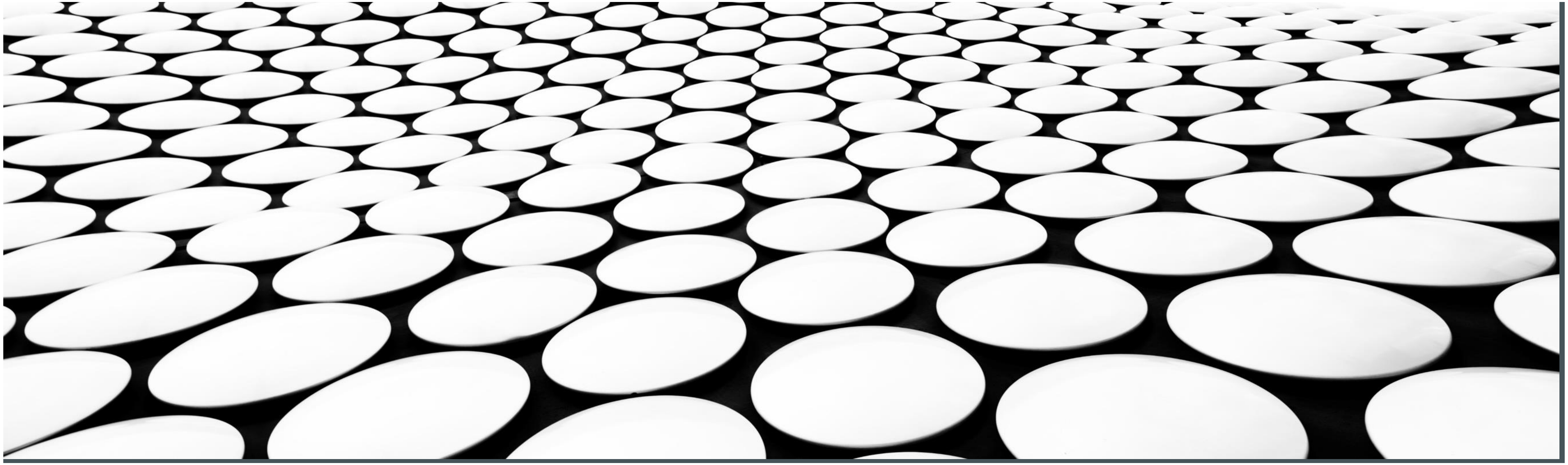
HANDS ON CYBER SECURITY ARCHITECTURE WORKSHOP USING THE SABSA FRAMEWORK

AUSCERT 2025

βLARGE
MISSION CRITICAL CYBER SECURITY



/whois @beLarge

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

βLARGE
MISSION CRITICAL CYBER SECURITY

- Director and Principal Cyber Security Architect at BLARGE
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for over 15 years
- Proud member of Professionals Australia
  The Union for STEM Workers – join your #STEMUNION
- Experience in Electricity Generation & Transmission, Railway, Aviation, Emergency Services and Consulting industries
- Bach Eng (Telecomms) QUT First Class Honours and Master Business (Applied Finance) with Distinction QUT

SABSA® Chartered Architect Foundation SCF

GIAC Industrial Cyber Security Professional GICSP

GIAC Response and Industrial Defense GRID

GIAC Security Operations Manager GSOM

ISA/IEC 62443 Cybersecurity Expert ISA

alc Cyber Security Foundation+Practitioner CERTIFIED

Why *this* presentation?

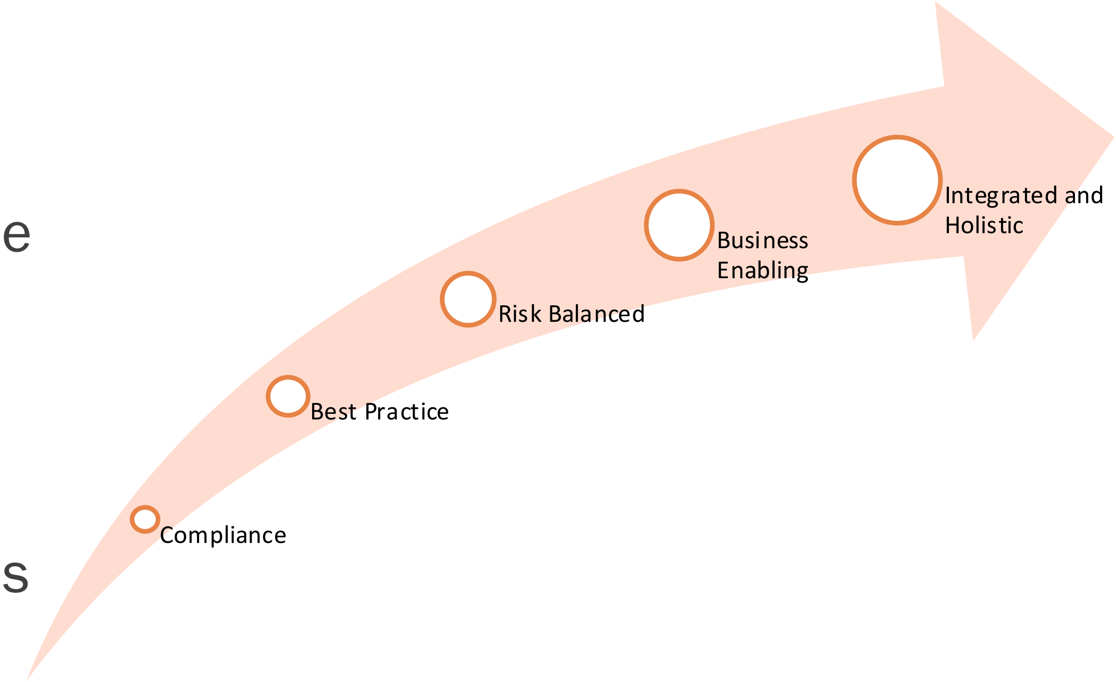
Agenda

1. An introduction to the SABSA Framework
2. Security Patterns
3. Security Architecture Program as per the C2M2
4. Q&A

WHAT IS 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 to business enabling and integrated and holistic



THE DIFFERENCE OF ENTERPRISE SECURITY ARCHITECTURE AND SECURITY SOLUTION ARCHITECTURE

Enterprise Security

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

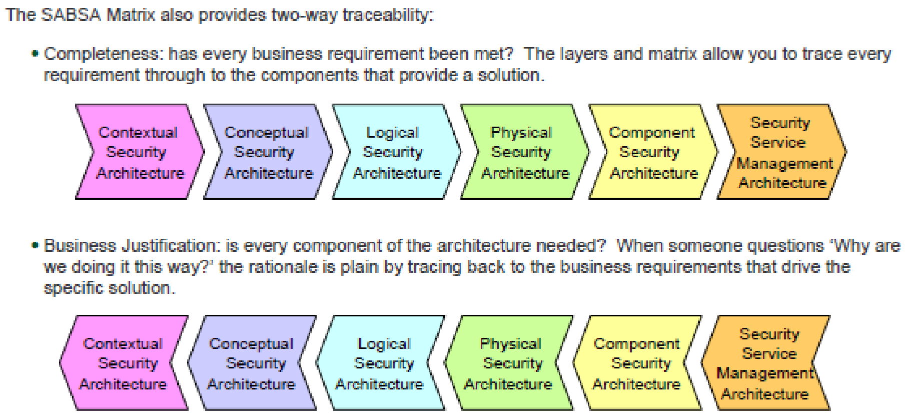
Security Solution Architecture

- A key pivot role between the whole of enterprise and delivering projects
- Focuses on producing solution designs that address cyber security requirements as per the enterprise methodology
- More than likely part of the projects team.

INTRODUCTION TO SABSA

SABSA® 101

- SABSA® has its origins as the Enterprise Security Architecture for the SWIFT Payments Network
- SABSA® is an Open Source framework and its Intellectual Property is maintained by The SABSA Institute C.I.C with a supported and active global volunteer membership
- Business Aligned, Top Down and Deliberate, not just *best practice*
- Focus on *Attributes* which are security goals/objectives/requirements
- Enables Two Way Traceability - For completeness and justification
- “The SABSA White Paper” is a fantastic resource to start with if you are new to SABSA
- The Chief Architects Blog Posts for the 21 Year History are a fantastic reference for the history of SABSA



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

Source – The SABSA White Paper

THE 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

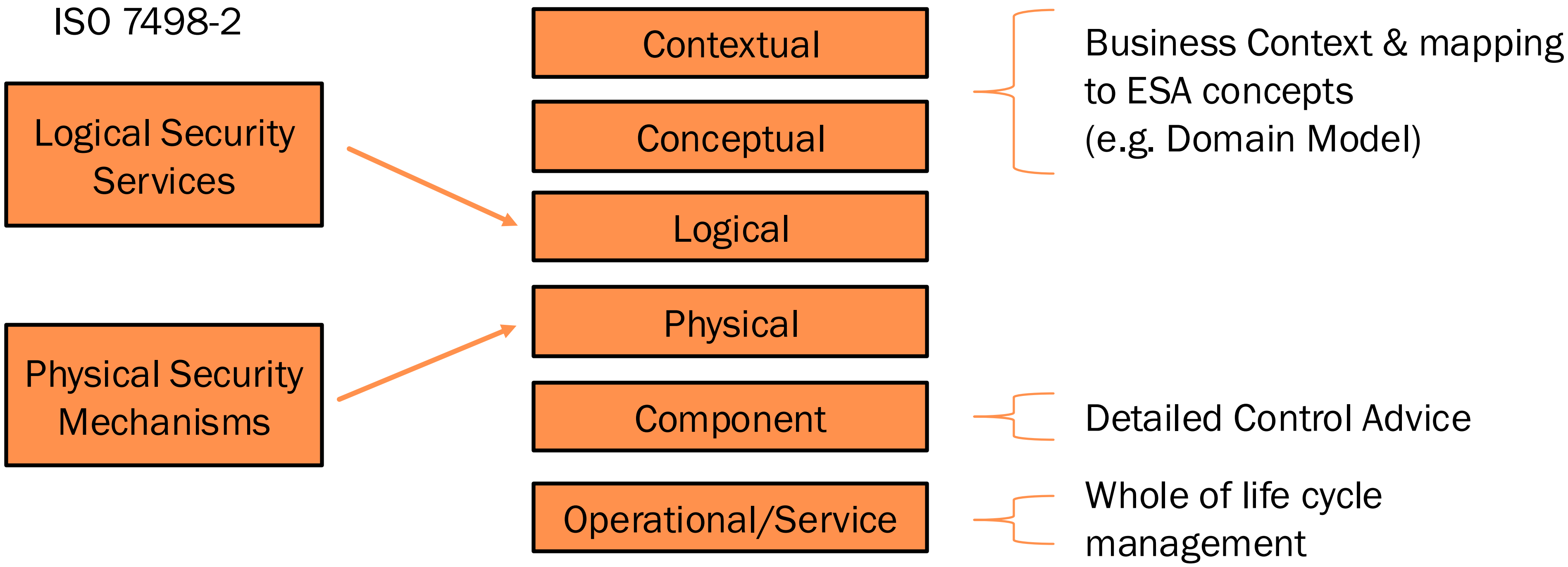
The Builder’s View

The Trades Person’s View

The Service Manager’s View

From W100 *SABSA White Paper (2009)* - https://sabsa.org/white-paper-requests/

WHY 6 LAYERS?



ISO 7498-2

Logical Security Services

Physical Security Mechanisms

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.)

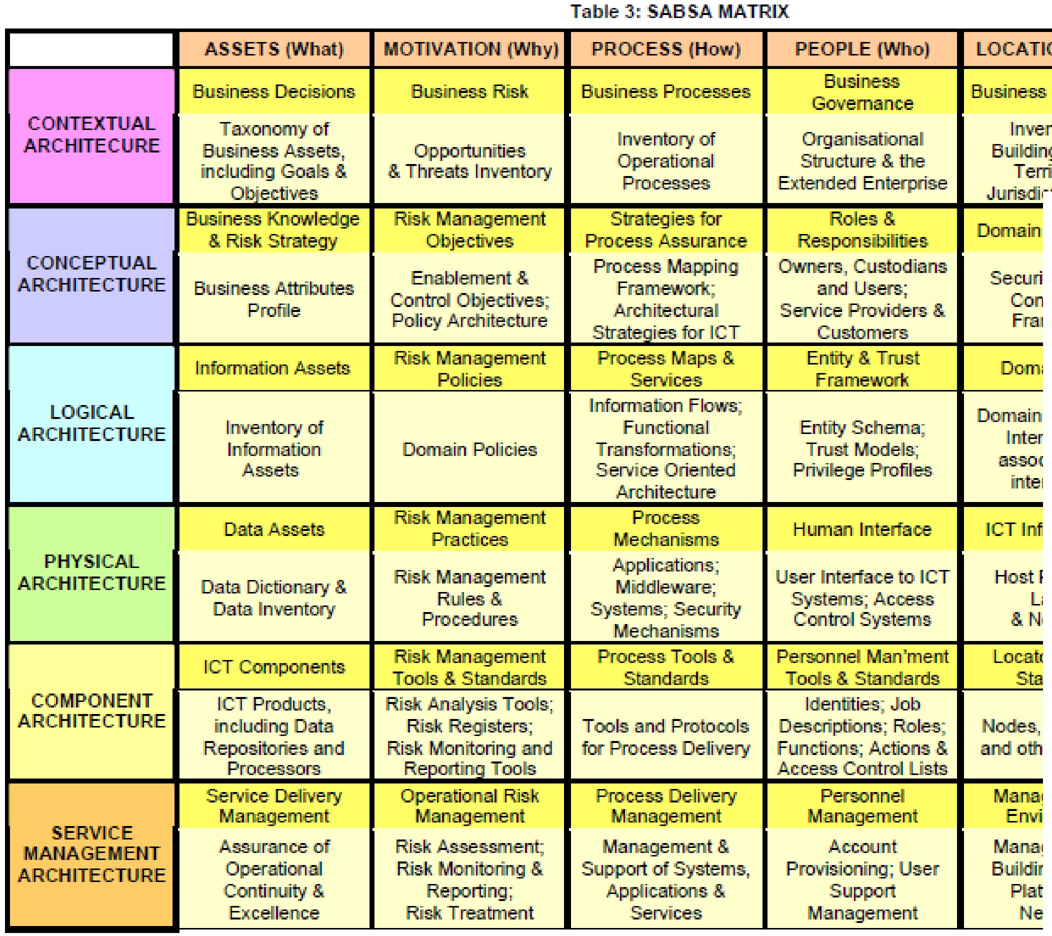


Table 3: SABSA MATRIX

	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, Jurisdictions, etc.	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 Frai	
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Doma	
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Inter assoc inter	
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 F La & N	
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locato 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	

