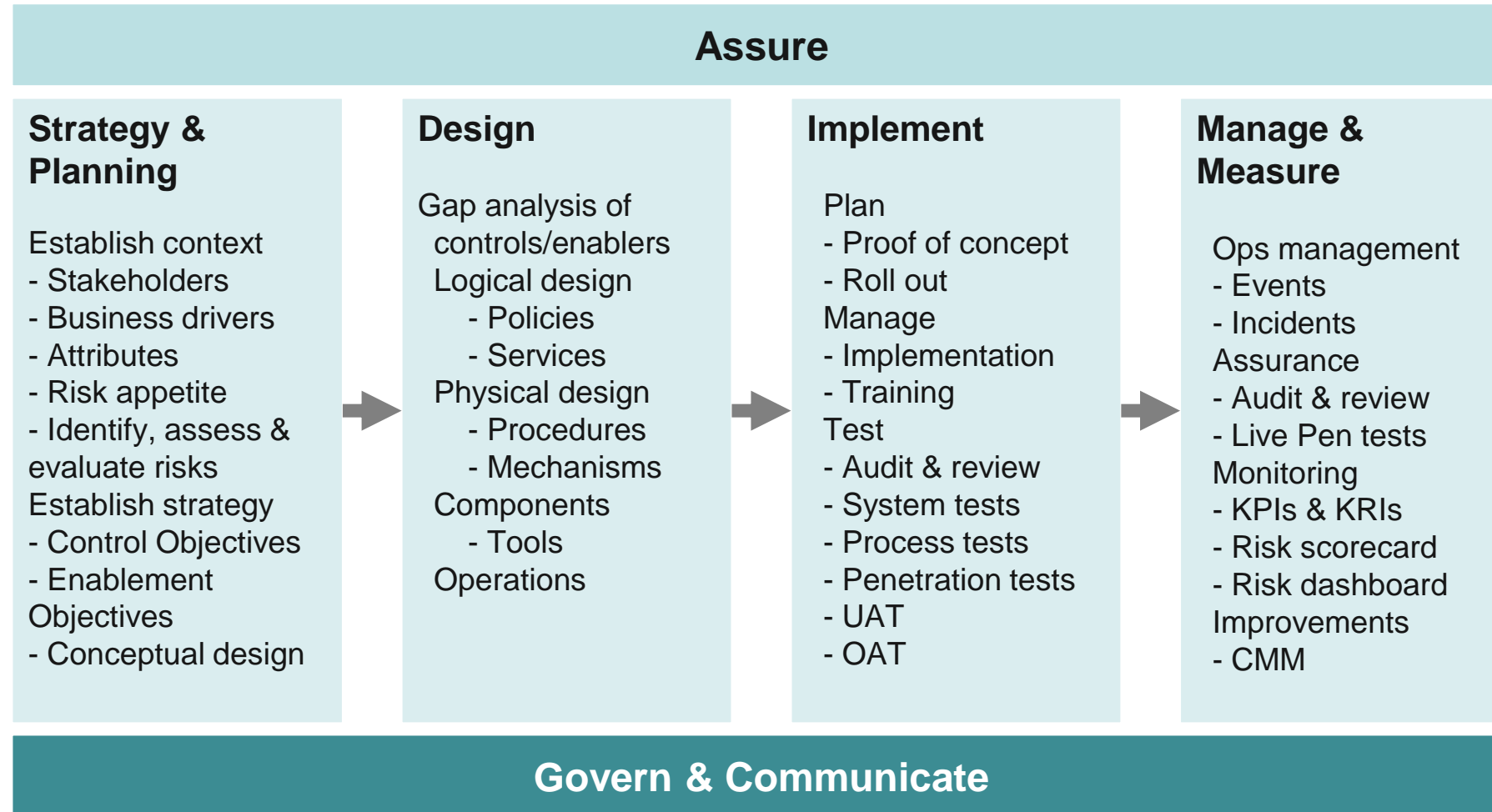
Characteristics of Through-life Risk Management

- Establishes an appropriate infrastructure and culture and applying a logical and systematic method of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risks in a way that enables organisations to minimize losses and maximize gains
- Embedded into the organisation's philosophy, practices and business processes rather than be viewed or practiced as a separate activity. When this is achieved, everyone in the organisation becomes involved in the management of risk
- Provides excellent corporate governance by managing, communicating and assuring risk treatment policies, targets and practices through every phase of the lifecycle

SABSA Risk Management Process

- The SABSA RMP is the primary subject matter of SABSA Advanced Module A1
- For this module our objectives are to gain a Foundation level comprehension of:
 - The RMP Strategy & Planning Phase
 - The Performance Management elements of the RMP Manage & Measure Phase
 - The relevance of the RMP to temporal business context (slide 261)
- The SABSA RMP embodies the SABSA method in a through-life Risk Management process to:
 - Contextualise business risks to targets, goals and objectives
 - Conceptualise security & risk management requirements & performance targets as measurable business attributes
 - Ensures subsequent design, implementation and management of risk & security solutions is business-driven, traceable, prioritised & assured

