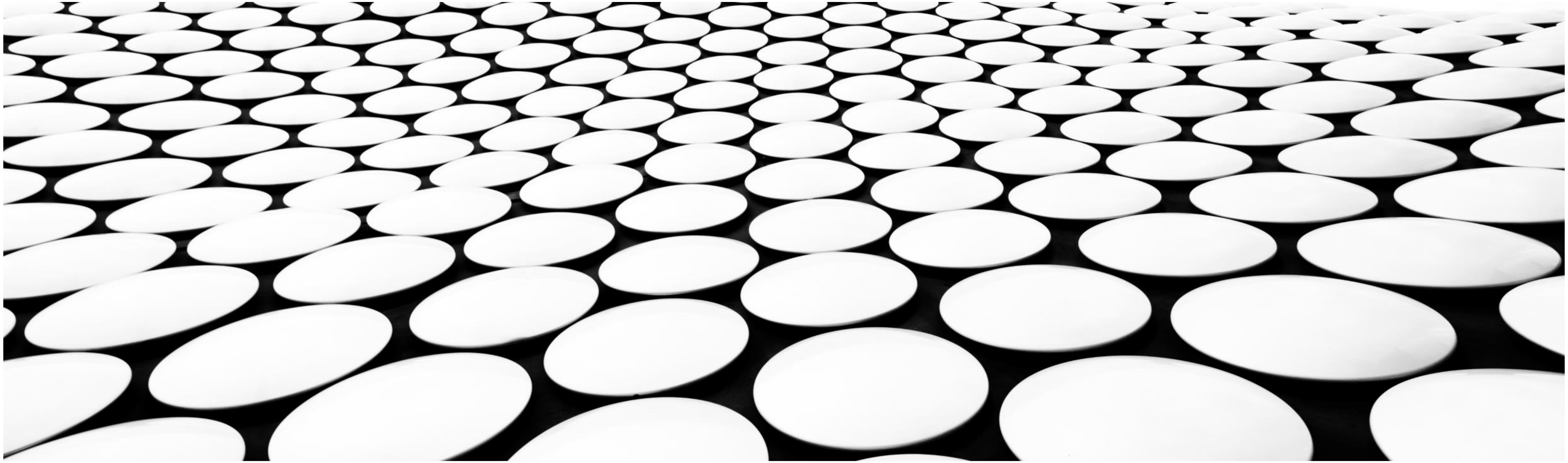
INTRODUCTION TO SECURITY ARCHITECTURE

BSIDES CANBERRA 2024



/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
- Proud member of Professionals Australia– join your #STEMUNION
- Chartered Engineer (CPEng) and Registered Professional Engineer of Queensland (RPEQ)
- Lead of the AISA Security Architecture Special Interest Group (SecARCH SIG) and Chair of the Queensland Branch of AISA
- 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

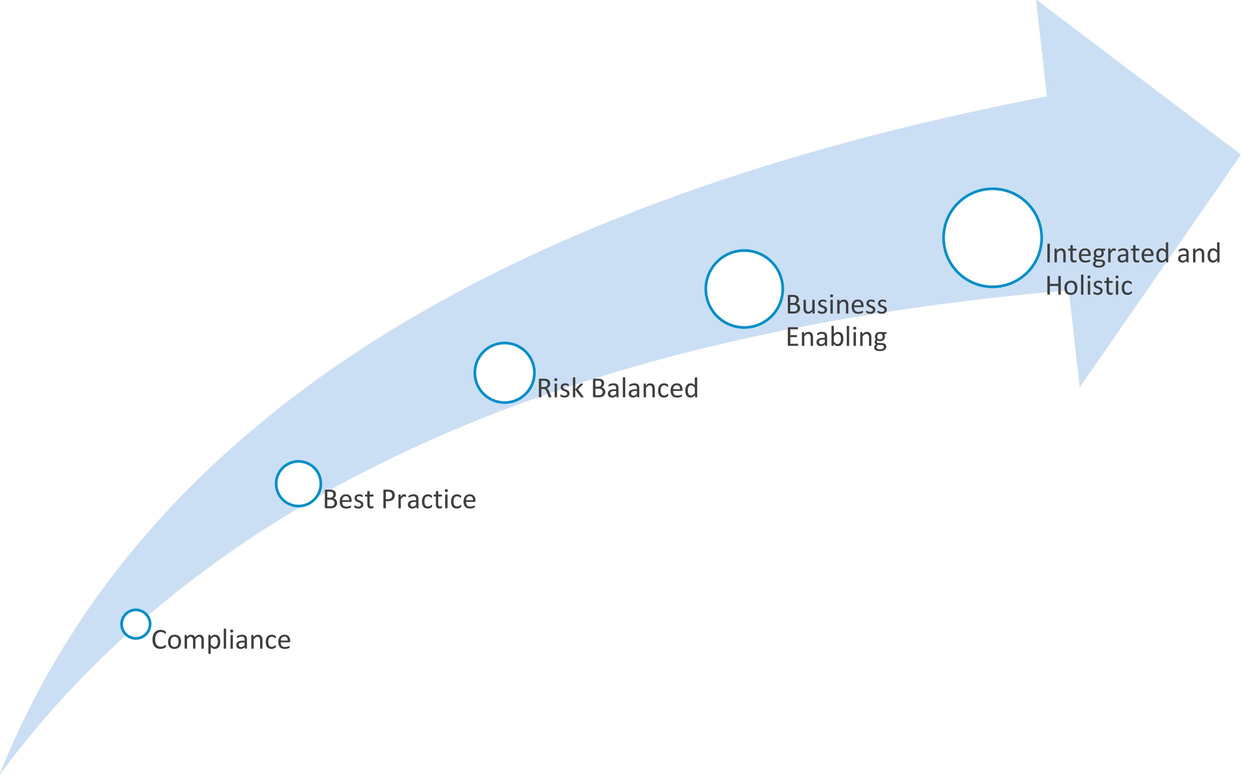
1. An Introduction to Security Architecture and Enterprise Security Architecture
2. Security Patterns
3. Introducing SABSA
4. Further Resources & Summary
5. Q&A

Why *this* presentation?

INTRODUCTION OF SECURITY ARCHITECTURE AND ENTERPRISE SECURITY ARCHITECTURE

SECURITY ARCHITECTURE

- Security Architecture enables us to consistently solve similar security problems
- **It is more than just a pick list of security controls** - it enables context and guidance on selection, placement, operation and maintenance of security controls
- It can help us move from being *compliance* and *best practice* based approach to *business enabling* and *integrated and holistic*



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

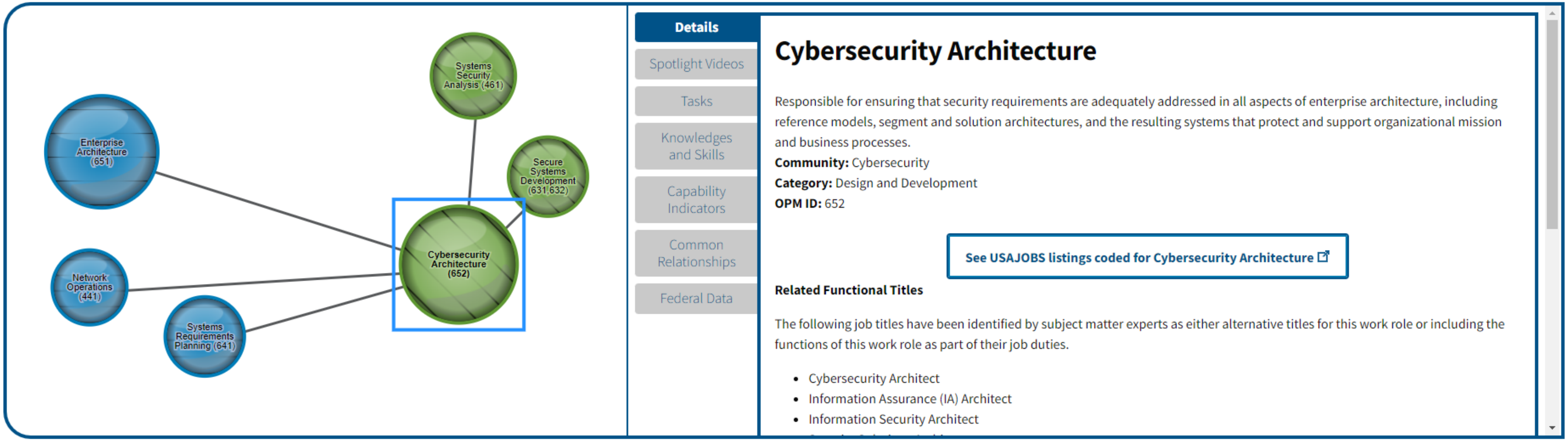
Enterprise Security Architecture

- 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

NIST NICE



Systems Security Analysis (461)
Enterprise Architecture (651)
Secure Systems Development (631,632)
Cybersecurity Architecture (652)
Network Operations (441)
Systems Requirements Planning (641)
Details
Spotlight Videos
Tasks
Knowledges and Skills
Capability Indicators
Common Relationships
Federal Data

Cybersecurity Architecture

Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems that protect and support organizational mission and business processes.

Community: Cybersecurity

Category: Design and Development

OPM ID: 652

See USAJOBS listings coded for Cybersecurity Architecture

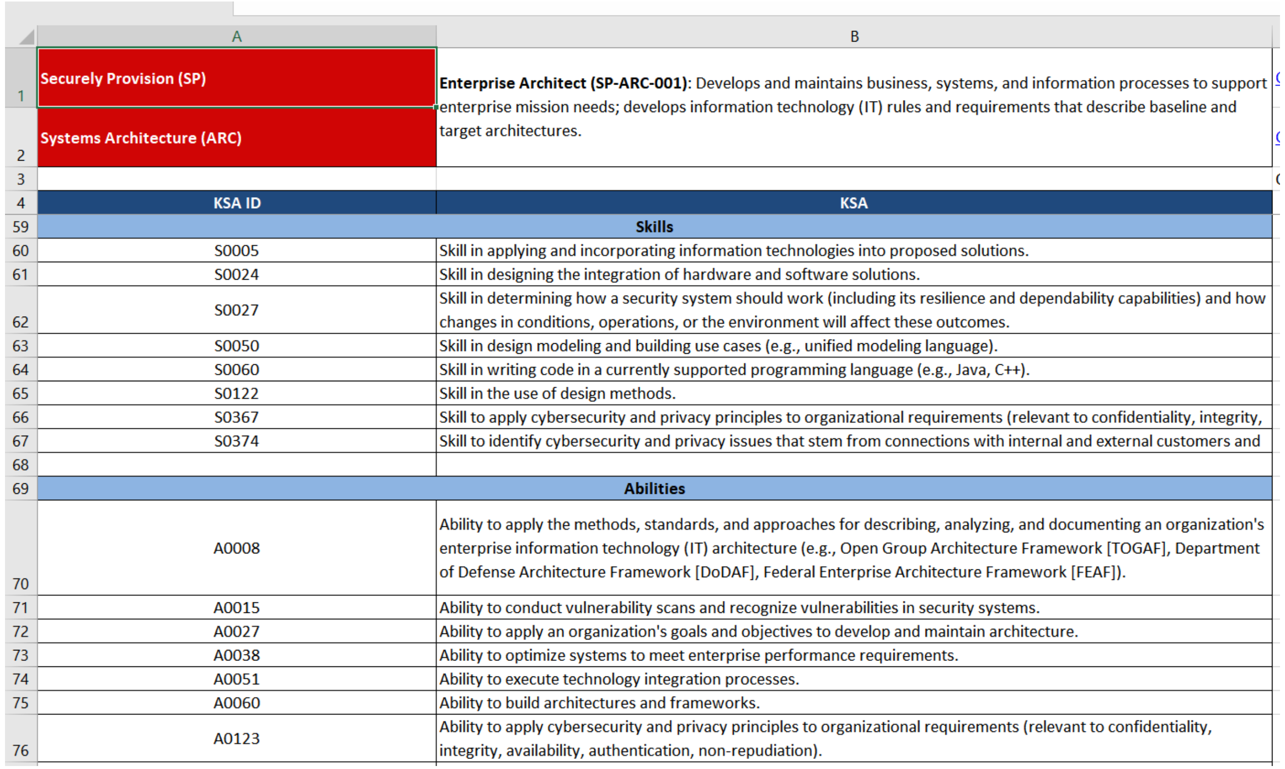
Related Functional Titles

The following job titles have been identified by subject matter experts as either alternative titles for this work role or including the functions of this work role as part of their job duties.

