Aligning System Engineering and Cyber Security Architecture using the SABSA Framework

Bruce Large, B Large

SYSTEMS ENGINEERING
TEST & EVALUATION
SETE
2024

22 - 25 SEPTEMBER 2024
Melbourne, Australia

ENGINEERS AUSTRALIA | Systems Engineering Society of Australia
INCOSE
ITEA
Simulation Australasia

/whois @beLarge

A cyber security architecture enthusiast, infrastructure tourist and "cyber hype guy"

- Principal Cyber Security Architect at B Large
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for over 15 years
- CPEng (ITEE) and RPEQ (IT&E)
- Chair of Information, Telecommunications and Electronics Engineering (ITEE) Queensland Branch of Engineers Australia
- President Queensland Professional Engineers Sub-Division of Professionals Engineers & Proud member of Professionals Australia (PA)
- Bach Eng (Telecomms) QUT First Class Honours and Master Business (Applied Finance) with Distinction QUT

SABSA FOUNDATION LEVEL SCF

GIAC INDUSTRIAL CYBER SECURITY PROFESSIONAL GICSP

GIAC RESPONSE AND INDUSTRIAL DEFENSE GRID

GIAC SECURITY OPERATIONS MANAGER GSOM

ISA/IEC 62443 CYBERSECURITY EXPERT ISA

Agenda

1. An Introduction to ESA and the SABSA Framework
2. Aligning SABSA with System Engineering Processes
3. Worked Example of OT Cloud SCADA
4. Further Resources & Summary
5. Q&A

INTRODUCTION OF ENTERPRISE SECURITY ARCHITECTURE AND THE SABSA FRAMEWORK

TYPES OF ARCHITECTURE

Term	Definition
cyber security architecture	How cybersecurity practices and controls are structured and implemented to maintain the confidentiality, integrity, and availability of the organization’s assets and services.
enterprise architecture	The design and description of an enterprise’s entire set of IT and OT assets: how they are configured, how they are integrated, how they interface to the external environment at the enterprise’s boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise’s overall security posture.

Ref – Cyber Security Capability Maturity Model (C2M2) - https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

ENTERPRISE SECURITY ARCHITECTURE & SECURITY SOLUTION ARCHITECTURE

Enterprise Security Architecture

- Defines the enterprise wide security artefacts such as:
  - Architectural Principles
  - Attributes Modelling (SABSA)
  - Domain Model
  - Trust Models
  - Pattern Repositories
- Run the Architectural Review Board (ARB)
- Should work with the business to define security strategy and justification

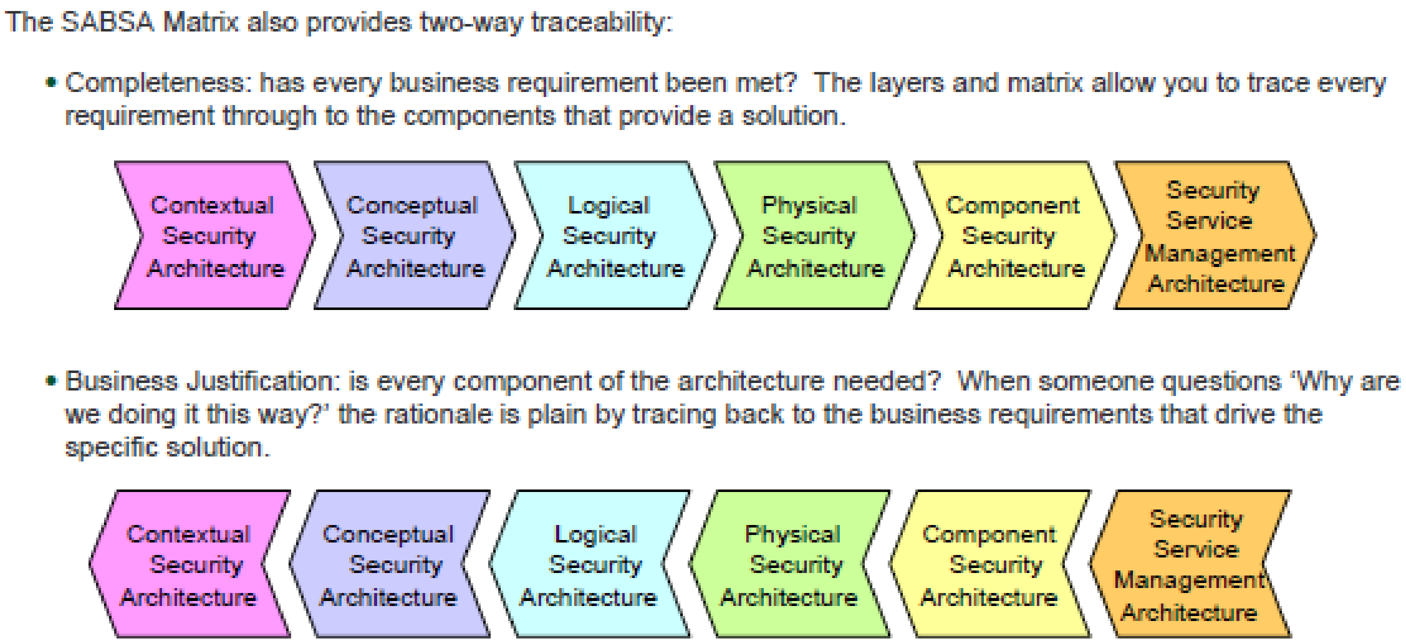
Solution Architecture (Security)

- Focuses on producing solution designs that address cyber security requirements as per the enterprise methodology
- A key pivot role between the whole of enterprise and delivering projects
- Are most likely aligned to projects

Some good material in NIST NICE (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center)
Worker Roles Enterprise Architect (SP-ARC-001) and Security Architect (SP-ARC-002)

OVERVIEW OF SABSA

- SABSA has its origins as the Enterprise Security Architecture for the SWIFT IP Payments Network
- Business Aligned, Top Down and Deliberate, not just *best practice*
- Focus on *Attributes* which are security goals/objectives/requirements
- Two Way Traceability



The SABSA Matrix also provides two-way traceability:

- Completeness: has every business requirement been met? The layers and matrix allow you to trace every requirement through to the components that provide a solution.

Contextual Security Architecture → Conceptual Security Architecture → Logical Security Architecture → Physical Security Architecture → Component Security Architecture → Security Service Management Architecture

- Business Justification: is every component of the architecture needed? When someone questions 'Why are we doing it this way?' the rationale is plain by tracing back to the business requirements that drive the specific solution.

Contextual Security Architecture ← Conceptual Security Architecture ← Logical Security Architecture ← Physical Security Architecture ← Component Security Architecture ← Security Service Management Architecture

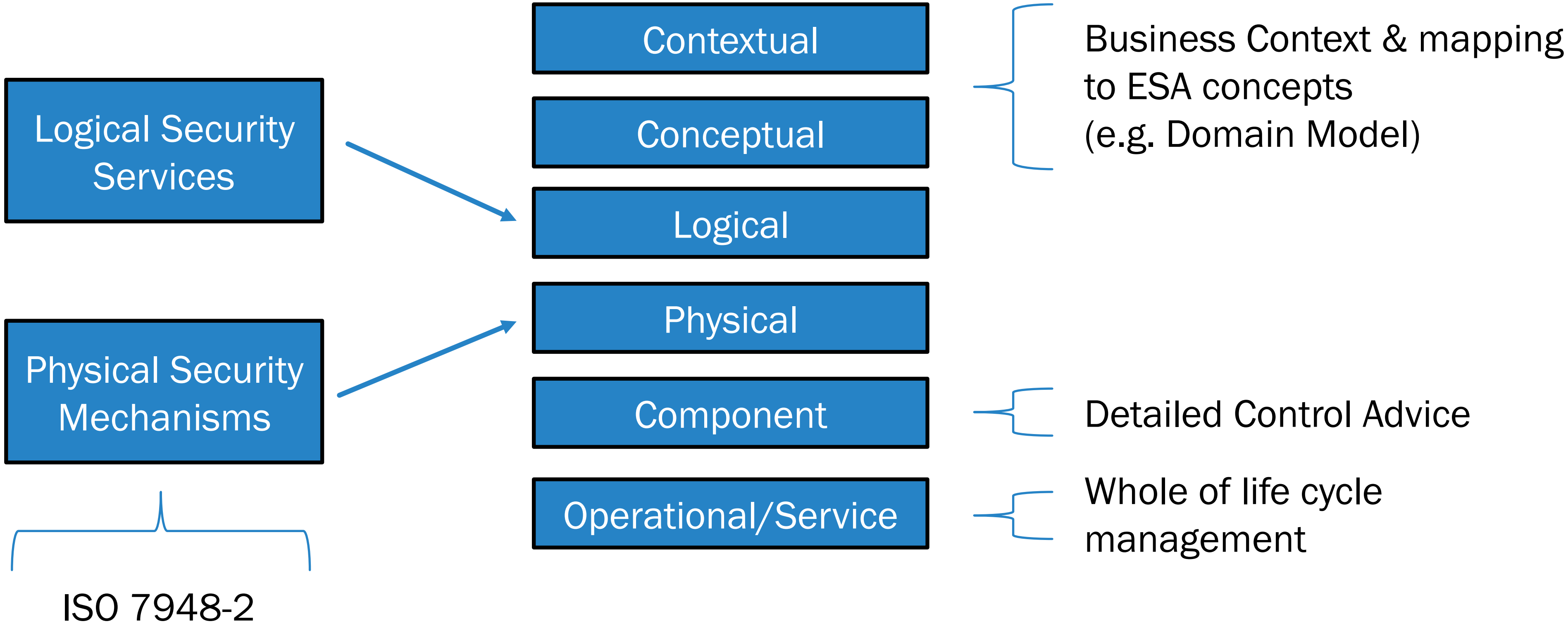
Ref – SABSA White Paper (W100)