SABSA Risk Management Process Overview



Risk Management and the SABSA Matrix

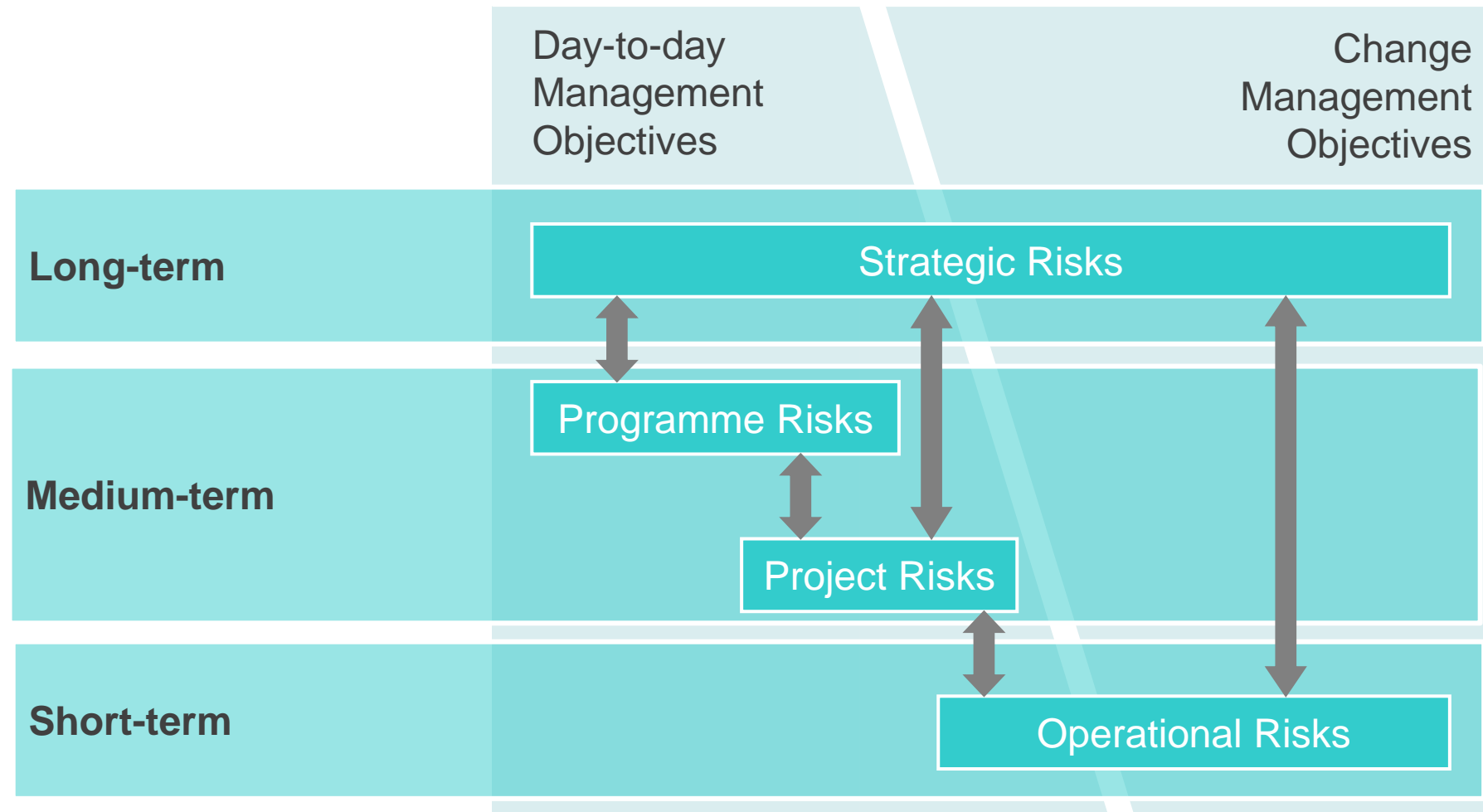
	Factors Affecting Risk	Control/Enablement Objectives & Targets	Risks	Assets at Risk	Risk Management Process	Risk Treatment and Control/Enablement Solutions
	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
CONTEXTUAL	Business Goals & Decisions	Business Risk	Business Meta-Processes	Business Governance	Business Geography	Business Time Dependence
CONCEPTUAL	Business Value & Knowledge Strategy	Risk Management Strategy & Objectives	Strategies for Process Assurance	Security & Risk Governance; Trust Framework	Domain Framework	Time Management Framework
LOGICAL	Information Assets	Risk Management Policies	Process Maps & Services	Trusts Relationships	Domain Maps	Calendar & Timetable
PHYSICAL	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	Infrastructure	Processing Schedule
COMPONENT	Component Assets	Risk Management Components & Standards	Process Components & Standards	Human Entities: Components & Standards	Locator Components & Standards	Step Timing & Sequencing Components and Standards
MANAGEMENT	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management