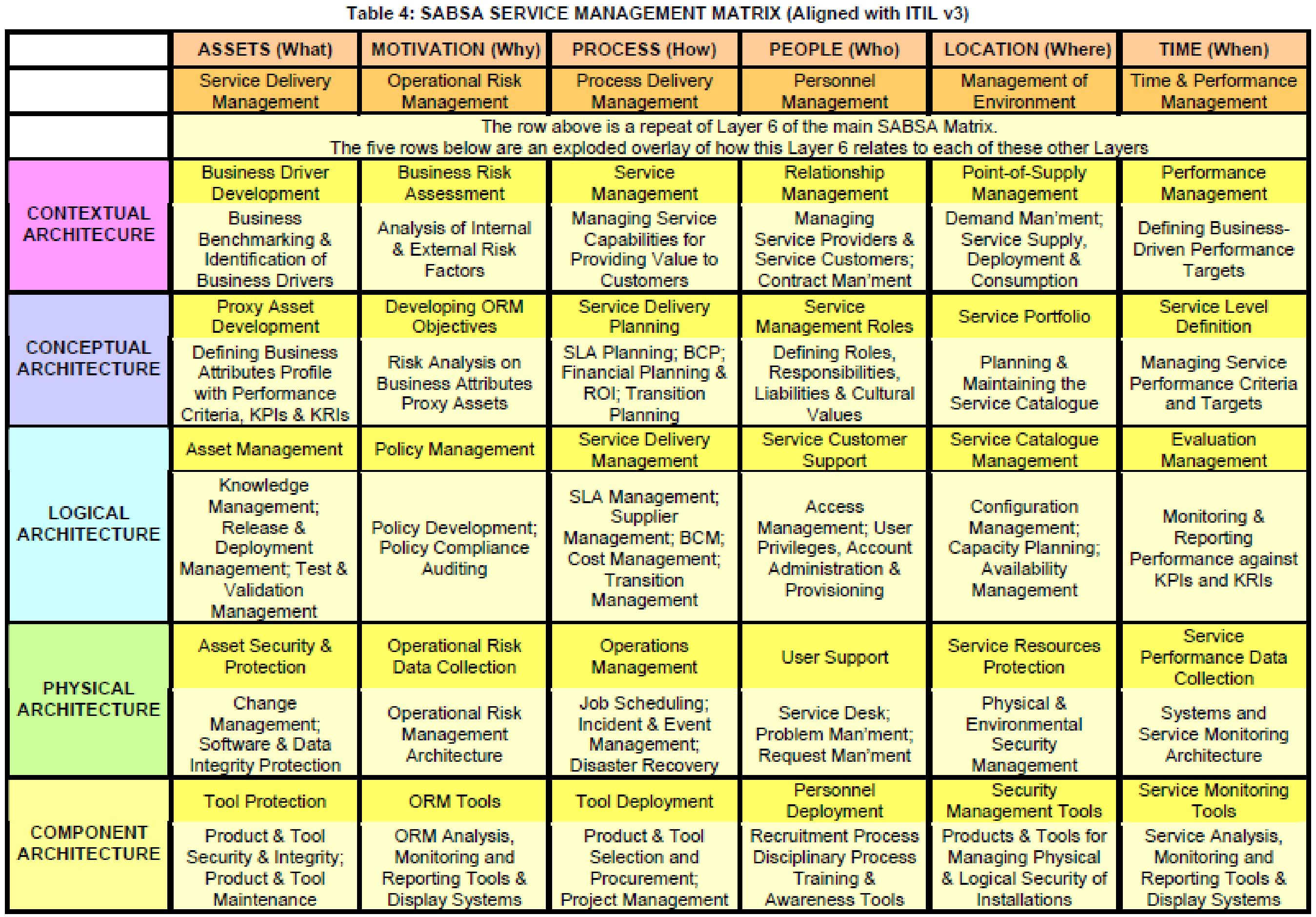
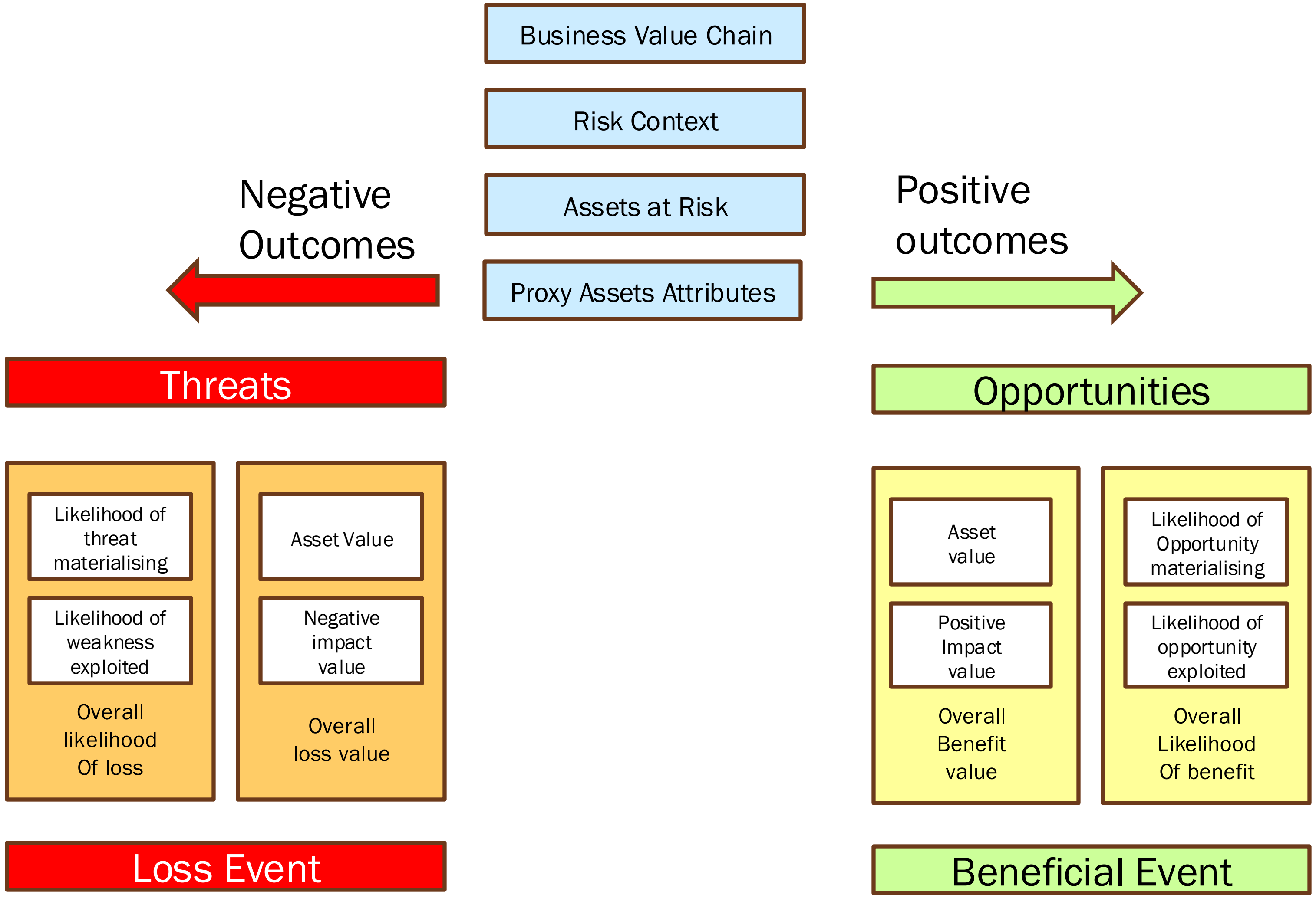


Table 4: SABSA SERVICE MANAGEMENT MATRIX (Aligned with ITIL v3)

	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

From W100 *SABSA White Paper (2009)* -
https://sabsa.org/white-paper-requests/

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

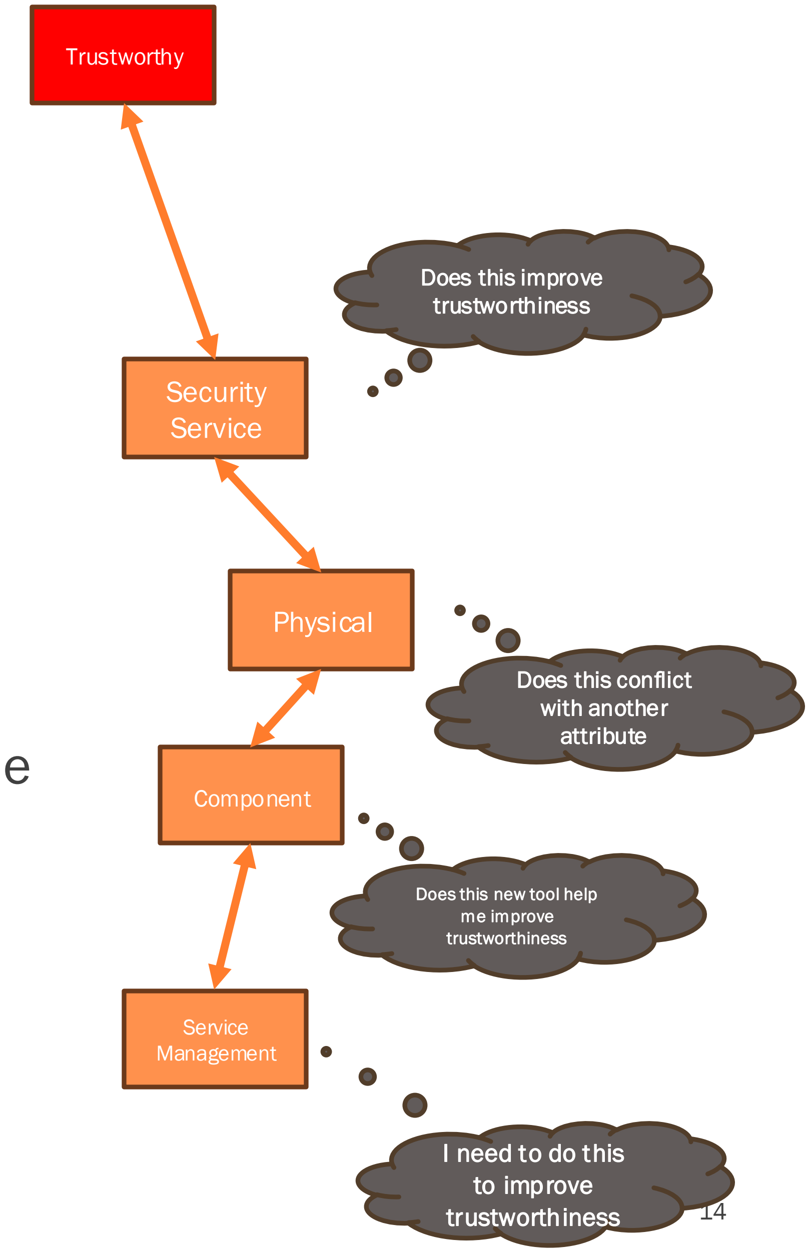
Overall Likelihood Of benefit

Beneficial Event

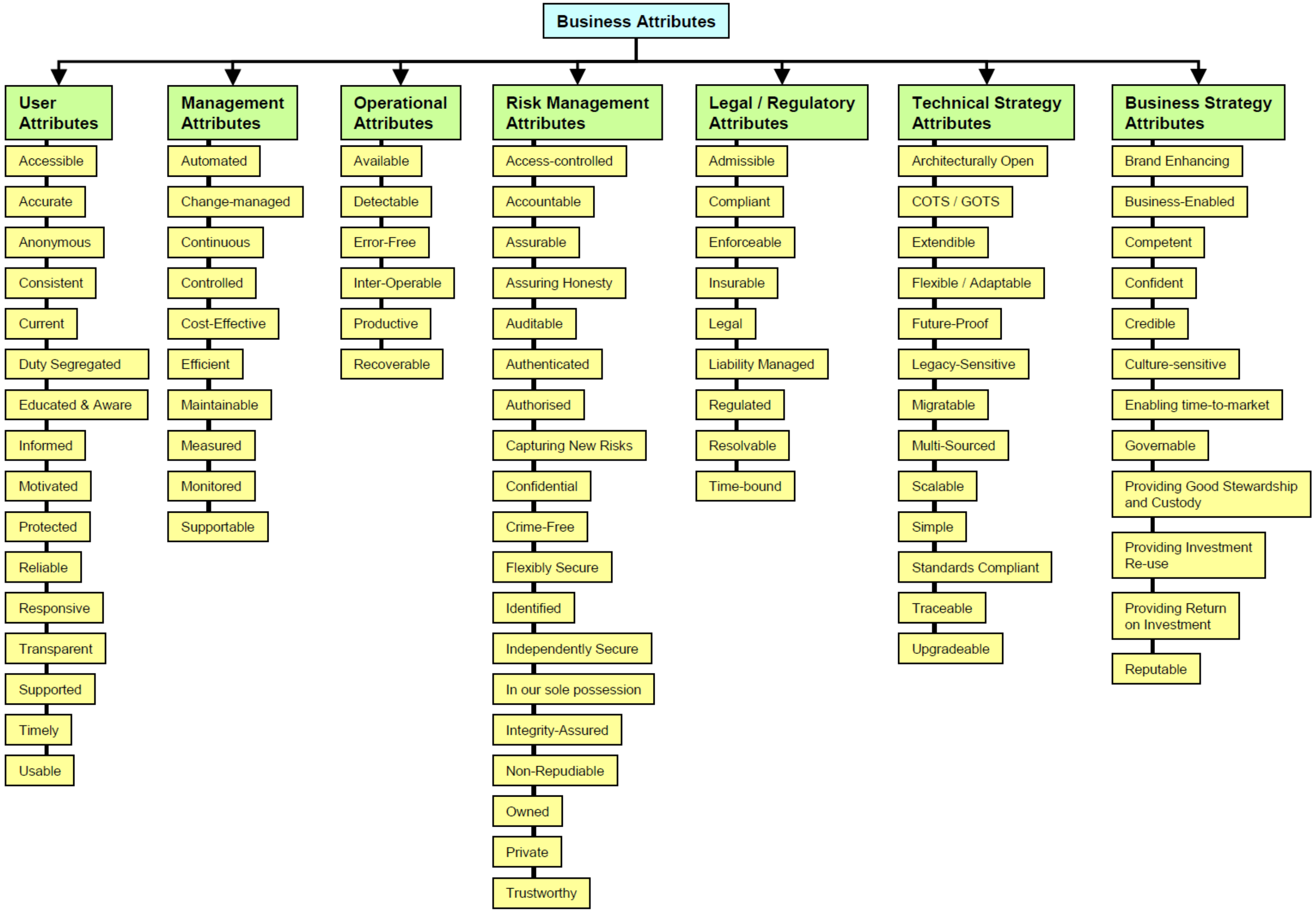
From W102 SABSA Risk Management Part One – The Meaning of Risk - https://sabsa.org/white-paper-requests/

SABSA ATTRIBUTES

- SABSA Attributes are 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
- But it is esoteric … so maybe don't start with them!