SABSA MATRIX

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)		PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Process	The Business View	Business Governance	Business Geography	Business Time Dependence
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Project Assurance	The Architect's View	Roles & Responsibilities	Domain Framework	Time Management Framework
LOGICAL ARCHITECURE	Information Assets	Risk Management Policies	Process Maps & Services	The Designer's View	Entity & Trust Framework	Domain Maps	Calendar & Timetable
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	The Builder's View	Human Interface	ICT Infrastructure	Process Schedule
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	The Tradeperson's View	Personnel Mgmt, Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
SERVICE MGMT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	The Service Manager's View	Personnel Management	Management of Environment	Time & Performance Management

https://sabsa.org/white-paper-requests/

WHY 6 LAYERS?



Logical Security Services

Physical Security Mechanisms

ISO 7948-2

Contextual

Conceptual

Logical

Physical

Component

Operational/Service

Business Context & mapping to ESA concepts (e.g. Domain Model)

Detailed Control Advice

Whole of life cycle management

SABSA MATRIX (CONT.)

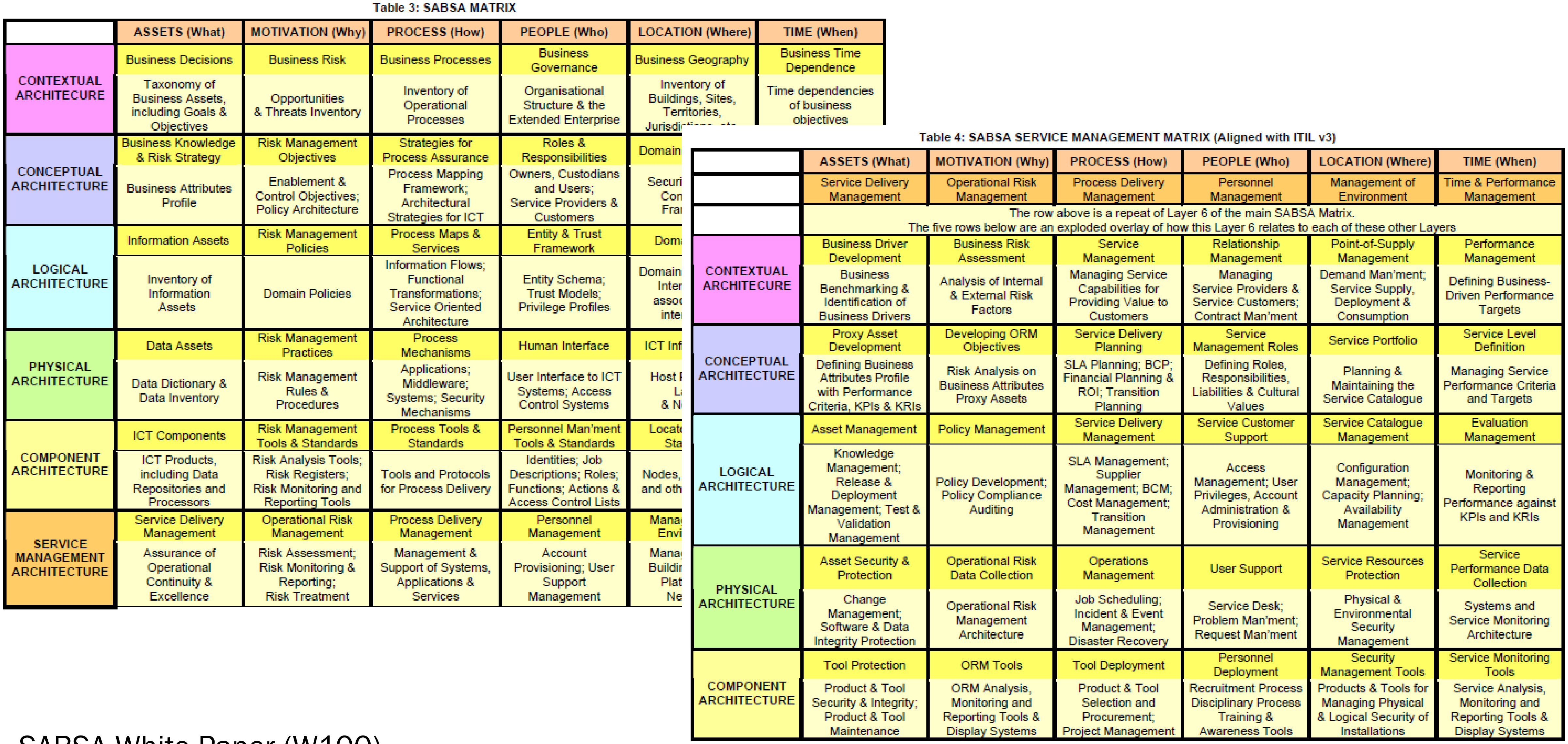


Table 3: SABSA MATRIX

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdi	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain	
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Securi Con Fra	
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Dom	
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Inter assoc inte	
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Inf	
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host L & N	
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locat Sta	
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, and oth	
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Mana Envi	
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Mana Buildir Plat Ne	

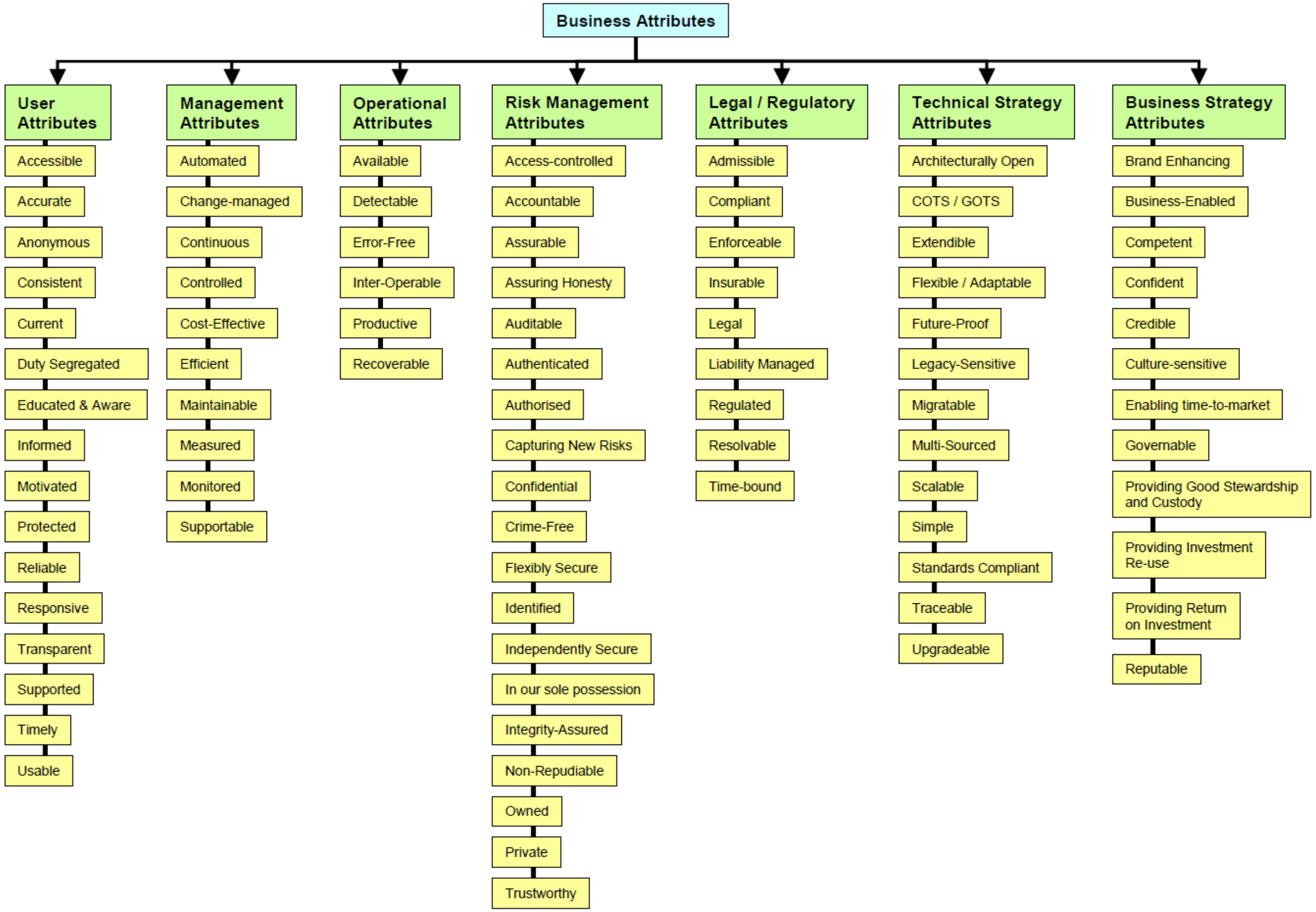
Table 4: SABSA SERVICE MANAGEMENT MATRIX (Aligned with ITIL v3)