SASBA Risk Management Activities

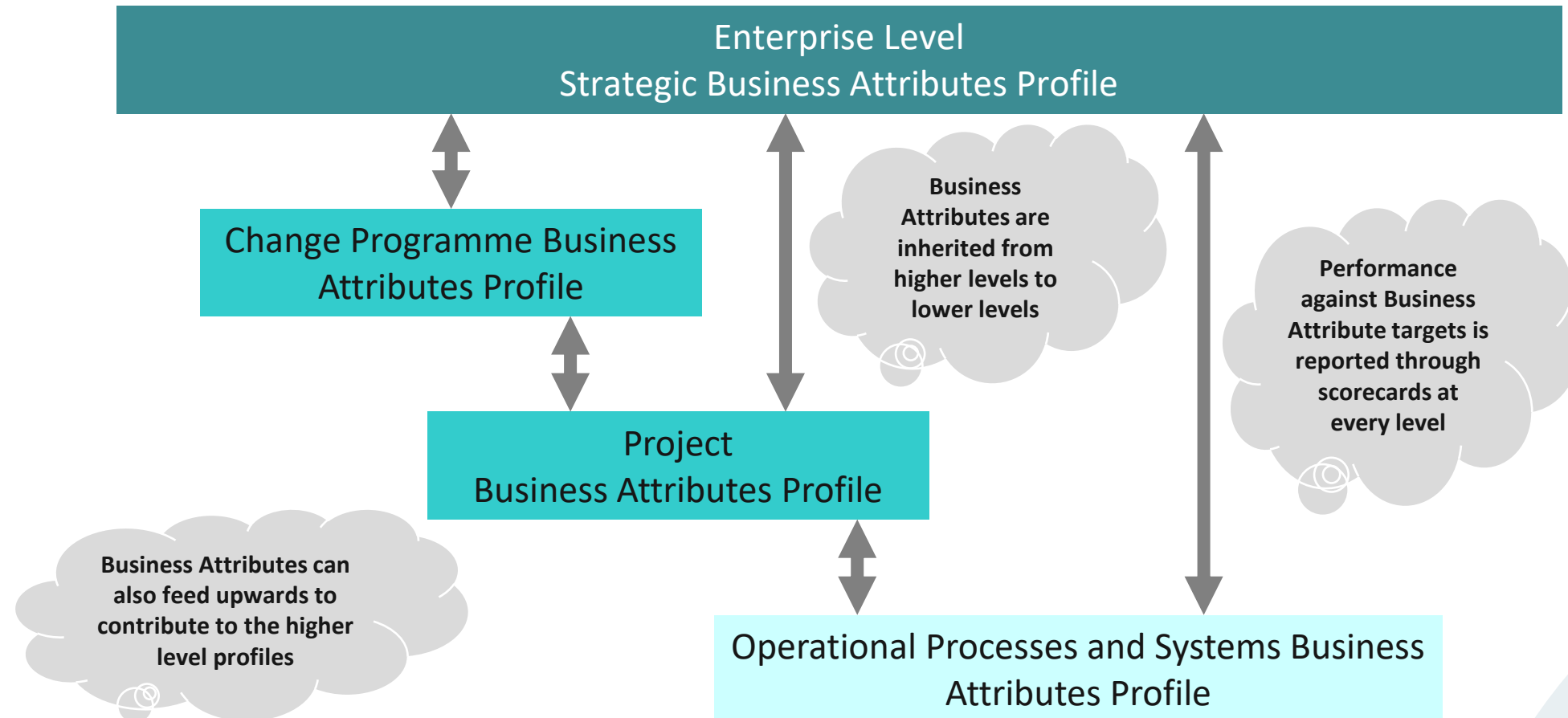
	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Management	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	The row above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