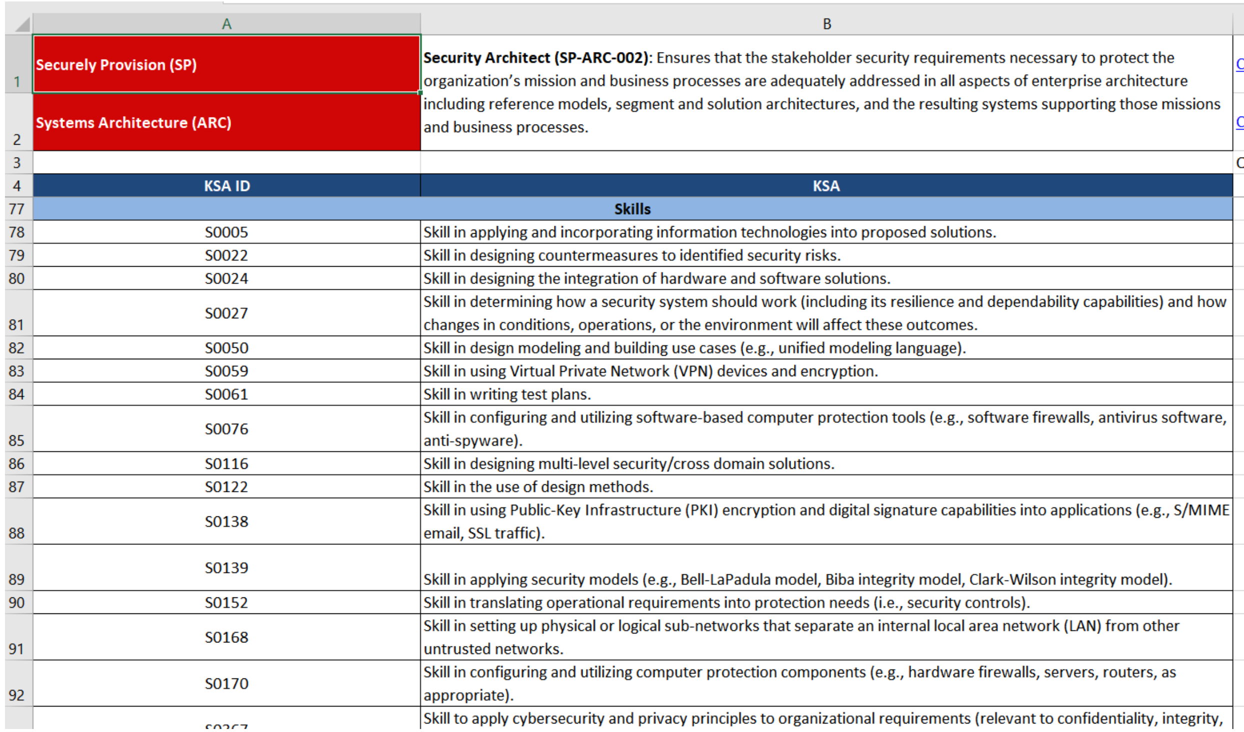
- Cybersecurity Architect
- Information Assurance (IA) Architect
- Information Security Architect

Ref - https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool

ENTERPRISE ARCHITECTURE VS SECURITY ARCHITECTURE



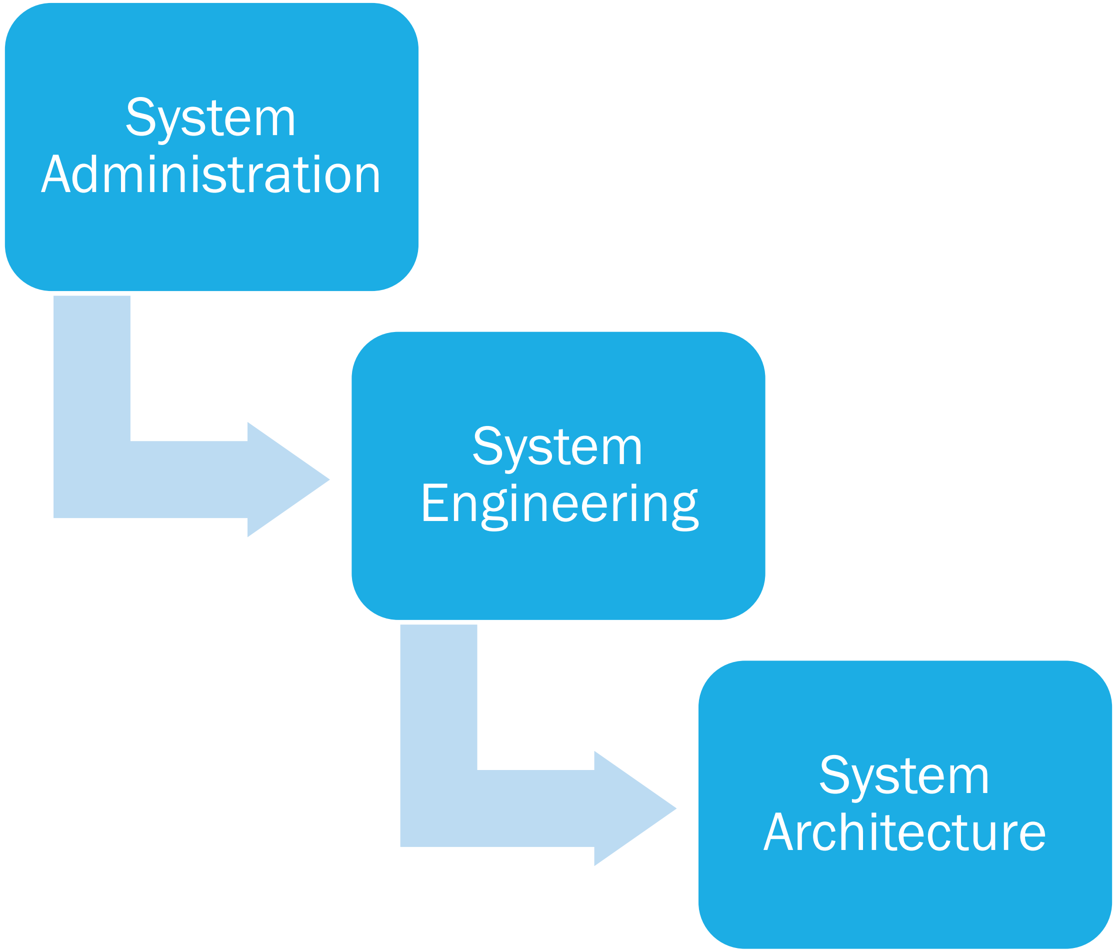
	A	B
1	Securely Provision (SP)	**Enterprise Architect (SP-ARC-001)**: Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
2	Systems Architecture (ARC)	
3		
4	KSA ID	KSA
59	Skills	
60	S0005	Skill in applying and incorporating information technologies into proposed solutions.
61	S0024	Skill in designing the integration of hardware and software solutions.
62	S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
63	S0050	Skill in design modeling and building use cases (e.g., unified modeling language).
64	S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).
65	S0122	Skill in the use of design methods.
66	S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity,
67	S0374	Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and
68		
69	Abilities	
70	A0008	Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]).
71	A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
72	A0027	Ability to apply an organization's goals and objectives to develop and maintain architecture.
73	A0038	Ability to optimize systems to meet enterprise performance requirements.
74	A0051	Ability to execute technology integration processes.
75	A0060	Ability to build architectures and frameworks.
76	A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).



	A	B
1	Securely Provision (SP)	**Security Architect (SP-ARC-002)**: Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
2	Systems Architecture (ARC)	
3		
4	KSA ID	KSA
77	Skills	
78	S0005	Skill in applying and incorporating information technologies into proposed solutions.
79	S0022	Skill in designing countermeasures to identified security risks.
80	S0024	Skill in designing the integration of hardware and software solutions.
81	S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
82	S0050	Skill in design modeling and building use cases (e.g., unified modeling language).
83	S0059	Skill in using Virtual Private Network (VPN) devices and encryption.
84	S0061	Skill in writing test plans.
85	S0076	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).
86	S0116	Skill in designing multi-level security/cross domain solutions.
87	S0122	Skill in the use of design methods.
88	S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).
89	S0139	Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
90	S0152	Skill in translating operational requirements into protection needs (i.e., security controls).
91	S0168	Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks.
92	S0170	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).
	S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity,

