Let’s get (Cyber) Physical

Aligning SABSA and the ISA/IEC 62443 Standard Series

/whois @beLarge

- Operational Technology (OT) Security Team Leader at Powerlink
- A cyber security architecture enthusiast & infrastructure tourist
- SABSA SCF and (*still…)* working on my SCP A3 Paper
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for 15 years
- I am the "*Bruce*" in Patrick Dunstan's SCM Thesis in Appendix A
- Chair of the Queensland Branch of the Information, Telecommunications and Electronics Engineering (ITEE) College of Engineers Australia
- Deputy Chair of the Queensland Branch of the Australian Information Security Association (AISA) and Chair of the AISA Security Architecture Special Interest Group (SIG)
- Bach Eng (Telecomms) QUT First Class Honours and Master Business (Applied Finance) with Distinction QUT

SABSA FOUNDATION LEVEL SCF

ISA/IEC 62443 CYBERSECURITY EXPERT ISA

GIAC RESPONSE AND INDUSTRIAL DEFENSE GRID

alc Cyber Security Foundation+Practitioner CERTIFIED

Audience Poll

Questions

1. Who has experience with [Operational Technology/Industrial Control Systems/Cyber Physical Systems]?
2. Who has had experience with ISA/IEC 62443?
3. Who is certified (any level) in ISA/IEC 62443?
4. Who is a ISA/IEC 62443 Certified Expert?