Enterprise Lifecycle Risk Perspectives

Source: OGC M_o_R 2007

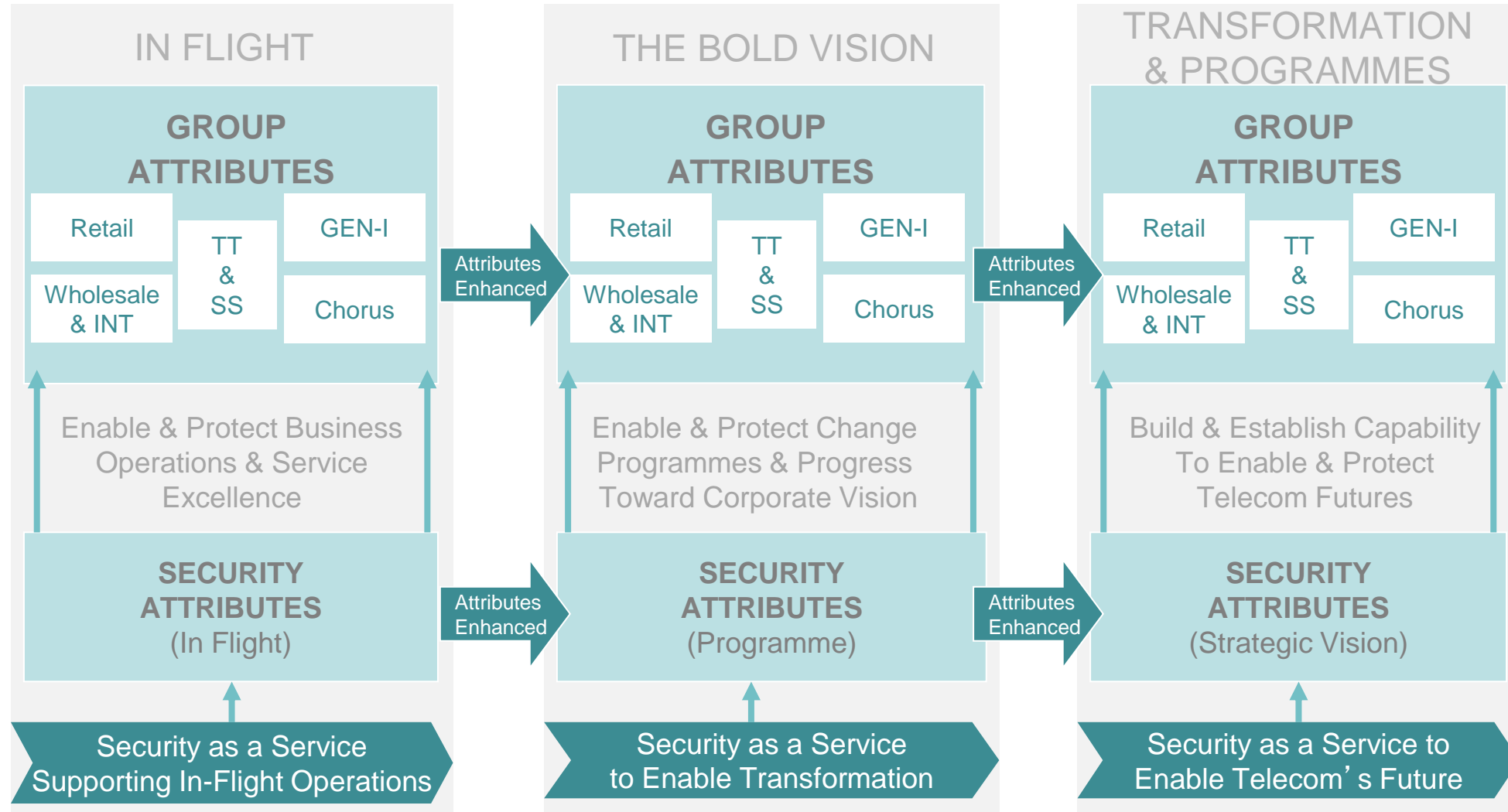


Enterprise Lifecycle Domain Risk Perspectives



SABSA Migration Strategy

Reproduced with permission from New Zealand Telecom



Process Improvement Framework – SABSA Maturity Profile (SMP)

- Coordinates SABSA process information from all parts of the business
 - Demonstrates due diligence to senior management, auditors and regulators
- Based on Capability Maturity Modelling (CMM) concepts
 - Qualitative measurement technique for maturity of processes
 - Six domains mapped onto the SABSA Matrix
 - Consistent, objective 5-point maturity scale
- Identifies, measures and reports compliance practices
 - Against the SABSA framework, model and processes
 - Provides a gap analysis to drive a SABSA improvement programme
- Can be implemented through a web-enabled tool for
 - Ease of use, wide involvement, quick responses
- Regular use tracks progress and measures changes
 - Benchmarking against target maturity