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	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 ARCHITECURE	Business Driver Development	Business Risk Assessment	Service Management	Relationship Management	Point-of-Supply Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Service Capabilities for Providing Value to Customers	Managing Service Providers & Service Customers; Contract Man'ment	Demand Man'ment; Service Supply, Deployment & Consumption	Defining Business-Driven Performance Targets
CONCEPTUAL ARCHITECTURE	Proxy Asset Development	Developing ORM Objectives	Service Delivery Planning	Service Management Roles	Service Portfolio	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Risk Analysis on Business Attributes Proxy Assets	SLA Planning; BCP; Financial Planning & ROI; Transition Planning	Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Service Catalogue	Managing Service Performance Criteria and Targets
LOGICAL ARCHITECTURE	Asset Management	Policy Management	Service Delivery Management	Service Customer Support	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management; Test & Validation Management	Policy Development; Policy Compliance Auditing	SLA Management; Supplier Management; BCM; Cost Management; Transition Management	Access Management; User Privileges, Account Administration & Provisioning	Configuration Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
PHYSICAL ARCHITECTURE	Asset Security & Protection	Operational Risk Data Collection	Operations Management	User Support	Service Resources Protection	Service Performance Data Collection
	Change Management; Software & Data Integrity Protection	Operational Risk Management Architecture	Job Scheduling; Incident & Event Management; Disaster Recovery	Service Desk; Problem Man'ment; Request Man'ment	Physical & Environmental Security Management	Systems and Service Monitoring Architecture
COMPONENT ARCHITECTURE	Tool Protection	ORM Tools	Tool Deployment	Personnel Deployment	Security Management Tools	Service Monitoring Tools
	Product & Tool Security & Integrity; Product & Tool Maintenance	ORM Analysis, Monitoring and Reporting Tools & Display Systems	Product & Tool Selection and Procurement; Project Management	Recruitment Process Disciplinary Process Training & Awareness Tools	Products & Tools for Managing Physical & Logical Security of Installations	Service Analysis, Monitoring and Reporting Tools & Display Systems

Ref – SABSA White Paper (W100)

ATTRIBUTES

- SABSA defines an attribute as “*A normalised, measurable, in-context definition of what is important*”
- There were originally 85 defined and organised into 7 categories
- Architects are encouraged to create new ones for their projects, and there is a SABSA Institute working group



Business Attributes

User Attributes
- Accessible
- Accurate
- Anonymous
- Consistent
- Current
- Duty Segregated
- Educated & Aware
- Informed
- Motivated
- Protected
- Reliable
- Responsive
- Transparent
- Supported
- Timely
- Usable

Management Attributes
- Automated
- Change-managed
- Continuous
- Controlled
- Cost-Effective
- Efficient
- Maintainable
- Measured
- Monitored
- Supportable

Operational Attributes
- Available
- Detectable
- Error-Free
- Inter-Operable
- Productive
- Recoverable

Risk Management Attributes
- Access-controlled
- Accountable
- Assurable
- Assuring Honesty
- Auditable
- Authenticated
- Authorised
- Capturing New Risks
- Confidential
- Crime-Free
- Flexibly Secure
- Identified
- Independently Secure
- In our sole possession
- Integrity-Assured
- Non-Repudiable
- Owned
- Private
- Trustworthy

Legal / Regulatory Attributes
- Admissible
- Compliant
- Enforceable
- Insurable
- Legal
- Liability Managed
- Regulated
- Resolvable
- Time-bound

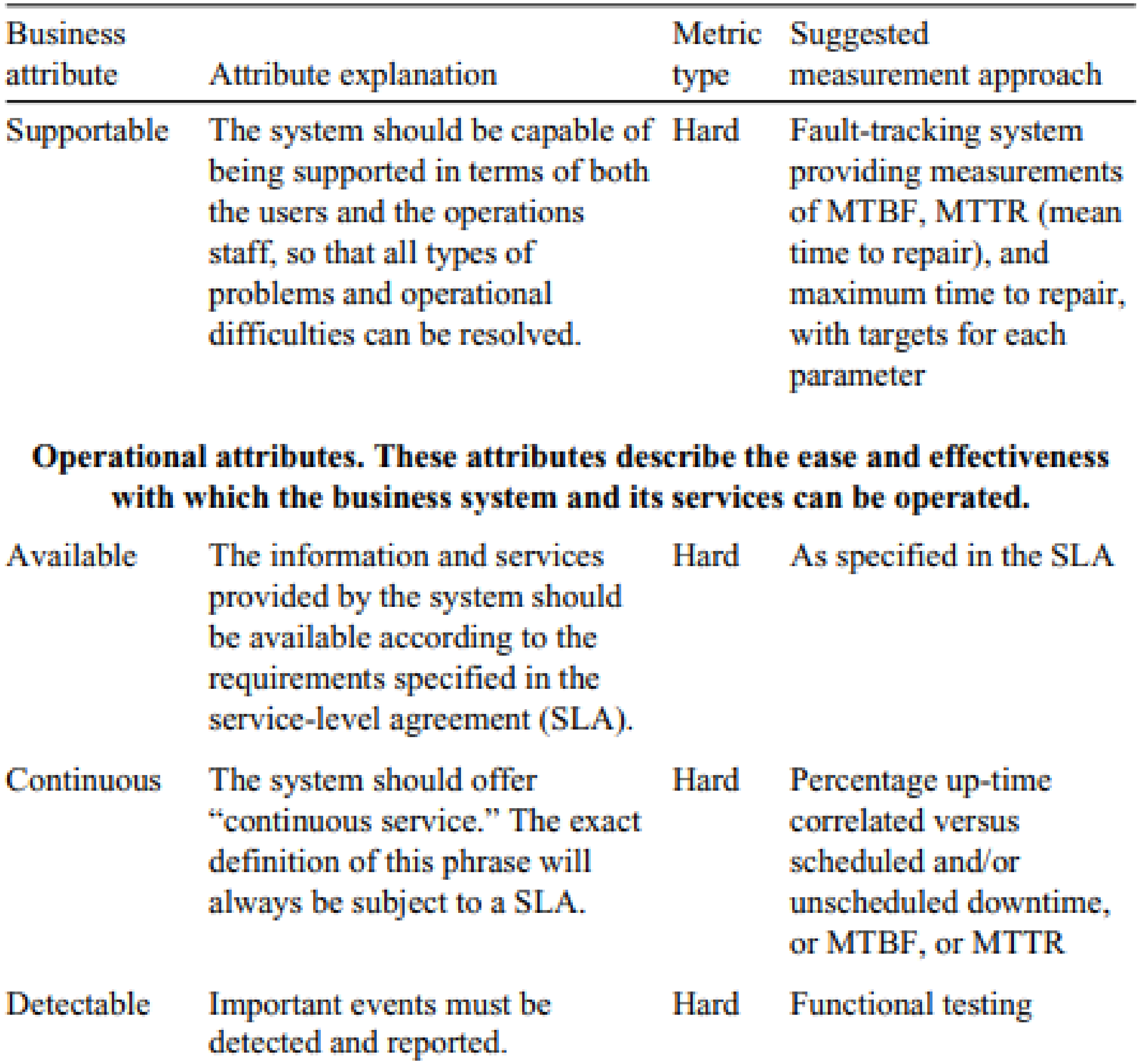
Technical Strategy Attributes
- Architecturally Open
- COTS / GOTS
- Extendible
- Flexible / Adaptable
- Future-Proof
- Legacy-Sensitive
- Migratable
- Multi-Sourced
- Scalable
- Simple
- Standards Compliant
- Traceable
- Upgradeable