Source - NIST NICE (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

THE COMMON WAY TO BECOME AN ARCHITECT



System Administration

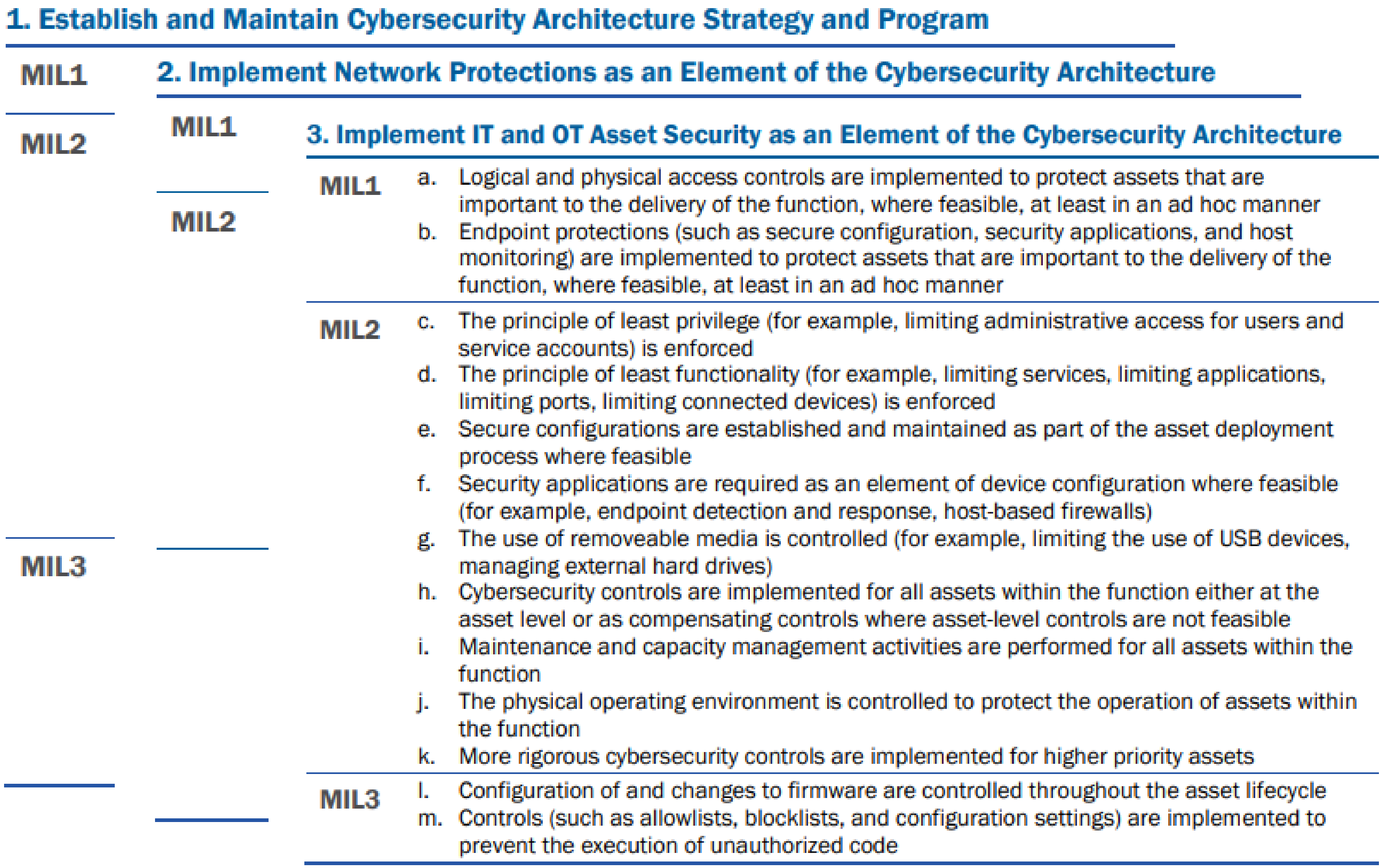
System Engineering

System Architecture

C2M2 ARCHITECTURE DOMAIN

- The US Cyber Security Capability Maturity Model (C2M2) has an ARCHITECTURE domain with 6 objectives:
  1. Establish and Maintain Cybersecurity Architecture Strategy and Program
  2. Implement Network Protections as an Element of the Cybersecurity Architecture
  3. Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture
  4. Implement Software Security as an Element of the Cybersecurity Architecture
  5. Implement Data Security as an Element of the Cybersecurity Architecture
  6. Management Activities for the ARCHITECTURE domain
- It has the concept of “Maturity Indicator Level” (MIL) to organise Practices into a Maturity Sequence – this helps with a Crawl, Walk & Run approach

C2M2 ARCHITECTURE DOMAIN (CONT.)



1. Establish and Maintain Cybersecurity Architecture Strategy and Program

MIL1

MIL2

MIL3

2. Implement Network Protections as an Element of the Cybersecurity Architecture

MIL1

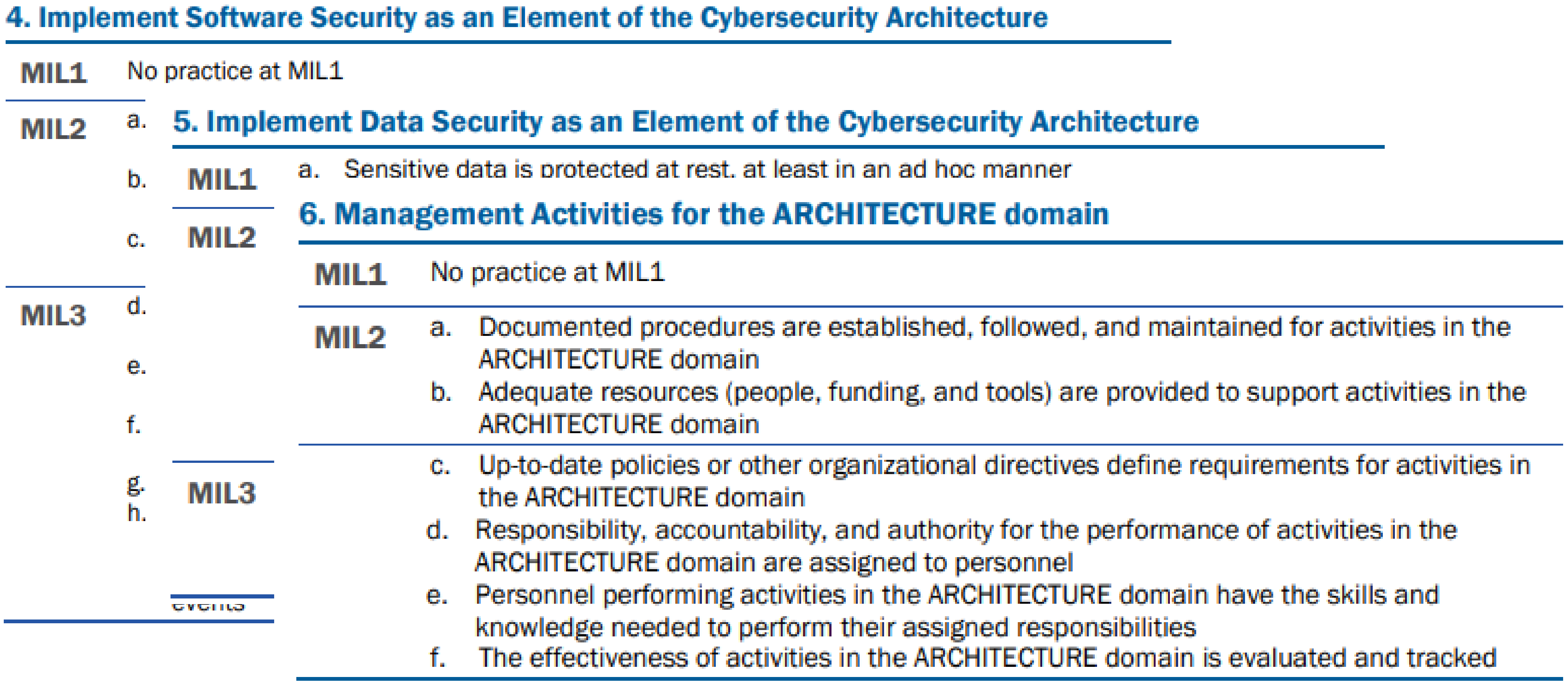
MIL2

3. Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture

MIL1	a. Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner b. Endpoint protections (such as secure configuration, security applications, and host monitoring) are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner
MIL2	c. The principle of least privilege (for example, limiting administrative access for users and service accounts) is enforced d. The principle of least functionality (for example, limiting services, limiting applications, limiting ports, limiting connected devices) is enforced e. Secure configurations are established and maintained as part of the asset deployment process where feasible f. Security applications are required as an element of device configuration where feasible (for example, endpoint detection and response, host-based firewalls) g. The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives) h. Cybersecurity controls are implemented for all assets within the function either at the asset level or as compensating controls where asset-level controls are not feasible i. Maintenance and capacity management activities are performed for all assets within the function j. The physical operating environment is controlled to protect the operation of assets within the function k. More rigorous cybersecurity controls are implemented for higher priority assets
MIL3	l. Configuration of and changes to firmware are controlled throughout the asset lifecycle m. Controls (such as allowlists, blocklists, and configuration settings) are implemented to prevent the execution of unauthorized code

Ref - https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

C2M2 ARCHITECTURE DOMAIN (CONT.)



4. Implement Software Security as an Element of the Cybersecurity Architecture

MIL1	No practice at MIL1
MIL2	a. b. c.
MIL3	d. e. f. g. h. events

5. Implement Data Security as an Element of the Cybersecurity Architecture

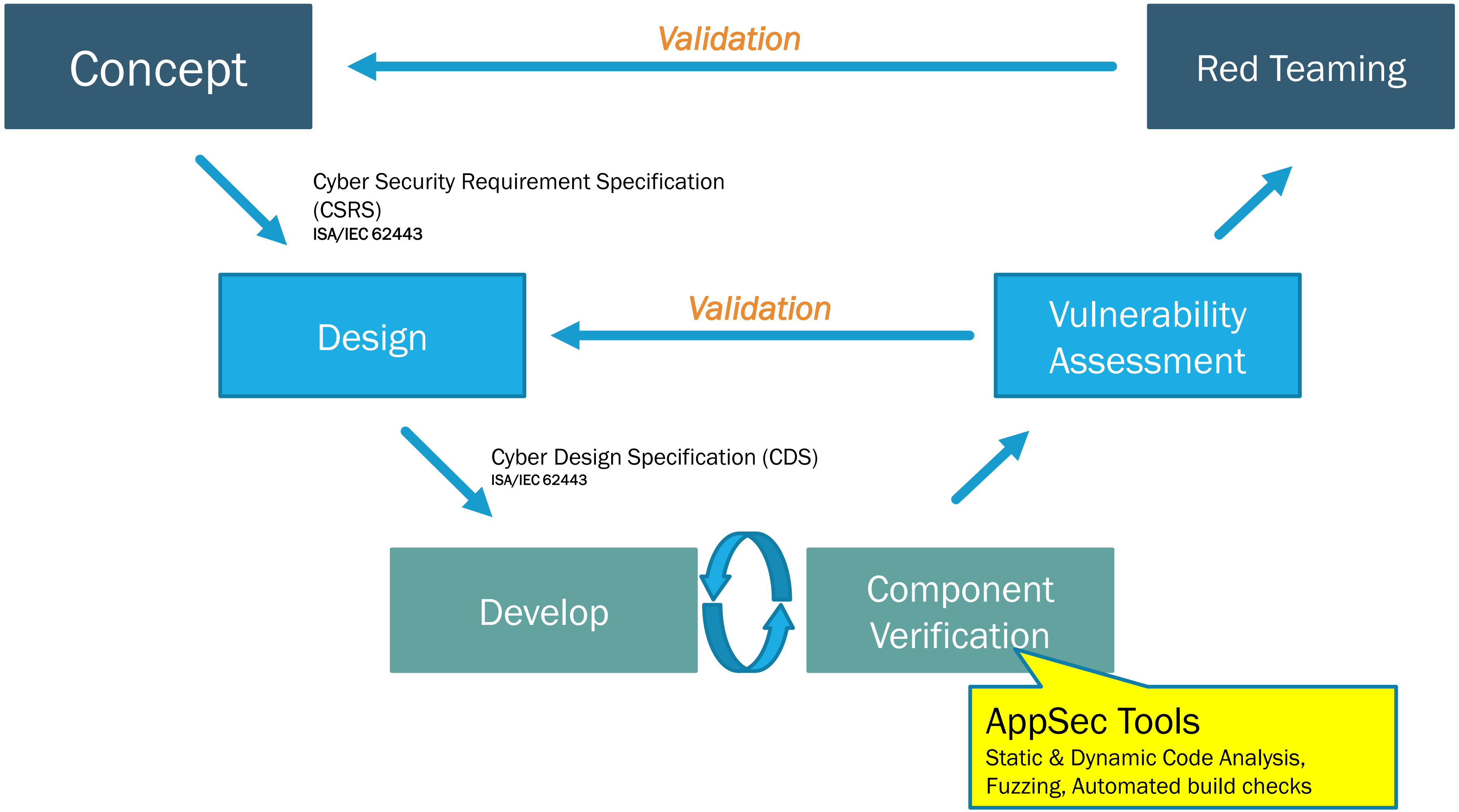
MIL1	a. Sensitive data is protected at rest, at least in an ad hoc manner
MIL2	
MIL3	