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

THE INITIAL 85 SABSA ATTRIBUTES



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

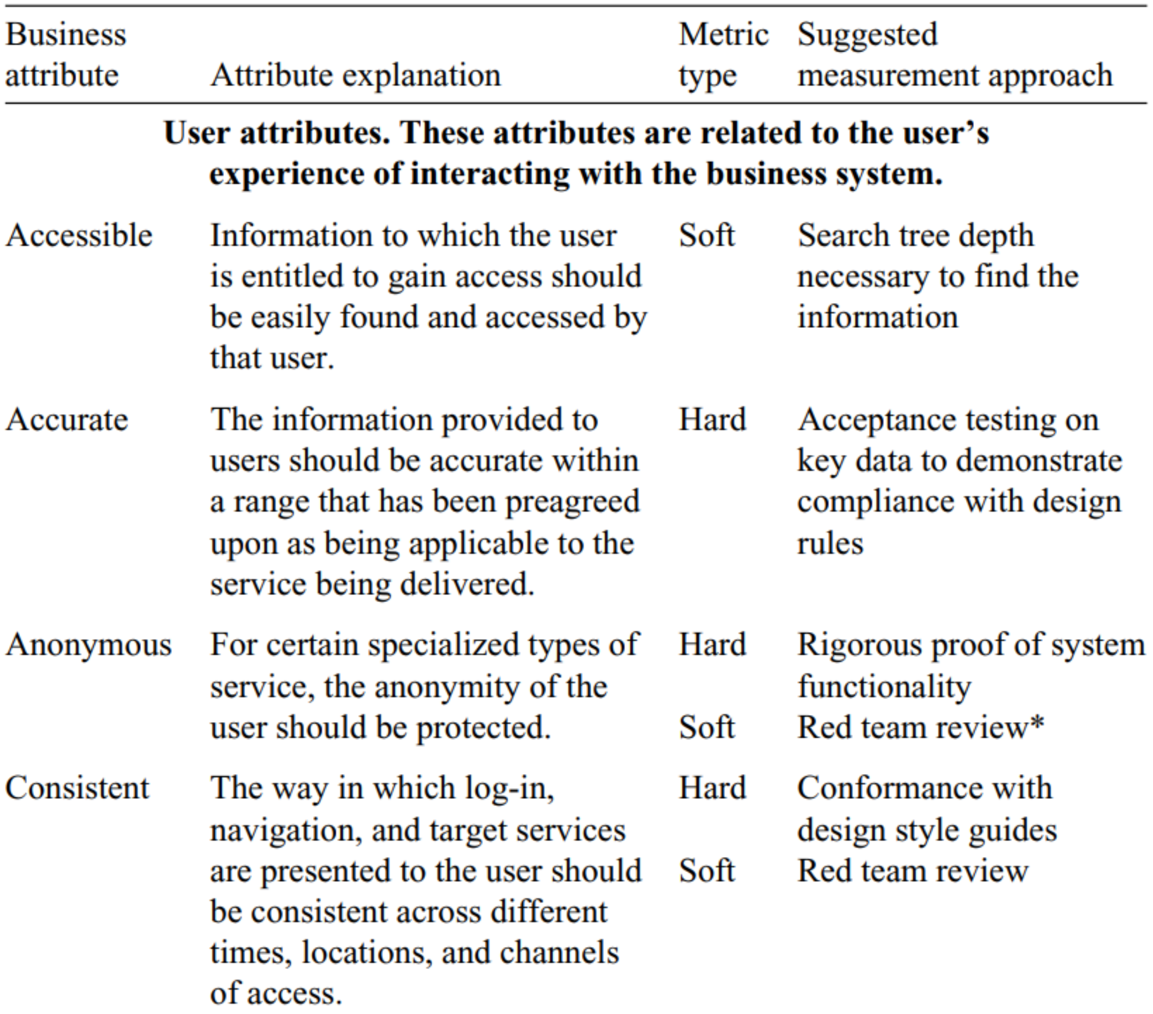
Business Strategy Attributes
- Brand Enhancing
- Business-Enabled
- Competent
- Confident
- Credible
- Culture-sensitive
- Enabling time-to-market
- Governable
- Providing Good Stewardship and Custody
- Providing Investment Re-use
- Providing Return on Investment
- Reputable

Figure 4: The SABSA Taxonomy of ICT Business Attributes

From W100 *SABSA White Paper (2009)* - https://sabsa.org/white-paper-requests/

EXAMPLE ATTRIBUTE DEFINITIONS

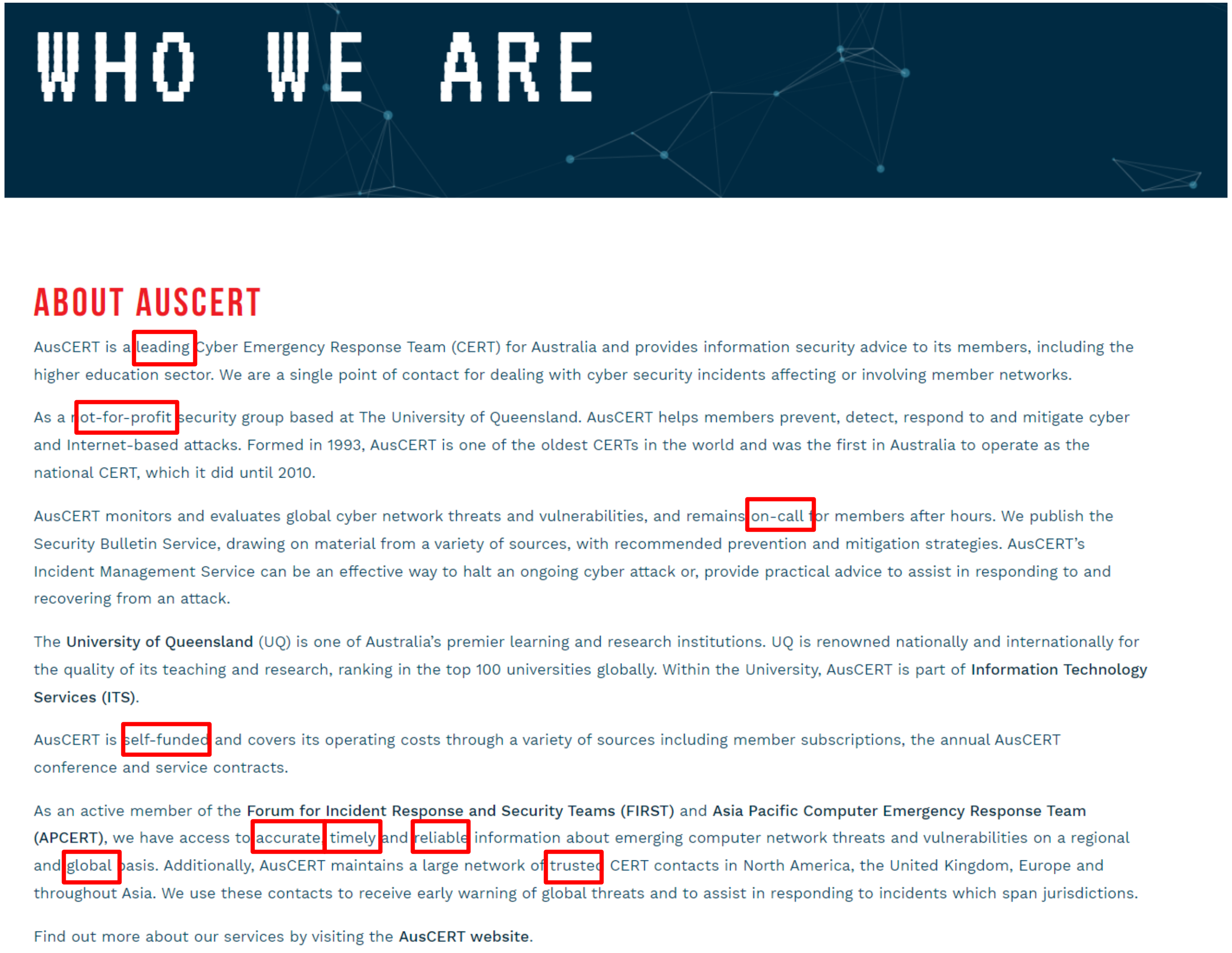
- Defines the Name, Definition and Suggested Metric Measurement approach
- Critical that an Attribute can be measured and Measurement Thresholds be defined
- You can find these definitions by searching for “Wiley SABSA Attributes”



Business attribute	Attribute explanation	Metric type	Suggested measurement approach
	User attributes. These attributes are related to the user’s experience of interacting with the business system.		
Accessible	Information to which the user is entitled to gain access should be easily found and accessed by that user.	Soft	Search tree depth necessary to find the information
Accurate	The information provided to users should be accurate within a range that has been preagreed upon as being applicable to the service being delivered.	Hard	Acceptance testing on key data to demonstrate compliance with design rules
Anonymous	For certain specialized types of service, the anonymity of the user should be protected.	Hard Soft	Rigorous proof of system functionality Red team review*
Consistent	The way in which log-in, navigation, and target services are presented to the user should be consistent across different times, locations, and channels of access.	Hard Soft	Conformance with design style guides Red team review

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

A PRO TIP FOR IDENTIFYING ATTRIBUTES



WHO WE ARE

ABOUT AUSCERT

AusCERT is a leading Cyber Emergency Response Team (CERT) for Australia and provides information security advice to its members, including the higher education sector. We are a single point of contact for dealing with cyber security incidents affecting or involving member networks.

As a not-for-profit security group based at The University of Queensland. AusCERT helps members prevent, detect, respond to and mitigate cyber and Internet-based attacks. Formed in 1993, AusCERT is one of the oldest CERTs in the world and was the first in Australia to operate as the national CERT, which it did until 2010.

AusCERT monitors and evaluates global cyber network threats and vulnerabilities, and remains on-call for members after hours. We publish the Security Bulletin Service, drawing on material from a variety of sources, with recommended prevention and mitigation strategies. AusCERT's Incident Management Service can be an effective way to halt an ongoing cyber attack or, provide practical advice to assist in responding to and recovering from an attack.

The **University of Queensland** (UQ) is one of Australia's premier learning and research institutions. UQ is renowned nationally and internationally for the quality of its teaching and research, ranking in the top 100 universities globally. Within the University, AusCERT is part of **Information Technology Services (ITS)**.

AusCERT is self-funded and covers its operating costs through a variety of sources including member subscriptions, the annual AusCERT conference and service contracts.

As an active member of the **Forum for Incident Response and Security Teams (FIRST)** and **Asia Pacific Computer Emergency Response Team (APCERT)**, we have access to accurate, timely and reliable information about emerging computer network threats and vulnerabilities on a regional and global basis. Additionally, AusCERT maintains a large network of trusted CERT contacts in North America, the United Kingdom, Europe and throughout Asia. We use these contacts to receive early warning of global threats and to assist in responding to incidents which span jurisdictions.

Find out more about our services by visiting the **AusCERT website**.

Credit Rob Laurie SCM for sharing his approach

CASE STUDY INTRODUCTION

THE STATE POWER CORPORATION

STATE POWER CORPORATION BACKGROUND

- *State Power Corporation* (SPC) owns, operates and maintains the electricity generation, transmission and distribution assets for the state
- The corporation is about to celebrate its 100th year anniversary and the current organisation is the amalgamation of multiple smaller government entities through it's life
- A change in government policy and economic conditions means SPC is investigating selling its existing fossil fuel assets to fund a 100% renewable assets electricity generation portfolio
- There has been a recent cyber security incident in it's electricity generation portfolio and the organisation is looking to conduct a root cause analysis to prevent a similar incident in it's other assets
- SPC has an inflight Digital Transformation program that is delivering change in both the IT and OT environments
- We have been engaged by the SPC Group CISO to articulate the Enterprise Conceptual Security Architecture and to inform their 5 year Security Management program

STATE POWER CORPORATION BACKGROUND (CONT.)

- Energy Market Strategy and Research and Development
- Energy System Planning and Asset Strategy
- Engineering Design and Procurement
- Electricity Generation Operations
- Electricity Network Operations
- Enterprise Group Support Services

EXAMPLE ATTRIBUTES – STATE POWER CORPORATION

Attribute	Definition
Providing Good Stewardship	Protecting other parties with whom we do business from abuse, loss of business, or personal information of value to those parties through inadequate stewardship on our part.
Reliable	The services provided to the user should be delivered at a reliable level of quality
Available	The information and services provided by the system should be available according to the requirements specified in the service-level agreement (SLA).
Multi-sourced	Critical system components should be obtainable from more than one source, to protect against the risk of the single source of supply and support being withdrawn.
Supported	When a user has problems or difficulties in using the system or its services, there should be a means by which the user can receive advice and support so that the problems can be resolved to the satisfaction of the user.
Architecturally Open	The system architecture should wherever possible, not be locked into specific vendor interface standards and should allow flexibility in the choice of vendors and products, both initially and in the future

EXERCISE 1 – DEVELOP AN EXAMPLE ATTRIBUTE PROFILE

In this exercise you can either use your company or use the 2032 Brisbane Olympics as an example.

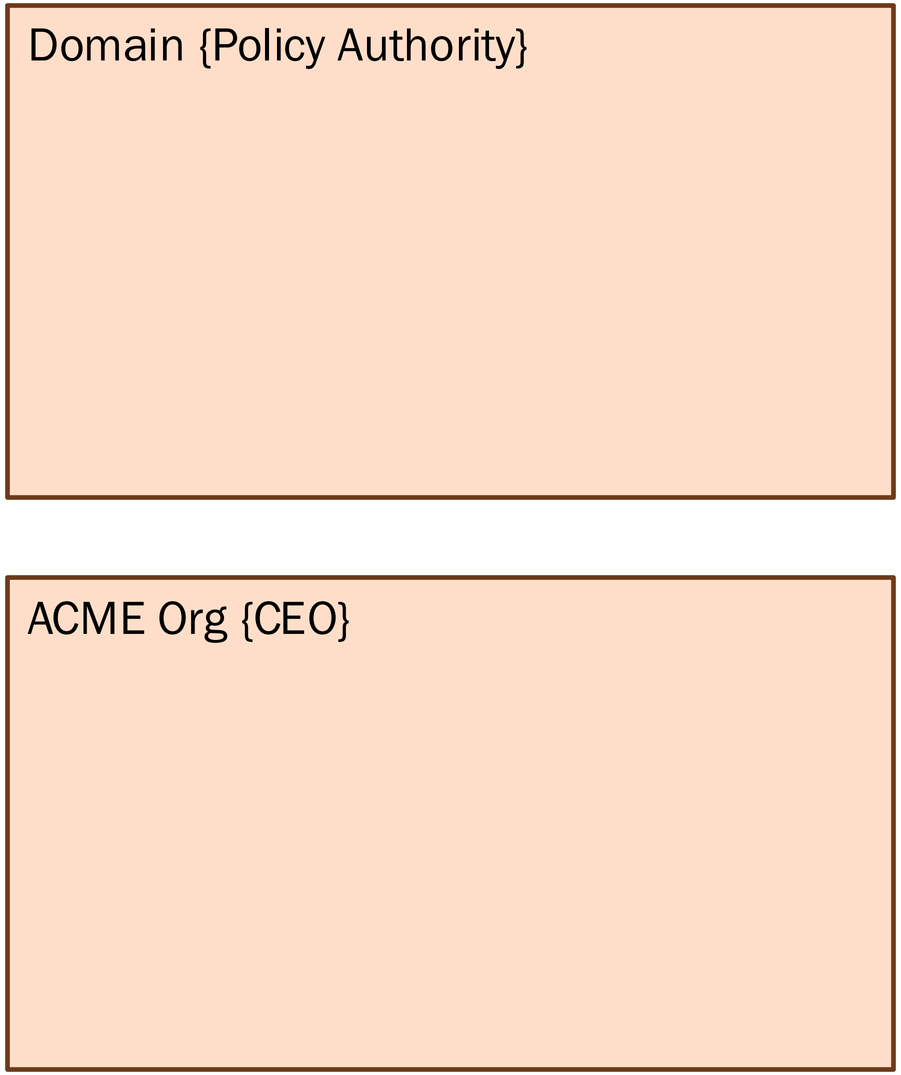
Develop 6 Attributes you think are relevant for your scenario and think about of methods of measurement

You will have 20 minutes for this exercise and then 10 minutes to discuss with your table

A useful reference for all the Attributes is – (Google Wiley SABSA attributes) - but also feel free to create your own (Max 2 New Attributes)