Business Strategy Attributes
- Brand Enhancing
- Business-Enabled
- Competent
- Confident
- Credible
- Culture-sensitive
- Enabling time-to-market
- Governable
- Providing Good Stewardship and Custody
- Providing Investment Re-use
- Providing Return on Investment
- Reputable

Figure 4: The SABSA Taxonomy of ICT Business Attributes

Ref – SABSA White Paper (W100)

EXAMPLE ATTRIBUTES

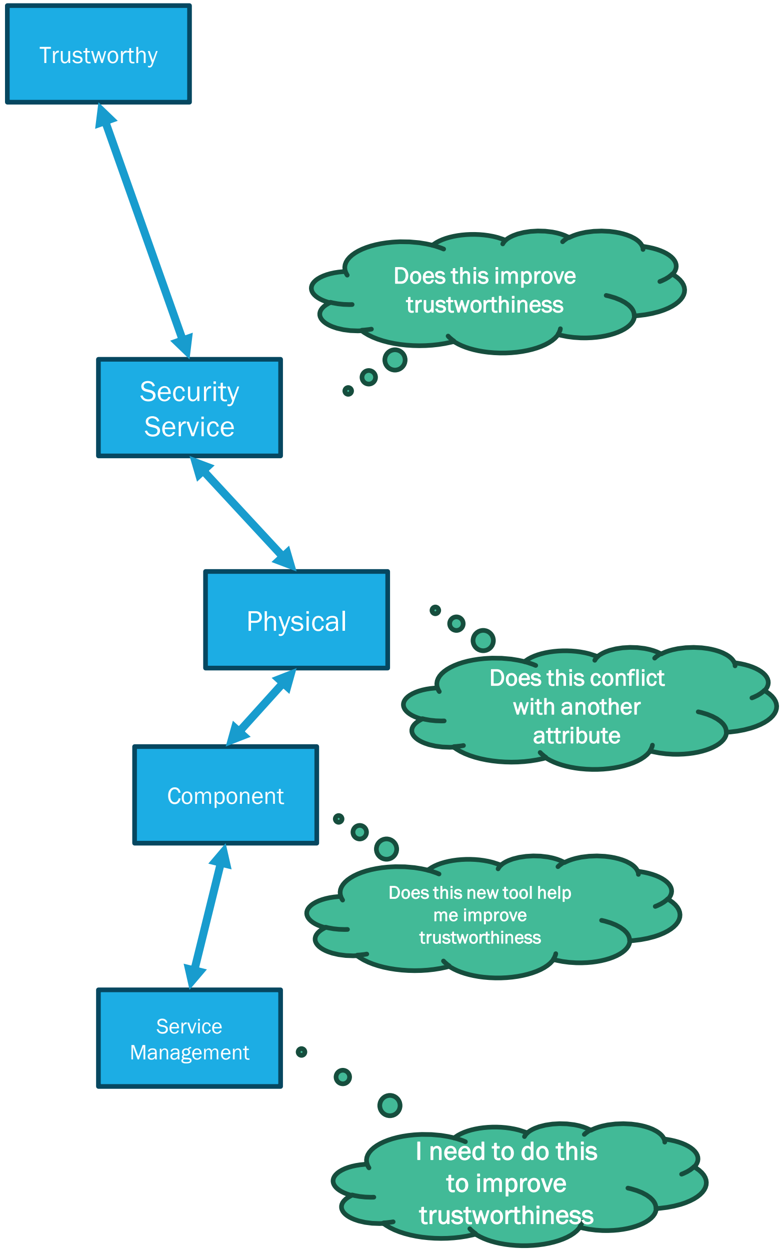


Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Supportable	The system should be capable of being supported in terms of both the users and the operations staff, so that all types of problems and operational difficulties can be resolved.	Hard	Fault-tracking system providing measurements of MTBF, MTTR (mean time to repair), and maximum time to repair, with targets for each parameter
Operational attributes. These attributes describe the ease and effectiveness with which the business system and its services can be operated.			
Available	The information and services provided by the system should be available according to the requirements specified in the service-level agreement (SLA).	Hard	As specified in the SLA
Continuous	The system should offer "continuous service." The exact definition of this phrase will always be subject to a SLA.	Hard	Percentage up-time correlated versus scheduled and/or unscheduled downtime, or MTBF, or MTTR
Detectable	Important events must be detected and reported.	Hard	Functional testing

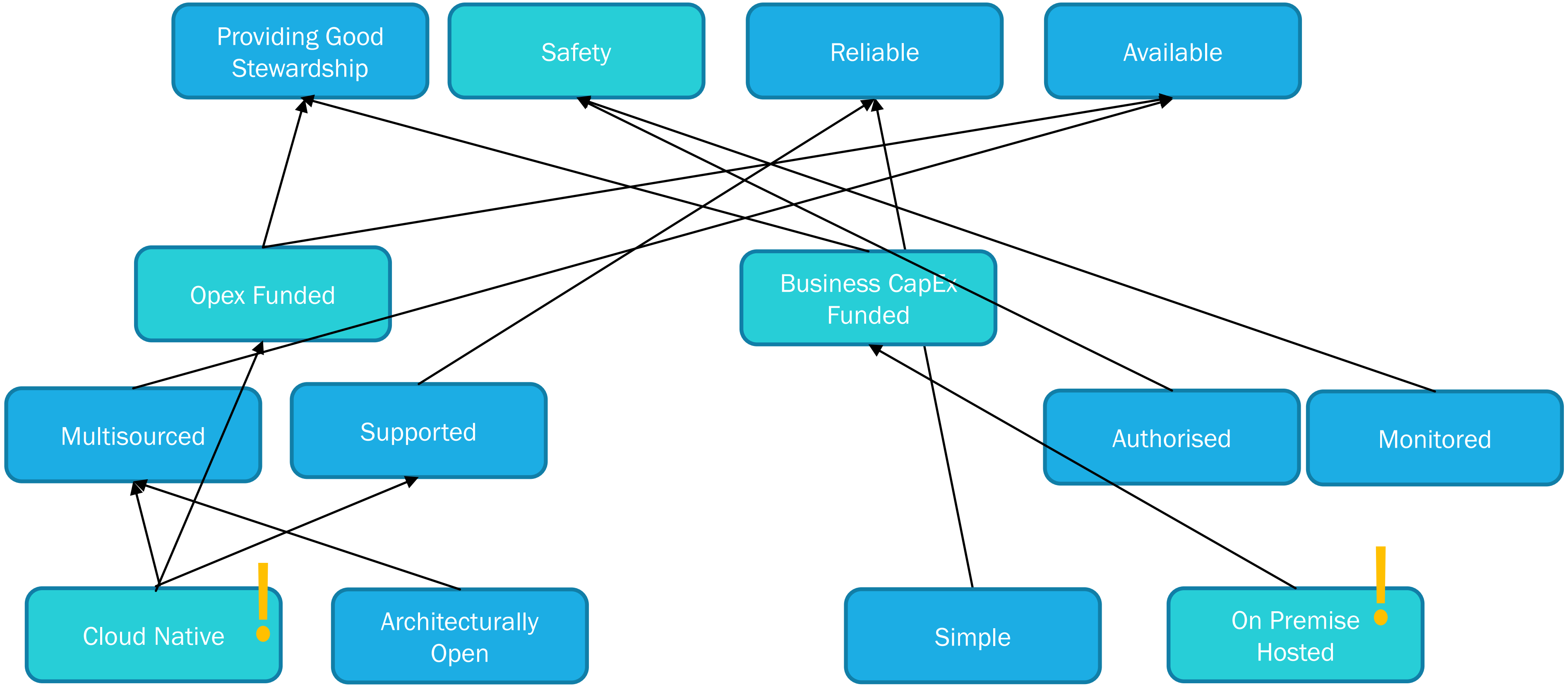
Ref - https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470476017.app1

ATTRIBUTES (CONT.)