6. Management Activities for the ARCHITECTURE domain

MIL1	No practice at MIL1
MIL2	a. Documented procedures are established, followed, and maintained for activities in the ARCHITECTURE domain b. Adequate resources (people, funding, and tools) are provided to support activities in the ARCHITECTURE domain
	c. Up-to-date policies or other organizational directives define requirements for activities in the ARCHITECTURE domain d. Responsibility, accountability, and authority for the performance of activities in the ARCHITECTURE domain are assigned to personnel e. Personnel performing activities in the ARCHITECTURE domain have the skills and knowledge needed to perform their assigned responsibilities f. The effectiveness of activities in the ARCHITECTURE domain is evaluated and tracked

Ref - https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

THE *CYBER* V-MODEL



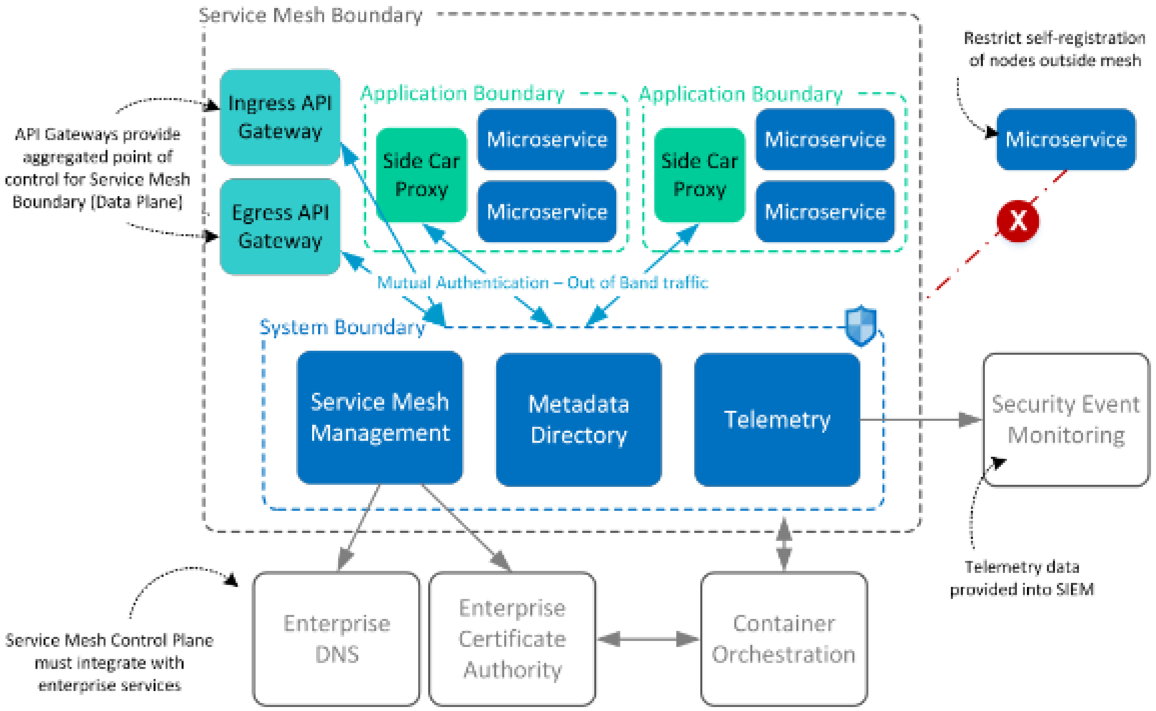
SECURITY PATTERNS

WHAT ARE SECURITY PATTERNS

- Security patterns are generalised security reference designs that can be used to give guidance on how to architect systems e.g. “self-service”
- They allow architects to build the “paved road” and encourage reuse of security solutions to common problems
- They assist in security architecture governance activities
- They are a very important tool in the security architecture toolkit

SECURITYPATTERNS.IO

- An awesome reference!
- Gives guidance on how to write security patterns and includes examples
- Their security pattern process:
  - Identity the problem and scope
  - Prepare and research
  - Identify the assets
  - Threat Modelling
  - Describe the target solution
  - Define and map security control objectives
  - Describe security pattern
  - Summary and conclusion
- Big shout out to Patterned Security for this awesome open and free resource!

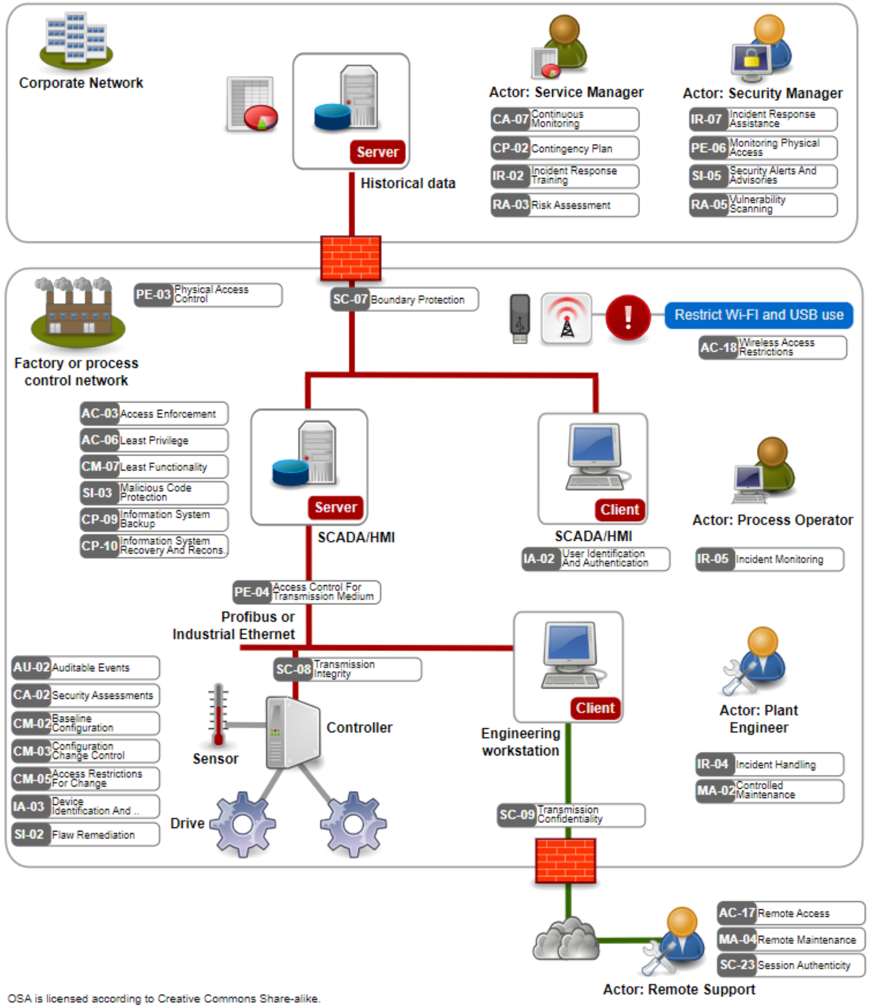


Service Mesh Boundary
API Gateways provide aggregated point of control for Service Mesh Boundary (Data Plane)
Ingress API Gateway
Egress API Gateway
Application Boundary
Side Car Proxy
Microservice
Microservice
Application Boundary
Side Car Proxy
Microservice
Microservice
Restrict self-registration of nodes outside mesh
Microservice
X
Mutual Authentication – Out of Band traffic
System Boundary
Service Mesh Management
Metadata Directory
Telemetry
Security Event Monitoring
Telemetry data provided into SIEM
Service Mesh Control Plane must integrate with enterprise services
Enterprise DNS
Enterprise Certificate Authority
Container Orchestration

Ref - https://securitypatterns.io/docs/04-service-mesh-security-pattern/

OPEN SECURITY ARCHITECTURE

- Another awesome example is OSA
- My favourite is SP-23 Cyber Security for Industrial Control Systems
- Designates Assets, Actors, Zones and Controls using NIST 800-53
- A lot simpler and a great starting point and has a lot more Patterns in it's library (https://www.opensecurityarchitecture.org/cms/library/patternlandscape)



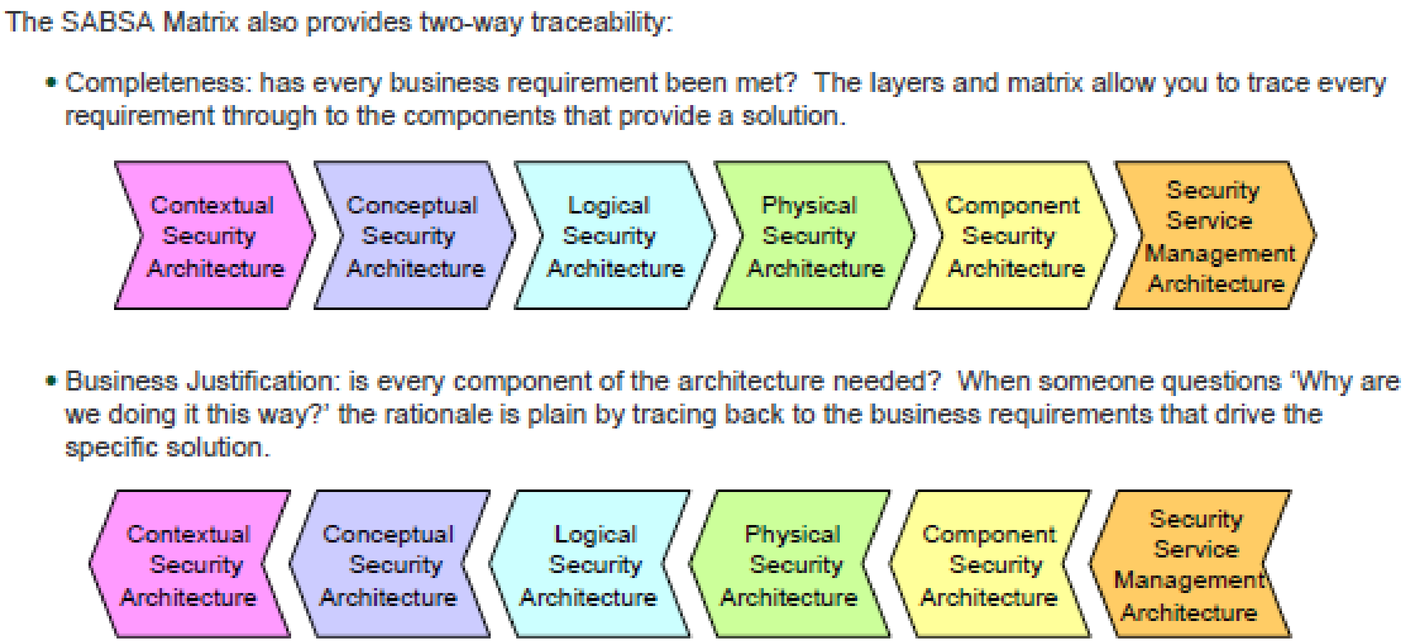
Corporate Network
Server
Historical data
Actor: Service Manager
CA-07 Continuous Monitoring
CP-02 Contingency Plan
IR-02 Incident Response Training
RA-03 Risk Assessment
Actor: Security Manager
IR-07 Incident Response Assistance
PE-06 Monitoring Physical Access
SI-05 Security Alerts And Advisories
RA-05 Vulnerability Scanning
Factory or process control network
PE-03 Physical Access Control
SC-07 Boundary Protection
Restrict Wi-FI and USB use
AC-18 Wireless Access Restrictions
AC-03 Access Enforcement
AC-06 Least Privilege
CM-07 Least Functionality
SI-03 Malicious Code Protection
CP-09 Information System Backup
CP-10 Information System Recovery And Recons..
Server
SCADA/HMI
Client
SCADA/HMI
IA-02 User Identification And Authentication
Actor: Process Operator
IR-05 Incident Monitoring
PE-04 Access Control For Transmission Medium
Profibus or Industrial Ethernet
SC-08 Transmission Integrity
AU-02 Auditable Events
CA-02 Security Assessments
CM-02 Baseline Configuration
CM-03 Configuration Change Control
CM-05 Access Restrictions For Change
IA-03 Device Identification And ..
SI-02 Flaw Remediation
Sensor
Controller
Drive
Client
Engineering workstation
SC-09 Transmission Confidentiality
Actor: Plant Engineer
IR-04 Incident Handling
MA-02 Controlled Maintenance
AC-17 Remote Access
MA-04 Remote Maintenance
SC-23 Session Authenticity
Actor: Remote Support