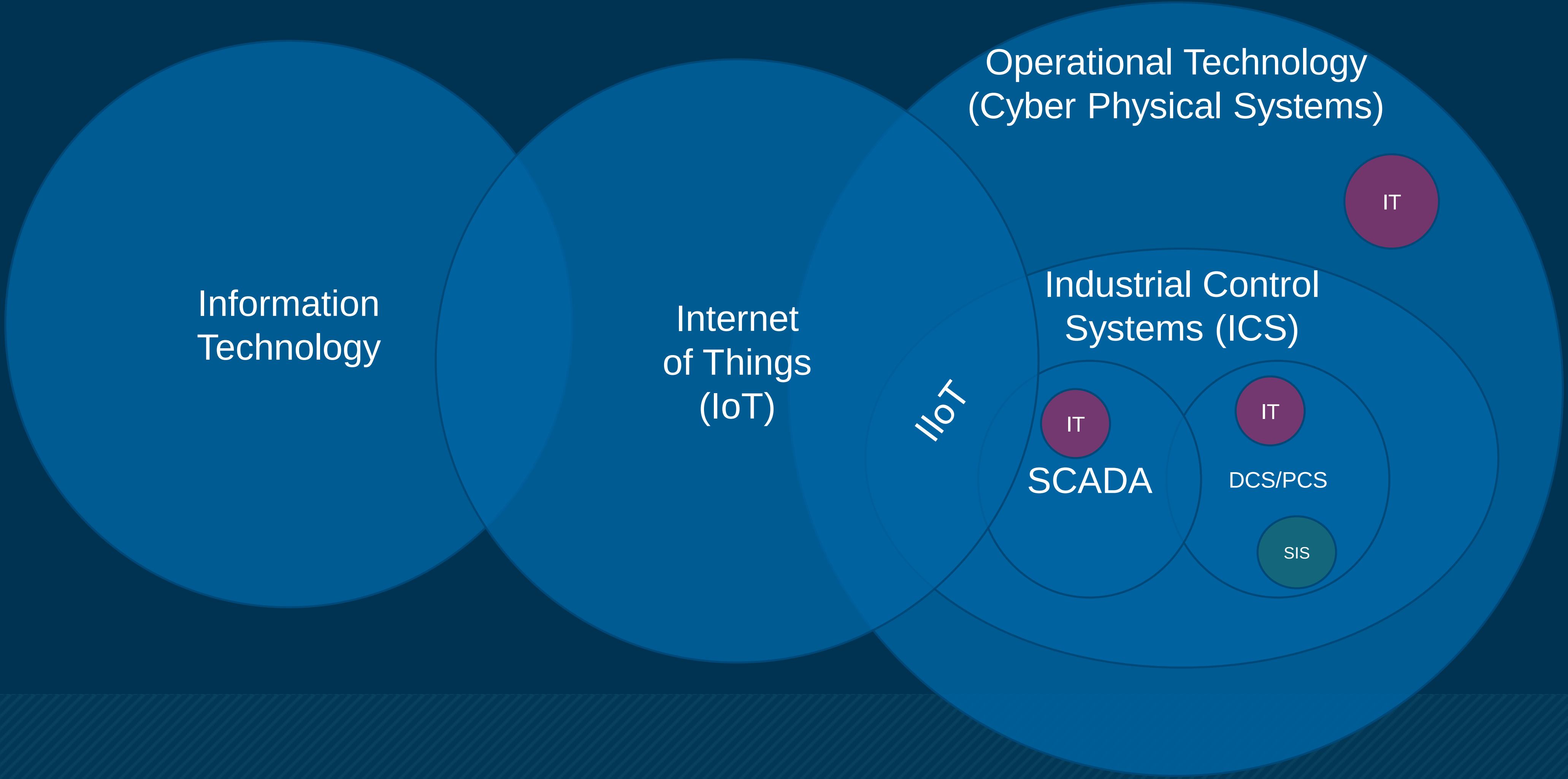
Agenda

1. An Introduction to OT and why SABSA for OT
2. Overview and Alignment to ISA/IEC 62443
3. A Practical Application for an OT Scenario
4. Tips & references for working with your OT Stakeholders
5. End of Session Q&A

An Introduction to OT

And why SABSA For OT

IT, OT, ICS, IoT, Cyber Physical Systems


Information Technology
Internet of Things (IoT)
IIoT
Operational Technology (Cyber Physical Systems)
IT
Industrial Control Systems (ICS)
IT
SCADA
IT
DCS/PCS
SIS

Industrial Automation & Control Systems (IACS)

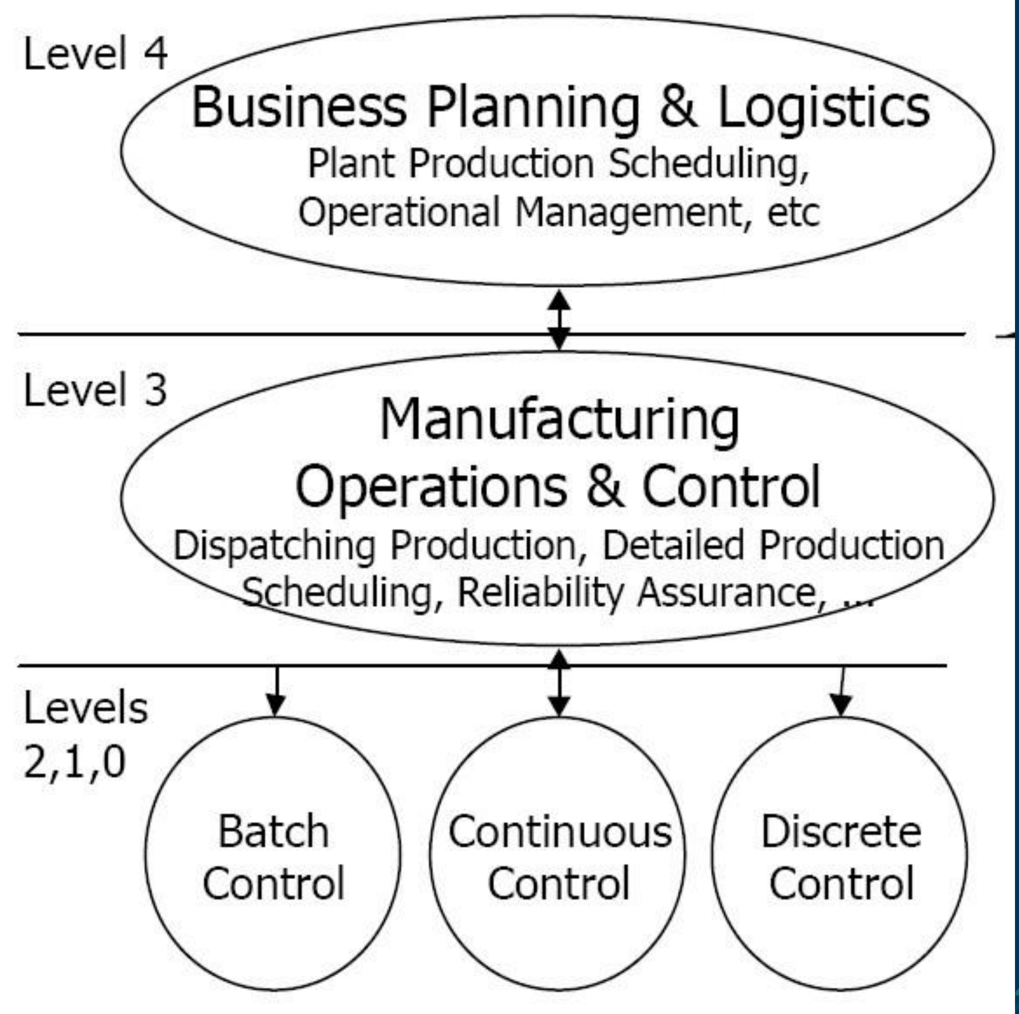
An IACS is defined as a:

> *collection of personnel, hardware, software, and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation.*

Source – ISAGCA Quick Start Guide: An Overview of ISA/IEC 62443 Standards

The Purdue Model

- Reference architecture developed in the 90s to guide the integration of business systems and Industrial Control Systems
- Originally was used to determine where best to interconnect different network technologies



Level 4
Business Planning & Logistics
Plant Production Scheduling, Operational Management, etc
Level 3
Manufacturing Operations & Control
Dispatching Production, Detailed Production Scheduling, Reliability Assurance, ...
Levels 2,1,0
Batch Control
Continuous Control
Discrete Control

Ref – https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

“IT/OT convergence has been occurring since at least the 1990s when HMI/Operator Stations began running on Windows … The skill sets required to deploy and manage these computer-, TCP-/IP-, Ethernet-based systems are the same in both IT and OT. So we are seeing some workforce convergence, as well.”

Source - https://www.tripwire.com/state-of-security/it-ot-convergence-or-it-ot-integration

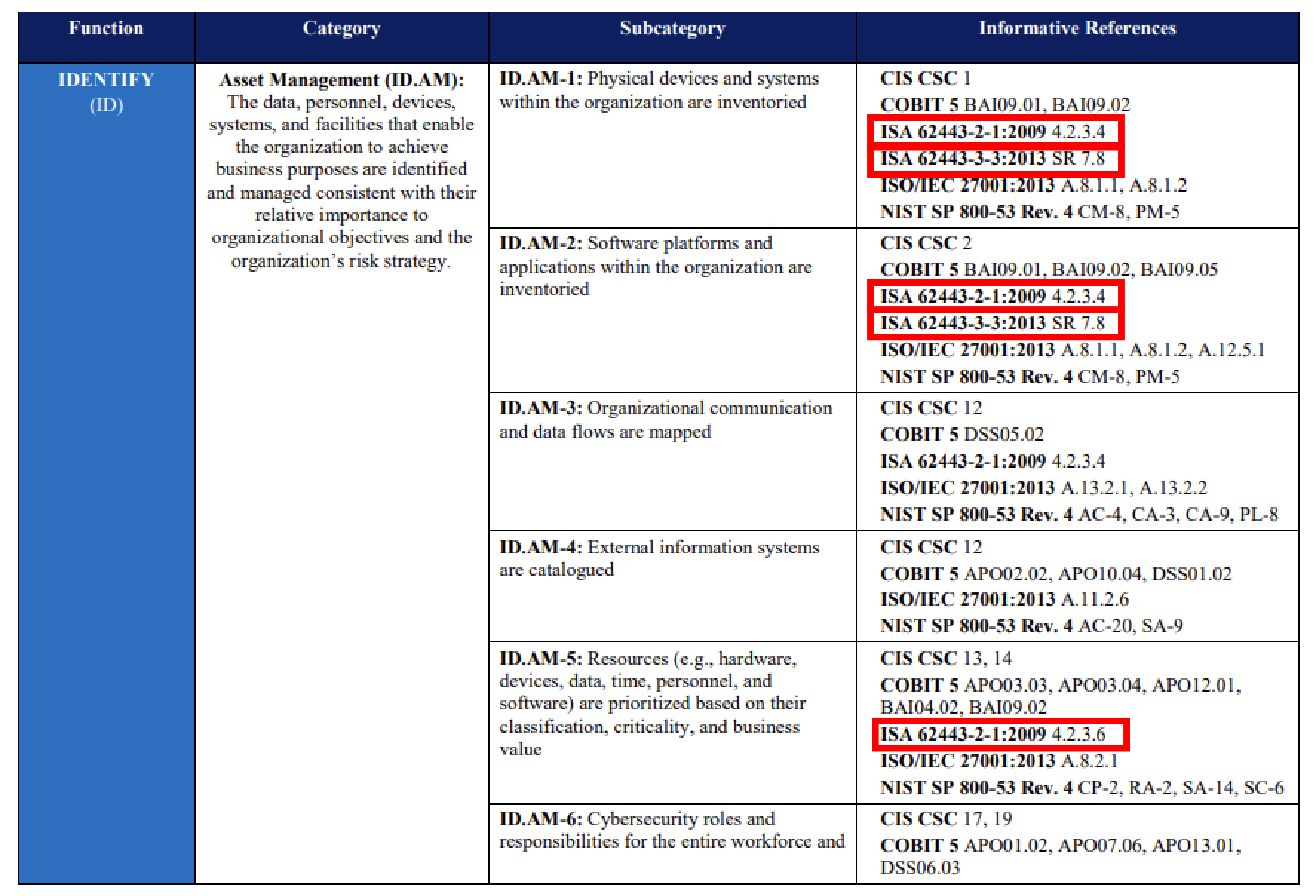
Motivation for this presentation

- To help enable the true management of business risk for the enterprise we must have a common language and shared understanding between IT and OT
- To help educate SABSA practitioners about the nuance of Operational Technology and the ISA/IEC 62443 standard series
- Operational Technology is super cool!

Overview of ISA/IEC 62443

And alignment with SABSA

Does this look familiar …



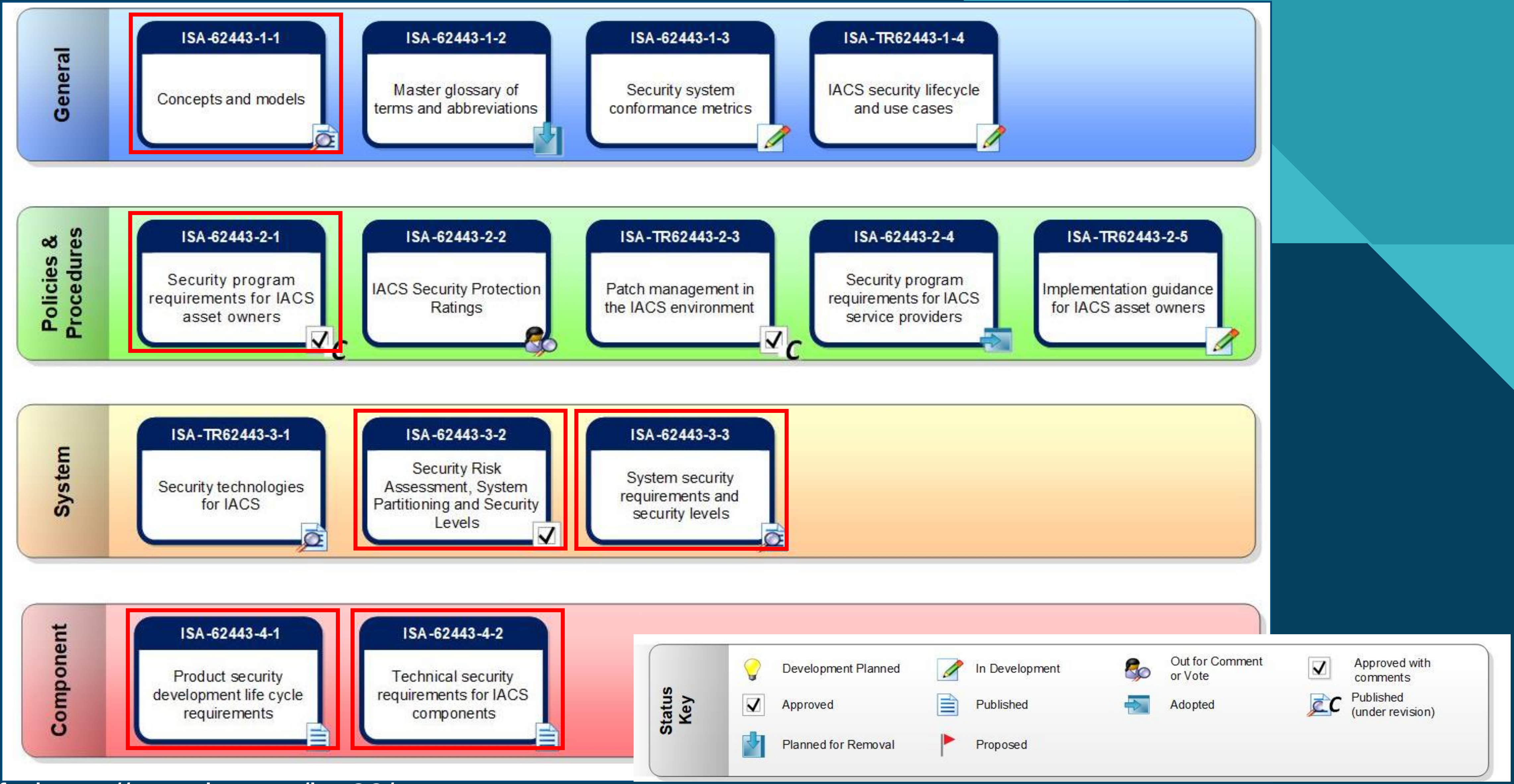
Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