- They are however a **very smart abstraction** of cyber security requirements management
- It provides a simple label for a complex interaction of security requirements to achieve a business goal
- It can be used to highlight the impact of an emerging business driver on the enterprise's ability to exploit an opportunity or manage a risk
- It uses the language of the stakeholder to make it relevant to the audience
- It can cascade, interact and even disrupt other requirements


Trustworthy
Does this improve trustworthiness
Security Service
Physical
Does this conflict with another attribute
Component
Does this new tool help me improve trustworthiness
Service Management
I need to do this to improve trustworthiness

MULTI TIER ATTRIBUTES



Providing Good Stewardship

Safety

Reliable

Available

Opex Funded

Business CapEx Funded

Multisourced

Supported

Authorised

Monitored

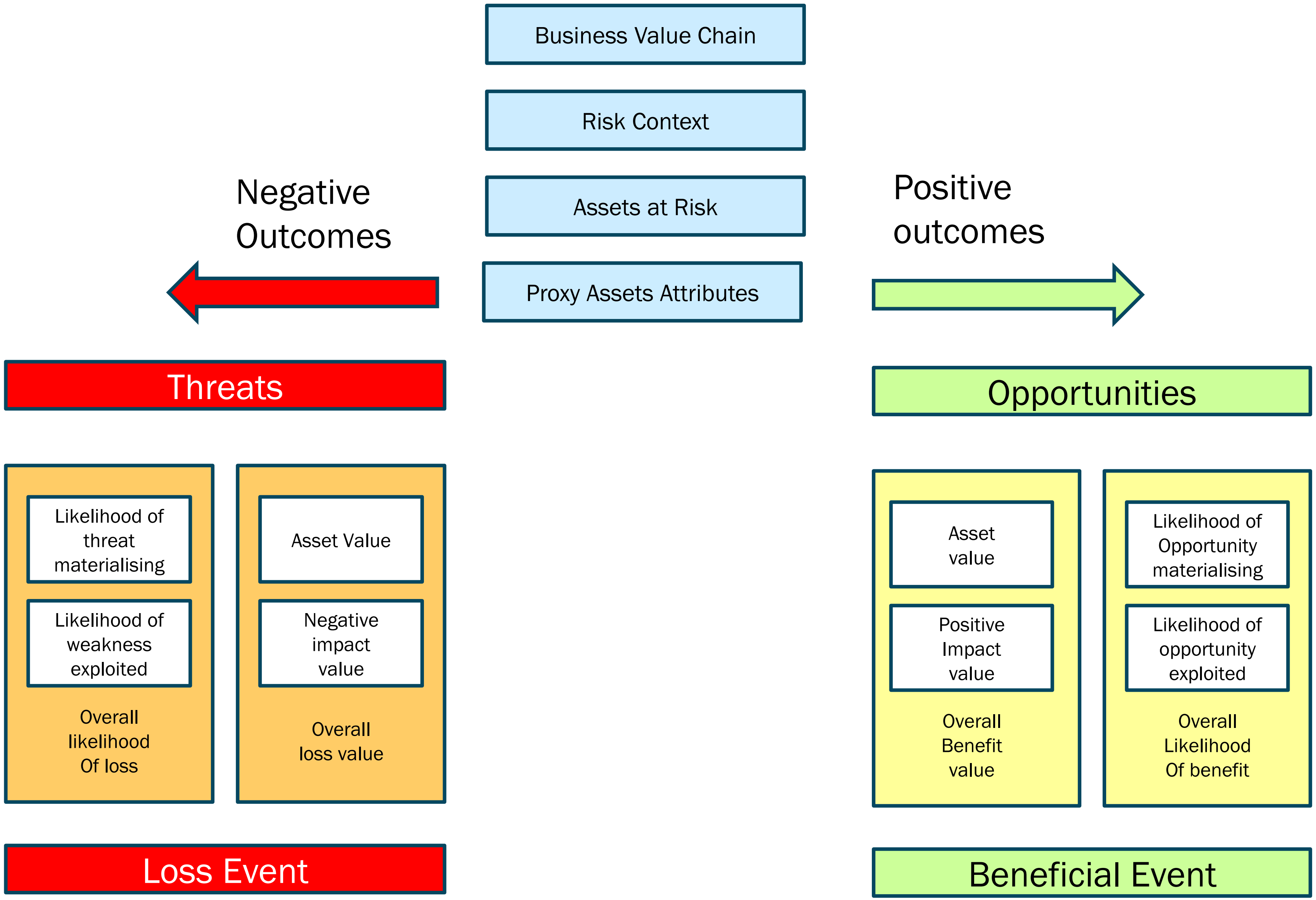
Cloud Native

Architecturally Open

Simple

On Premise Hosted

BALANCED RISK MANAGEMENT



Business Value Chain

Risk Context

Assets at Risk

Proxy Assets Attributes

Negative Outcomes

Positive outcomes

Threats

Likelihood of threat materialising

Likelihood of weakness exploited

Overall likelihood Of loss

Asset Value

Negative impact value

Overall loss value

Loss Event

Opportunities

Asset value

Positive Impact value

Overall Benefit value

Likelihood of Opportunity materialising

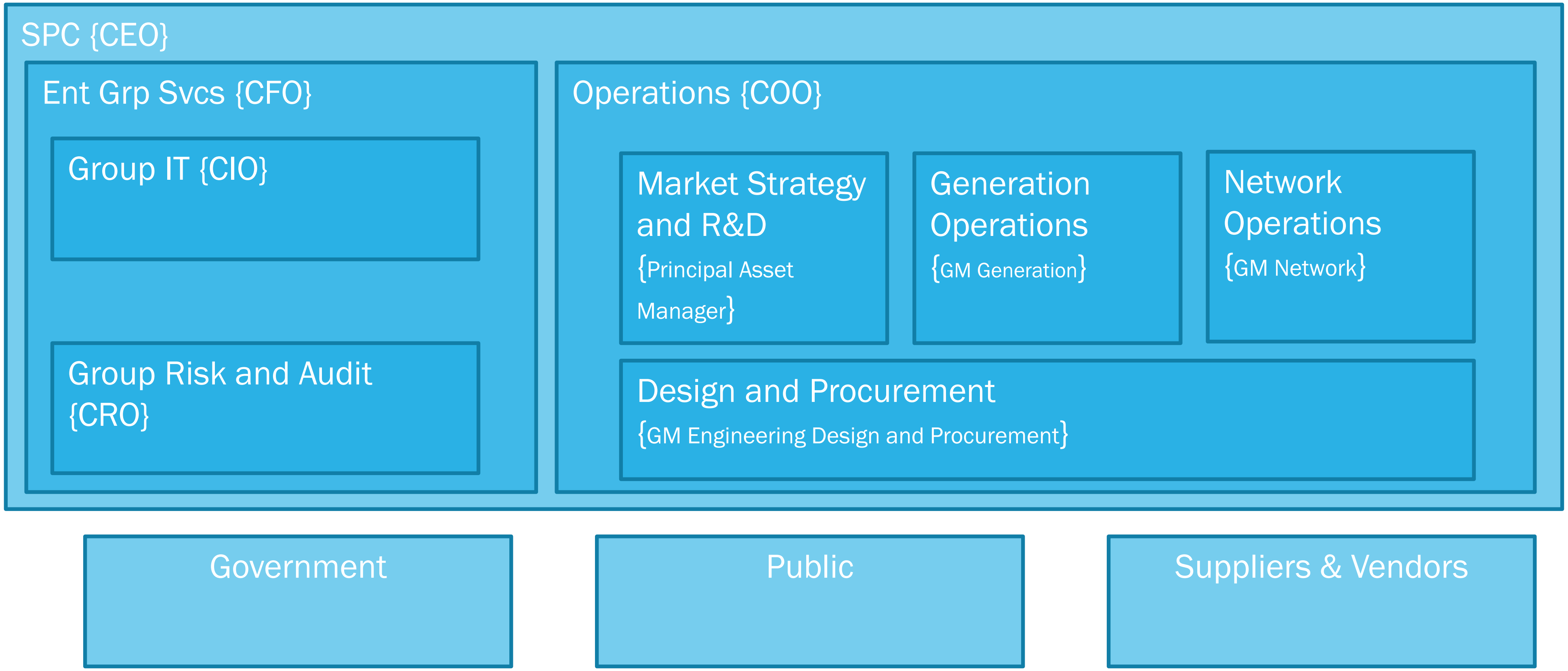
Likelihood of opportunity exploited

Overall Likelihood Of benefit

Beneficial Event

DOMAIN MODELS

- A domain is defined as *“A set of elements, area of knowledge or activity, subject to a common (security) dominion of a single accountable authority”*
- Can have Sub Domains, Peer Domains, External Domains