Ref - https://www.opensecurityarchitecture.org/cms/en/library/patternlandscape/293-sp-023-industrial-control-systems

AN INTRODUCTION TO SABSA

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 CENSUS

As at August 2023

Foundation

Region	Count
Europe	1,895
Oceania	1,531
North America	939
Asia	352
Middle East	246
Africa	177
South America	11

Practitioner

Certification(s)	Count
Architecture Design (SCPA)	231
Risk, Assurance & Governance (SCPR)	112
SCPA & SCPR	67

Learn more at https://sabsa.org/sabsa-census/

SABSA MATRIX

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

The Business View

The Architect's View

The Designer's View

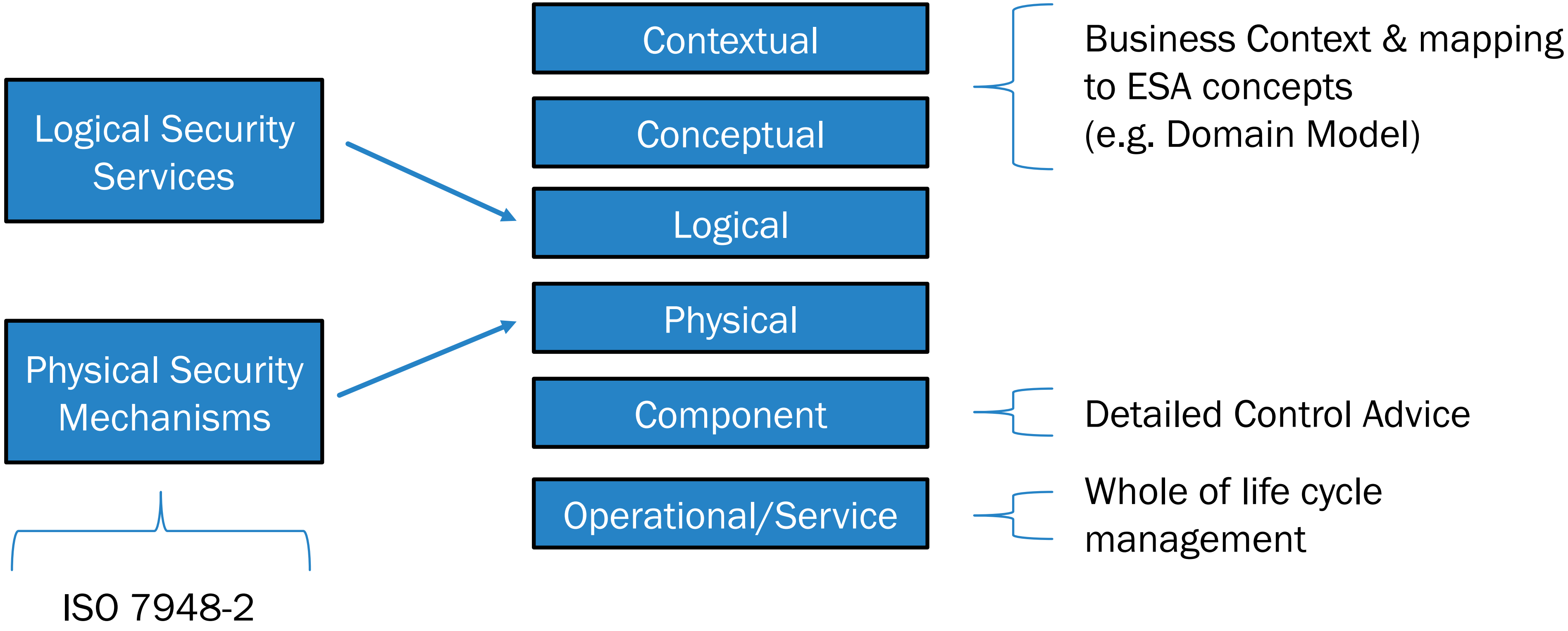
The Builder's View

The Tradeperson's View

The Service Manager's View

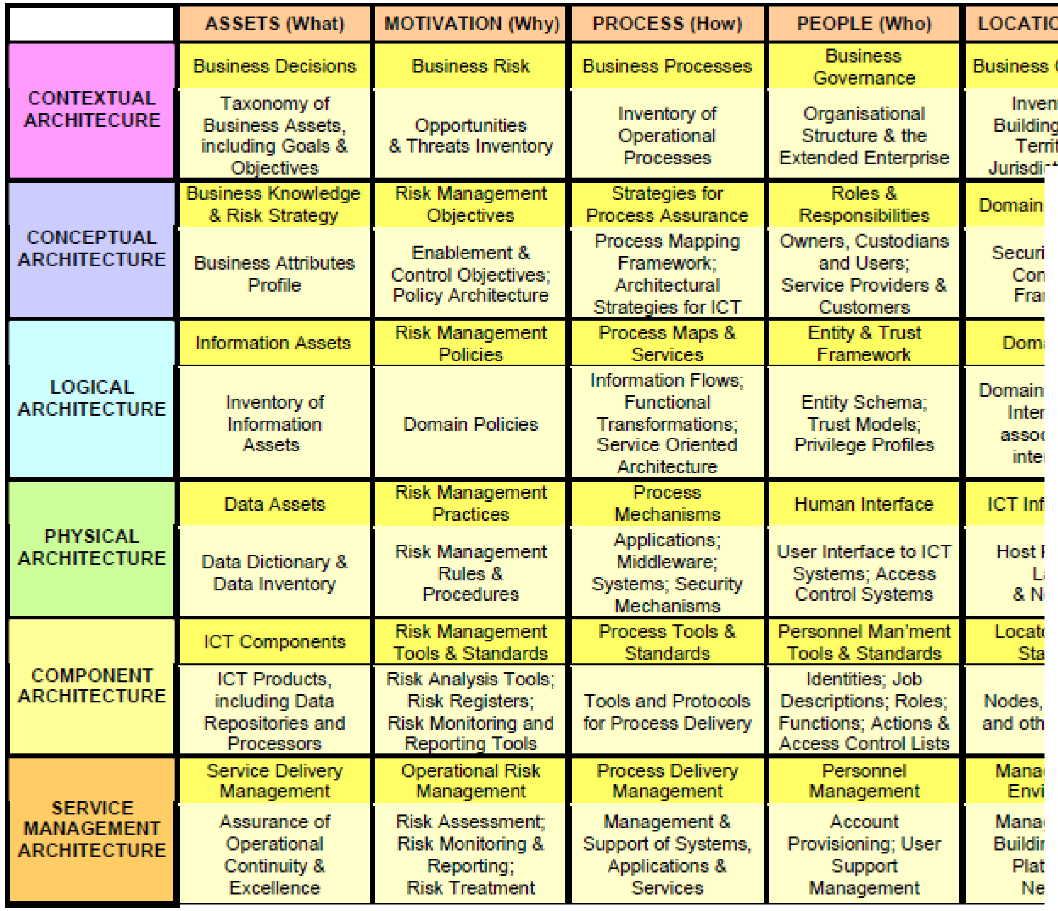
https://sabsa.org/white-paper-requests/

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

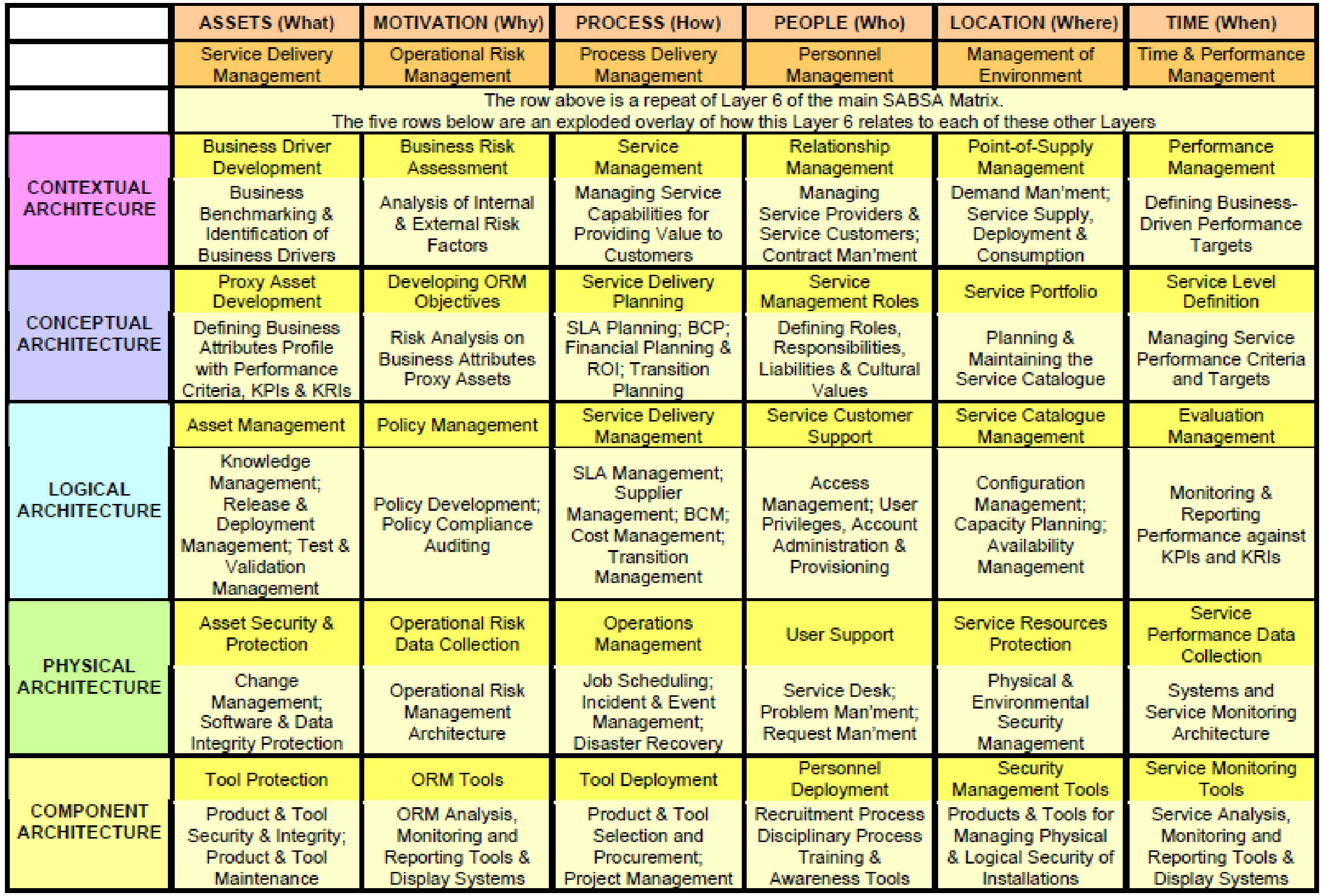
SABSA MATRIX (CONT.)

