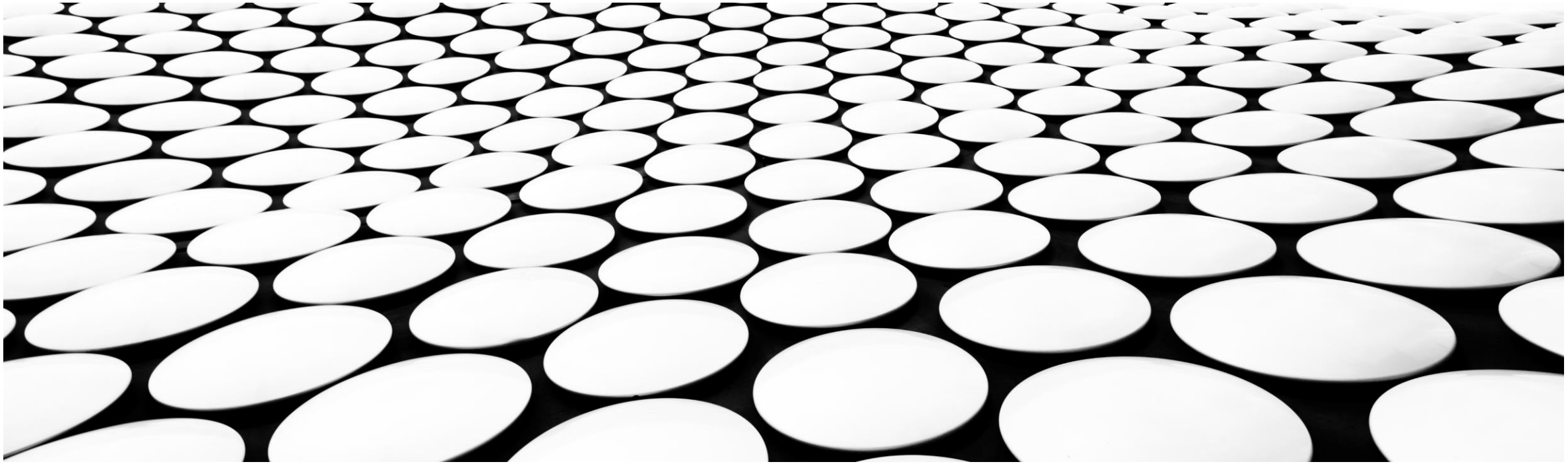
USING SABSA AND ISA/IEC 62443 TO BUILD A DEFENSIBLE ARCHITECTURE



/whois @beLarge

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

- Principal Cyber Security Architect at *ß 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
- Experience in Electricity Generation & Transmission, Railway, Aviation, Emergency Services and Consulting industries
- Chartered Engineer (CPEng) and Registered Professional Engineer of Queensland (RPEQ)
- Bach Eng (Telecomms) QUT First Class Honours and Master Business (Applied Finance) with Distinction QUT

ß Large

Why *this* presentation?

ß Large

Agenda

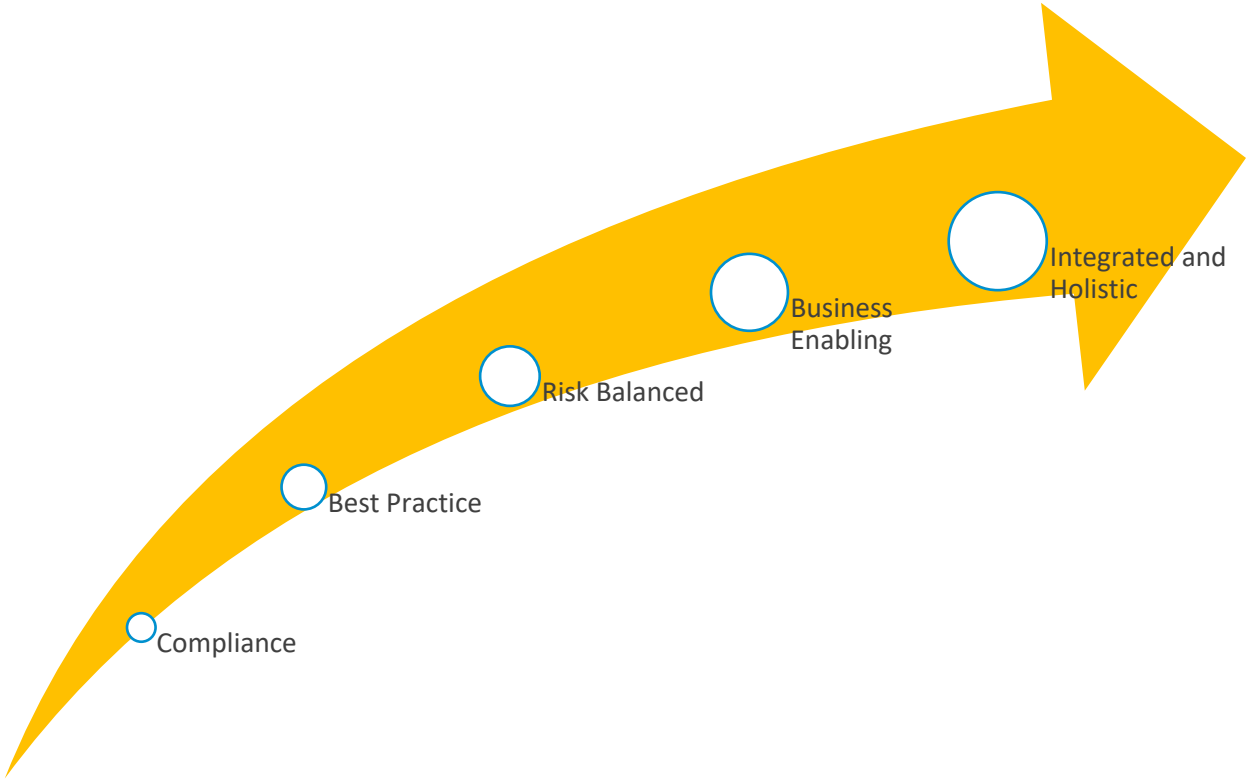
1. An Introduction to Security Architecture and Enterprise Security Architecture
2. Introducing SABSA
3. Introducing ISA/IEC 62443
4. Aligning SABSA & ISA/IEC 62443
5. Resources To Learn More
6. Q&A

ß Large

INTRODUCTION TO 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

ß Large

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

ß Large

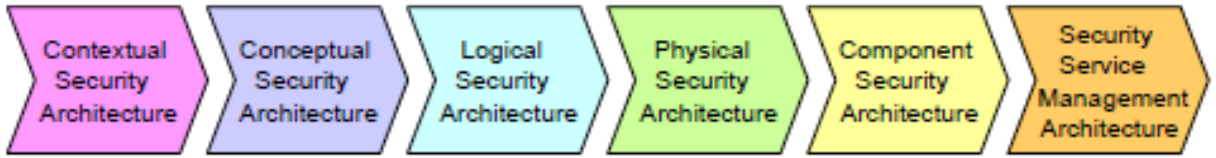
AN INTRODUCTION TO SABSA

OVERVIEW OF SABSA

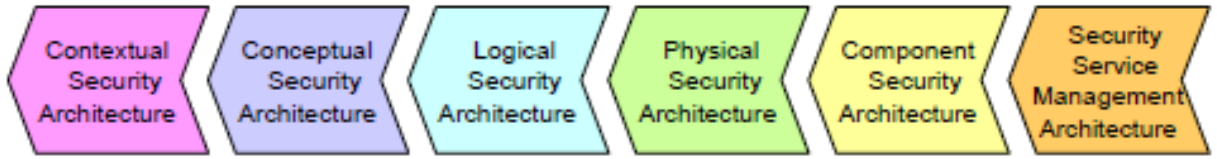
- SABSA has its origins as the Enterprise Security Architecture for the SWIFT IP Payments Network
- Business Aligned, Top Down and Deliberate, not just *best practice*
- Focus on *Attributes* which are security goals/objectives/requirements
- Two Way Traceability

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.



- 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.



Ref – SABSA White Paper (W100)

SABSA MATRIX

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Process	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

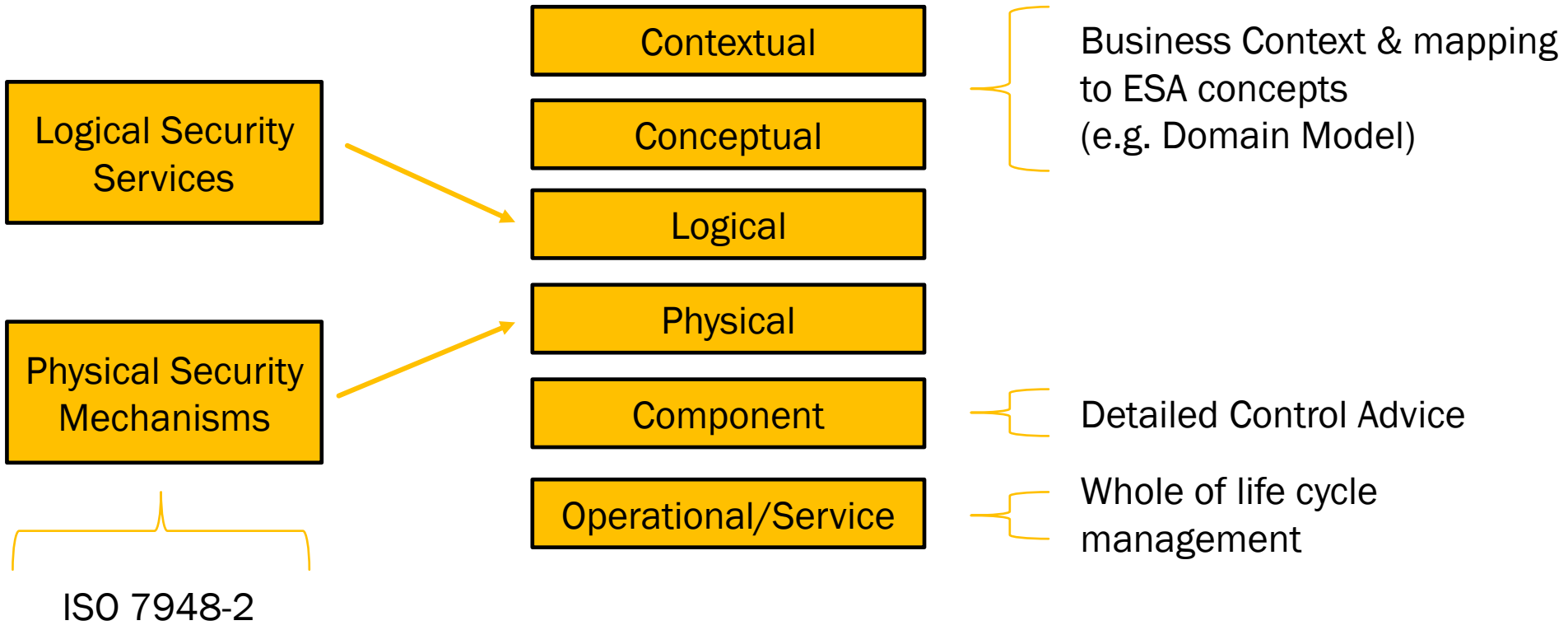
The Builder's View

The Tradeperson's View

The Service Manager's View

Ref - W100 *SABSA White Paper (2009)* - 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

ß Large

AN EXAMPLE OF HOW TO THINK OF THE 6 LAYERS

Contextual	*Business Context*
Conceptual	*Security Domain Framework*
Logical	*Network Segmentation Services*
Physical	*NGFW Appliance (it has a place)*
Component	*Firewall Rule Base*
Operational/Service	*Firewall Rule Maintenance, System Admin, Patching etc*

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... asso... 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