SPC {CEO}

Ent Grp Svcs {CFO}

Group IT {CIO}

Group Risk and Audit {CRO}

Operations {COO}

Market Strategy and R&D {Principal Asset Manager}

Generation Operations {GM Generation}

Network Operations {GM Network}

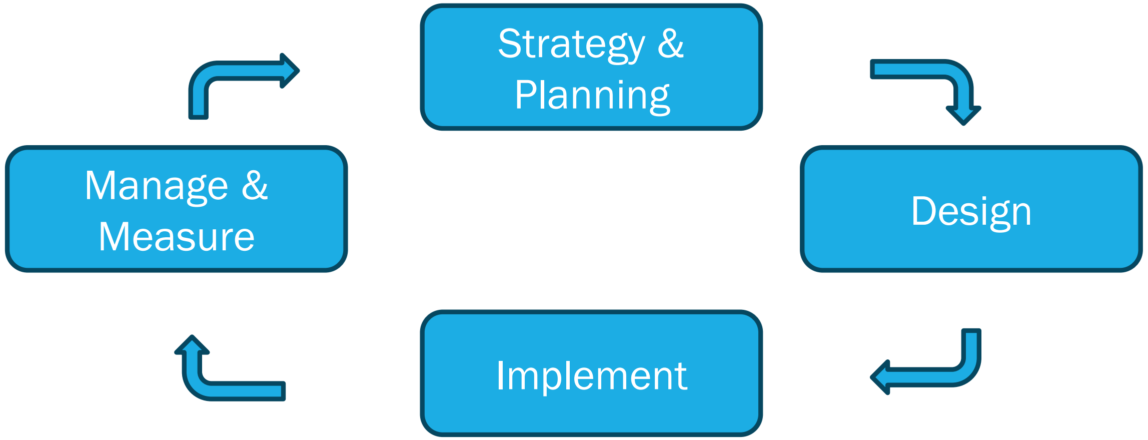
Design and Procurement {GM Engineering Design and Procurement}

Government

Public

Suppliers & Vendors

SABSA LIFE CYCLE



Strategy & Planning

Design

Implement

Manage & Measure

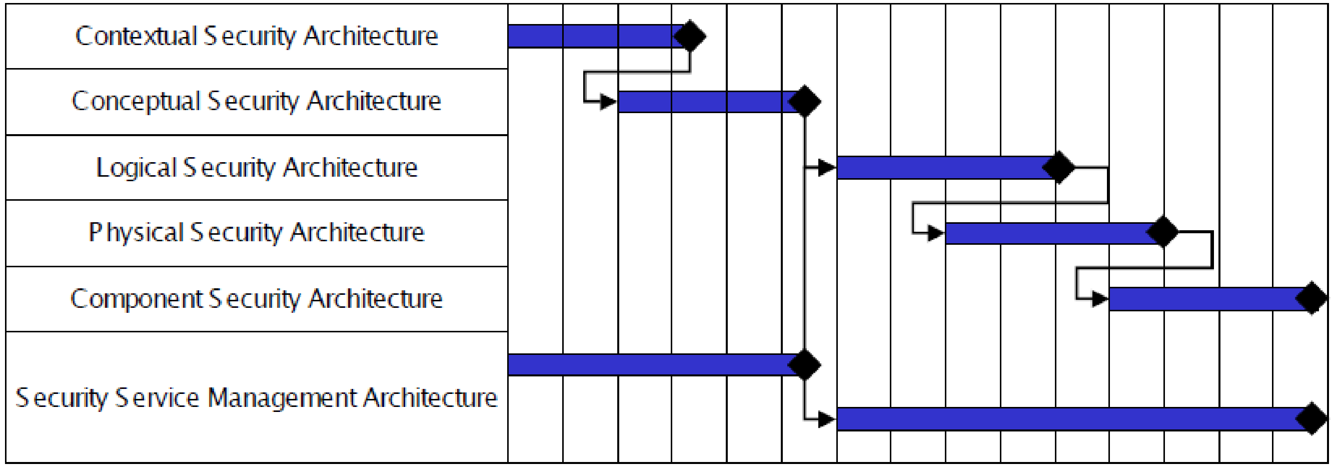


Figure 2: The SABSA Development Process

Ref – SABSA White Paper (W100)

BONUS SLIDE –SABSA & TOGAF INTEGRATION

- TSI & Open Group White Paper that describes how to integrate SABASA and TOGAF

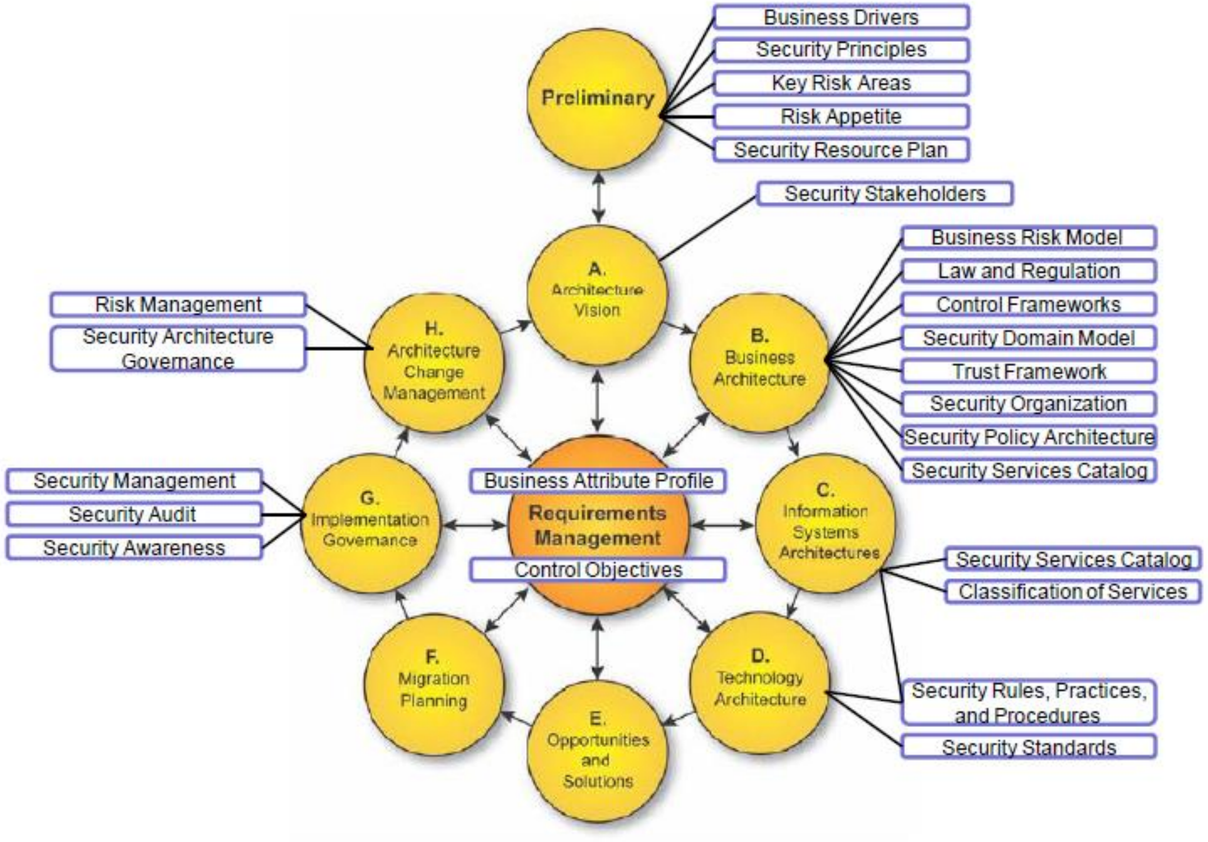


Figure 16: Overview of Security-Related Artifacts in the TOGAF ADM

Ref - TSI-W117-SABSA-TOGAF-Integration - https://sabsa.org/sabsa-togaf-integration-white-paper-download-request/