Ref - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

A quick overview

- 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)

ISA 62443 Framework



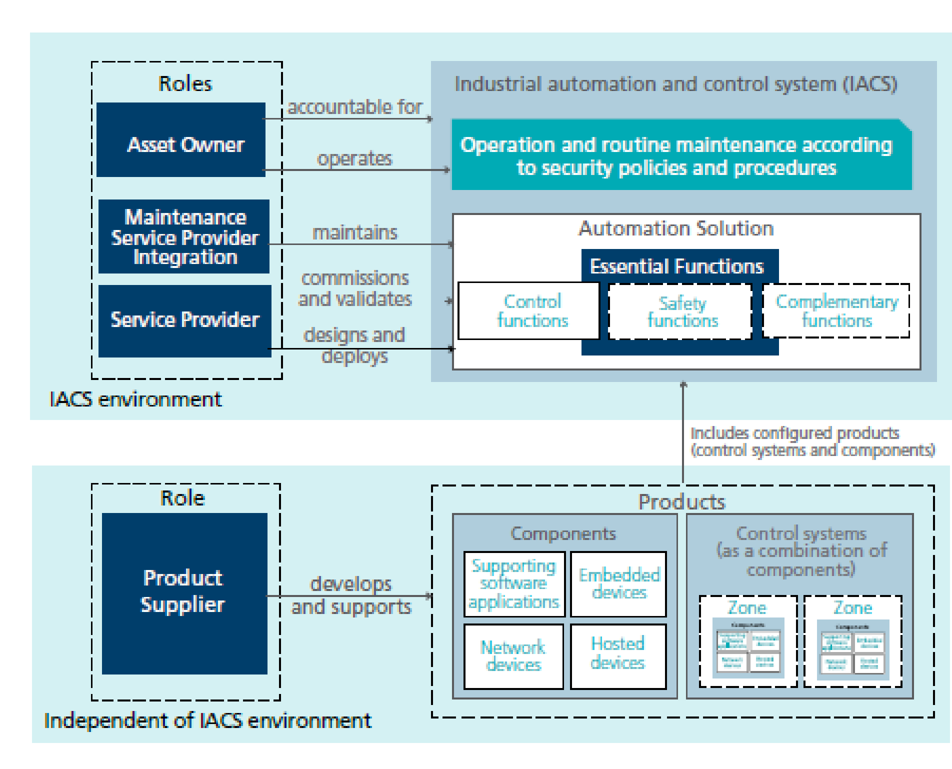
General	ISA-62443-1-1 Concepts and models	ISA-62443-1-2 Master glossary of terms and abbreviations	ISA-62443-1-3 Security system conformance metrics	ISA-TR62443-1-4 IACS security lifecycle and use cases	
Policies & Procedures	ISA-62443-2-1 Security program requirements for IACS asset owners	ISA-62443-2-2 IACS Security Protection Ratings	ISA-TR62443-2-3 Patch management in the IACS environment	ISA-62443-2-4 Security program requirements for IACS service providers	ISA-TR62443-2-5 Implementation guidance for IACS asset owners
System	ISA-TR62443-3-1 Security technologies for IACS	ISA-62443-3-2 Security Risk Assessment, System Partitioning and Security Levels	ISA-62443-3-3 System security requirements and security levels		
Component	ISA-62443-4-1 Product security development life cycle requirements	ISA-62443-4-2 Technical security requirements for IACS components			

Status Key

- Development Planned
- Approved
- Planned for Removal
- In Development
- Published
- Proposed
- Out for Comment or Vote
- Adopted
- Approved with comments
- Published (under revision)