DOMAIN MODELLING

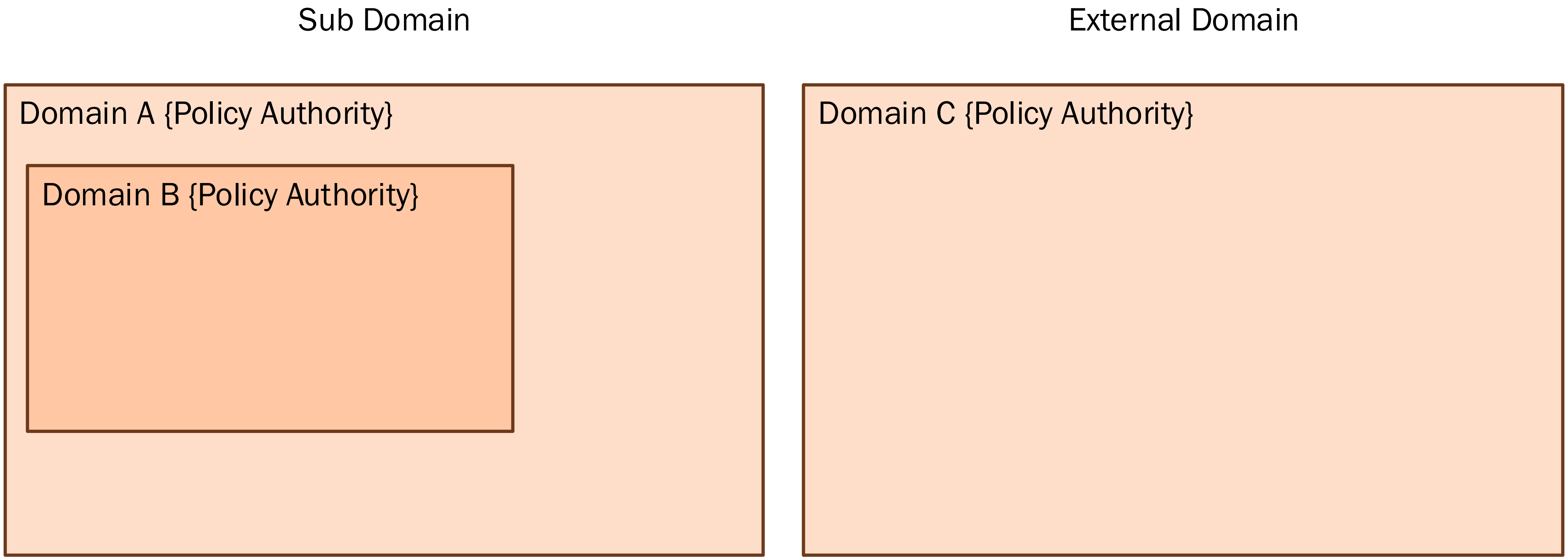
- I find domain modelling the most useful tool in my SABSA toolbox
- It can be used for multiple dimensions but the most useful is to understand Policy Architecture
- Domain – “A set of assets under a common policy”
- Policy Authority – The Accountable Entity for the Domain



Domain {Policy Authority}

ACME Org {CEO}

DOMAIN RELATIONSHIPS



Sub Domain

Domain A {Policy Authority}

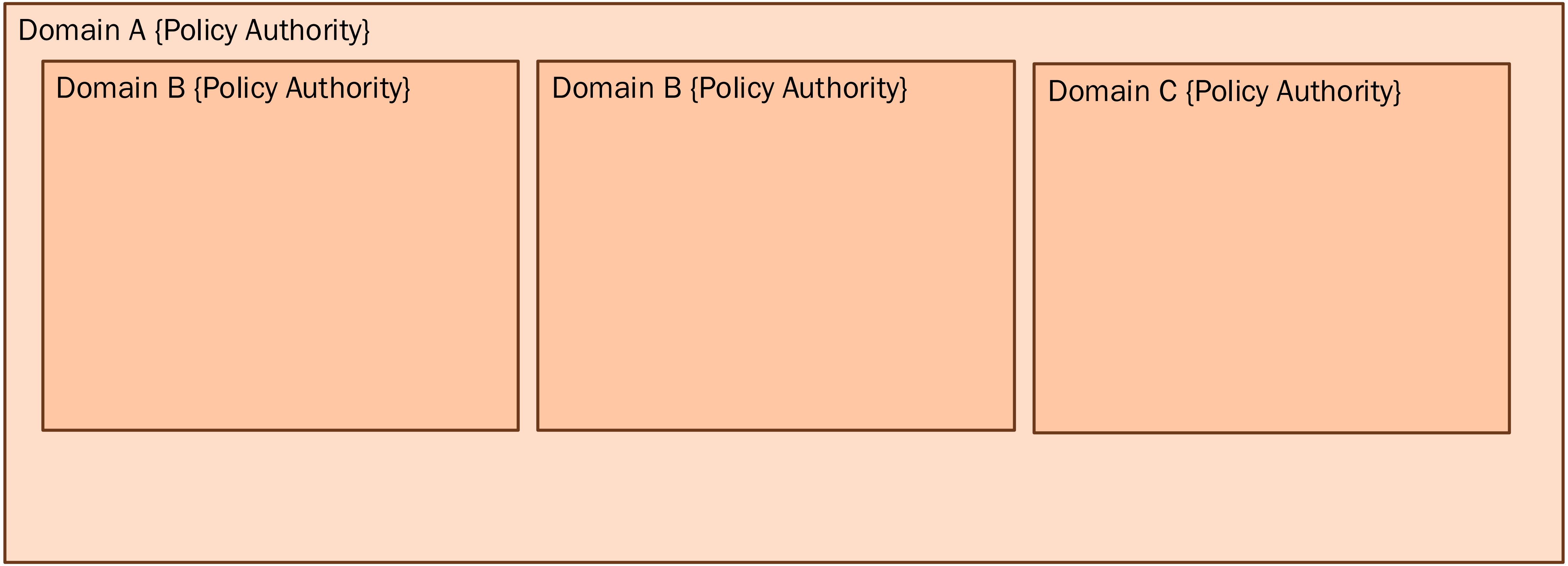
Domain B {Policy Authority}

External Domain

Domain C {Policy Authority}

DOMAIN RELATIONSHIPS

Peer Domains



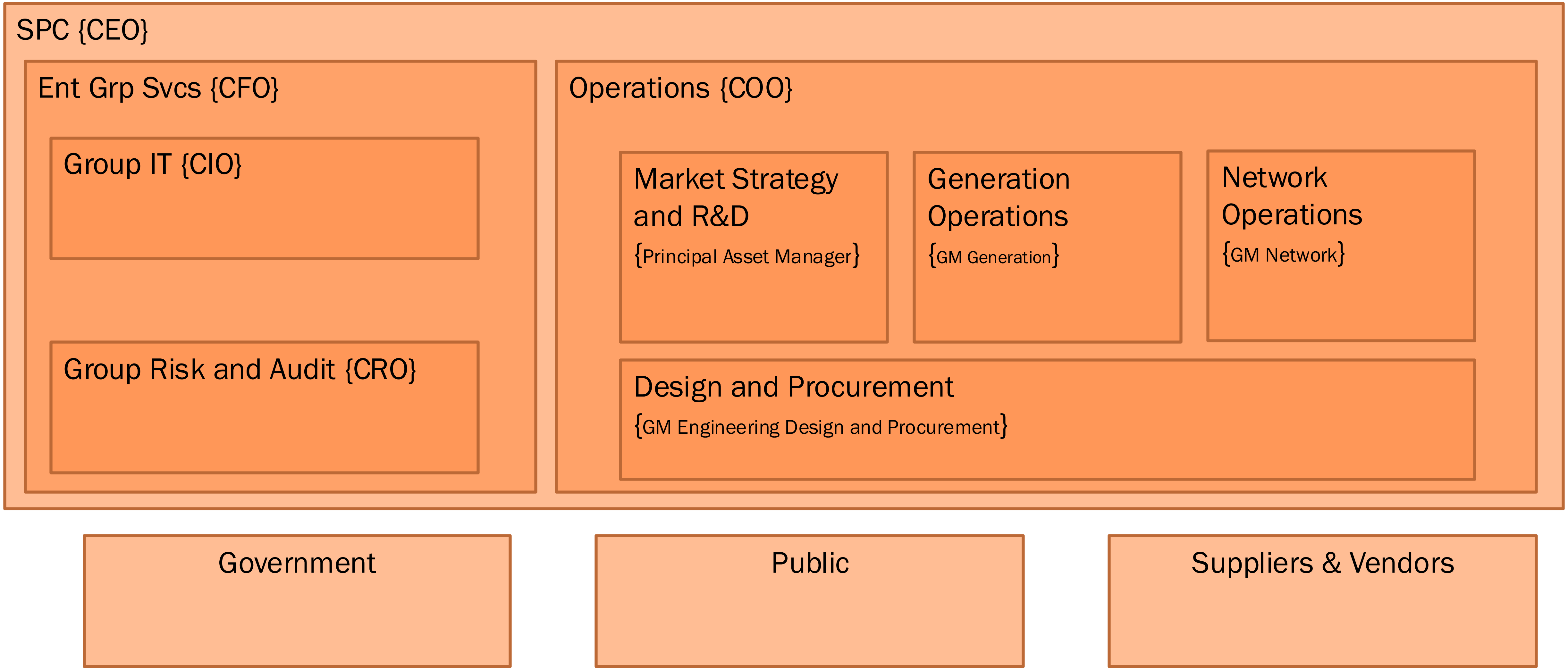
Domain A {Policy Authority}

Domain B {Policy Authority}

Domain B {Policy Authority}

Domain C {Policy Authority}

WORKED EXAMPLE – STATE POWER CORPORATION



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}

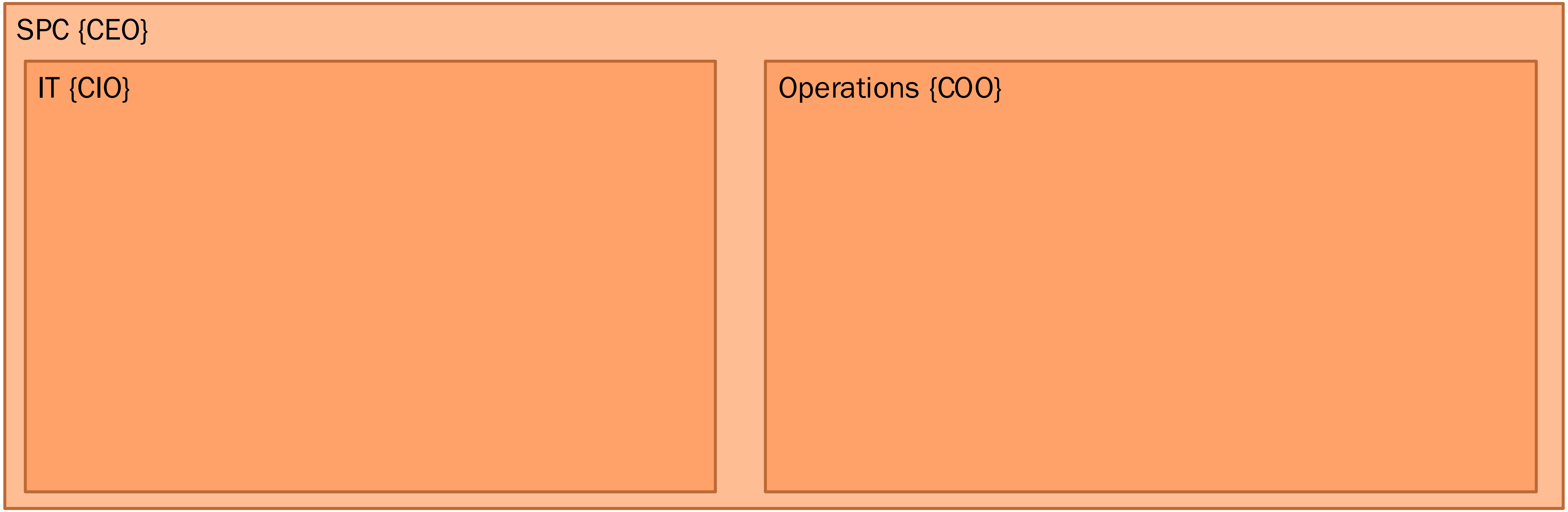
Design and Procurement {GM Engineering Design and Procurement}

Government

Public

Suppliers & Vendors

USEFUL FOR UNDERSTANDING IT/OT CONVERGENCE RISK



SPC {CEO}

IT {CIO}

Operations {COO}

EXERCISE 2 – BUILD A DOMAIN MODEL

For this exercise, either use your company example or the 2032 Olympics as an example

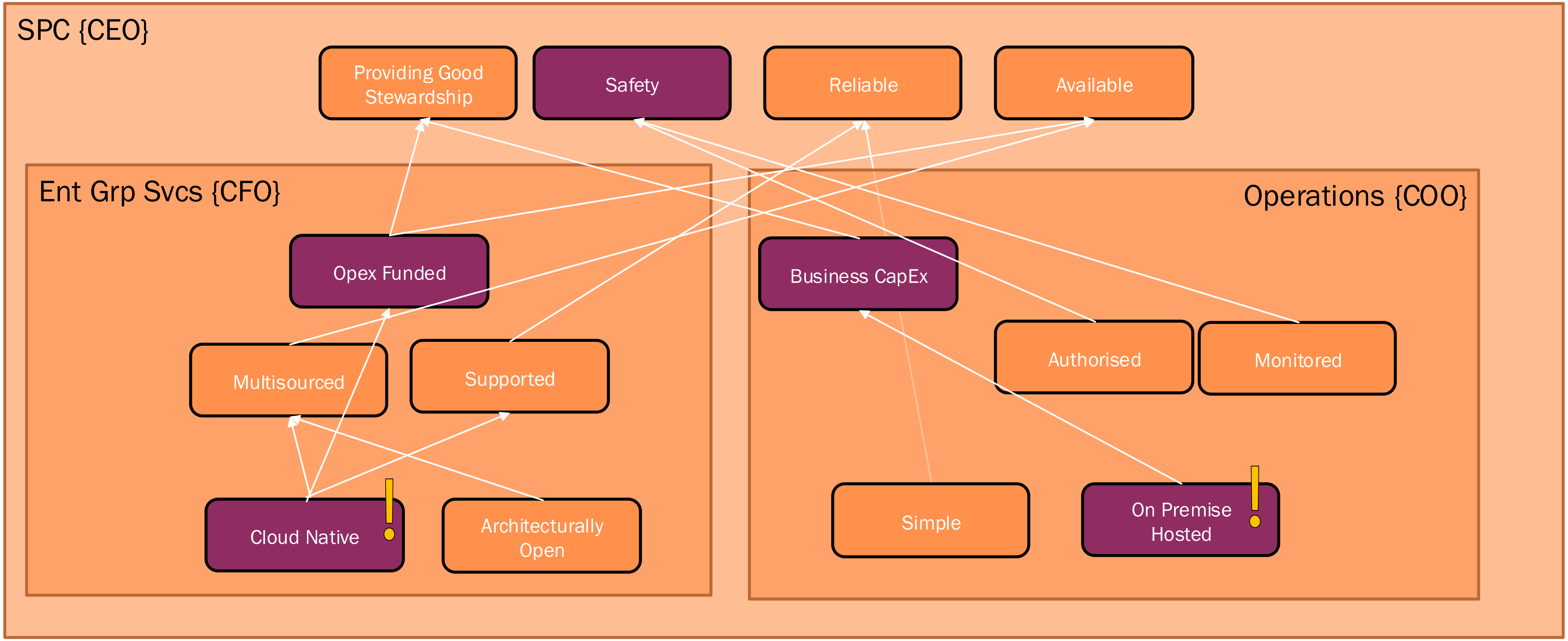
20 Minutes to define your Domain Model and we can discuss as a group for 10 minutes