ALIGNING SABSA TO SYSTEM ENGINEERING

ALIGNING SABSA ATTRIBUTES WITH REQUIREMENTS ENGINEERING

- A critical interface activity between System Engineering and Security Architects is Requirements Management
- Use existing SE artifacts such as:
  - Business Needs and Requirements (BNR)
  - Stakeholder Needs and Requirements (SNR)
  - System Requirements Specification (SySR)
- I suggest using SABSA Attributes as a “category” group for Requirements in Requirements Management tool and use as a Traceability Tool

USING DOMAIN MODELS TO MANAGE RISK TREATMENT

- The domain model clearly articulates the Policy Authority
- The domain model can also be used to understand risk dependencies and risk interactions for sub domains
    - Treating a risk in one domain may adversely impact risks in other domains for example a trade off financial risks may incur physical safety risks
- SE Context Diagrams are a useful reference for Domain Modelling

USING LOGICAL LAYER AS THE DEMARCATION OF SE AND CYBER SECURITY

- The Contextual and Conceptual Layers demonstrate the *what and intent*
- The logical and below is the *how*
- Similar to Functional and Physical demarcation in System Engineering

WORKED EXAMPLE

CLOUD SCADA SYSTEM

SCENARIO BACKGROUND

- The project is to build a Cloud hosted SCADA platform for a small water utility (WaterCo)
- The utility currently does not have a SCADA system but relies on manual operation of dispersed assets
- NCSC Cloud SCADA guidance (https://www.ncsc.gov.uk/collection/operational-technology/cloud-hosted-scada)

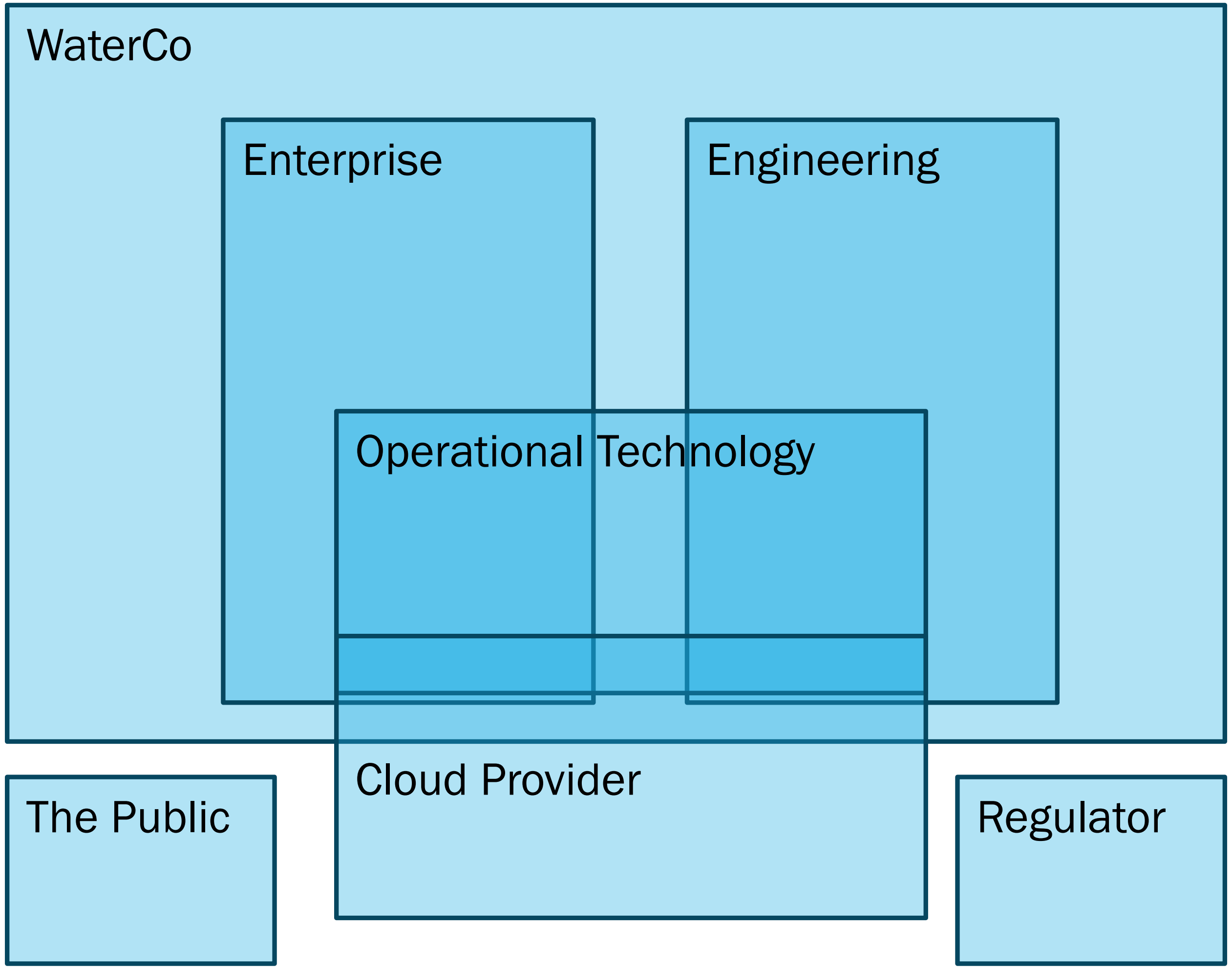
SCENARIO APPROACH

- ✓ Definite Attributes Hierarchy
- ✓ Understand Domain Model
- ✓ Identify and Manage Cyber Security Risks

ATTRIBUTE HIERARCHY

- Example Attributes –
    - Reliable
    - Supportable
    - Cost-Effective
    - Legacy-Sensitive
- New Attributes
    - Sovereign
    - Safety