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 Buildi Plat Ne	

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

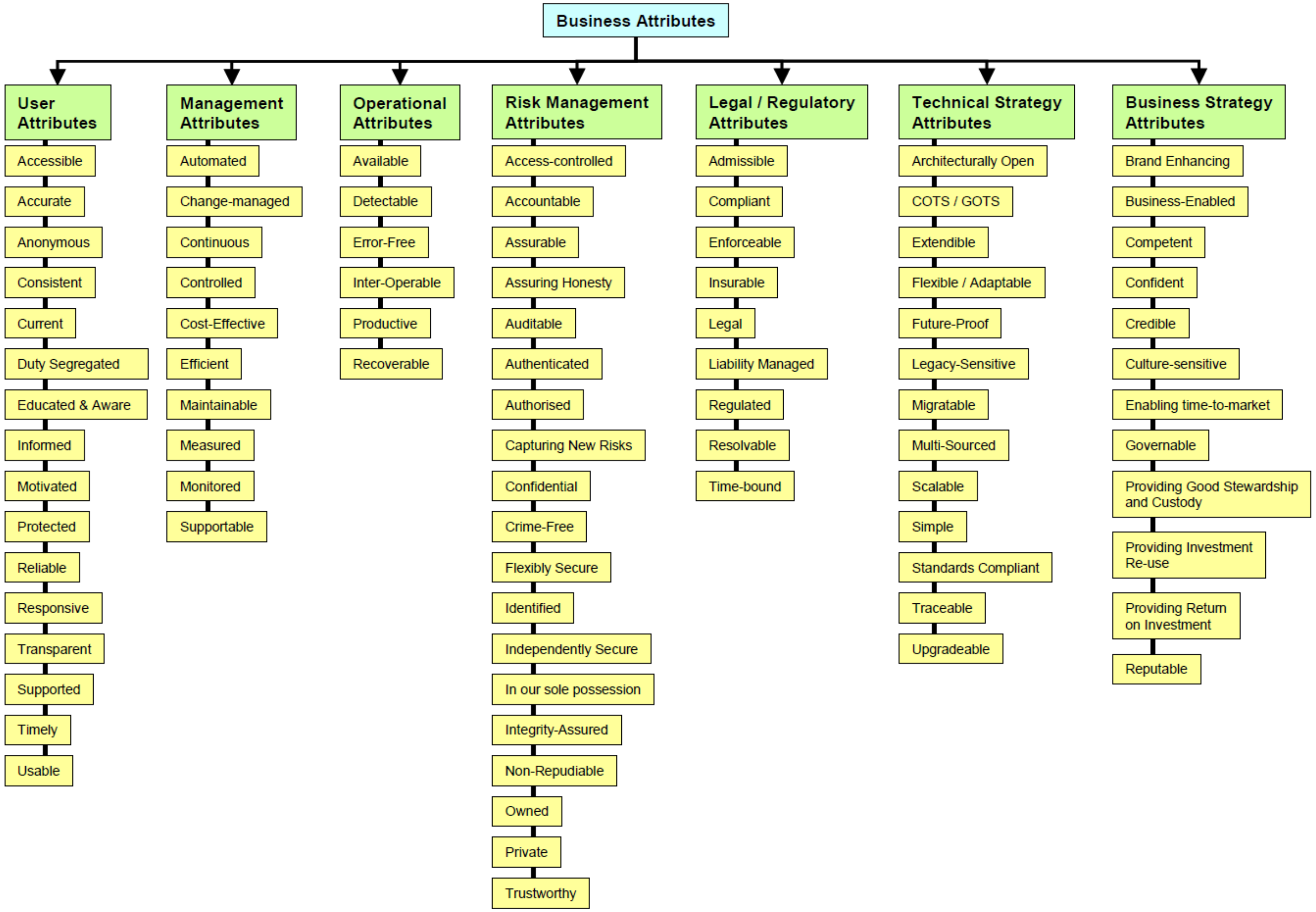


	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	The row above is a repeat of Layer 6 of the main SABSA 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

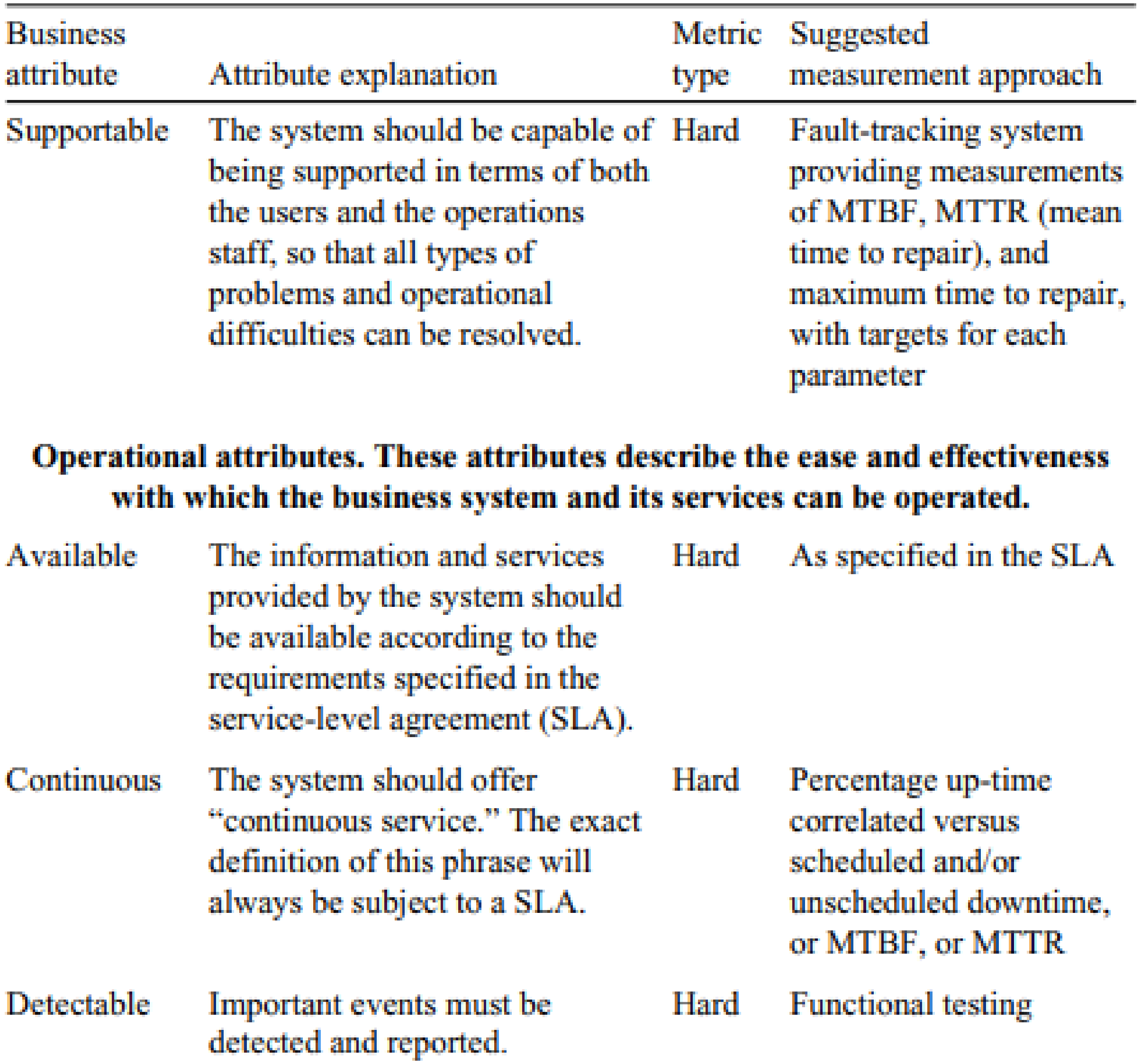
Technical Strategy Attributes
- Architecturally Open
- COTS / GOTS
- Extendible
- Flexible / Adaptable
- Future-Proof
- Legacy-Sensitive
- Migratable
- Multi-Sourced
- Scalable
- Simple
- Standards Compliant
- Traceable
- Upgradeable

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

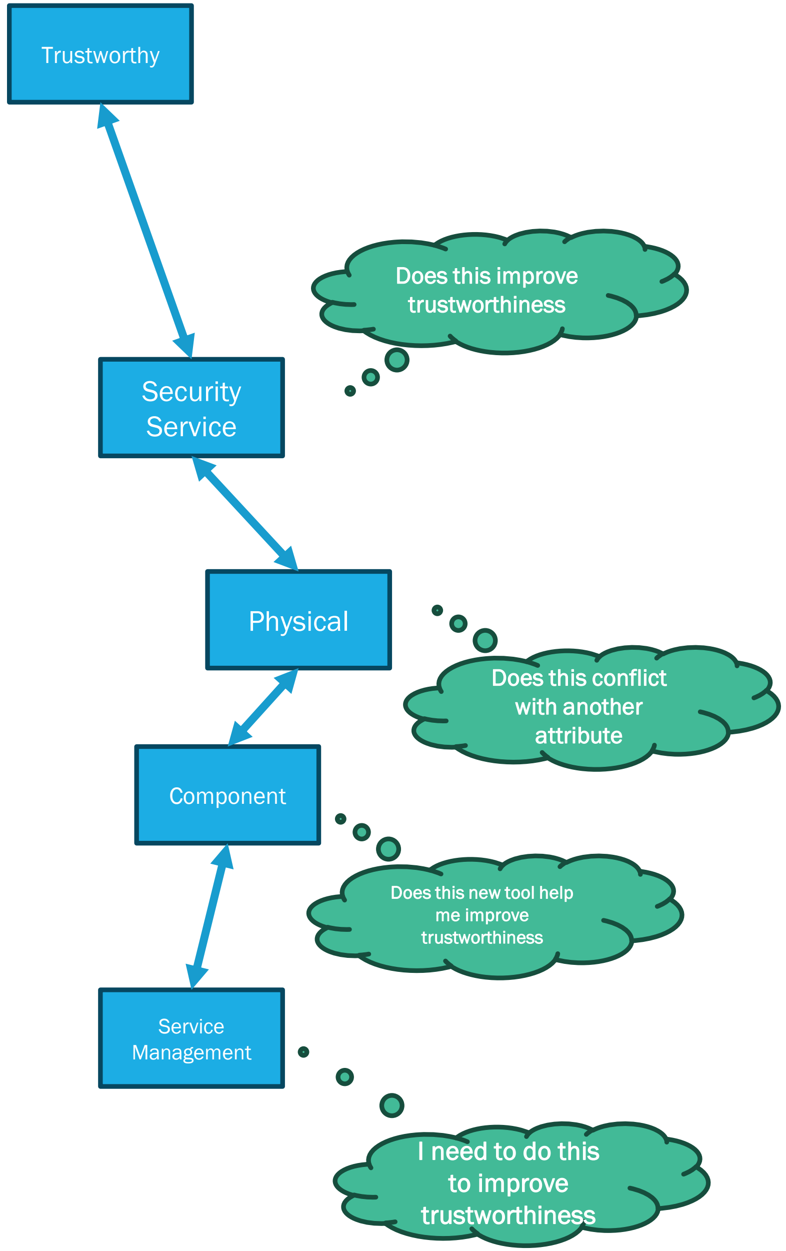


Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Supportable	The system should be capable of being supported in terms of both the users and the operations staff, so that all types of problems and operational difficulties can be resolved.	Hard	Fault-tracking system providing 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