Note – don’t fall for the trap of just making it the org chart …

TYING IT TOGETHER – MULTI-TIERED ATTRIBUTES

- You can overlay Attributes applicable to domains and model their dependencies
- This creates a very powerful view for stakeholders to understand the interdepdencies of security decisions between different viewpoints
- This also helps with how to communicate with stakeholders
  - "Use the language of the stakeholder" – for example, do not talk to Technical Security Metrics to the Executive Leadership team

EXAMPLE – STATE POWER CORPORATION



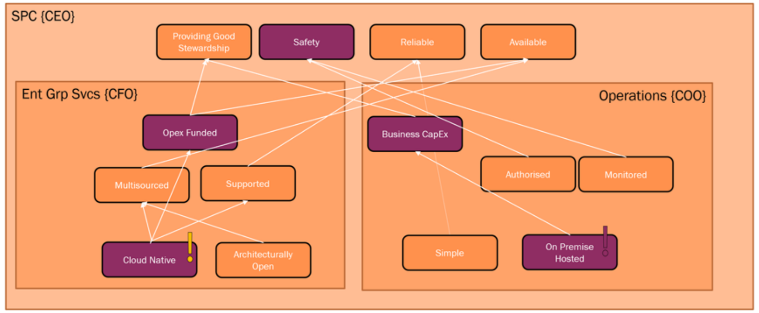
EXERCISE 3 – BUILD A MULTI-TIER ATTRIBUTE MODEL

In this exercise, take your original Attribute Profile and your domain model and overlay the Attributes – think about how the attributes relate to each other

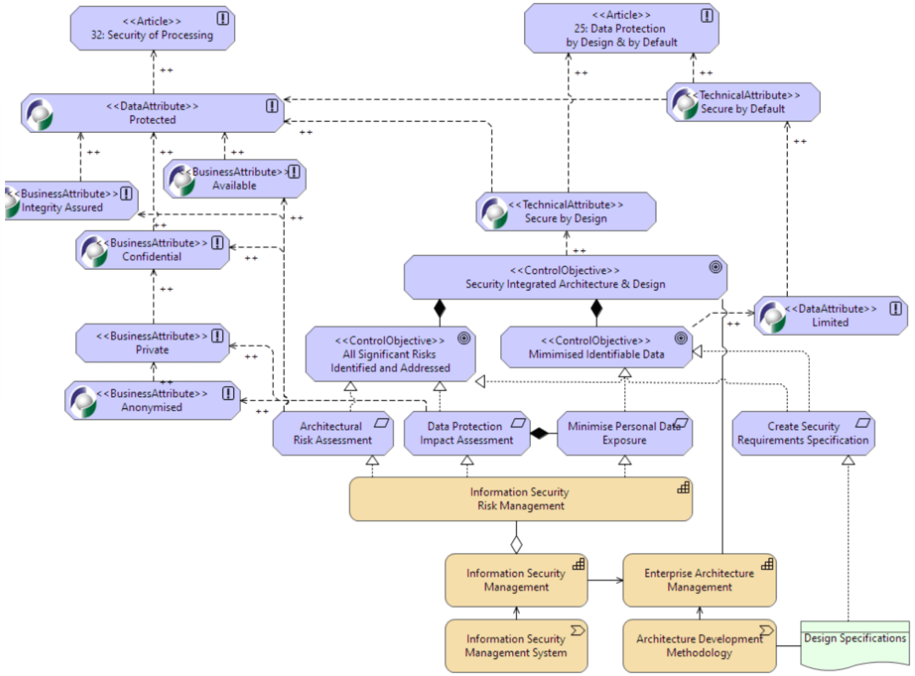
You will have 10 minutes to do this and then 10 minutes to discuss

EXAMPLE SABSA TOOLS

Powerpoint and Word Docs

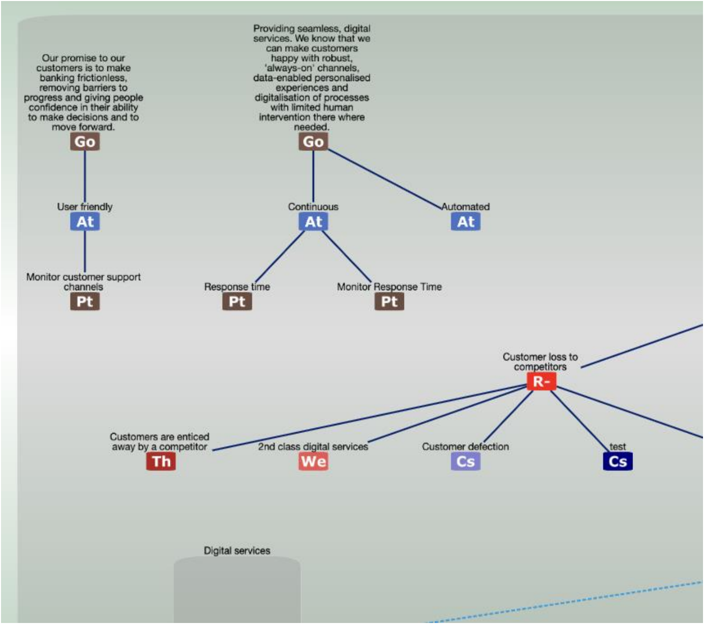


ArchiMate™


<<Article>>
32: Security of Processing
<<Article>>
25: Data Protection by Design & by Default
<<DataAttribute>>
Protected
<<TechnicalAttribute>>
Secure by Default
<<BusinessAttribute>>
Available
<<BusinessAttribute>>
Integrity Assured
<<TechnicalAttribute>>
Secure by Design
<<BusinessAttribute>>
Confidential
<<ControlObjective>>
Security Integrated Architecture & Design
<<DataAttribute>>
Limited
<<BusinessAttribute>>
Private
<<ControlObjective>>
All Significant Risks Identified and Addressed
<<ControlObjective>>
Mimimised Identifiable Data
<<BusinessAttribute>>
Anonymised
Architectural Risk Assessment
Data Protection Impact Assessment
Minimise Personal Data Exposure
Create Security Requirements Specification
Information Security Risk Management
Information Security Management
Enterprise Architecture Management
Information Security Management System
Architecture Development Methodology
Design Specifications
++

Ref - https://sabsacourses.com/sabsa-training/sabsa-model/

HelloRisk™

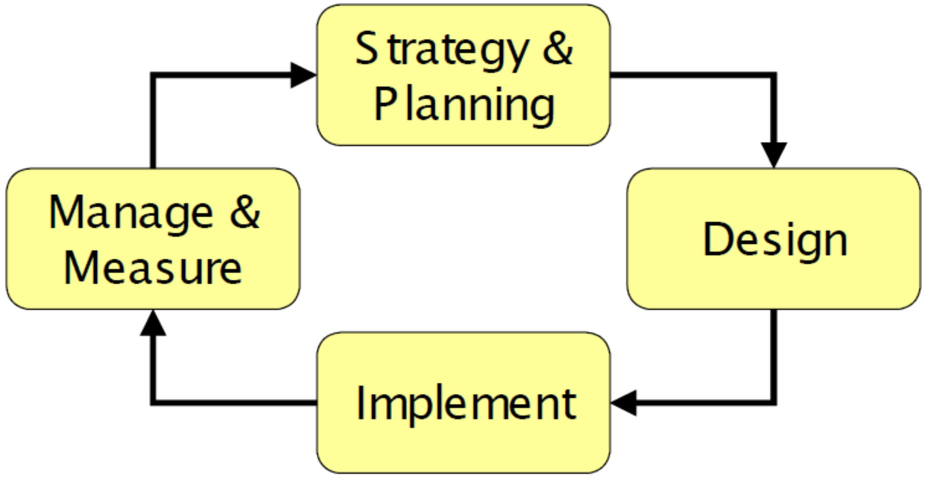


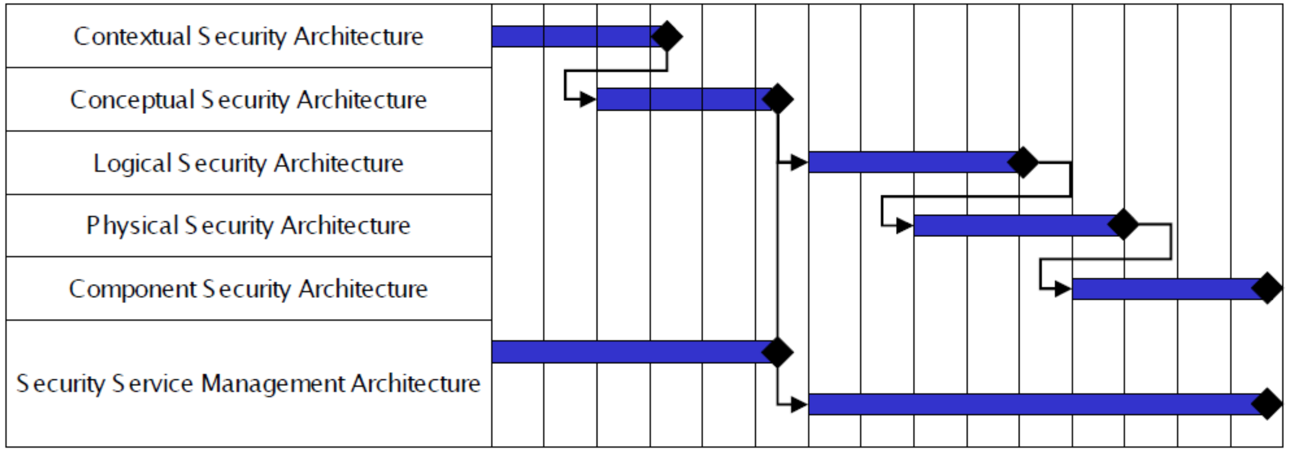
Our promise to our customers is to make banking frictionless, removing barriers to progress and giving people confidence in their ability to make decisions and to move forward.

Providing seamless, digital services. We know that we can make customers happy with robust, 'always-on' channels, data-enabled personalised experiences and digitalisation of processes with limited human intervention there where needed.

Ref - https://hellorisk.net/

HOW TO DELIVER A SABSA ARCHITECTURE?



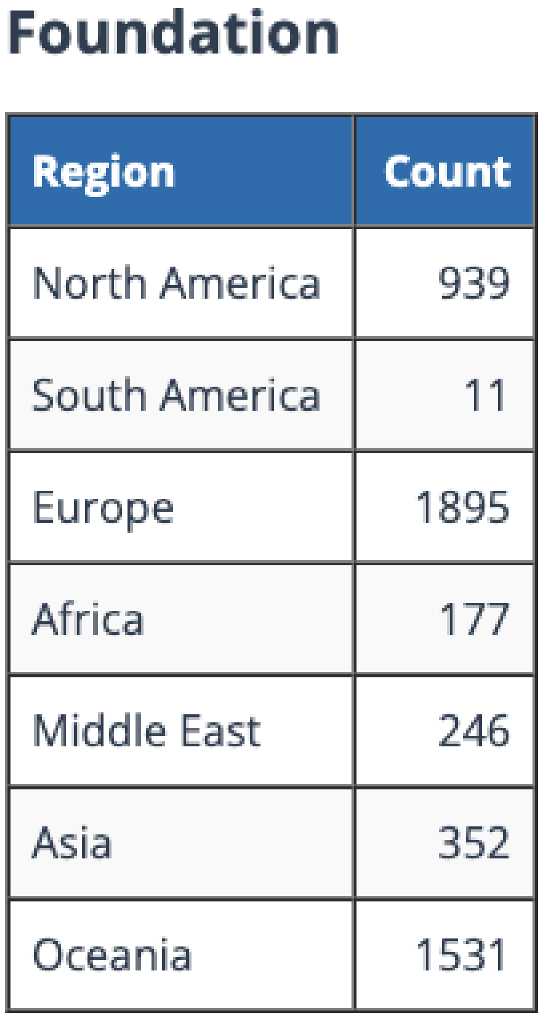


From W100 *SABSA White Paper (2009)* - https://sabsa.org/white-paper-requests/

SABSA FAST TRACK

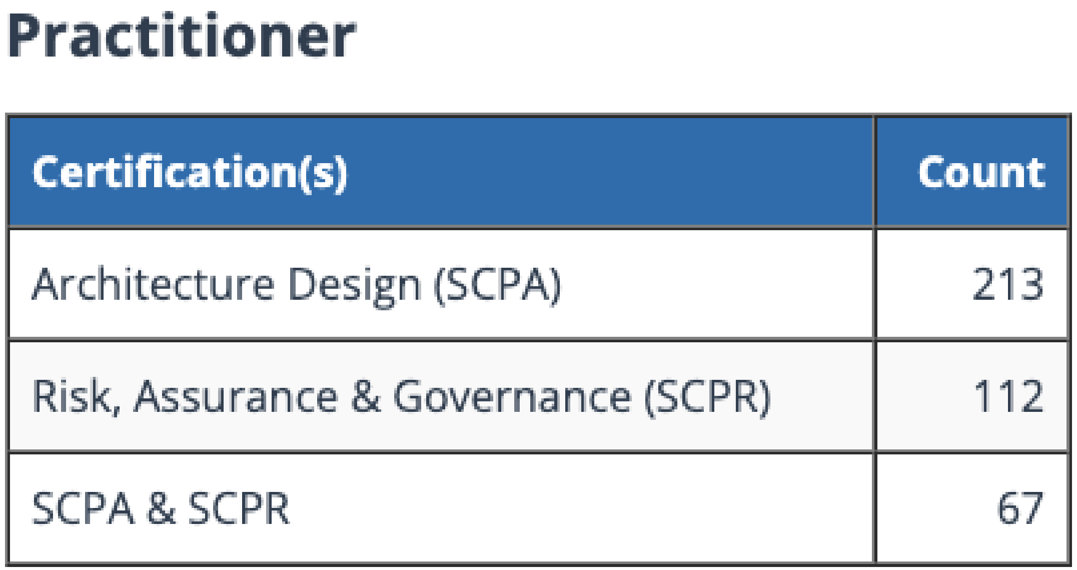
- Methodology to limit the scope to quickly deliver value via a Proof of Concept ESA
- Relies on intensive time-boxed expert facilitated workshops
- Should make use of software tools and automation
- There is some information regarding the approach outlined in the SABSA F1 & F2 training materials and the “Blue Book”

HOW MANY PEOPLE USE SABSA? THE SABSA CENSUS



Foundation

Region	Count
North America	939
South America	11
Europe	1895
Africa	177
Middle East	246
Asia	352
Oceania	1531



Practitioner

Certification(s)	Count
Architecture Design (SCPA)	213
Risk, Assurance & Governance (SCPR)	112
SCPA & SCPR	67