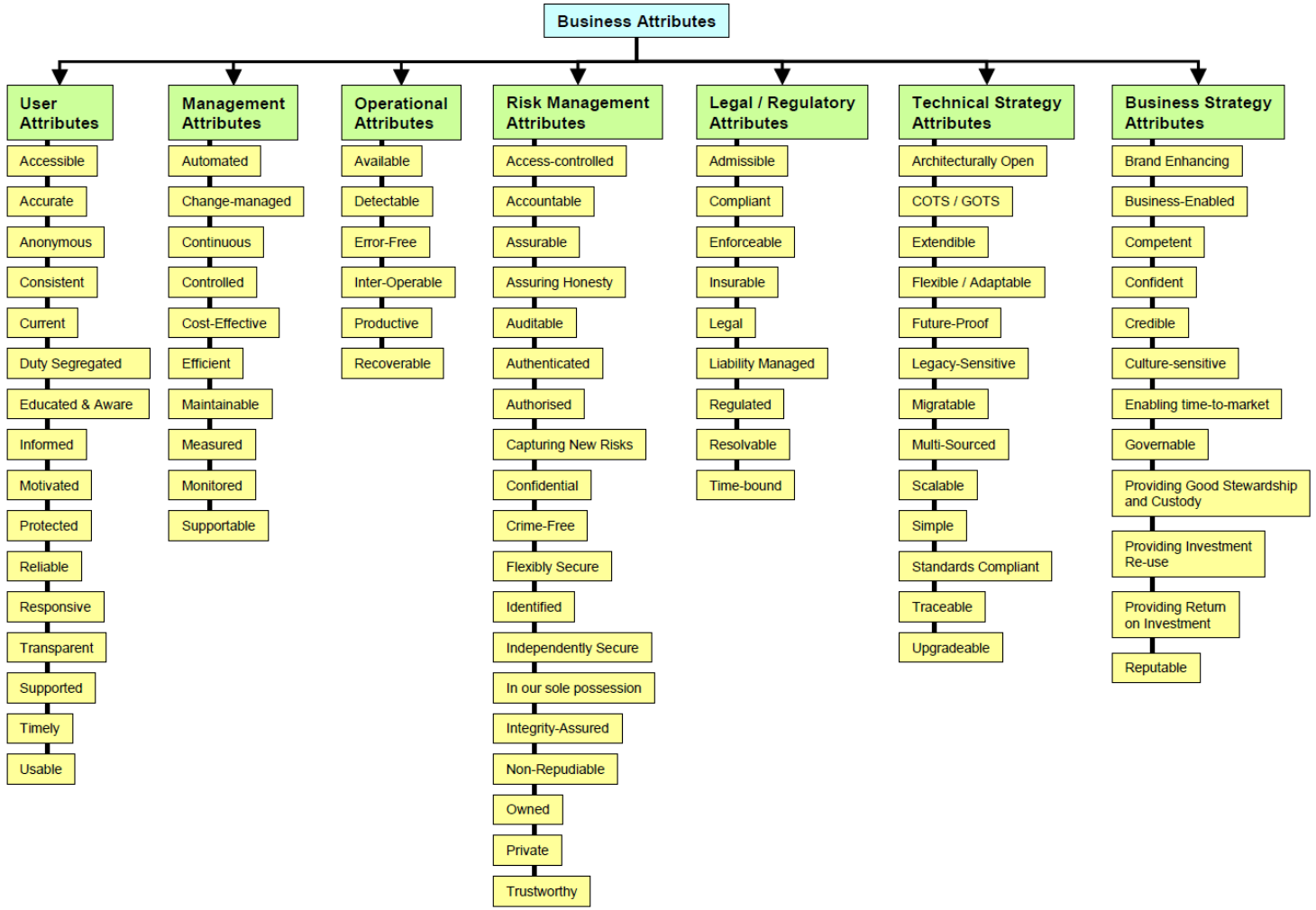


Figure 4: The SABSA Taxonomy of ICT Business Attributes

Ref – SABSA White Paper (W100)

EXAMPLE ATTRIBUTES

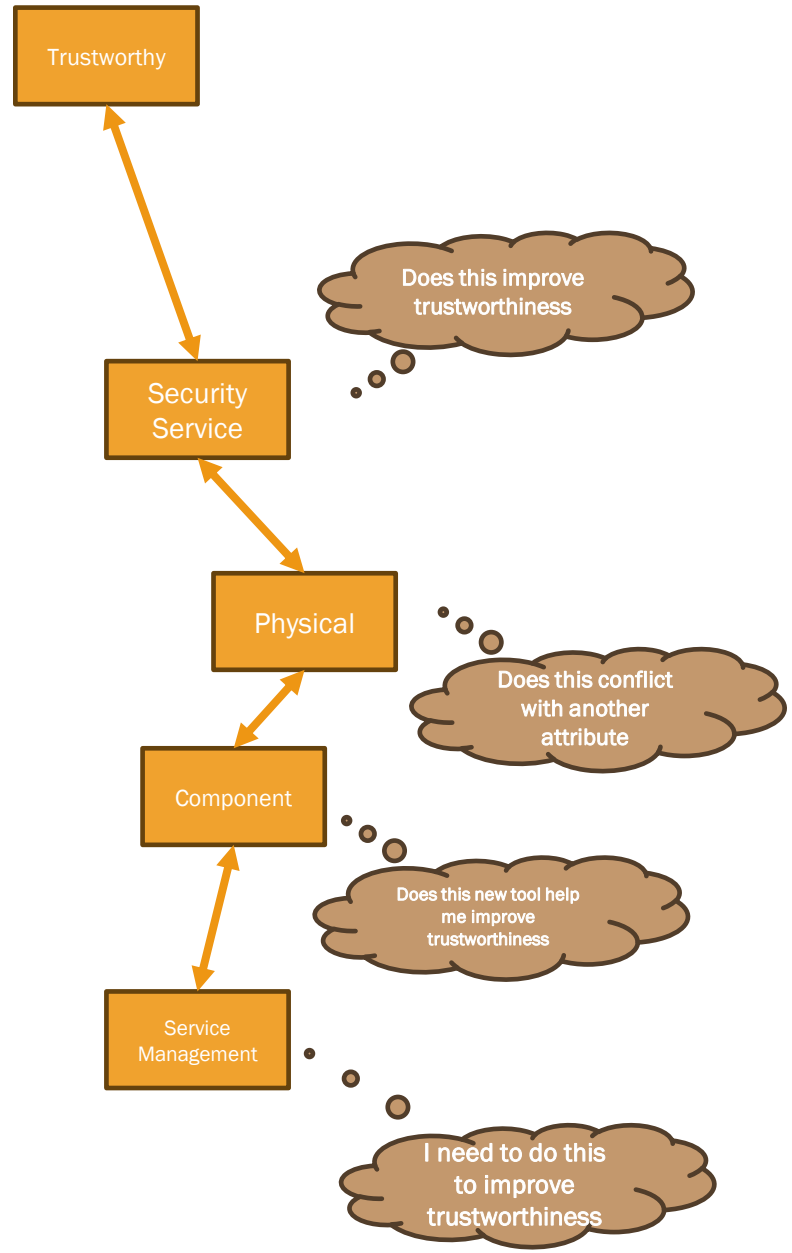
- Example attributes from the *Blue Book* with their Explanation and Metric Approach

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

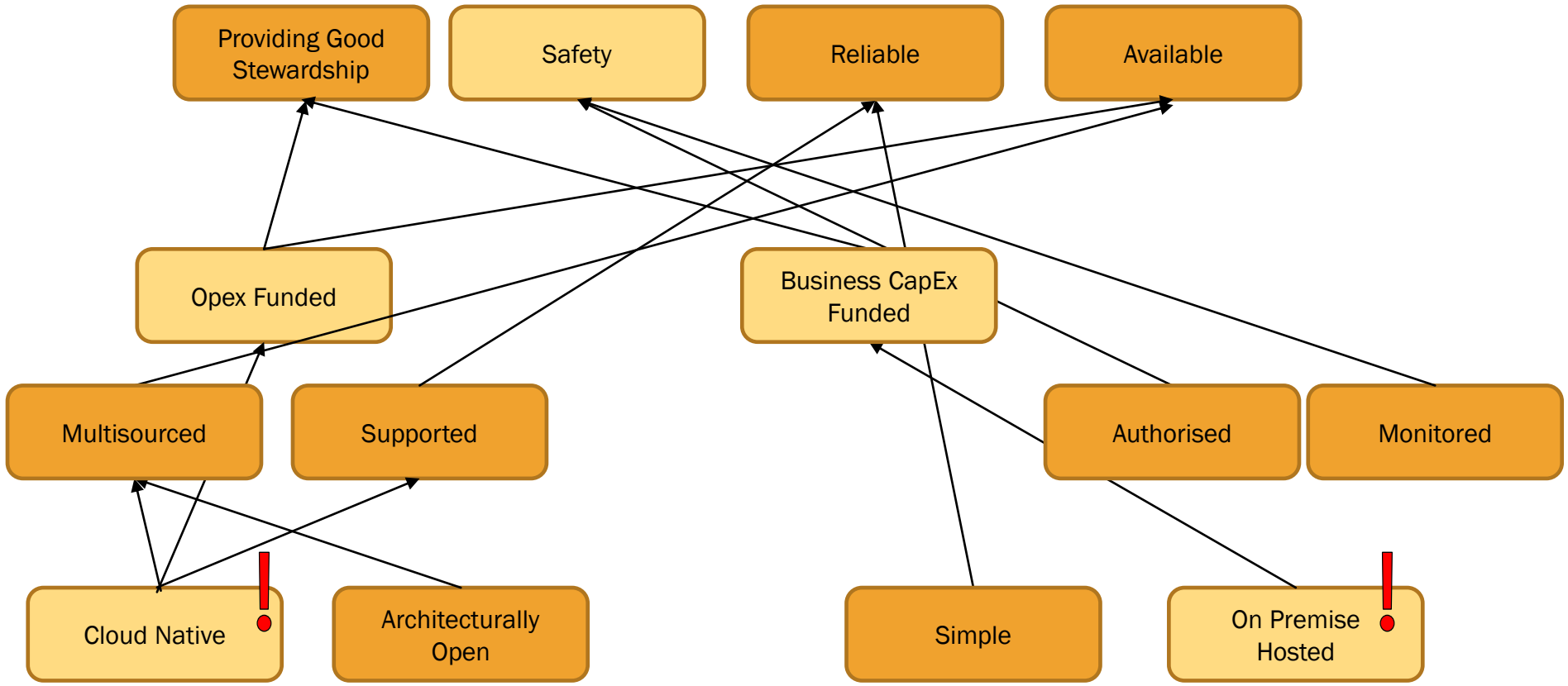
Ref - https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470476017.app1