SABSA Maturity Profile Domains

The SABSA application of CMM concept for measuring maturity of SABSA processes

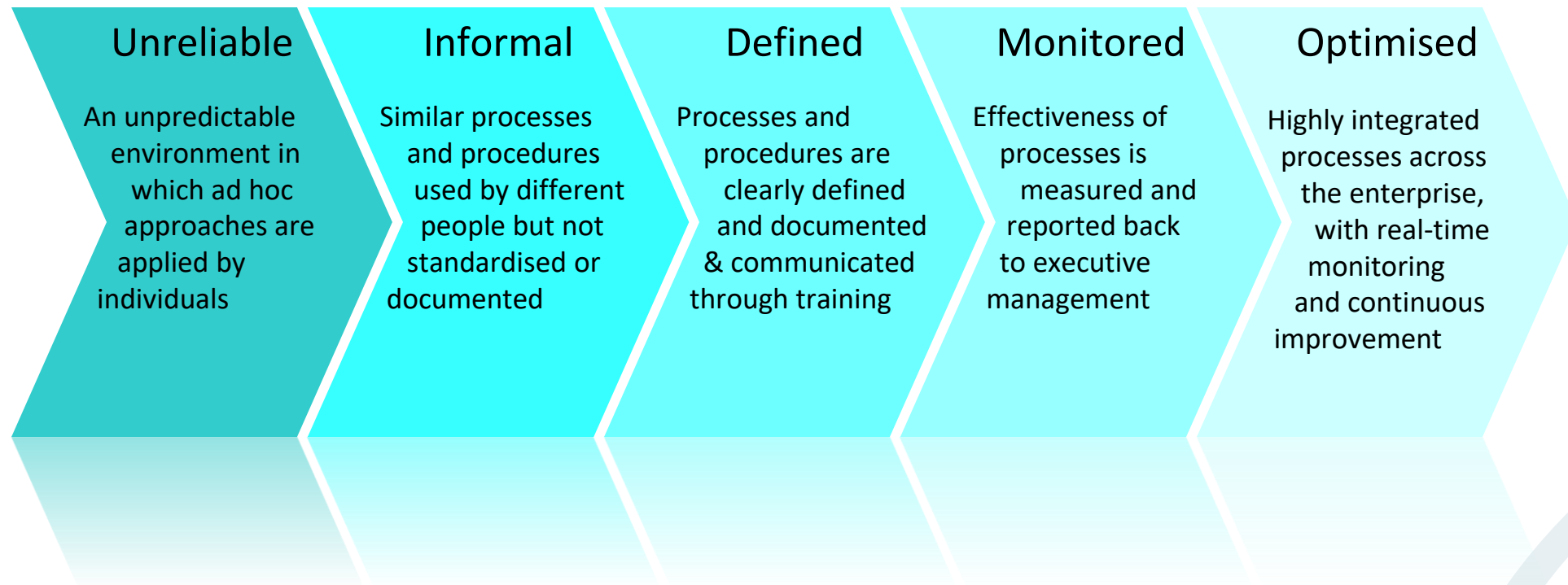
- The six SMP domains are:
 - Contextual architecture
 - Conceptual architecture
 - Logical architecture
 - Physical architecture
 - Component architecture
 - Management architecture

SABSA Maturity Profile Process Areas

SMP Process Areas and SMP Process Activities

- Each of the six SMP domains is decomposed into six SMP Process Areas
- These SMP Process Areas map onto the six cells of the row of the SABSA Matrix corresponding to the particular SMP domain
- The SMP Process Activities are then derived by overlaying the SABSA Management Matrix onto the SMP Process Areas