Figures as at Aug 2023 - https://sabsa.org/sabsa-census/

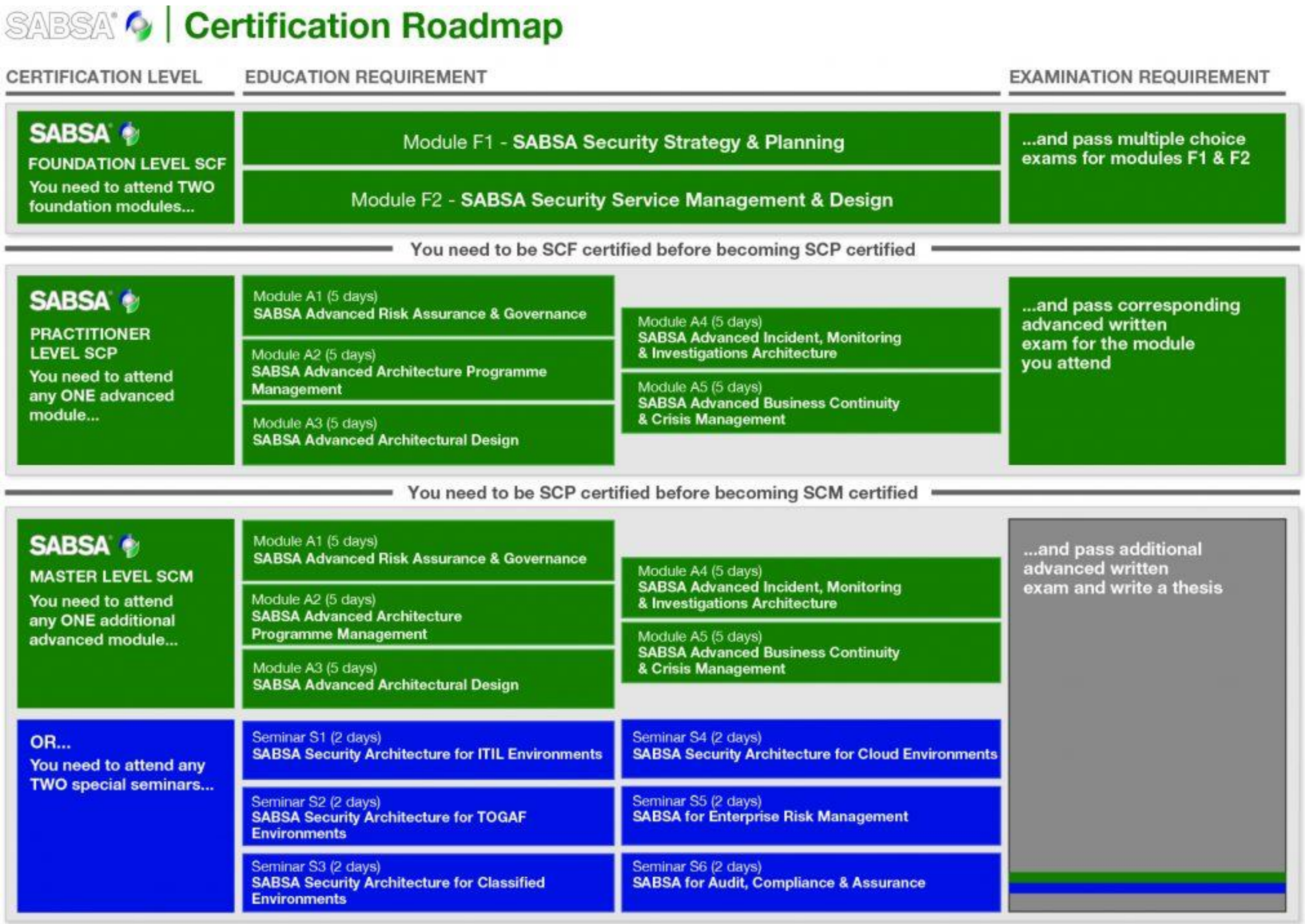
SABSA CERTIFICATION LEVELS & BLOOMS TAXONOMY

SABSA Chartered Architect Foundation SCF

SABSA Chartered Architect Practitioner Architecture Design & Development SCPA

SABSA Chartered Architect Practitioner Risk, Assurance & Governance SCPR

SABSA Chartered Architect Master SCM



SABSA | Certification Roadmap

CERTIFICATION LEVEL

EDUCATION REQUIREMENT

EXAMINATION REQUIREMENT

SABSA FOUNDATION LEVEL SCF
You need to attend TWO foundation modules...

Module F1 - SABSA Security Strategy & Planning

Module F2 - SABSA Security Service Management & Design

...and pass multiple choice exams for modules F1 & F2

You need to be SCF certified before becoming SCP certified

SABSA PRACTITIONER LEVEL SCP
You need to attend any ONE advanced module...

Module A1 (5 days)
SABSA Advanced Risk Assurance & Governance

Module A2 (5 days)
SABSA Advanced Architecture Programme Management

Module A3 (5 days)
SABSA Advanced Architectural Design

Module A4 (5 days)
SABSA Advanced Incident, Monitoring & Investigations Architecture

Module A5 (5 days)
SABSA Advanced Business Continuity & Crisis Management

...and pass corresponding advanced written exam for the module you attend

You need to be SCP certified before becoming SCM certified

SABSA MASTER LEVEL SCM
You need to attend any ONE additional advanced module...

Module A1 (5 days)
SABSA Advanced Risk Assurance & Governance

Module A2 (5 days)
SABSA Advanced Architecture Programme Management

Module A3 (5 days)
SABSA Advanced Architectural Design

Module A4 (5 days)
SABSA Advanced Incident, Monitoring & Investigations Architecture

Module A5 (5 days)
SABSA Advanced Business Continuity & Crisis Management

OR...
You need to attend any TWO special seminars...

Seminar S1 (2 days)
SABSA Security Architecture for ITIL Environments

Seminar S2 (2 days)
SABSA Security Architecture for TOGAF Environments

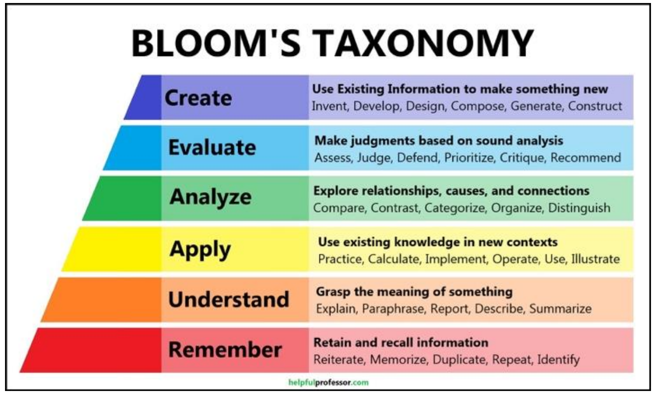
Seminar S3 (2 days)
SABSA Security Architecture for Classified Environments

Seminar S4 (2 days)
SABSA Security Architecture for Cloud Environments

Seminar S5 (2 days)
SABSA for Enterprise Risk Management

Seminar S6 (2 days)
SABSA for Audit, Compliance & Assurance

...and pass additional advanced written exam and write a thesis



BLOOM'S TAXONOMY

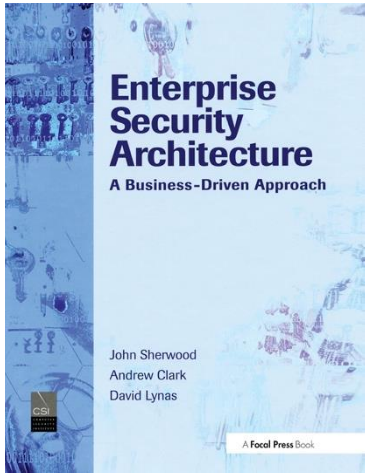
Create	Use Existing Information to make something new	Invent, Develop, Design, Compose, Generate, Construct
Evaluate	Make judgments based on sound analysis	Assess, Judge, Defend, Prioritize, Critique, Recommend
Analyze	Explore relationships, causes, and connections	Compare, Contrast, Categorize, Organize, Distinguish
Apply	Use existing knowledge in new contexts	Practice, Calculate, Implement, Operate, Use, Illustrate
Understand	Grasp the meaning of something	Explain, Paraphrase, Report, Describe, Summarize
Remember	Retain and recall information	Reiterate, Memorize, Duplicate, Repeat, Identify

helpfulprofessor.com

Ref - https://sabsa.org/certification/, https://sabsa.org/digital-badges/, https://helpfulprofessor.com/levels-of-understanding/

FURTHER SABSA RESOURCES

- The SABSA White paper (W100) https://sabsa.org/white-paper-requests/
- The "Bluebook“ (Enterprise Security Architecture – A Business-Driven Approach) https://www.amazon.com.au/Enterprise-Security-Architecture-Business-Driven-Approach/dp/157820318X
- Connect with SABSA World Australia – We have meetups, resources and a Discord Group - https://www.sabsaworldaus.org/
- Come to COSAC (Melbourne or Ireland) – it is the conference for SABSA security architects



HOMEWORK – USING SABSA IN YOUR WORKPLACE

Next Week

- Read the SABSA White Paper

Next Month

- Do a SABSA Fast-Track for a subset of a domain/system
- Work with stakeholders to educate about SABSA concepts

Next 6 Months

- Define your Organisations Domain Model
- Define your Attribute Hierarchy
- Start to build your SABSA toolbox

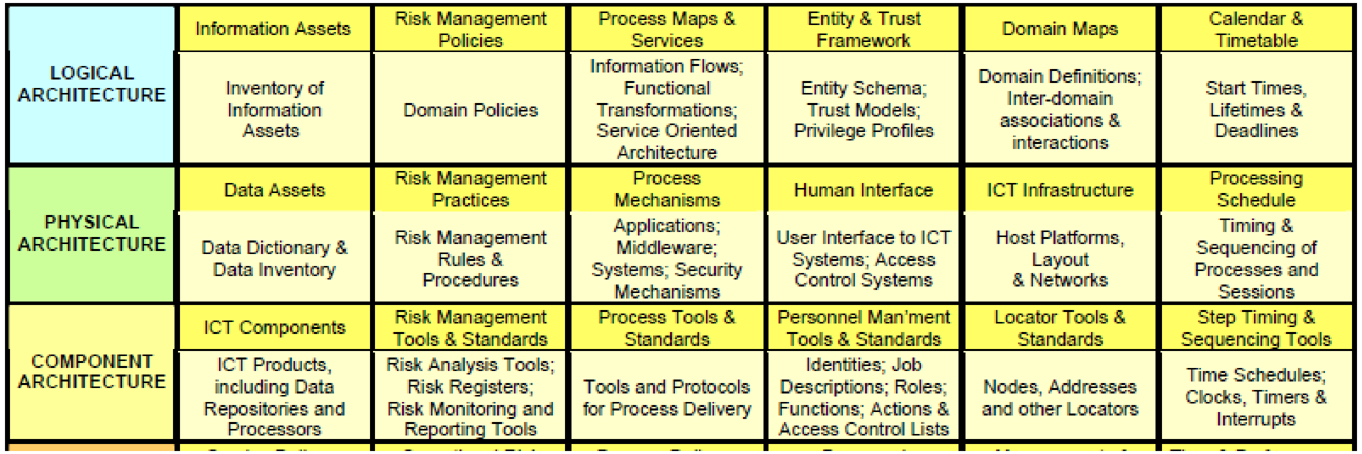
QUESTIONS?

INTRODUCTION TO SABSA

SECURITY PATTERNS

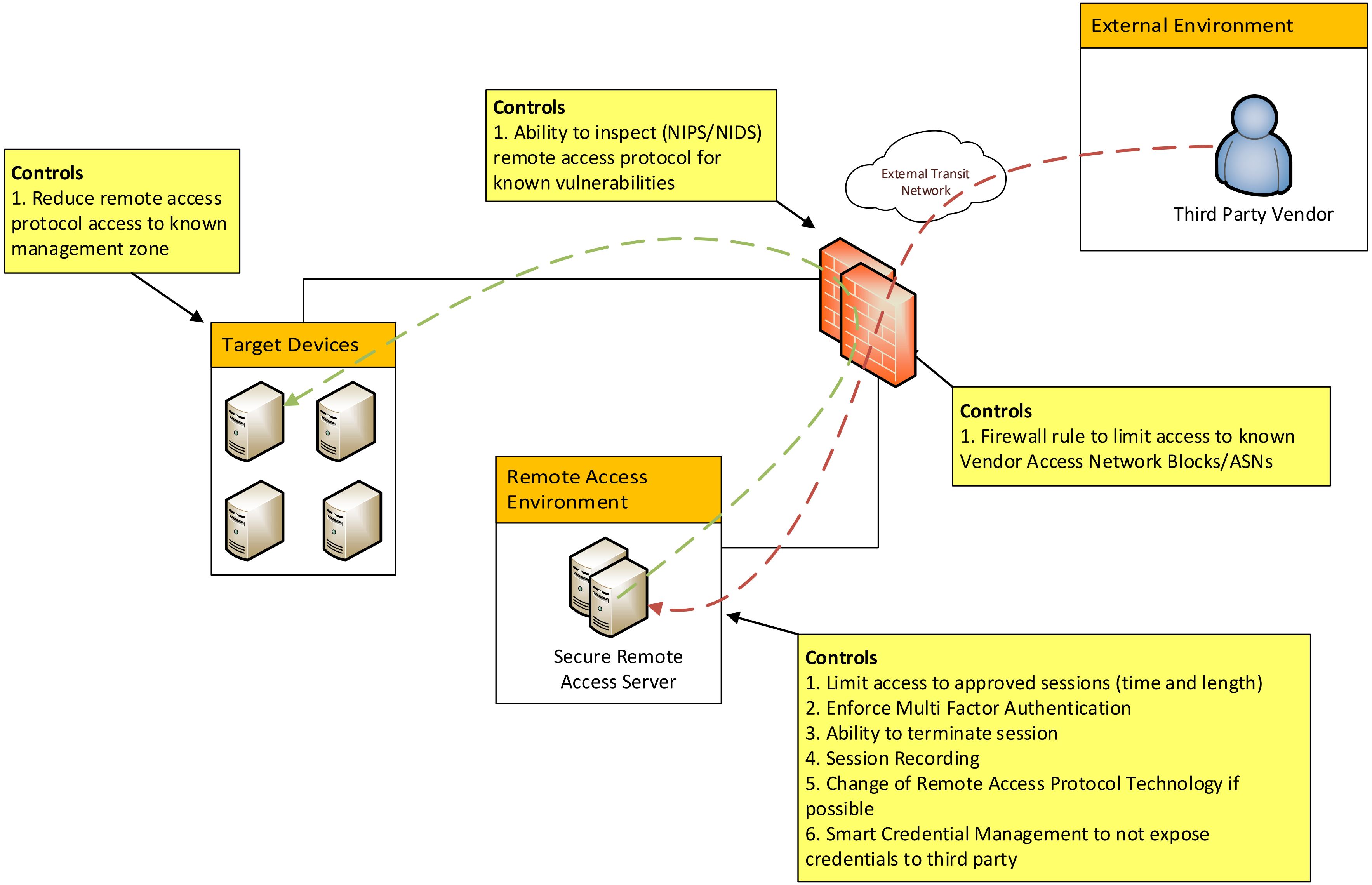
THINKING ABOUT PATTERNS USING THE SABSA MATRIX

- I like to use Security Patterns for the Logical, Physical and Component Layers and the Design Activities
- They are useful for the “Design & Implement” Phases of the SABSA design lifecycle



LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man’ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	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, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts