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

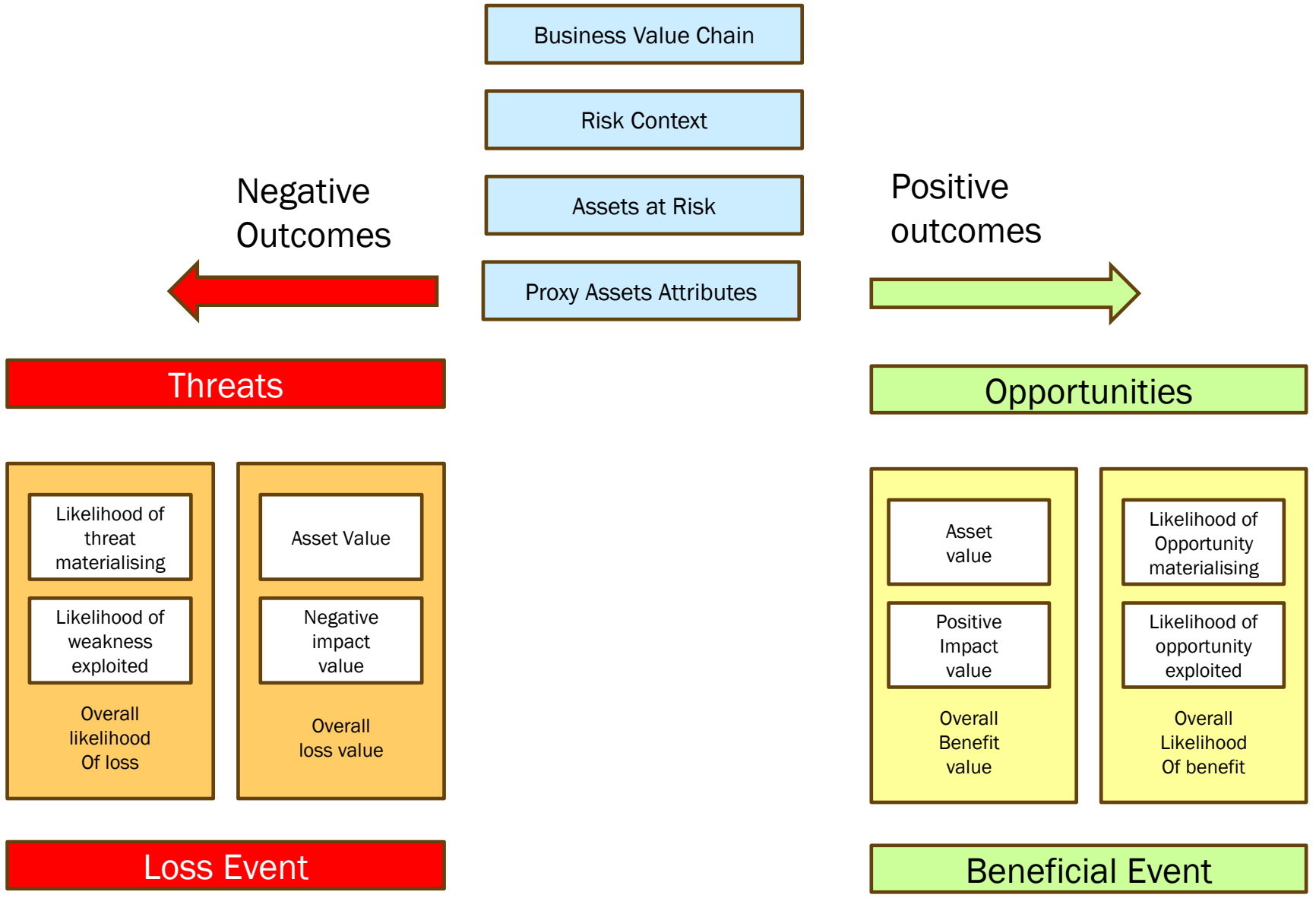


MULTI TIER ATTRIBUTES



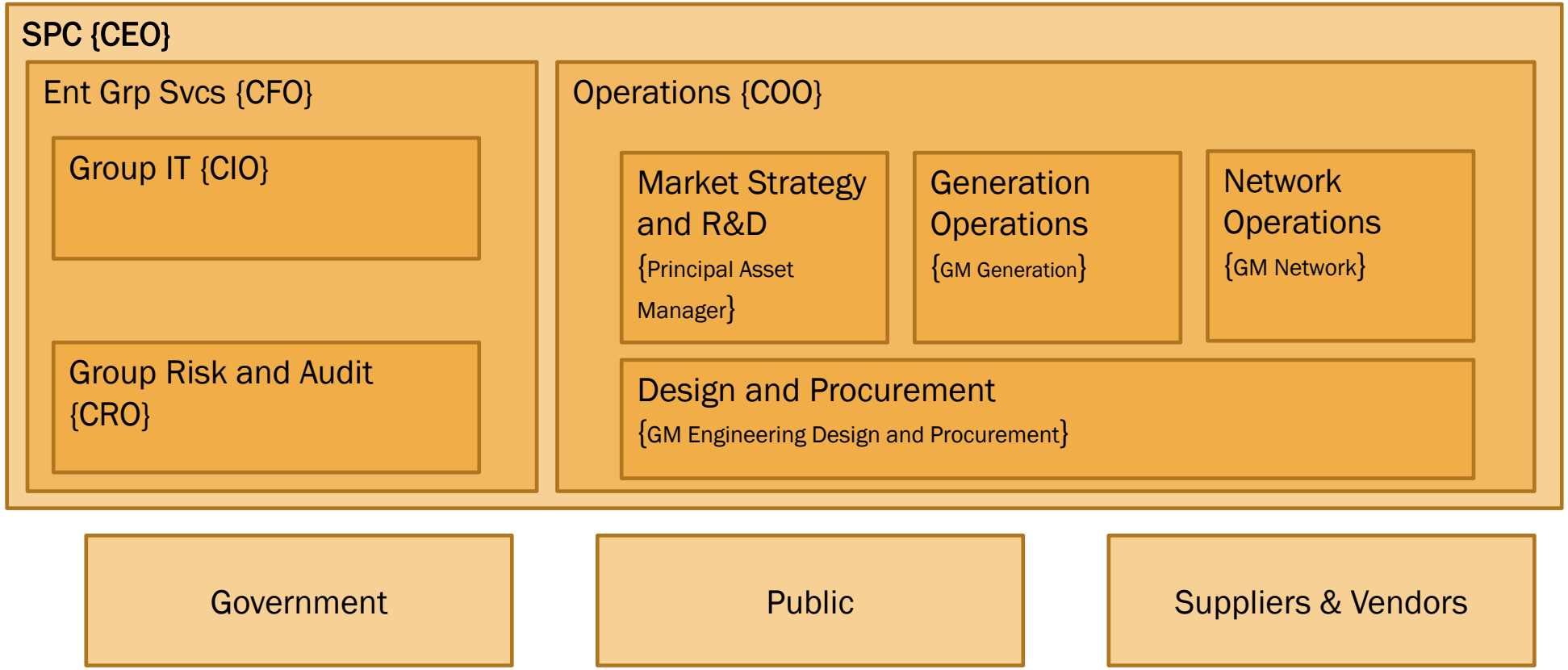
ß Large

BALANCED RISK MANAGEMENT

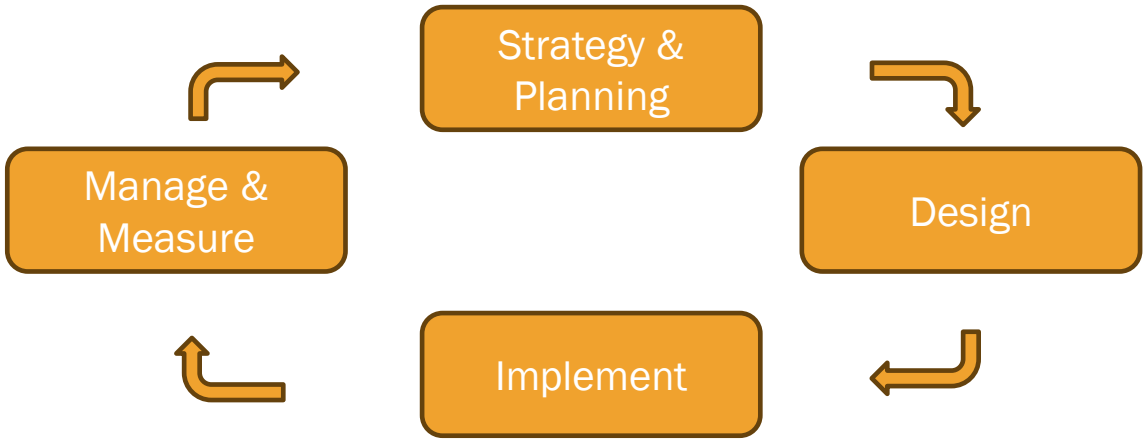


DOMAIN MODELS

- 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



SABSA LIFE CYCLE



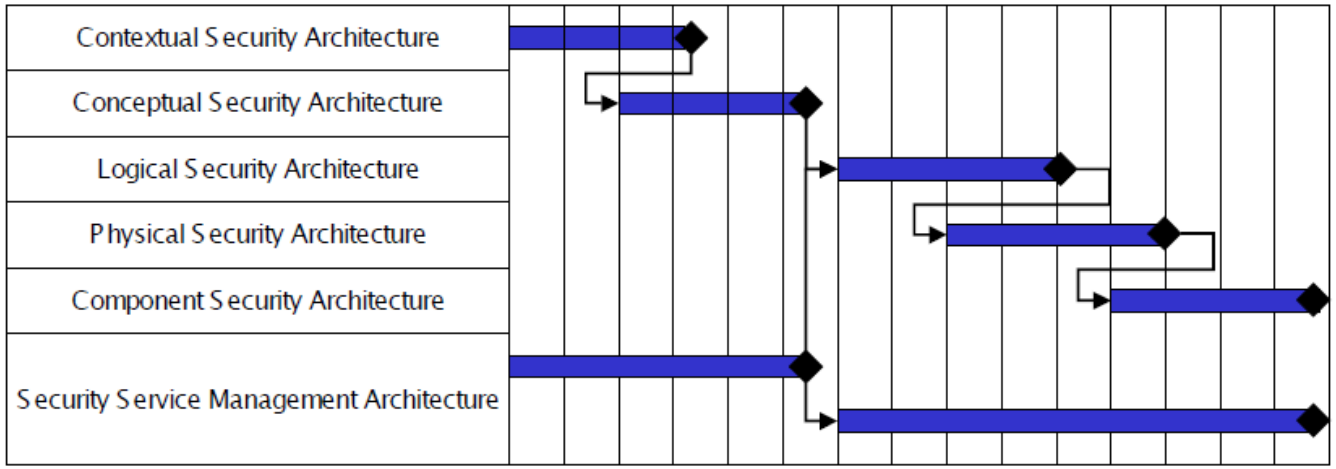


Figure 2: The SABSA Development Process

Ref – SABSA White Paper (W100)