SMP Maturity Levels



SMP Generic Practices

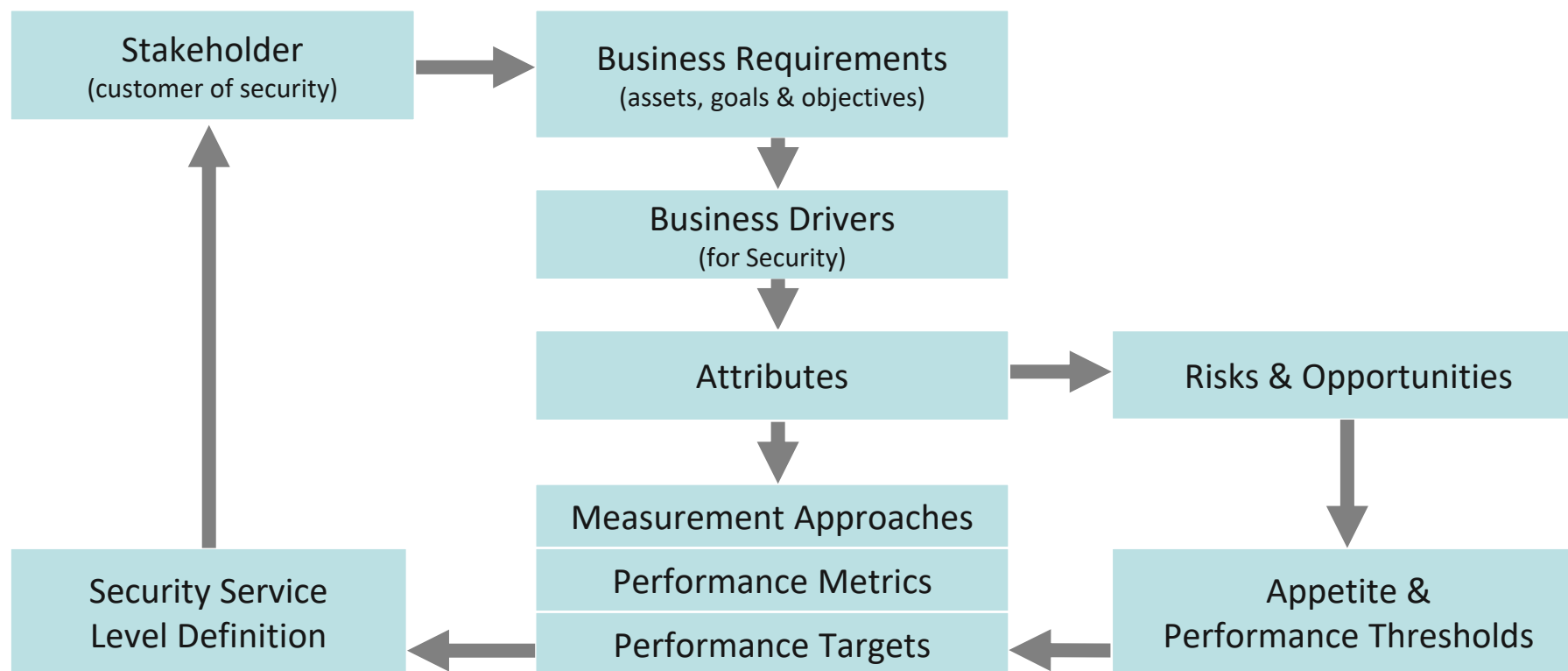
	Maturity Level	Generic Practices
1	Unreliable	An unpredictable environment in which individuals apply ad hoc approaches case-by-case.
2	Informal	Similar processes and procedures are followed by different people undertaking the same task, but There are no formal standardised procedures, no formal training or communication, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and the sustainability of consistency is doubtful.
3	Defined	Procedures have been standardised and documented and are communicated through training It is left to the individual to follow the processes; deviations are unlikely to be detected. The procedures are not sophisticated – usually the formalisation of existing practices.
4	Monitored	Adherence to defined processes and procedures is monitored and measured and reported back to executive management. This monitoring and reporting is often supported by the limited and somewhat fragmented deployment of automation tools, but on a silo basis. Action is taken where procedures appear not to be working effectively and processes are under constant improvement and provide good practice.
5	Optimised	Management processes have been refined to a high level of good practice and a comprehensive programme of continuous improvement builds on this. There is an enterprise-wide, integrated, highly automated approach to monitoring and reporting. A consistent enterprise-wide stance on compliance and risk management is maintained to maximise return on investment. The enterprise is quick to identify, assess and adapt to changes.

© The SABSA Institute C.I.C 2021

312


Performance Management Framework

Defining Business-driven Performance Targets



Architecture Needs a Holistic Approach

- Do we understand all of the requirements?
- Do we have a design philosophy?
- Do we have all of the components?
- Do these components work together?
- Do they form an integrated system?
- Does the system run smoothly?
- Are we assured that it is properly assembled?
- Is the system properly tuned?
- Do we operate the system correctly?
- Do we maintain the system?
- Do we comply with the rules?



**All aspects can
be measured –
using five
measurement
categories**

Architecture Measurement Categories

- Completeness
 - Do we have all of the components?
 - Do they form an integrated system?
- Assurance
 - Does the system run smoothly?
 - Are we assured that it is properly assembled?
 - Is the system fit-for-purpose?
- Compliance
 - Do we maintain the system?
 - Do we follow the architecture roadmap
 - Do we comply with the rules?
- Performance
 - Is the system properly tuned?
 - Do the components work together?
 - Do we operate the system correctly?
- Justification & significance
 - Does the system have business value?

Measurement Approaches

- High level statements of the approach to obtaining a measurement
- Appropriate to the business need
- In the language of the intended audience
- Culturally specific

Measurement Guidelines

- Measurement should be a repeatable process (for comparison & prediction)
- Measurement should have a clear communications role
 - Tracking performance
 - Assigning resources
- Measurement should yield quantifiable metrics (percentage, average, numbers, values, etc)

Metrics Guidelines

- Data used to calculate metrics should be readily obtainable
- Metrics may (should) be calculated independently of parties with vested interest
- The type of metric used may change in line with the maturity of the security process e.g. when you are highly compliant, consider changing from conformance measure to significance measure
- Performance metric / trend should be tested prior to going 'live'
- Expectations management is key

Types of Metric

- Soft Metrics
 - Usually qualitative
 - Subjective
 - Open to interpretation and opinion (usually of the authority setting the target or of an official compliance agent such as a regulator or auditor)
- Hard Metrics
 - Usually quantitative
 - Objective
 - Fixed, not open to opinion or interpretation

Types of Metric

- Descriptive
 - Describes the current-state of the object / attribute being measured
- Comparative
 - Describes the current-state of the object / attribute being measured in comparison with a similar object / attribute relating to a different place and/or time
- Predictive
 - Describes the current-state of the object / attribute being measured in relation to its trend in order to project and predict a future state

Conceptual Measures & Metrics Framework

Business Requirement			
Business Driver for Security			
Attribute with risk-proportional performance target	Measurement Category What achievement or value are we trying to communicate? <ul style="list-style-type: none"> - completeness - assurance - compliance - performance - justification & significance 	Measurement Approach High-level statement of approach to obtaining the measurement <ul style="list-style-type: none"> - analyse - survey - monitor - time period - etc. 	Metric <ul style="list-style-type: none"> - hard - soft -descriptive -comparative -predictive Format of the metric <ul style="list-style-type: none"> - value - percentage - volume - etc.