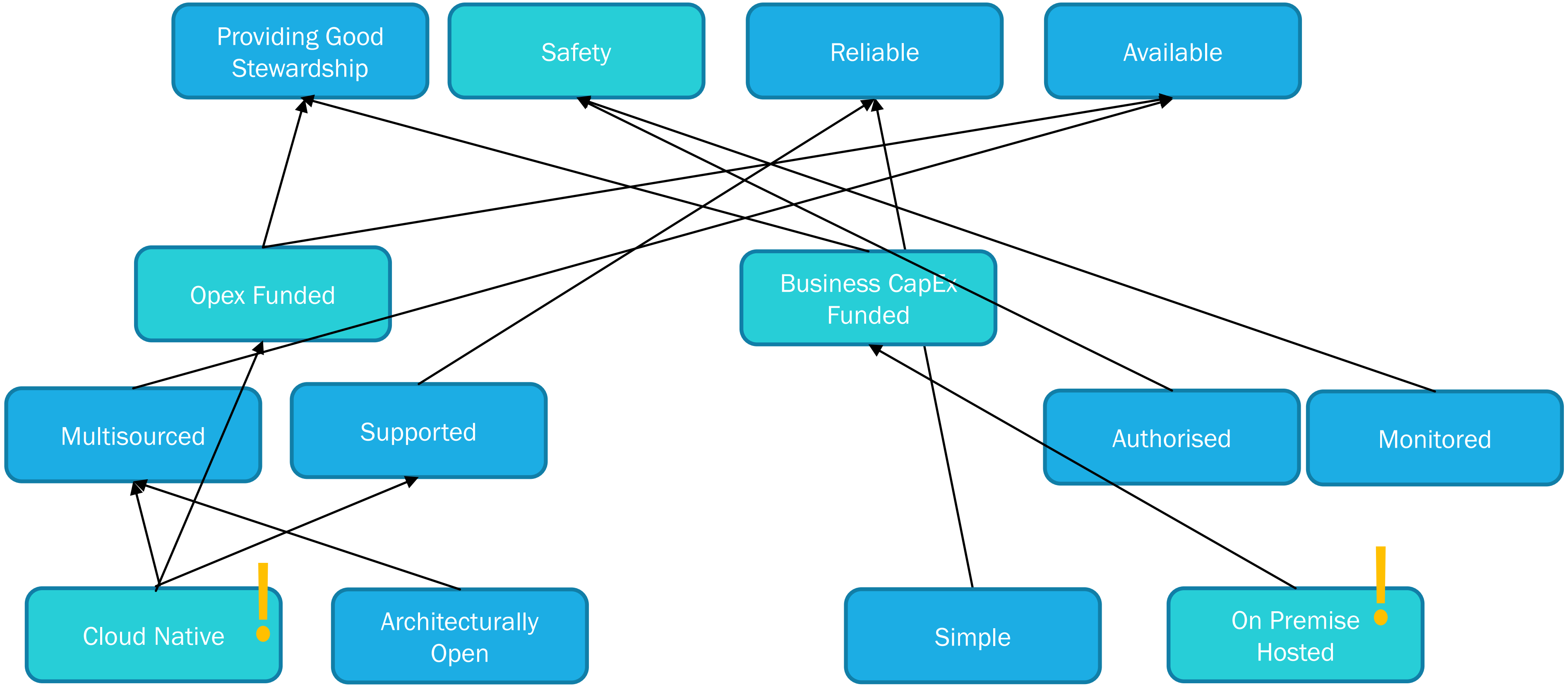
Ref - https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470476017.app1

ATTRIBUTES (CONT.)

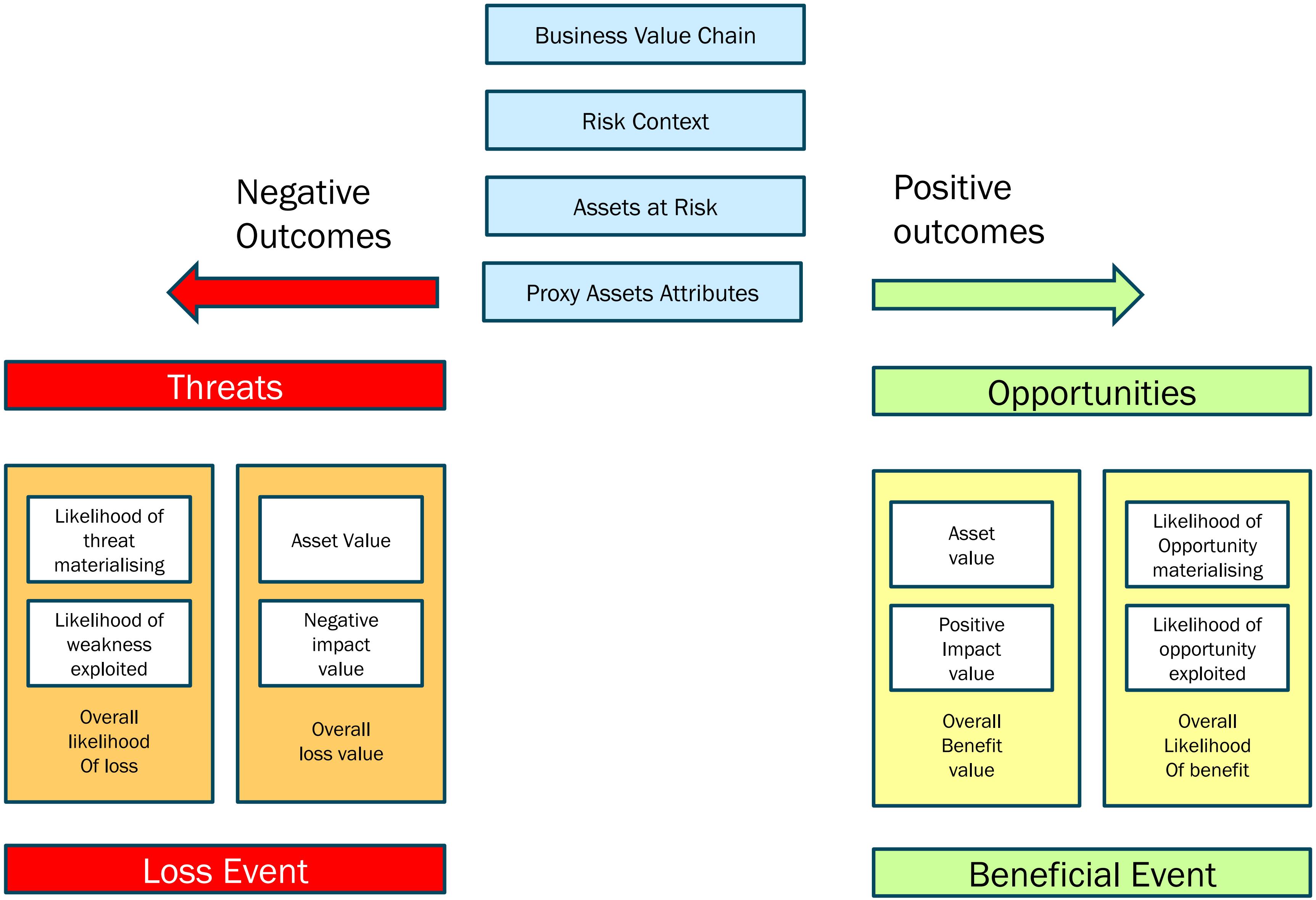
- They are however a **very smart abstraction** of cyber security requirements management
- It provides a simple label for a complex interaction of security requirements to achieve a business goal
- It can be used to highlight the impact of an emerging business driver on the enterprise's ability to exploit 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
Security Service
Physical
Component
Service Management
Does this improve trustworthiness
Does this conflict with another attribute
Does this new tool help me improve trustworthiness
I need to do this to improve trustworthiness