BONUS SLIDE –SABSA & TOGAF INTEGRATION

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

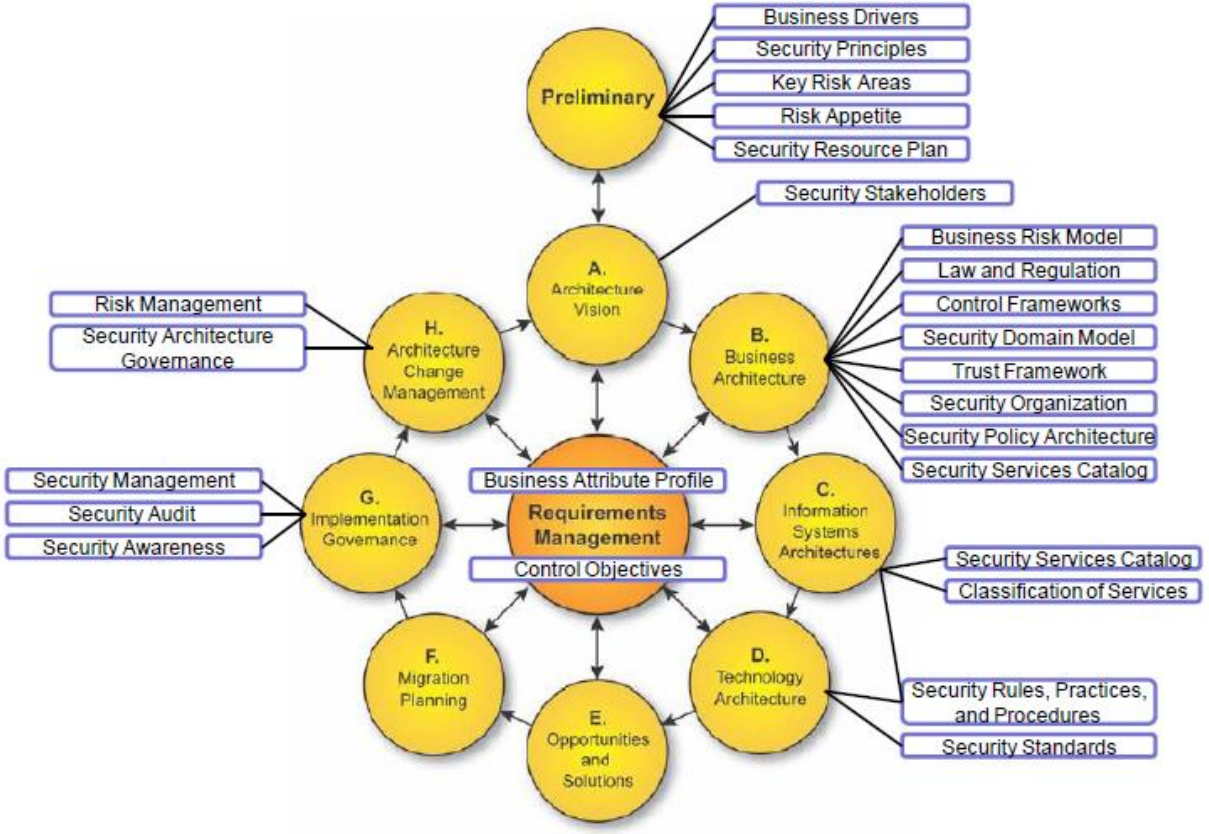


Figure 16: Overview of Security-Related Artifacts in the TOGAF ADM

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

ß Large

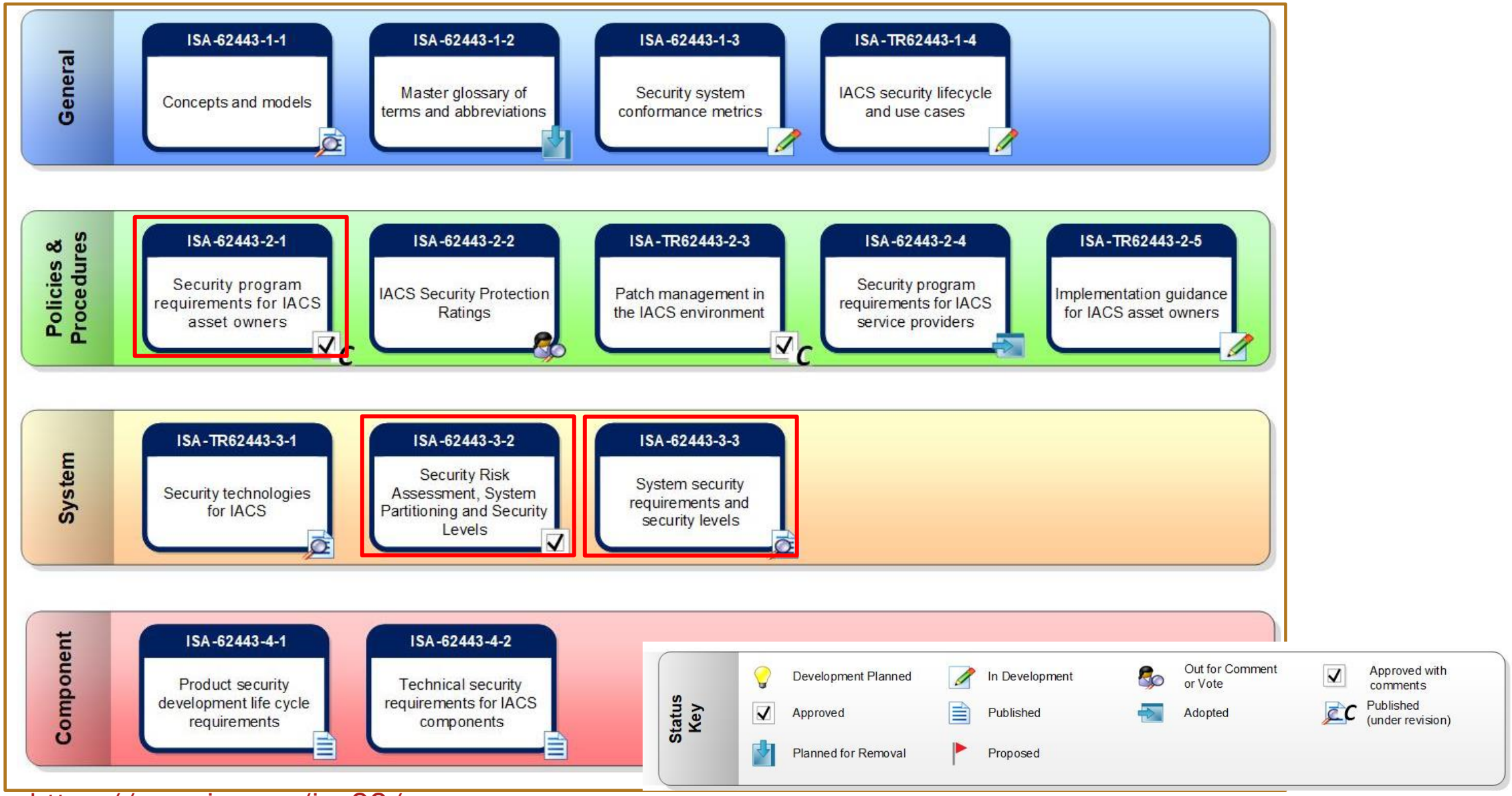
AN INTRODUCTION TO ISA/IEC 62443

ß Large

A QUICK OVERVIEW OF ISA/IEC 62443

- ISA/IEC 62443 is a Standards Framework of Cyber Security Publications for Industrial Automation and Control Systems (IACS)
- The International Society for Automation (ISA) Working Group 99 are the main produces of the publications
- Originally published with ANSI as ISA 99 but are now published in partnership with the IEC and are designated ISA/IEC 62443
- You might see ISA 95 – Enterprise-Control System Integration – it is based on the Purdue Model but it is separate to ISA 62443
- ISA 62443 is referenced by the NIST Cyber Security Framework but only 2 of the 14 publications referenced (2-1 and 3-3)

ß Large



https://www.isa.org/isa99/

OTHER VIEWS

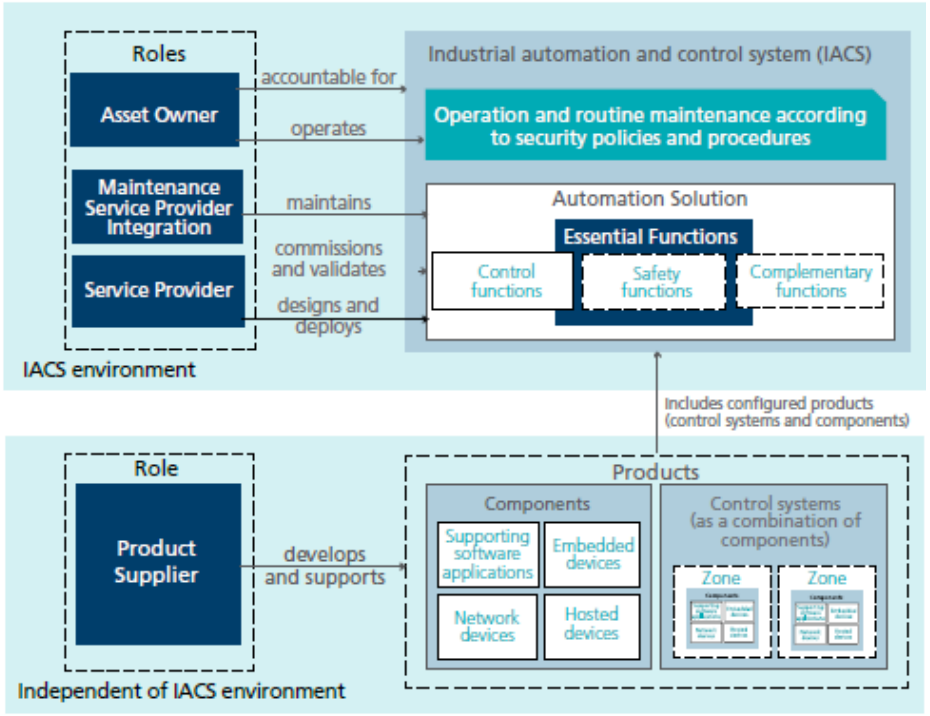


Figure 4: Roles, Products, Automation Solution, and IACS

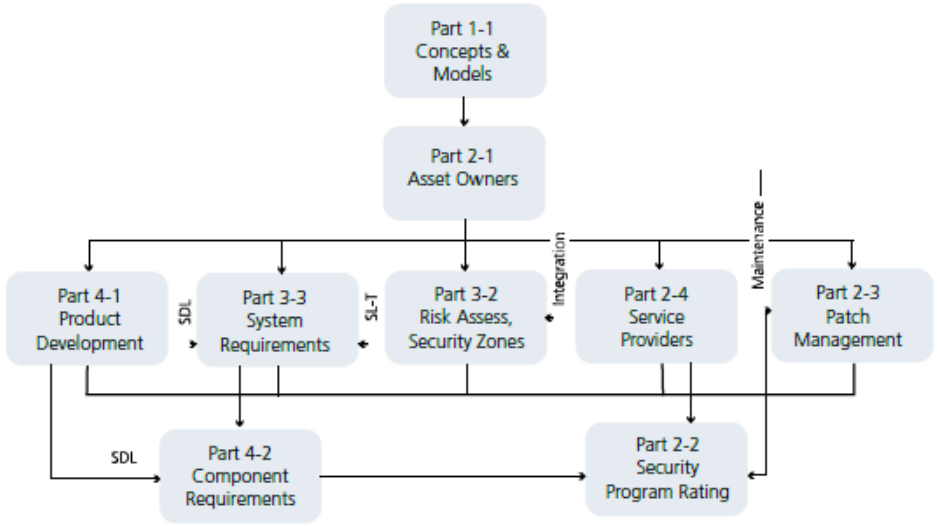


Figure 5: ISA/IEC 62443 Standards – Hierarchical View

Product Development Lifecycle	Automation Solution Lifecycle	
	Integration	Operation and Maintenance
Part 1-1: Concepts and Models		
	Part 2-1: IACS requirements for Asset Owners	
	Part 2-2: IACS Security Program Rating	
	Part 2-3: IACS Patch management	
	Part 2-4: Security program requirements for IACS service providers	
	Part 3-2: Security risk assessment, system partitioning, and security levels	
Part 3-3: System security requirements and Security levels		
Part 4-1: Product development lifecycle		
Part 4-2: Technical security requirements for IACs components		

Figure 6: ISA/IEC 62443 Standards - Lifecycle View

Ref - ISAGCA Quick Start Guide: An Overview of the ISA/IEC 62443 Standard

ß Large

ISA/IEC 62443 PART 2-1

ß Large

PART 2-1 – ESTABLISHING AN IACS SECURITY PROGRAM

- Defines a Cyber Security Management System (CSMS); The “OT ISMS”
- The Standard consists of:
  - Elements of the CSMS
  - Guidance for the development of the CSMS
  - Processes to develop a CSMS

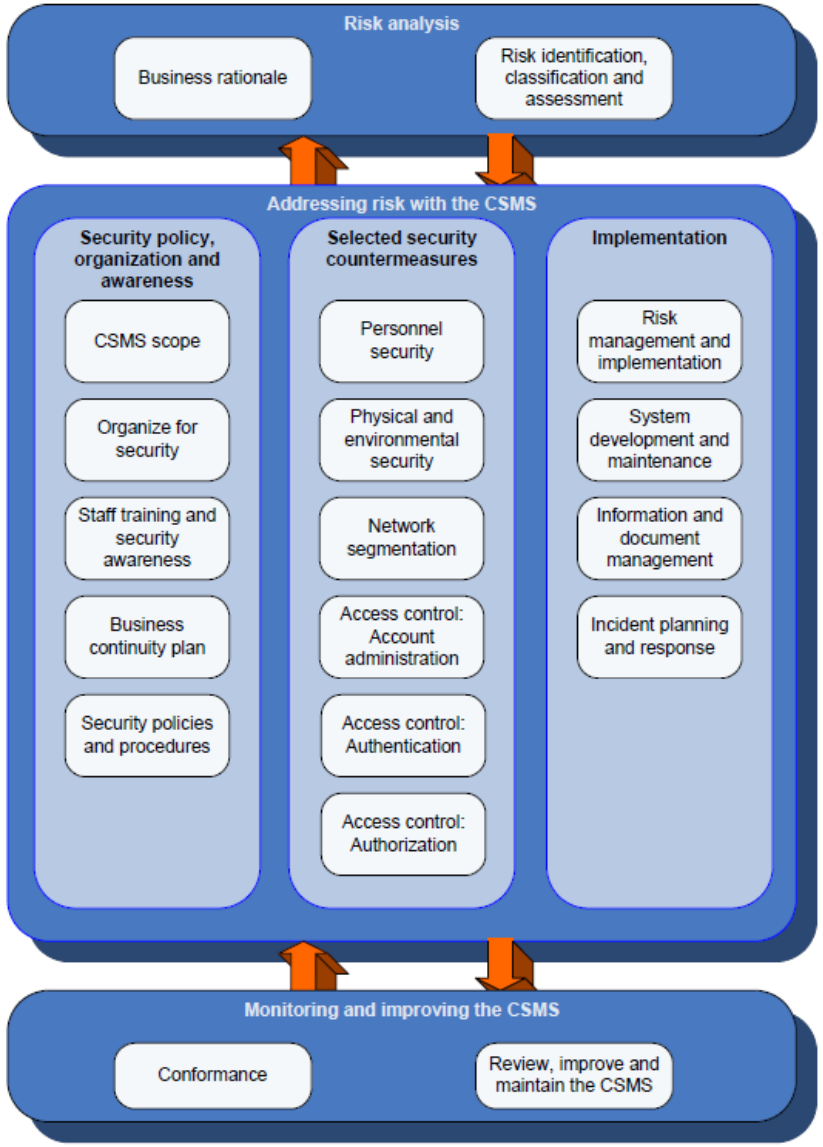


Figure 1 – Graphical view of elements of a cyber security management system

Ref – ISA/IEC 62443 Part 2-1

ß Large

PART 2-1 – ESTABLISHING AN IACS SECURITY PROGRAM (CONT.)