Monitoring & Reporting Service Performance

- The conceptual model on the previous slide can be applied to any scenario
- The performance management aspects of lower layers (specific services, mechanisms, components & management activities) we will look at in module F2

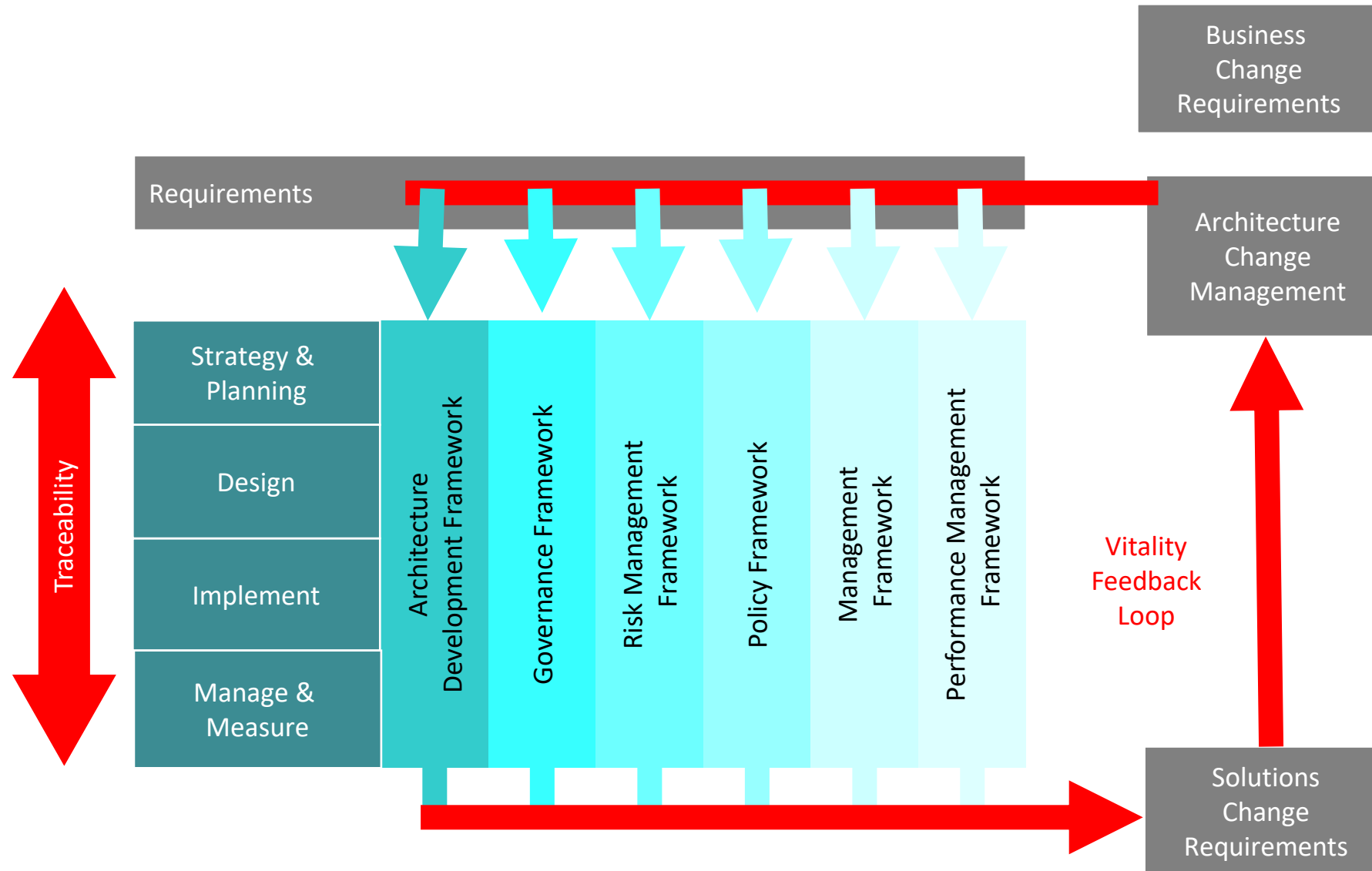
Through-life Vitality Framework

- We defined an Architecture Framework as:
 - A consistent set of principles, policies, capabilities and standards that sets the direction and vision for the development and operation of the organisation's business information systems so as to ensure alignment with and support for the business needs
- We also stated a SABSA Guiding Principle to be an enabler of change:
 - Provide the roadmap for joining together all of your requirements, whatever they might be, or become
- Architecture Vitality is the Architecture's capacity to live, breathe and adapt its principles, policies, capabilities and standards such that it is viable in supporting dynamic business needs