AN EXAMPLE PATTERN FOR SECURE REMOTE ACCESS



Controls
1. Reduce remote access protocol access to known management zone

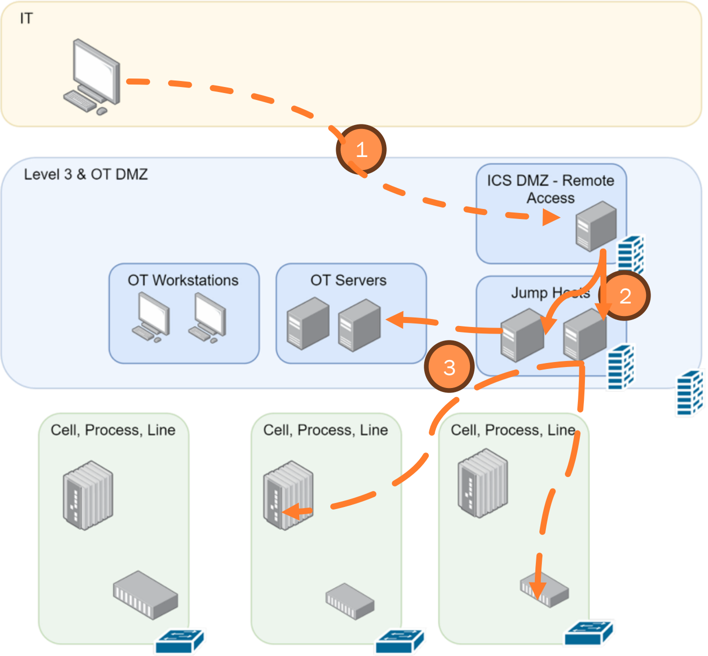
Controls
1. Ability to inspect (NIPS/NIDS) remote access protocol for known vulnerabilities

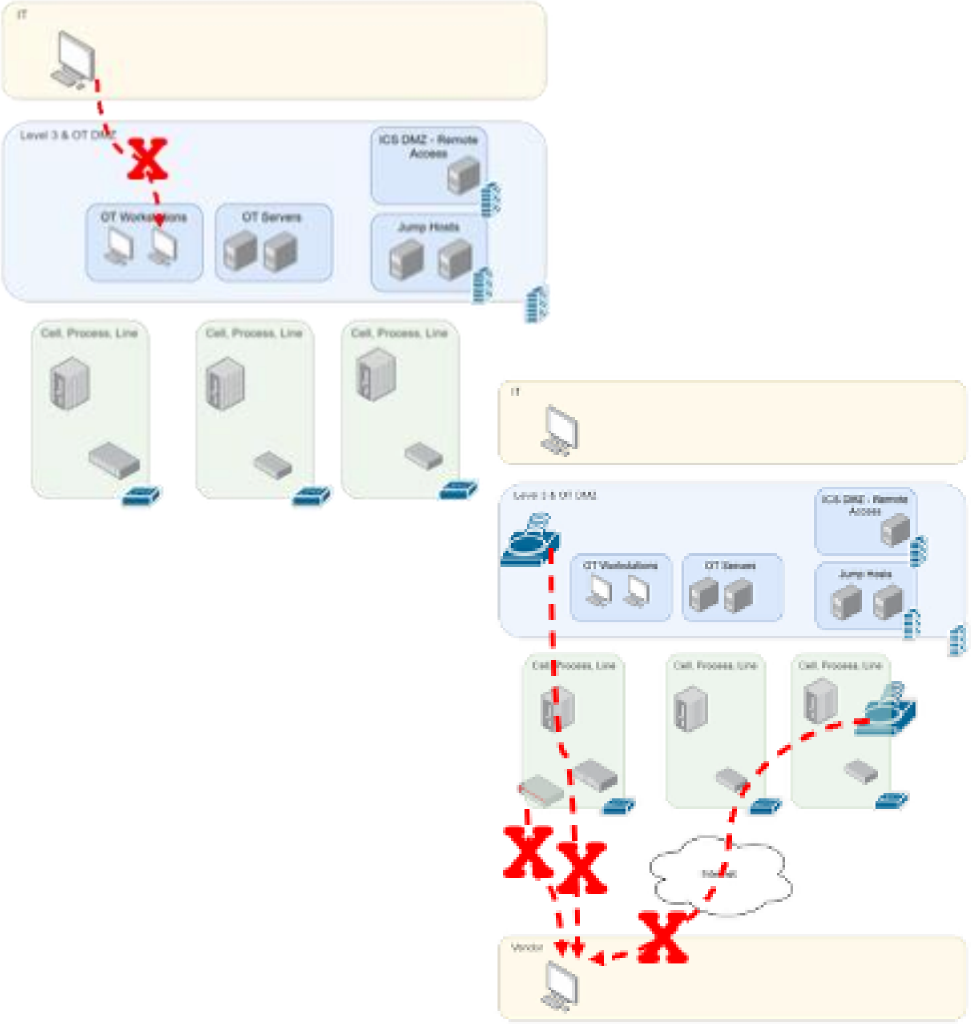
Controls
1. Firewall rule to limit access to known Vendor Access Network Blocks/ASNs

Controls
1. Limit access to approved sessions (time and length)
2. Enforce Multi Factor Authentication
3. Ability to terminate session
4. Session Recording
5. Change of Remote Access Protocol Technology if possible
6. Smart Credential Management to not expose credentials to third party

AN EXAMPLE PATTERN FOR SECURE REMOTE ACCESS (CONT.)

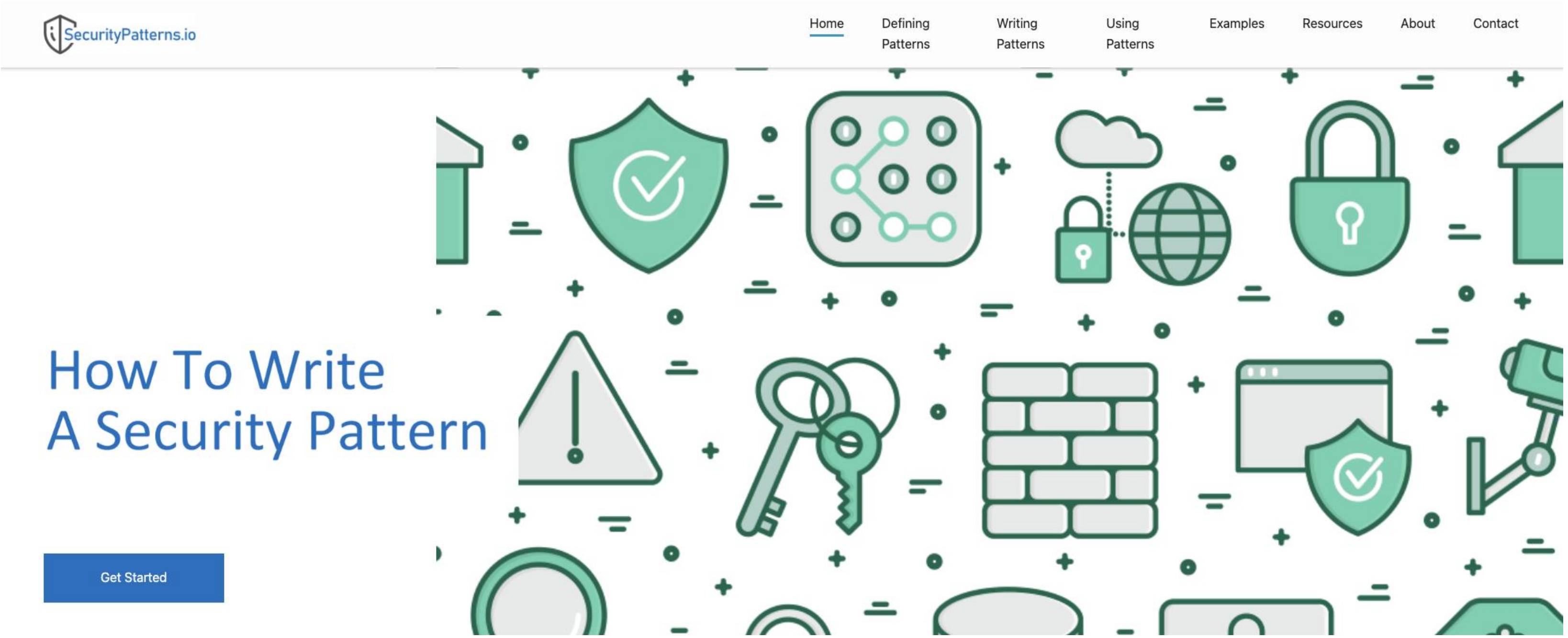
1. A user in the Business Network connects to the ICS DMZ Remote Access Device using an IT Identity and MFA. This device could be a server, connection broker or a VPN pool
2. The User then connects to the Jump Host using an OT Identity and OT MFA if required
3. Jump Boxes can be restricted to different functions/use cases. Network Access to Cell, Process, Line can be controlled using Network Access Control Lists in local switching infrastructure





SECURITYPATTERNS.IO

- A fantastic reference to help you build a security pattern
- A big shout out to Ken Fitzpatrick from Patterned Security
- Includes
  - How to write a pattern
  - Example patterns
  - How to use Patterns



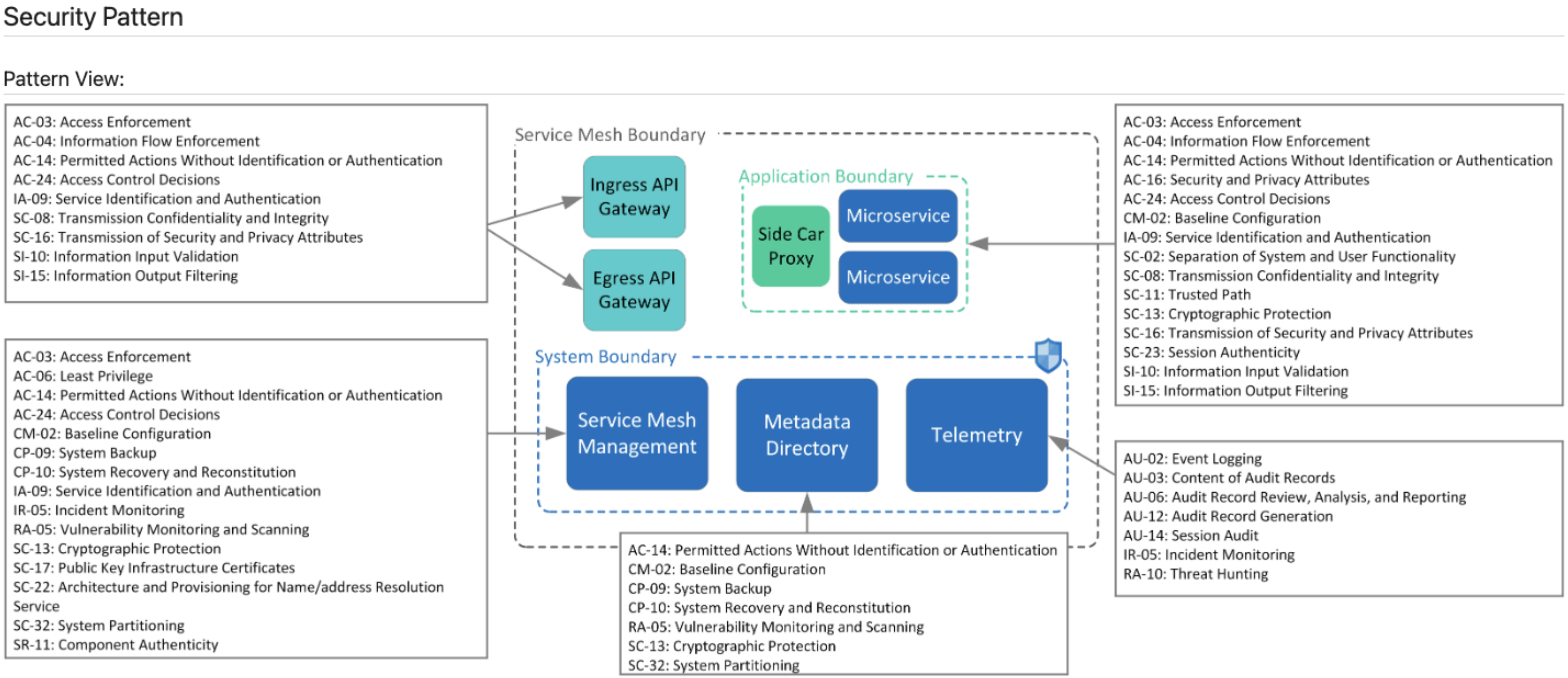
SECURITYPATTERNS.IO (CONT.)

Ken’s Process to writing a pattern -

1. Identify the Problem and Scope
2. Prepare and Research
3. Identify the Assets
4. Threat Modelling
5. Describe the Target State Solution
6. Define and Map Security Control Objectives
7. Describe Security Pattern
8. Summary and Conclusion

Ref - https://securitypatterns.io/docs/how-to-write-a-security-pattern/

EXAMPLE SECURITY PATTERN AS PER SECURITYPATTERNS.IO



Security Pattern

Pattern View:

AC-03: Access Enforcement
AC-04: Information Flow Enforcement
AC-14: Permitted Actions Without Identification or Authentication
AC-24: Access Control Decisions
IA-09: Service Identification and Authentication
SC-08: Transmission Confidentiality and Integrity
SC-16: Transmission of Security and Privacy Attributes
SI-10: Information Input Validation
SI-15: Information Output Filtering

AC-03: Access Enforcement
AC-06: Least Privilege
AC-14: Permitted Actions Without Identification or Authentication
AC-24: Access Control Decisions
CM-02: Baseline Configuration
CP-09: System Backup
CP-10: System Recovery and Reconstitution
IA-09: Service Identification and Authentication
IR-05: Incident Monitoring
RA-05: Vulnerability Monitoring and Scanning
SC-13: Cryptographic Protection
SC-17: Public Key Infrastructure Certificates
SC-22: Architecture and Provisioning for Name/address Resolution Service
SC-32: System Partitioning
SR-11: Component Authenticity

AC-14: Permitted Actions Without Identification or Authentication
CM-02: Baseline Configuration
CP-09: System Backup
CP-10: System Recovery and Reconstitution
RA-05: Vulnerability Monitoring and Scanning
SC-13: Cryptographic Protection
SC-32: System Partitioning

AC-03: Access Enforcement
AC-04: Information Flow Enforcement
AC-14: Permitted Actions Without Identification or Authentication
AC-16: Security and Privacy Attributes
AC-24: Access Control Decisions
CM-02: Baseline Configuration
IA-09: Service Identification and Authentication
SC-02: Separation of System and User Functionality
SC-08: Transmission Confidentiality and Integrity
SC-11: Trusted Path
SC-13: Cryptographic Protection
SC-16: Transmission of Security and Privacy Attributes
SC-23: Session Authenticity
SI-10: Information Input Validation
SI-15: Information Output Filtering

AU-02: Event Logging
AU-03: Content of Audit Records
AU-06: Audit Record Review, Analysis, and Reporting
AU-12: Audit Record Generation
AU-14: Session Audit
IR-05: Incident Monitoring
RA-10: Threat Hunting

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

TIPS FOR MANAGING PATTERN LIBRARIES

- Don’t try and make patterns for everything!
- A good approach is to think about whether a solution should be turned into a pattern
- Iterating patterns is also a great approach to developing a pattern library

EXERCISE 4

In this exercise, you will read through the “how to write a Pattern” https://securitypatterns.io/docs/how-to-write-a-security-pattern/ - and then have a look at the example patterns at https://securitypatterns.io/security-patterns/

You will have 20 minutes for this activity and we will then have 10 minutes to discuss as a group

ANTI-PATTERNS AS A TOOL

- Another useful concept is Security Architecture Anti-Patterns
- The NCSC defines an Anti-Pattern as “The term 'anti-pattern' is now used to refer to any repeated (but ineffective) solution to a common problem, it is credited to Andrew Koenig who coined it in response to the seminal book 'Design Patterns: Elements of Reusable Object-Oriented Software’.”
- The NSCS lists the below example Anti-Patterns
  - Browse Up for Administration
  - Management bypass
  - Back to Back Firewalls
  - Build ‘on-prem’ solution in the crowd
  - Uncontrolled and Unobserved Third party Access
  - The Unpatchable system

Ref - https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns

EXERCISE 4 - DEFINE A PATTERN THAT WOULD BE USEFUL AT YOUR WORK

Using the Pattern Approach as per SecurityPatterns.io consider if you have a security problem at your work that would benefit from being a pattern? Then work through the process at a high level to start to define

HOMEWORK – USING PATTERNS IN YOUR WORK PLACE

Next Week	Next Month	Next 6 Months
▪ Review SecurityPatterns.io	▪ Look for Security Solutions that you reference multiple times, create a list of target patterns ▪ Educate the teams you work with on the benefits of patterns and discuss which patterns would work for them	▪ Establish a Pattern Library

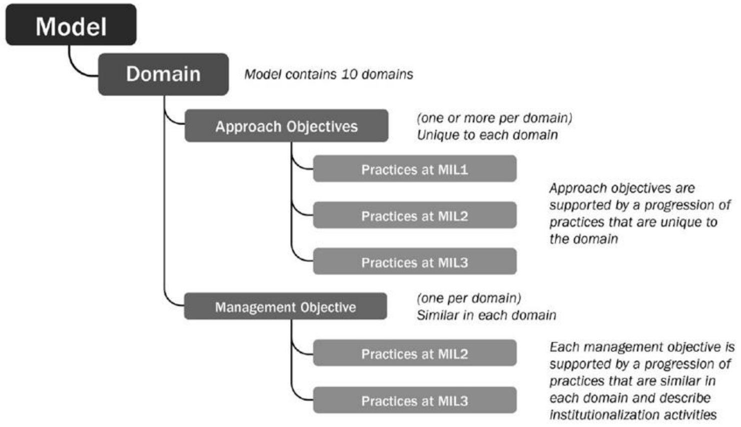
QUESTIONS?