Figure A.2 – Graphical view of category: Risk analysis

4.2.3 Element: Risk identification, classification, and assessment

Objective:

Identify the set of IACS cyber risks that an organization faces and assess the likelihood and severity of these risks.

Description:

Organizations protect their abilities to perform their missions by systematically identifying, prioritizing and analyzing potential security threats, vulnerabilities, and consequences using accepted methodologies. The first set of requirements presents the actions an organization takes to carry out both a high level and a detailed risk assessment that incorporates vulnerability assessment, in a typical chronological order. Among these requirements, those related to preparing for high level and detailed risk assessments are 4.2.3.1, 4.2.3.2 and 4.2.3.8. The last few requirements (4.2.3.10 to 4.2.3.14) are general requirements that apply to the overall risk assessment process. Section 4.3.4.2 covers the process of taking action based upon this assessment.

Rationale:

Since the purpose of investing in cyber security is to lower risk, it is driven by an understanding of level of risk and potential mitigations.

Requirements:

Description		Requirement
4.2.3.1	**Select a risk assessment methodology**	The organization shall select a particular risk assessment and analysis approach and methodology that identifies and prioritizes risks based upon security threats, vulnerabilities and consequences related to its IACS assets.
4.2.3.2	**Provide risk assessment background information**	The organization should provide participants in the risk assessment activity with appropriate information including methodology training, before beginning to identify the risks.
4.2.3.3	**Conduct a high-level risk assessment**	A high-level system risk assessment shall be performed to understand the financial and HSE consequences in the event that availability, integrity or confidentiality of the IACS is compromised.
4.2.3.4	**Identify the industrial automation and control systems**	The organization shall identify the various IACS, gather data about the devices to characterize the nature of the security risk, and group the devices into logical systems.
4.2.3.5	**Develop simple network diagrams**	The organization shall develop simple network diagrams for each of the logically integrated systems showing the major devices, network types, and general locations of the equipment.
4.2.3.6	**Prioritize systems**	The organization shall develop the criteria and assign a priority rating for mitigating the risk of each logical control system.
4.2.3.7	**Perform a detailed vulnerability assessment**	The organization shall perform a detailed vulnerability assessment of its individual logical IACS, which may be scoped based on the high-level risk assessment results and prioritization of IACS subject to these risks.
4.2.3.8	**Identify a detailed risk assessment methodology**	The organization's risk assessment methodology shall include methods for prioritizing detailed vulnerabilities identified in the detailed vulnerability assessment.
4.2.3.9	**Conduct a detailed risk assessment**	The organization shall conduct a detailed risk assessment incorporating the vulnerabilities identified in the detailed vulnerability assessment.
4.2.3.10	**Identify the reassessment frequency and triggering criteria**	The organization shall identify the risk and vulnerability reassessment frequency as well as any reassessment triggering criteria based on technology, organization, or industrial operation changes.
4.2.3.11	**Integrate physical, HSE and cyber security risk assessment results**	The results of physical, HSE and cyber security risk assessments shall be integrated to understand the assets' overall risk.
4.2.3.12	**Conduct risk assessments throughout the lifecycle of the IACS**	Risk assessments shall be conducted through all stages of the technology lifecycle including development, implementation, changes, and retirement.
4.2.3.13	**Document the risk assessment**	The risk assessment methodology and the results of the risk assessment shall be documented.
4.2.3.14	**Maintain vulnerability assessment records**	Up-to-date vulnerability assessment records should be maintained for all assets comprising the IACS.

Ref – ISA/IEC 62443 Part 2-1

PART 2-1 – ESTABLISHING AN IACS SECURITY PROGRAM (CONT.)

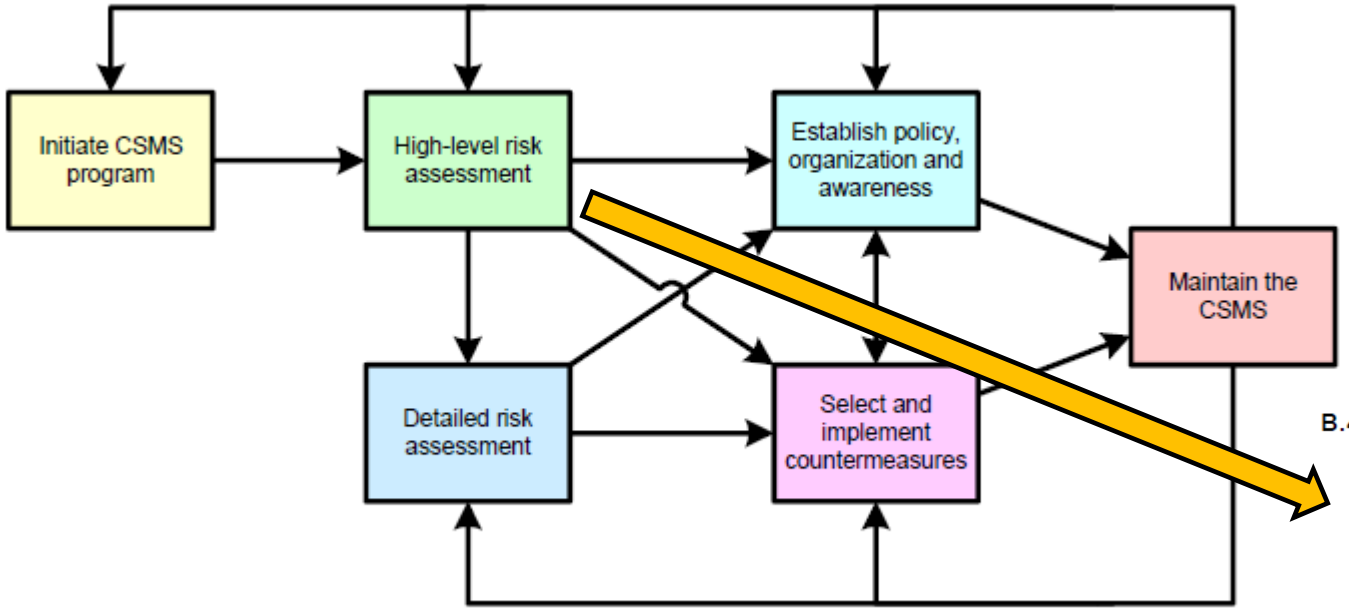


Figure B.1 – Top level activities for establishing a CSMS

B.4 Activity: High-level risk assessment

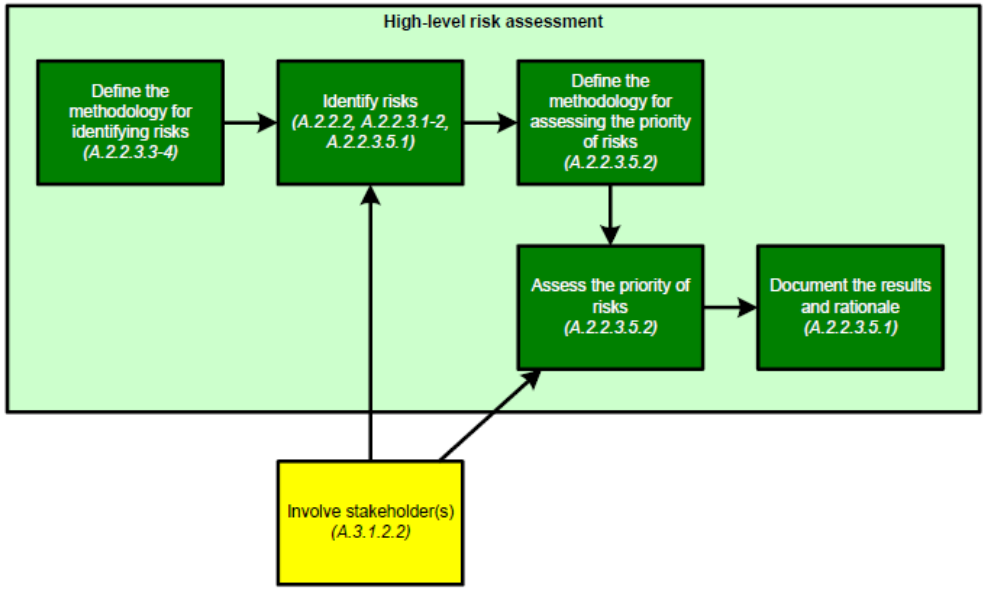


Figure B.3 – Activities and dependencies for activity: High-level risk assessment