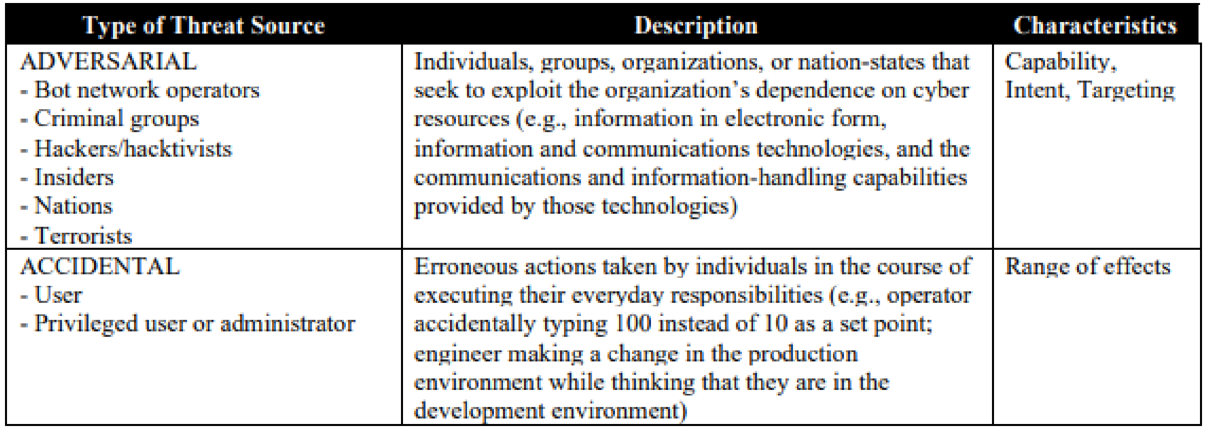
EXAMPLE DOMAIN MODEL



DEFINE RISK SCENARIOS

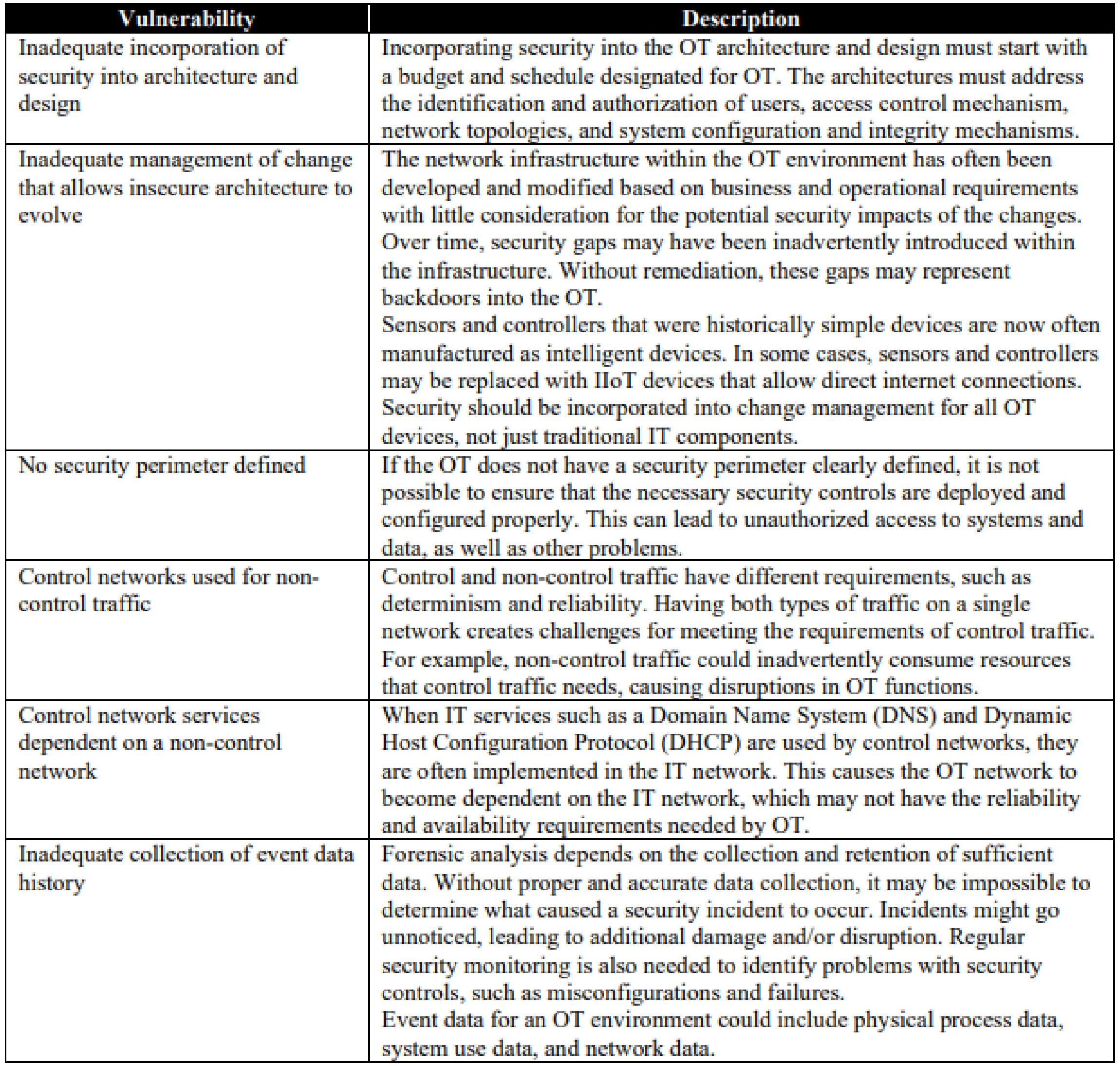
- Risks that Impact Integrity of Control
- Risks that impact availability of control
- Risks of unauthorised access to systems
- Use the attributes profile to prioritise
- NIST 800-82 R3 Appendix C is an awesome pick list of threats and vulnerabilities

Table 13. Threats to OT



Type of Threat Source	Description	Characteristics
ADVERSARIAL - Bot network operators - Criminal groups - Hackers/hacktivists - Insiders - Nations - Terrorists	Individuals, groups, organizations, or nation-states that seek to exploit the organization's dependence on cyber resources (e.g., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies)	Capability, Intent, Targeting
ACCIDENTAL - User - Privileged user or administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities (e.g., operator accidentally typing 100 instead of 10 as a set point; engineer making a change in the production environment while thinking that they are in the development environment)	Range of effects

Table 15. Architecture and design vulnerabilities and predisposing conditions



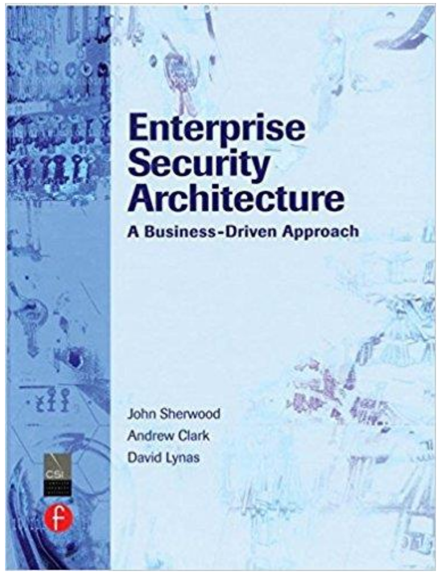
Vulnerability	Description
Inadequate incorporation of security into architecture and design	Incorporating security into the OT architecture and design must start with a budget and schedule designated for OT. The architectures must address the identification and authorization of users, access control mechanism, network topologies, and system configuration and integrity mechanisms.
Inadequate management of change that allows insecure architecture to evolve	The network infrastructure within the OT environment has often been developed and modified based on business and operational requirements with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within the infrastructure. Without remediation, these gaps may represent backdoors into the OT. Sensors and controllers that were historically simple devices are now often manufactured as intelligent devices. In some cases, sensors and controllers may be replaced with IIoT devices that allow direct internet connections. Security should be incorporated into change management for all OT devices, not just traditional IT components.
No security perimeter defined	If the OT does not have a security perimeter clearly defined, it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data, as well as other problems.
Control networks used for non-control traffic	Control and non-control traffic have different requirements, such as determinism and reliability. Having both types of traffic on a single network creates challenges for meeting the requirements of control traffic. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in OT functions.
Control network services dependent on a non-control network	When IT services such as a Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) are used by control networks, they are often implemented in the IT network. This causes the OT network to become dependent on the IT network, which may not have the reliability and availability requirements needed by OT.
Inadequate collection of event data history	Forensic analysis depends on the collection and retention of sufficient data. Without proper and accurate data collection, it may be impossible to determine what caused a security incident to occur. Incidents might go unnoticed, leading to additional damage and/or disruption. Regular security monitoring is also needed to identify problems with security controls, such as misconfigurations and failures. Event data for an OT environment could include physical process data, system use data, and network data.

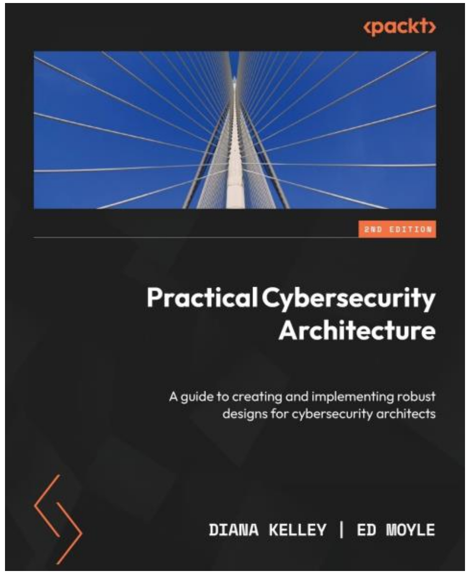
Ref - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

FURTHER RESOURCES & SUMMARY

FURTHER RESOURCES

- SABSA White Paper (W100)
- Enterprise Security Architecture
  A Business- Driven Approach
- Practical Cyber Security Architecture
- Join The SABSA Institute
  - Webinar – SABSA Architecture in Mission Critical System Engineering Projects – Alex Parkinson
- Join SABSA World Australia




‹packt›
2ND EDITION
Practical Cybersecurity Architecture
A guide to creating and implementing robust designs for cybersecurity architects
DIANA KELLEY | ED MOYLE

SUMMARY

- Understand the difference between Enterprise Security Architecture (ESA) and Security Solution Architecture
- Understand the key features of SABSA
  - The SABSA Matrix
  - SABSA Attributes
  - Domain Modelling
- Understand the key Interaction of System Engineering and ESA
  - Use of Attributes to align Requirements Engineering & Requirements Management
  - Use of Doman Models to understand Risk Treatment Authority
  - Using The Logical Layer as the Demarcation of SE and Security Solution Architecture Teams

THANK YOU, QUESTIONS?

https://linkedin.com/in/blargeau

https://github.com/beLarge

bruce@blarge.io