SECURITY PATTERNS

C2M2 &
THE ARCHITECTURE DOMAIN

THE CYBER SECURITY CAPABILITY MATURITY MODEL (C2M2)

- US Department of Energy Cyber Security Capability Maturity Model
- Defines 10 domains
  - (ASSET) - Asset, Change, and Configuration Management
  - (THREAT) - Threat and Vulnerability Management
  - (RISK) - Risk Management
  - (ACCESS) - Identity and Access Management
  - (SITUATION) - Situational Awareness
  - (RESPONSE) - Event and Incident Response, Continuity of Operations
  - (THIRD-PARTIES) - Third-Party Risk Management
  - (WORKFORCE) - Workforce Management
  - (ARCHITECTURE) - Cybersecurity Architecture
  - **(PROGRAM) - Cybersecurity Program Management**
- Has the Concept of Maturity Indicator Levels (MIL)



Model

Domain

Model contains 10 domains

Approach Objectives

(one or more per domain)
Unique to each domain

Practices at MIL1

Practices at MIL2

Practices at MIL3

Approach objectives are supported by a progression of practices that are unique to the domain

Management Objective

(one per domain)
Similar in each domain

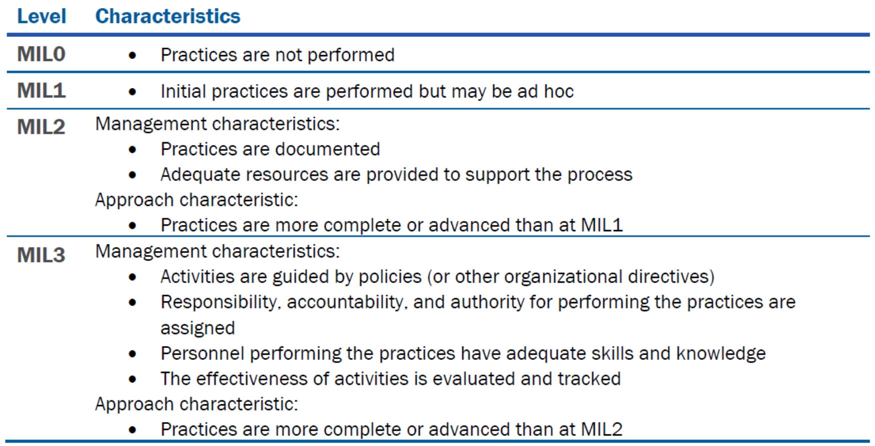
Practices at MIL2

Practices at MIL3

Each management objective is supported by a progression of practices that are similar in each domain and describe institutionalization activities

Figure 3: Model and Domain Elements

Table 4: Summary of Maturity Indicator Level Characteristics



Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial practices are performed but may be ad hoc
MIL2	Management characteristics: • Practices are documented • Adequate resources are provided to support the process Approach characteristic: • Practices are more complete or advanced than at MIL1
MIL3	Management characteristics: • Activities are guided by policies (or other organizational directives) • Responsibility, accountability, and authority for performing the practices are assigned • Personnel performing the practices have adequate skills and knowledge • The effectiveness of activities is evaluated and tracked Approach characteristic: • Practices are more complete or advanced than at MIL2

Source – C2M2 v2.1

HOW THE C2M2 DEFINES ARCHITECTURE

- 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.”*

C2M2 – ARCHITECTURE DOMAIN

1. Establish and Maintain Cybersecurity Architecture Strategy and Program

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

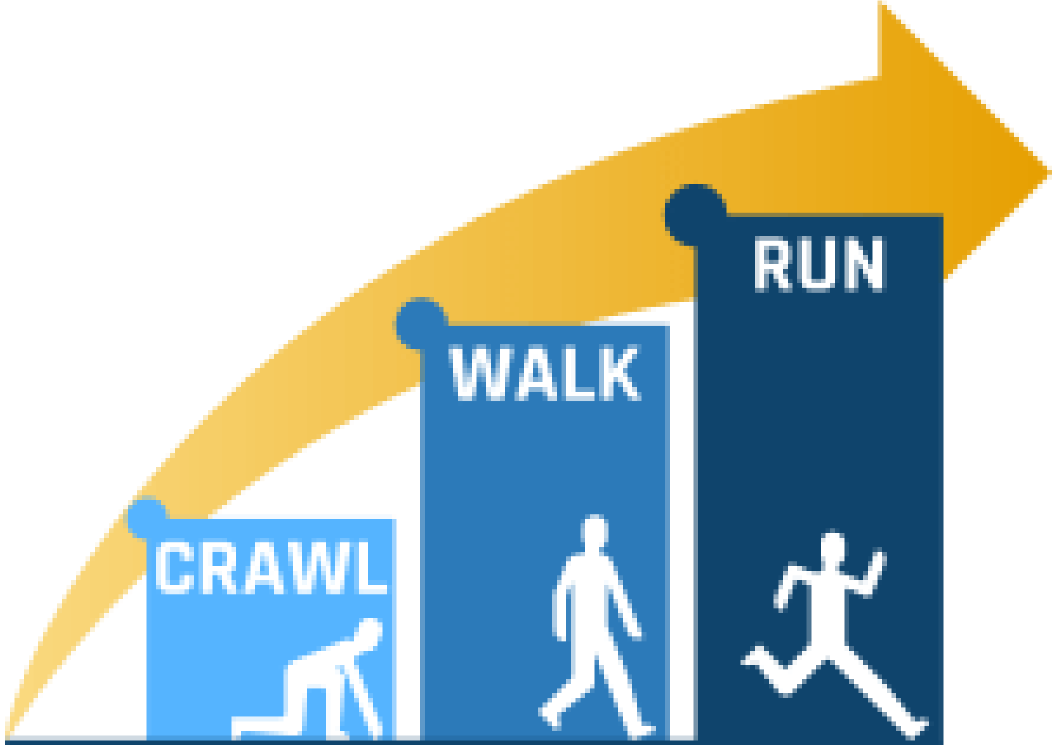
3. Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture

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

CRAWL, WALK & RUN



Source - https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

ESTABLISH AND MAINTAIN ARCH STRATEGY AND PROGRAM

MIL1

a. The organization has a strategy for cybersecurity architecture, which may be developed and managed in an ad hoc manner

MIL2

b. A strategy for cybersecurity architecture is established and maintained in alignment with the organization’s cybersecurity program strategy (PROGRAM-1b) and enterprise Architecture

c. A documented cybersecurity architecture is established and maintained that includes IT and OT systems and networks and aligns with system and asset categorization and prioritization

d. Governance for cybersecurity architecture (such as an architecture review process) is established and maintained that includes provisions for periodic architectural reviews and an exceptions process

e. Senior management sponsorship for the cybersecurity architecture program is visible and active

f. The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization’s assets

g. Cybersecurity controls are selected and implemented to meet cybersecurity requirements

MIL3

h. The cybersecurity architecture strategy and program are aligned with the organization’s enterprise architecture strategy and program

i. Conformance of the organization’s systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events

j. The cybersecurity architecture is guided by the organization’s risk analysis information (RISK-3d) and threat profile (THREAT-2e)

k. The cybersecurity architecture addresses predefined states of operation (SITUATION-3g)

Source – C2M2 v2.1

IMPLEMENT NETWORK PROTECTIONS AS AN ELEMENT OF THE CYBERSECURITY ARCHITECTURE

MIL1

a. Network protections are implemented, at least in an ad hoc manner

b. The organization’s IT systems are separated from OT systems through segmentation, either through physical means or logical means, at least in an ad hoc manner

MIL2

c. Network protections are defined and enforced for selected asset types according to asset risk and priority

d. Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements

e. Network protections incorporate the principles of least privilege and least functionality

f. Network protections include monitoring, analysis, and control of network traffic for selected security zones

g. Web traffic and email are monitored, analyzed, and controlled

MIL3

h. All assets are segmented into distinct security zones based on cybersecurity requirements

i. Separate networks are implemented, where warranted, that logically or physically segment assets into security zones with independent authentication

j. OT systems are operationally independent from IT systems so that OT operations can be sustained during an outage of IT systems

k. Device connections to the network are controlled to ensure that only authorized devices can connect

l. The cybersecurity architecture enables the isolation of compromised assets

Source – C2M2 v2.1

IMPLEMENT SOFTWARE SECURITY AS AN ELEMENT OF THE CYBERSECURITY ARCHITECTURE

MIL1	MIL2	MIL3
a. No practice at MIL1	b. Software developed in-house for deployment on higher priority assets is developed using secure software development practices c. The selection of procured software for deployment on higher priority assets includes consideration of the vendor’s secure software development practices d. Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house	e. All software developed in-house is developed using secure software development practices f. The selection of all procured software includes consideration of the vendor’s secure software development practices g. The architecture review process evaluates the security of new and revised applications prior to deployment h. The authenticity of all software and firmware is validated prior to deployment i. Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to defined triggers, such as system changes and external events

Source – C2M2 v2.1

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

b. All data at rest is protected for selected data categories

c. All data in transit is protected for selected data categories

d. Cryptographic controls are implemented for data at rest and data in transit for selected data categories

e. Key management infrastructure (that is, key generation, key storage, key destruction, key update, and key revocation) is implemented to support cryptographic controls

f. Controls to restrict the exfiltration of data (for example, data loss prevention tools) are implemented

MIL3

g. The cybersecurity architecture includes protections (such as full disk encryption) for data that is stored on assets that may be lost or stolen

h. The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and data

Source – C2M2 v2.1

MANAGEMENT ACTIVITIES FOR THE ARCHITECTURE DOMAIN

MIL1

a. No practice at MIL1

MIL2

b. Documented procedures are established, followed, and maintained for activities in the ARCHITECTURE domain

c. Adequate resources (people, funding, and tools) are provided to support activities in the ARCHITECTURE domain

MIL3

d. Up-to-date policies or other organizational directives define requirements for activities in the ARCHITECTURE domain

e. Responsibility, accountability, and authority for the performance of activities in the ARCHITECTURE domain are assigned to personnel

f. Personnel performing activities in the ARCHITECTURE domain have the skills and knowledge needed to perform their assigned responsibilities

g. The effectiveness of activities in the ARCHITECTURE domain is evaluated and tracked

Source – C2M2 v2.1

FOR EXAMPLE, WHAT DOES IT LOOK LIKE AT MIL-1 COMBINED

1. Establish and Maintain Cybersecurity Architecture Strategy and Program	• The organization has a strategy for cybersecurity architecture, which may be developed and managed in an ad hoc manner
2. Implement Network Protections …	• Network protections are implemented, at least in an ad hoc manner • The organization's IT systems are separated from OT systems through segmentation, either through physical means or logical means, at least in an ad hoc manner
3. Implement IT and OT Asset Security …	• 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 • Endpoint protections are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner
4. Implement Software Security …	• No practice at MIL1
5. Implement Data Security …	• Sensitive data is protected at rest, at least in an ad hoc manner
6. Management Activities	• No practice at MIL1

Source – C2M2 v2.1

EXERCISE – WHAT IS YOUR CYBER SECURITY ARCHITECTURE PROGRAM?

Think about your environment, do an assessment of how you manage architecture using the framework? Think about how you could use the framework to build a 12-18 Month Road Map to improve architecture at your company

Exercise Time – 20 minutes – Then 10 Minutes to Discuss with your group

https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources (offline toolkit)

HOMEWORK

Next Week	Next Month	Next Six Months
Review the C2M2 V2.1 Architecture Domain Material	Develop your Architecture Road Maturity Road Map as per the C2M2	Start reporting on your architecture progress

QUESTIONS?

ARCHITECTURE PROGRAMS USING THE C2M2

COMBINED HOMEWORK ON A PAGE

Next Week

- SABSA
  - Read the SABSA White Paper
- Security Patterns
  - Review SecurityPatterns.io
- C2M2 Architecture Domain
  - Review the C2M2 V2.1 Architecture Domain Material

Next Month

- SABSA
  - Do a SABSA Fast-Track for a subset of a domain/system
  - Work with stakeholders to educate about SABSA concepts
- Security Patterns
  - Look for Security Solutions that you reference multiple times, create a list of target patterns
  - Educate the teams you work with on the benefits of patterns and discuss which patterns would work for them
- C2M2 Architecture Domain
  - Develop your Architecture Road Maturity Road Map as per the C2M2

Next Six Months

- SABSA
  - Define your Organisations Domain Model
  - Define your Attribute Hierarchy
  - Start to build your SABSA toolbox
- Security Patterns
  - Establish a Pattern Library
- C2M2 Architecture Domain
  - Start reporting on your architecture progress

SUMMARY

- SABSA
  - SABSA is an Enterprise Security Architecture Framework that is Business Driven, Traceable and Justified
  - Use Security Attributes to understand the priorities of stakeholders and consider how security decisions through the matrix impact attributes
  - Domain modelling is an important tool to understand policy architecture and risk ownership
  - Consider a SABSA Fast-Track™ to help you quickly build a MVP to engage stakeholders

- Security Patterns
  - Use security patterns to support other teams to understand how to "do security"
  - SecurityPatterns.io is an awesome reference
  - Also consider using Anti Patterns – the NCSC reference is a useful reference
- C2M2 Architecture Domain
  - Use the C2M2 Architecture domain to help guide your architecture program
  - Remember, Crawl, Walk, Run – you don't have to run

THANK YOU!

- https://linkedin.com/in/blargeau
- bruce@blarge.io
- https://blarge.io
- https://www.blarge.io/04-contact
- https://github.com/beLarge

βLARGE
MISSION CRITICAL CYBER SECURITY