Ref – ISA/IEC 62443 Part 2-1

ß Large

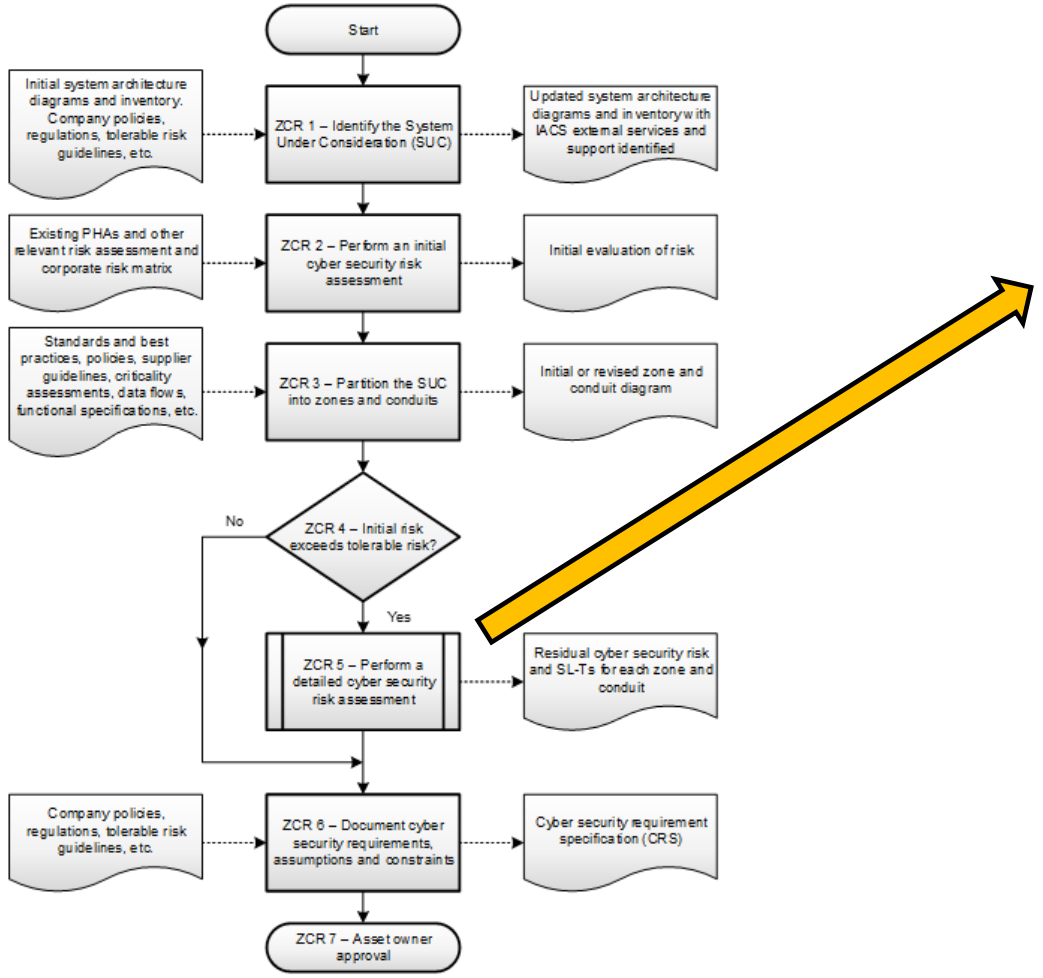
ISA/IEC 62443 PART 3-2

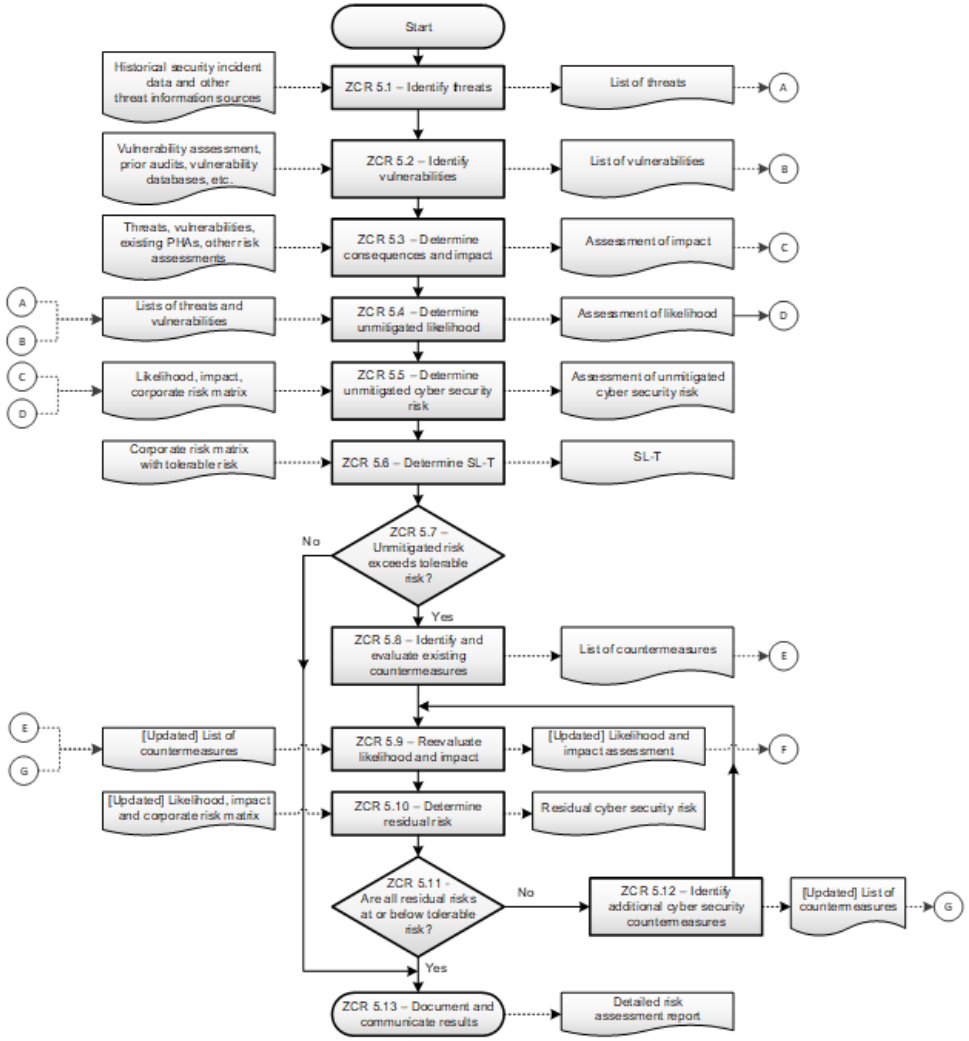
PART 3-2 – SECURITY RISK ASSESSMENT, SYSTEM PARTITIONING AND SECURITY LEVELS

- Defines Cyber Vulnerability Assessments (CVA), Cyber Risk Assessment (CRA) and the Cyber Security Risk Assessment
- Types of Cyber Vulnerability Assessments:
  - Bench Mark assessment (Gap Assessment)
  - Passive Vulnerability Assessment
  - Active Vulnerability Assessment
  - Penetration Testing
- This is the Standard that describes the process of determining Zones and Conduits and their respective Security Levels (Target, Capability and Achieved)

Ref – ISA/IEC 62443 Part 3-2

PART 3-2 – CONT.





Ref – https://gca.isa.org/blog/white-paper-excerpt-leveraging-isa-62443-3-2-for-iacs-risk-assessment-and-risk-related-strategies

PART 3-2 – CONT.

				Consequence														
	Threat Scenario				Impact													
Zone	Threat Source	Threat Action	Vulnerabilities	Consequence Description	S	E	F	R	Max	UTL	Risk	SL-T	Countermeasures	MTL	Risk	Recommendations	ATL	Risk
Process Control Zone	Authorised Personnel	Inserts USB into Operation Station (OS) with General Malware	* OS Computers are in the Control Room * USB Ports are not blocked or disabled * Autorun not disabled * No Antivirus	* Denial of service on operator station that spreads to all OS on PCN * All OS and Servers need to be rebuilt * 24-72 hours downtime * Rework batch * Supply chain impact	1	1	2	3	3	5	15	2	* Policies and Procedures	5	15	* Disable unused USB prots (E.g. GPO, Registry, SEP, etc) * Relocate OS computers to the server room and KVM to Control Room * Segment the Tag & Batch servers and the EWS from the PCN and Control Lan (e.g. Elimiate all Dual Homed Computers) * Install and maintain Antivirus * Stricter enforcement of policies * Upgrade OS and application software to supported version	2	6
		Inserts USB into Operator Station with targeted malware	* OS Computers are in the Control Room * USB Ports are not blocked or disabled * Autorun not disabled * No Antivirus	* Loss of control with potential compromise of the safety of the process * Runaway reaction leading to explosion	5	5	5	5	5	2	10	1	* Policies and Procedures	2	10	* Disable unused USB prots (E.g. GPO, Registry, SEP, etc) * Relocate OS computers to the server room and KVM to Control Room * Segment the Tag & Batch servers and the EWS from the PCN and Control Lan (e.g. Elimiate all Dual Homed Computers) * Install and maintain Antivirus * Stricter enforcement of policies * Upgrade OS and application software to supported version	1	5
		Plugs laptop infected with general malware into the Control LAN	* Unused ports on the Control LAN switch are enabled * No Policy governing use of Laptops * No antivirus on Tag and Batch servers * Lack of segmentation allows for propergation	* Denial of service on operator station that spreads to all OS on PCN * All OS and Servers need to be rebuilt * 24-72 hours downtime * Rework batch * Supply chain impact	1	1	2	3	3	4	12	2	* Laptops are running a supported OS, are patched and running Anti-Virus	4	12	* Develop policies to prohibit use of laptops on Control LAN * Block unused porst on Control LAN Switch * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and Maintain Antivirus	1	3
		Plugs laptop infected with targeted malware into the Control LAN	* Unused ports on the Control LAN switch are enabled * No Policy governing use of Laptops * No antivirus on Tag and Batch servers * Lack of segmentation allows for propergation	* Loss of control with potential compromise of the safety of the process * Runaway reaction leading to explosion	5	5	5	5	5	2	10	1		2	10	* Develop policies to prohibit use of laptops on Control LAN * Block unused porst on Control LAN Switch * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and Maintain Antivirus	1	5
		Engineer remotes into the EWS from the Plant Business Zone using VNC and makes changes without knowledge of current process conditions	* By defualt VNC credentials are in 'clear text' * VNC file transfer capabilities * EWS is dua- homed	* Possible process upset or modification leading to loss of batch	1	1	2	1	2	4	8	1		4	8	* Develop and enforce MoC Process * Eliminate VNC	1	2
		Unauthorised person uses the VNC credentials to gain access to the EWS	* No lock-out on VNC	* Loss of control with potential compromise of the safety of the process * Runaway reaction leading to explosion	5	5	5	5	5	3	15	2		3	15	* Develop and enforce MoC Process * Eliminate VNC	1	5

Ref – ISA IC33M Assessing the Cybersecurity of New or Existing IACS Systems Training

PART 3-2 – RISK (CONT.)

!! Key Concept !!

- The Cyber Security Requirements Specification (CSRS) documents:
  - ZCR 6.2: System under Consideration (SuC) Description
  - ZCR 6.3: Zone and Conduit drawings
  - ZCR 6.4: Zone and Conduit Characteristics
  - ZCR 6.5: Operating environment assumptions
  - ZCR 6.6: Threat Environment
  - ZCR 6.7: Organisational security policies
  - ZCR 6.8: Tolerable Risk
  - ZCR 6.9: Regulatory Requirements

Ref – ISA/IEC 62443 Part 3-2

ß Large

ISA/IEC 62443 PART 3-3

PART 3-3 – CONTROLS

- Defines 100 System Requirements (SR) which include Requirement Enhancements (RE)
- Grouped by 7 Foundational Requirements (FRs)
  1. IAC - Identification and Authentication Control
  2. UC - Use Control
  3. SI - System Integrity
  4. DC - Data Confidentiality
  5. RDF - Restricted Data Flow
  6. TRE - Timely Response to Events
  7. RA - Resource Availability

Ref – ISA/IEC 62443 Part 3-3

ß Large

PART 3-3 – CONTROLS (CONT.)

The 100 Requirements are assigned to Security Levels 1 to 4:

- SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or **casual exposure.**
- SL 2 - Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means **with low resources, generic skills and low motivation.**
- SL 3 - Prevent the unauthorized disclosure of information to an entity actively searching for it **using sophisticated means with moderate resources, IACS specific skills and moderate motivation.**
- SL 4 - Prevent the unauthorized disclosure of information to an entity actively searching for it **using sophisticated means with extended resources, IACS specific skills and high motivation.**

Security level *–*
level corresponding to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit.
From Part 1-1

Ref – ISA/IEC 62443 Part 3-3

ß Large

PART 3-3 – CONTROLS (CONT.)

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 5 – Restricted data flow (RDF)				
SR 5.1 – Network segmentation				
RE (1) Physical network seg				
RE (2) Independence from n networks				
RE (3) Logical and physical networks				
SR 5.2 – Zone boundary protecti				
RE (1) Deny by default, allov				
RE (2) Island mode				
RE (3) Fail close				

9.3 SR 5.1 – Network segmentation

9.3.1 Requirement

The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

9.3.2 Rationale and supplemental guidance

Network segmentation is used by organizations for a variety of purposes, including cyber security. The main reasons for segmenting networks are to reduce the exposure, or ingress, of network traffic into a control system and reduce the spread, or egress, of network traffic from a control system. This improves overall system response and reliability as well as provides a measure of cyber security protection. It also allows different network segments within the control system, including critical control systems and safety-related systems, to be segmented from other systems for an additional level of protection.

Access from the control system to the World Wide Web should be clearly justified based on control system operational require

Network segmentation and the le overall network architecture used within their control systems. Logic some measure of protection, but compromised. Physically segment that single-point-of-failure case, These trade-offs will need to ISA-62443-2-1 (99.02.01)).

In response to an incident, it m network segments. In that event,

9.3.3 Requirement enhancements

(1) Physical network segmentation

The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.

(2) Independence from non-control system networks

The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.