Traceability in SABSA Frameworks

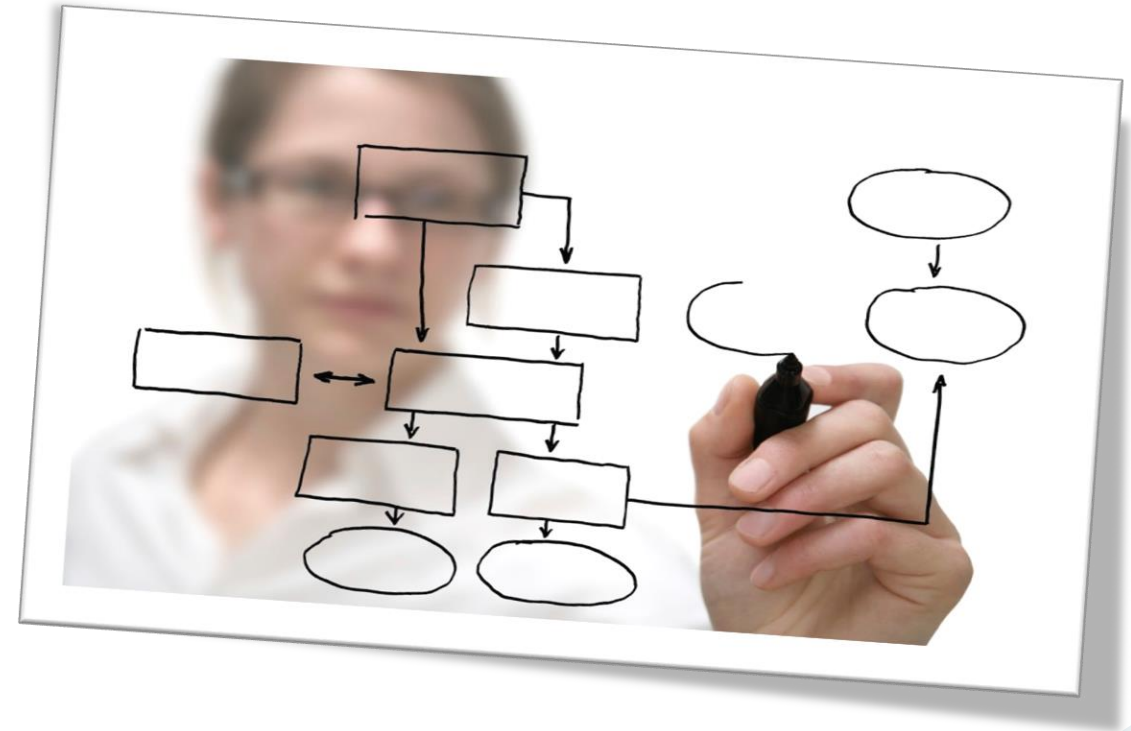
- Each of the major SABSA Frameworks incorporates traceability from contextual requirements through solution design, implementation & management
 - Architecture Development Framework
 - Governance Framework
 - Risk Management Framework
 - Policy Framework
 - Management Framework
 - Performance Management Framework
- The Manage & Measure Phase incorporates Feedback Loops for each in order to detect requirements to change the solutions
- Vitality is achieved by adding to these feedback loops:
 - Detection mechanism for brand new business requirements
 - Architectural change management

SABSA Vitality Framework



Workshop F1-5

Time & Performance Management



Sample Questions

Competency Domain 6

Working as individuals, answer the following two questions.

Time limit is 2 minutes 30 seconds.

As a group we will then discuss the questions.



Competency Domain 6

- A break is shown between phases of the SABSA Development Process in order to gain consensus agreement, buy-in and sign-off of stakeholder management to the solution concepts. Between which SABSA Development Process phases is the break positioned?
 - A. After Strategy & Planning Phase and before Design Phase
 - B. After Design Phase and before Implement Phase
 - C. After Implement Phase and before Manage & Measure Phase
 - D. After Manage & Measure Phase

Competency Domain 6

- Which ONE of the following statements about the SABSA Performance Management Framework is FALSE?
 - A. Security metrics should be calculated independently of parties with vested interest
 - B. All security metrics should be 'hard', objective and not open to interpretation and opinion
 - C. Security measures should be repeatable for comparison and prediction
 - D. The type of security metric used may change in line with the maturity of the security process