MULTI TIER ATTRIBUTES



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

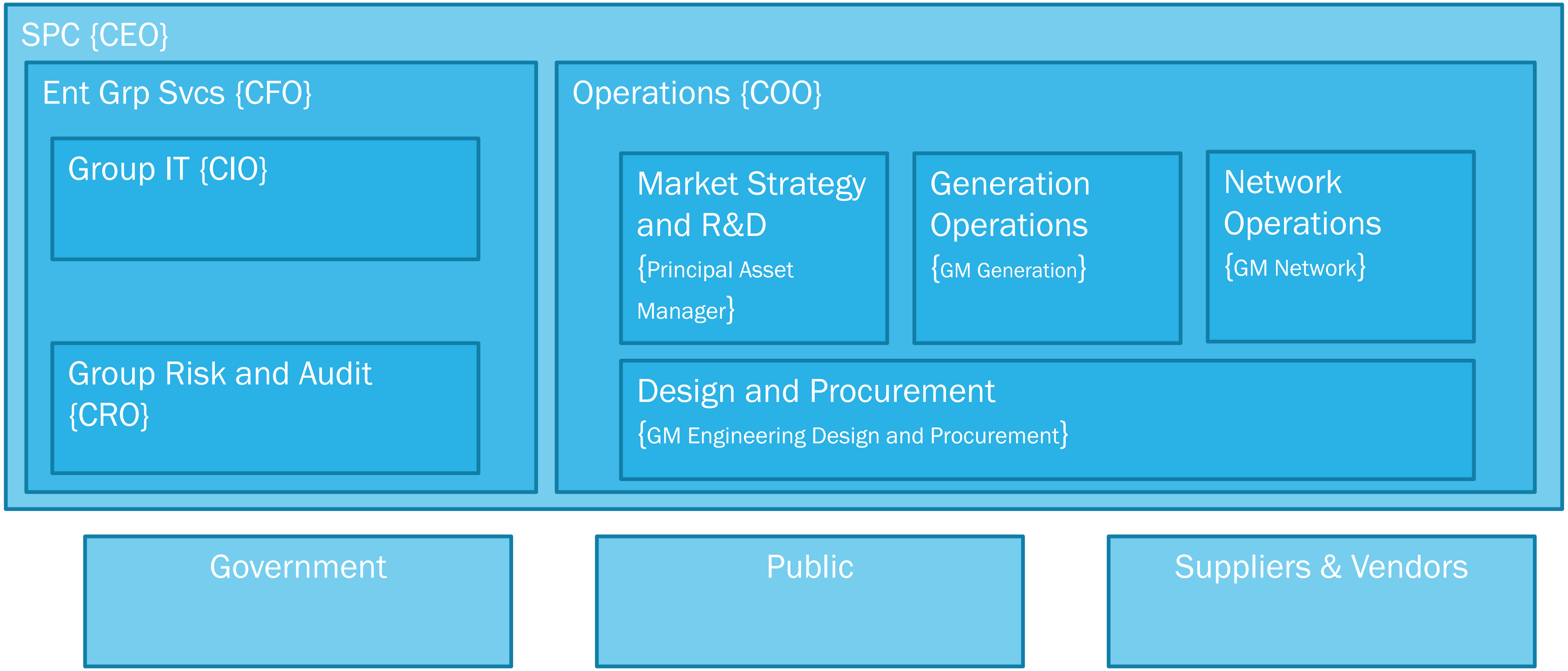
Likelihood of opportunity exploited

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}

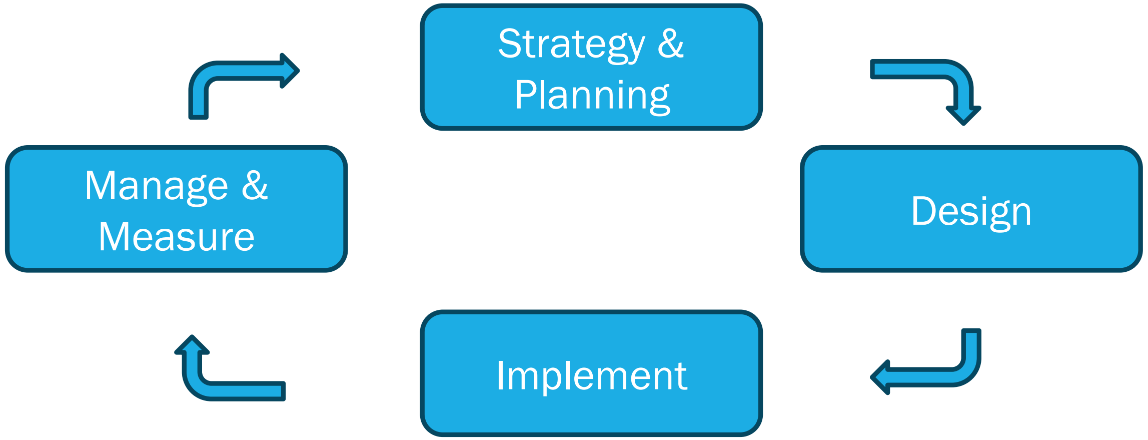
Design and Procurement {GM Engineering Design and Procurement}

Government

Public

Suppliers & Vendors

SABSA LIFE CYCLE



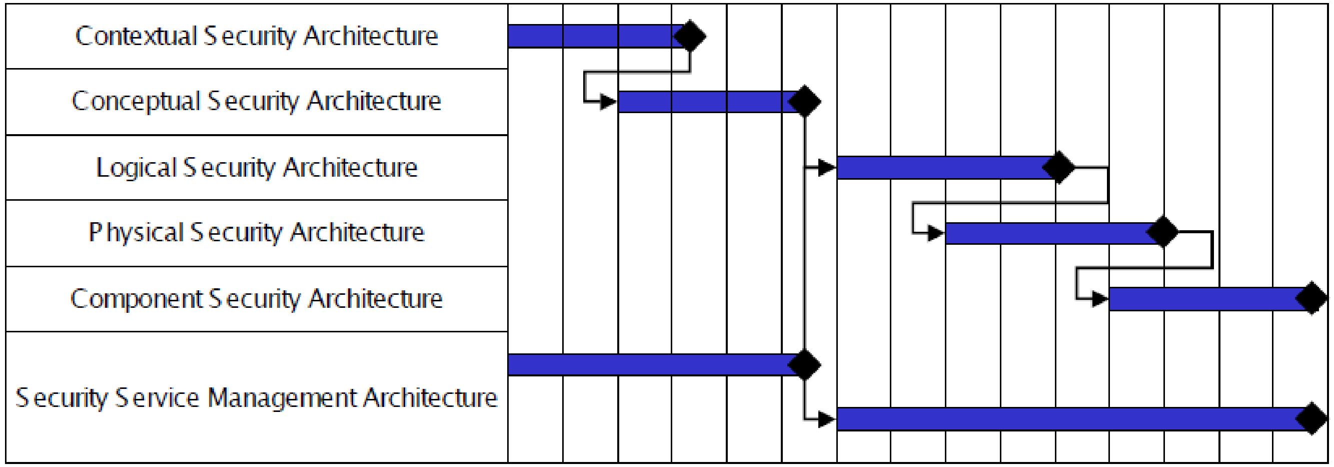


Figure 2: The SABSA Development Process

Ref – SABSA White Paper (W100)

BONUS SLIDE –SABSA & TOGAF INTEGRATION

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

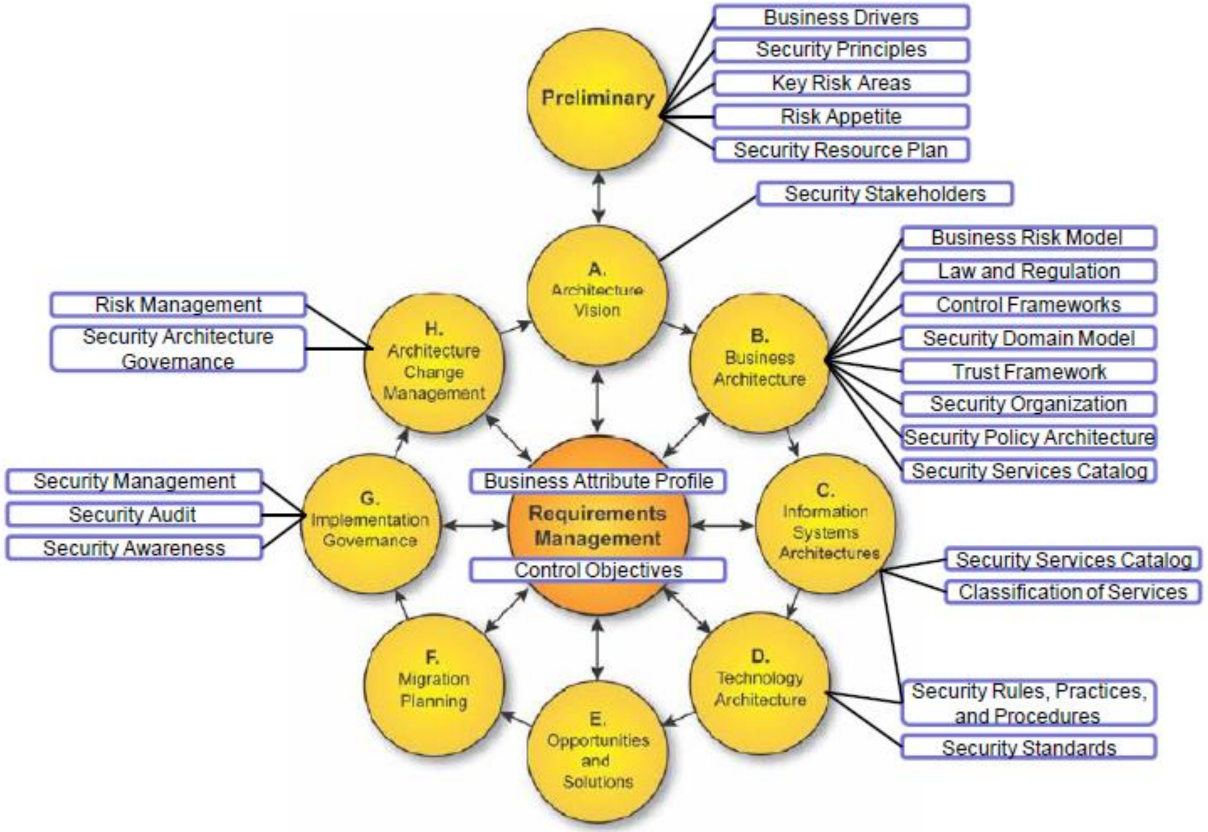


Figure 16: Overview of Security-Related Artifacts in the TOGAF ADM

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

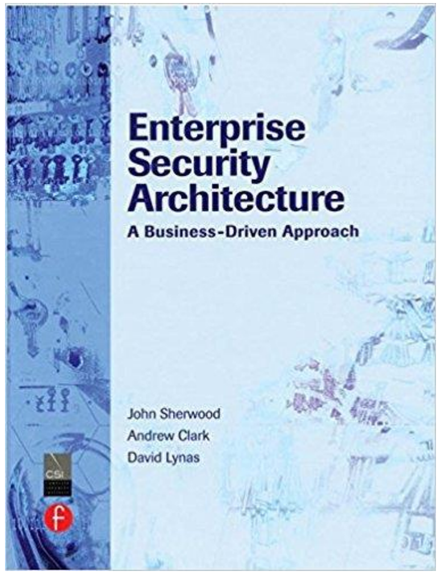
FURTHER RESOURCES & SUMMARY

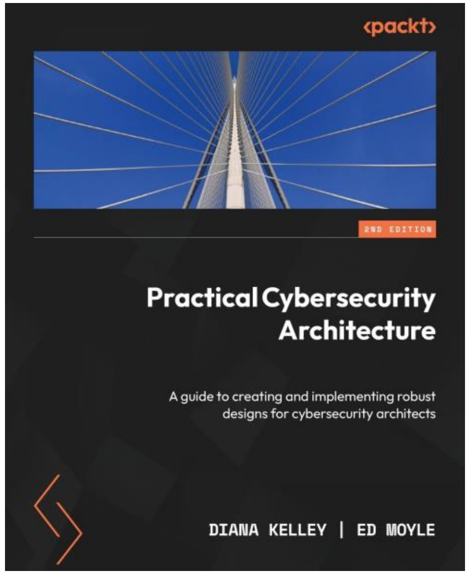
SECURITY ARCHITECTURE GROUPS IN AUSTRALIA

- The SABSA Institute - https://sabsa.org/membership-benefits/
- COSAC APAC (MEL) – https://www.cosac.net/apac
- SABSA World Australia (MEL, SYD, BNE) - https://www.linkedin.com/company/sabsa-world-australia
- AISA SecARCH SIG (BNE, MEL) – keep an eye out for emails for invites but some recordings are available - https://vimeo.com/user98993502
- ISACA SAWG (MEL) - https://www.linkedin.com/company/isaca-melbourne-chapter/

FURTHER RESOURCES

- SABSA White Paper (W100)
- US DoE C2M2 v2.1
- Enterprise Security Architecture
  A Business- Driven Approach
- Practical Cyber Security Architecture
- Join The SABSA Institute
- 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

- Security Architecture
  - Security architecture provides context and risk balance for control selection through a whole of system life view
  - The difference of Security Solution Architecture and Enterprise Security Architecture
- Security Patterns
  - Generalised security designs to help distribute cyber security architecture activities
  - Securitypatterns.io
  - Open Security Architecture
- Understand the key features of SABSA
  - The SABSA Matrix
  - SABSA Attributes
  - Domain Modelling

THANK YOU, QUESTIONS?

https://linkedin.com/in/blargeau

https://github.com/beLarge

bruce@blarge.io