(3) Logical and physical isolation of critical networks

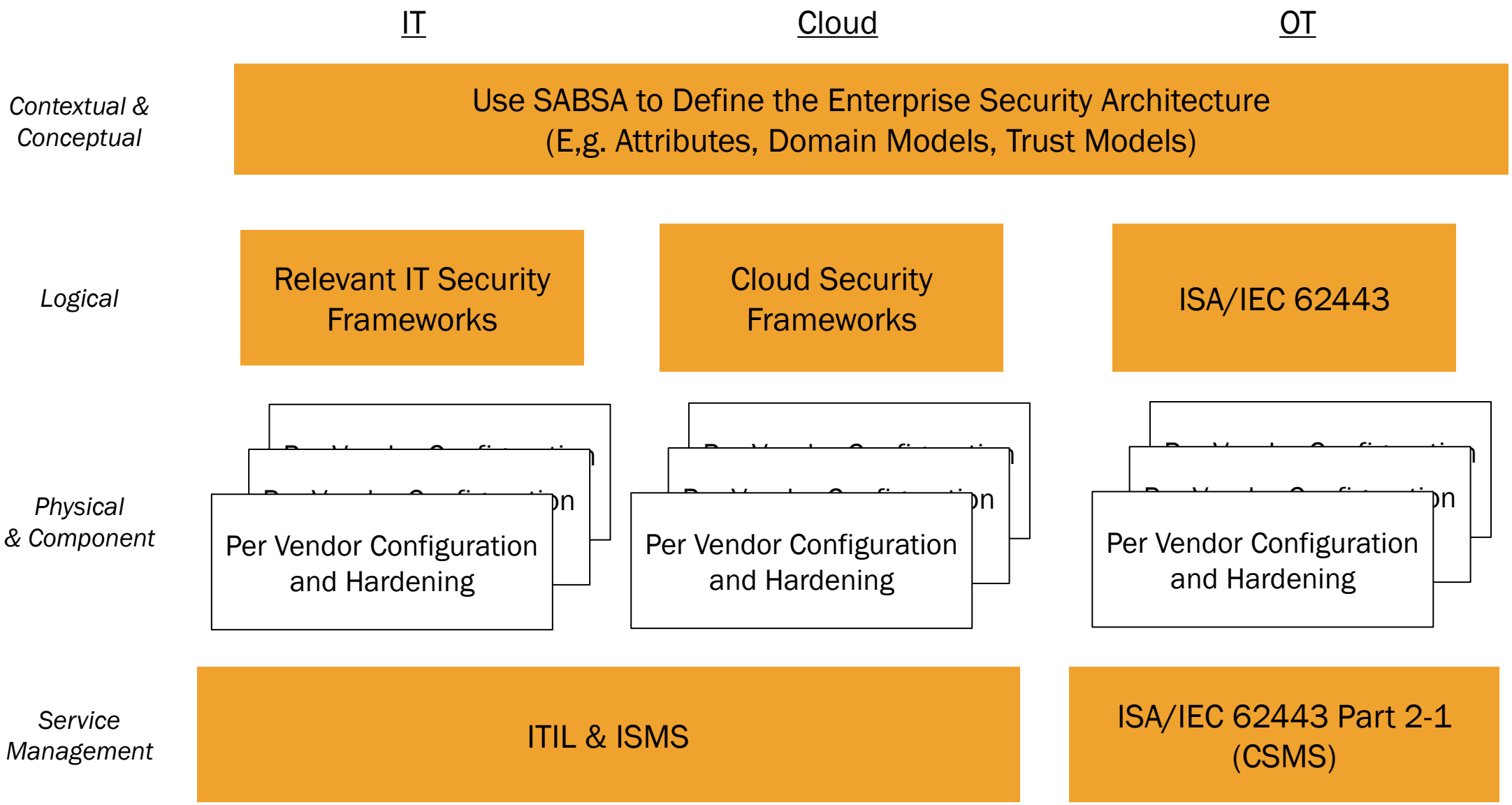
The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.

Ref – ISA/IEC 62443 Part 3-3

ß Large

ALIGNING SABSA AND ISA/IEC 62443

HOW TO ALIGN THE FRAMEWORKS CONCEPTUALLY



ß Large

HOW TO ALIGN THE FRAMEWORKS FOR OT

- Use SABSA to set the Whole of Enterprise understanding of security
  - Define Attributes Hierarchy, Domain Models
  - Define common security service objectives for the entire enterprise
  - Use Attributes to achieve traceability of cyber security (Think Requirements Engineering)
- Use ISA/IEC 62443 to develop the Logical & Service Management Views – Use ISA/IEC 62443 to inform Physical and Component Requirements
- Use Vendor Security Reference Architectures to support Physical and Component (e.g. Control System Vendor Guidance, Cisco SAFe, Cloud Security Reference Architectures etc)
- Use ISA/IEC 62443 to Define your Cyber Security Management System
- I have included in the Appendix of the Slides Alignment of SABSA Matrix Cells and ISA/IEC 62443 Concepts

ß Large

HIGH LEVEL ALIGNMENT OF SABSA AND ISA/IEC 62443

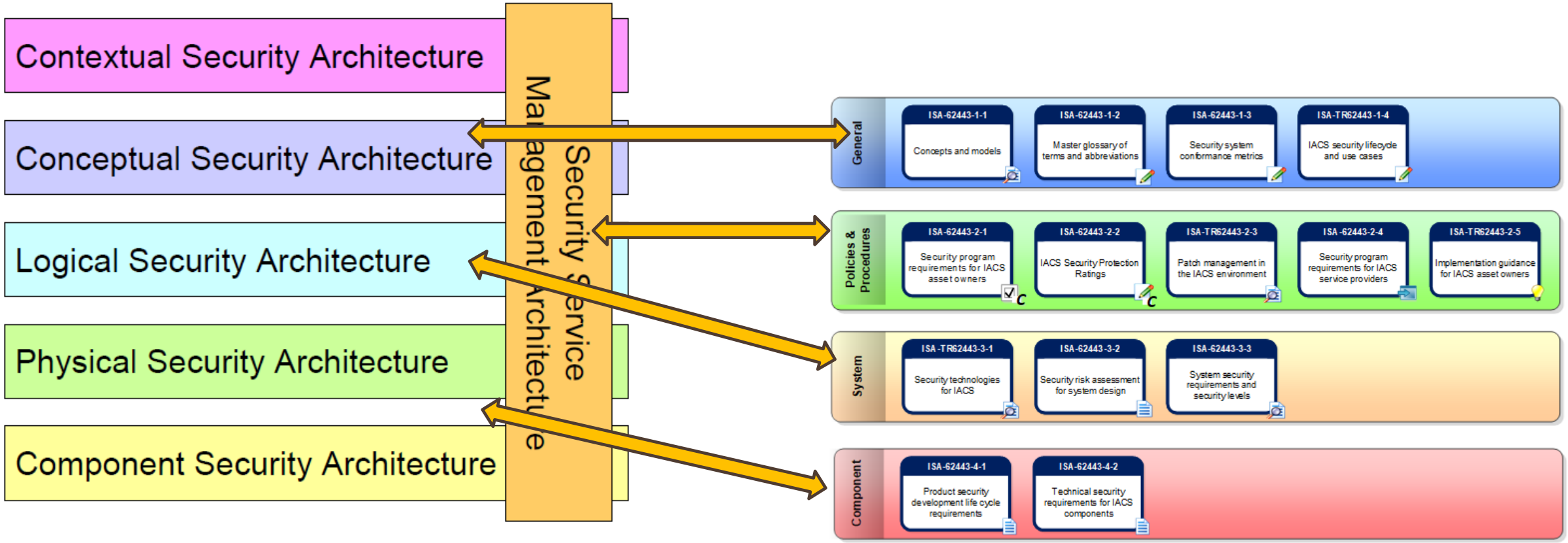


Figure 1: The SABSA Model for Security Architecture

WORKED EXAMPLE

THE STATE POWER CORPORATION

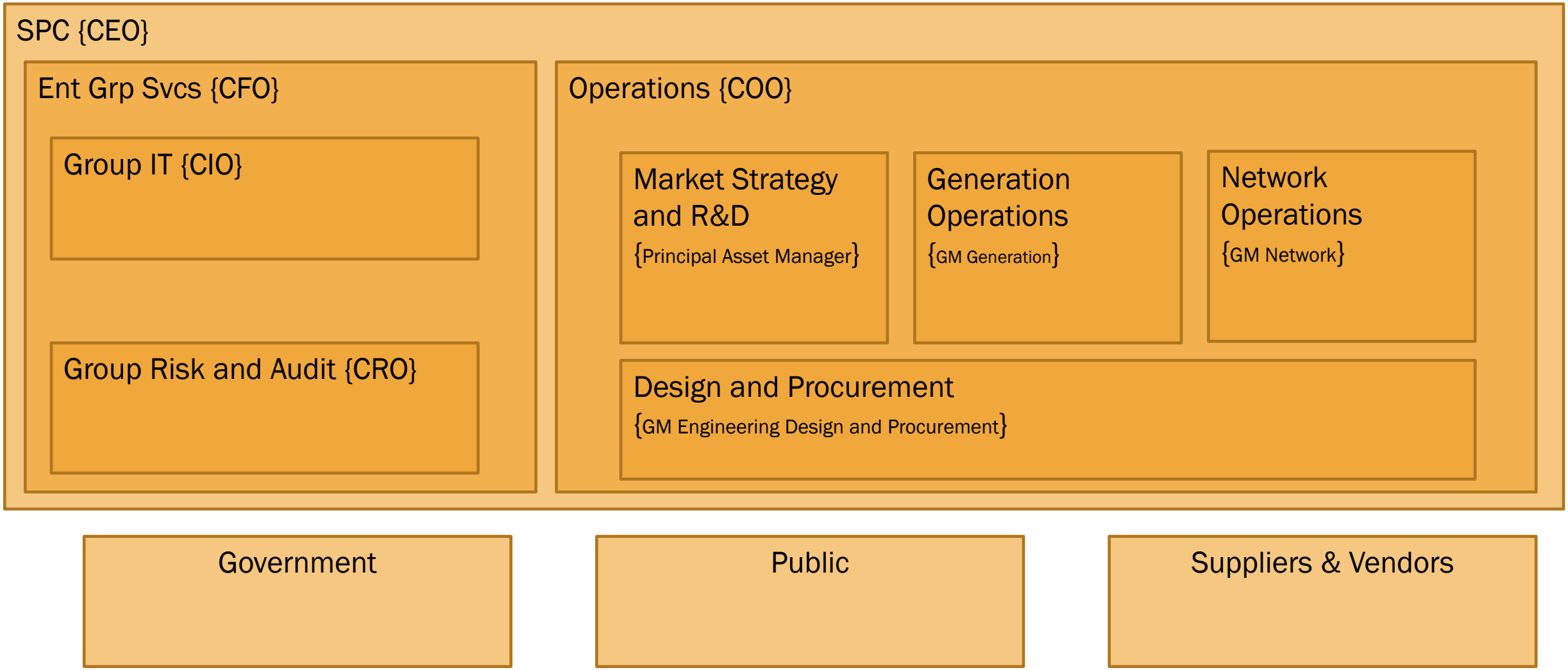
AN OVERVIEW OF STATE POWER CORPORATION

- *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

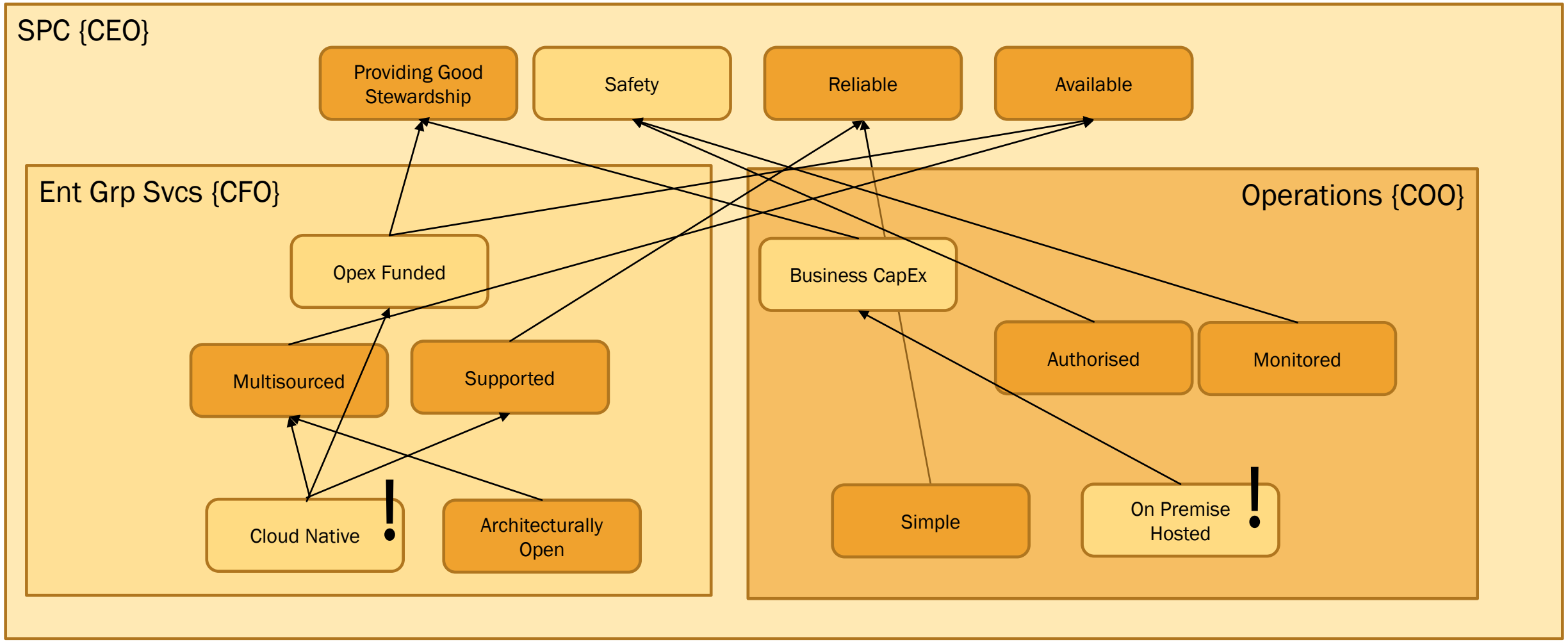
AN OVERVIEW OF STATE POWER CORPORATION (CONT.)

- 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

DOMAIN MODEL DERIVATION



SAMPLE ATTRIBUTE TAXONOMY



NEW ATTRIBUTES FOR THIS EXAMPLE

Management Attributes

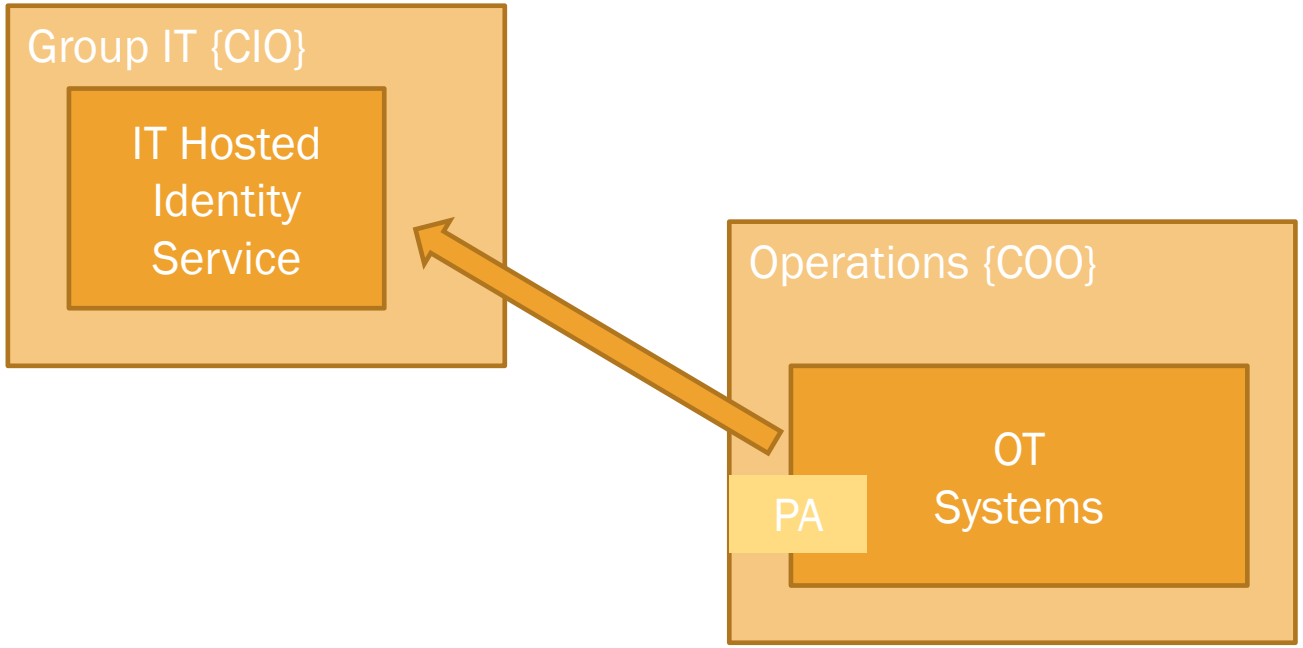
- *Safety* – Does the security solution impact the safe operation of the system
- *Business Capex Funded* – Given the regulated environment of utilities, Capital Expenditure (CapEx) solutions are preferred to Operational Expense Funded (OpEx) for the regulated network parts of the business

Technical

- *On Premise Hosted* – For reliability and survivability reasons, solutions that are hosted on premise are preferred for OT
- *Cloud Native* – For the Support Services group, the business strategy prefers and embraces cloud native solutions

TRUST DECOMPOSITION FOR THE AN IDENTITY SERVICE

- Conflicting priorities of domain authorities!
- Conflict of attributes (OnPrem vs Cloud, Cost vs Availability, Fail-Open vs Fail-Close)
- Ongoing support and management of system
- What about cloud hosted identity infrastructure?
- … All good sensible and traceable reasons for OT Hosted Identity Infrastructure

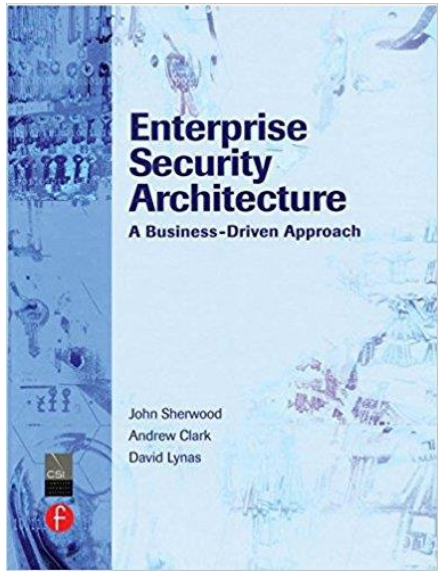


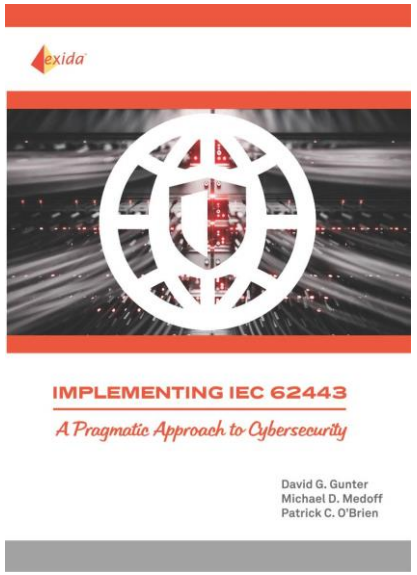
RESOURCES TO LEARN MORE

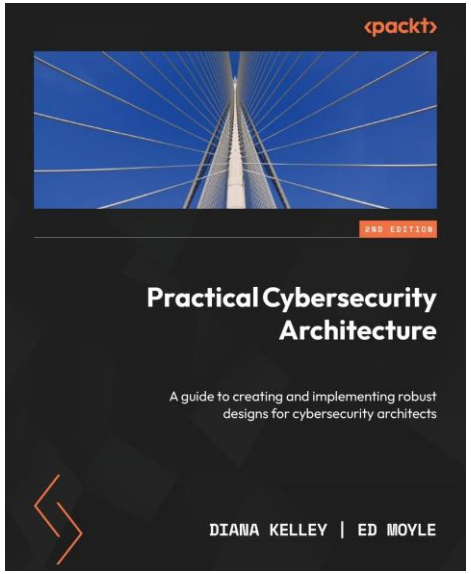
ß Large

FURTHER RESOURCES

- SABSA White Paper (W100)
- ISA/IEC 62443 Quick Start Guide
- Enterprise Security Architecture
  A Business- Driven Approach
- Implementing IEC 62443 - A Pragmatic Approach to Cybersecurity
- Practical Cyber Security Architecture
- Join The SABSA Institute
- Join SABSA World Australia







THANK YOU, QUESTIONS?


https://linkedin.com/in/blargeau


https://github.com/beLarge


bruce@blarge.io

ß Large

APPENDIX

ALIGNMENT OF SABSA MATRIX AND ISA/IEC 62443 CONCEPTS

ß Large

SABSA MATRIX - CONTEXTUAL & CONCEPTUAL LAYER

	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
		Part 3-2: Initial Risk Assessment		**Part 3-2: Initial Risk Assessment (ZCR - 1)**	**Part 3-2: System Under Consideration (SuC)**	

CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
		Part 3-2: Initial Risk Assessment			**Part 3-2: System Under Consideration (SuC) & Part 1-1: Zones & Conduits**	

SABSA MATRIX – LOGICAL

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
		Part 2-1 : Security Policies & Procedures	**Part 3-2: ZCR Partition the SuC into Zones & Conduits**	**Part 3-2: ZCR Partition the SuC into Zones & Conduits**	**Part 3-2: ZCR Partition the SuC into Zones & Conduits**	

SABSA MATRIX – PHYSICAL AND COMPONENT

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
		Part 2-1: Risk Identification, classification and assessment & Part 3-2: all	**Part 3-3 & Part 4-2**	**Part 3-3 & Part 4-2**	**Part 3-3 FR SI, RDF, TRE and RA & Relevant Part 4-2 Sections**	
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management 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
		Part 2-1: & Part 3-2: Cyber Security Requirements Specification		**Part 3-3: FR IAC and FR UC**		**Part 3-3: FR UC**

SABSA MATRIX – SERVICE MANAGEMENT

SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable
		Part 2-1: Risk Identification, Classification and Assessment		Part 2-1: Access control: [Account Administration, Authentication, Authorisation]	Part 2-1: Physical and environmental security	Part 2-1: Conformance

SABSA SERVICE LIFE CYCLE MATRIX – CONTEXTUAL AND CONCEPTUAL

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
	Part 2-1: Business Rationale	Part 2-1: Risk Identification, Classification and Assessment		Part 2-4: Security Program Requriements for IACS Service Providers		Part 2-1: CSMS Scope; Business Rationale

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
	Part 2-1: Risk Identification, Classification and Assessment	Part 2-1: Risk Identification, Classification and Assessment		Part 2-1: Organising for security		

SABSA SERVICE LIFE CYCLE MATRIX – LOGICAL

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
	Part 2-1: System development and maintenance	Part 2-1: Security policies and procedures	Part 2-1: Business Continuity Plan	Part 2-1: Access control: [Account Administration, Authentication, Authorisation]	Part 2-1: System development and maintenance	Part 2-1: Conformance

SABSA SERVICE LIFE CYCLE MATRIX – PHYSICAL AND COMPONENT

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
	Part 2-1: Physical and environmental security	**Part 2-1: Risk management and implementation**		**Part 2-1: Access control: [Account Administration, Authentication, Authorisation]**	**Part 2-1: Physical and environmental security**	
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
		Part 2-1: Risk management and implementation		**Part 2-1: Staff training and security awareness; Part 2-1:Personnel security**		

ALIGNMENT OF FRS AND SAMPLE SECURITY SERVICES

62443 FR	Sample Security Services
Identification and Authentication Control	Entity Authentication, User Authentication
Use Control	Entity authorisation, Logical Access Control
System Integrity	Software Integrity Protection
Data Confidentiality	Traffic Flow Confidentiality
Restricted Data Flow	???
Timely Response to Events	Security monitoring Security alarm management Incident Response*
Resource Availability	???