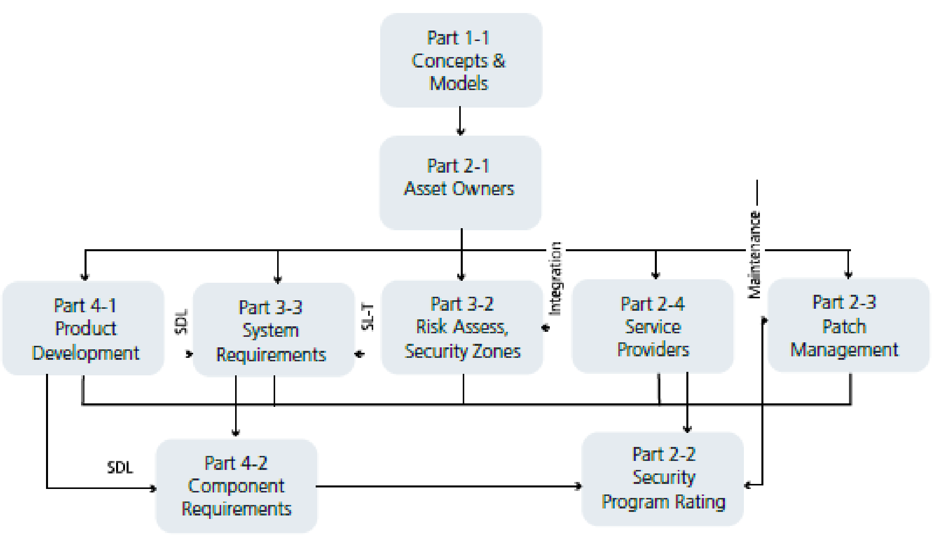
Ref - https://www.isa.org/isa99/

Other perspectives and views …



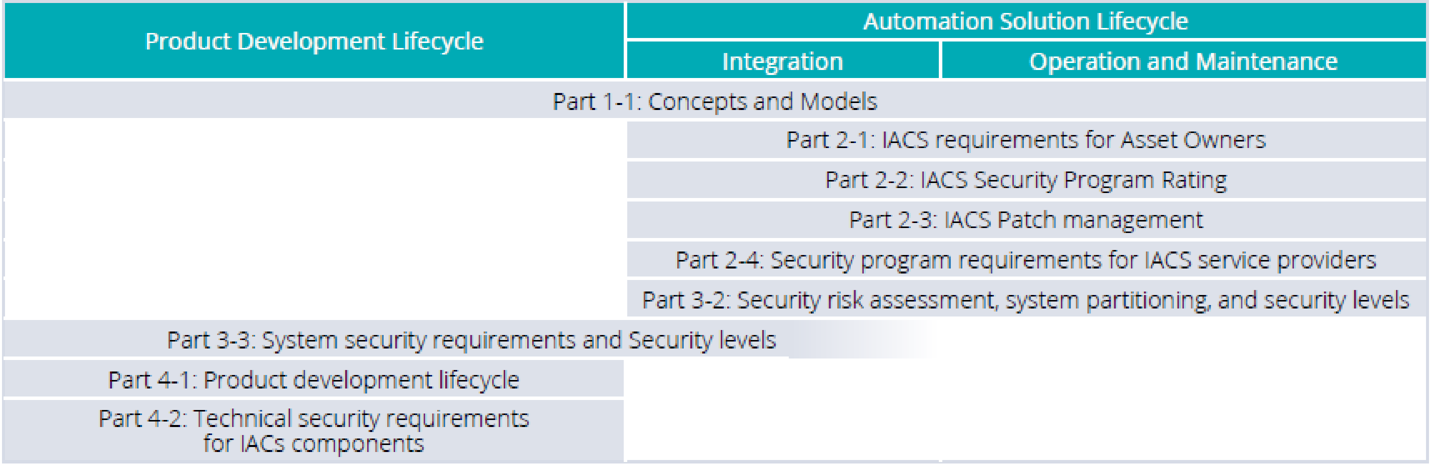
Roles
Asset Owner
Maintenance Service Provider Integration
Service Provider
accountable for
operates
maintains
commissions and validates
designs and deploys
Industrial automation and control system (IACS)
Operation and routine maintenance according to security policies and procedures
Automation Solution
Essential Functions
Control functions
Safety functions
Complementary functions
IACS environment
Includes configured products (control systems and components)
Role
Product Supplier
develops and supports
Products
Components
Supporting software applications
Embedded devices
Network devices
Hosted devices
Control systems (as a combination of components)
Zone
Zone
Independent of IACS environment

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



Part 1-1 Concepts & Models
Part 2-1 Asset Owners
Integration
Maintenance
Part 4-1 Product Development
SDL
Part 3-3 System Requirements
SL-T
Part 3-2 Risk Assess, Security Zones
Part 2-4 Service Providers
Part 2-3 Patch Management
SDL
Part 4-2 Component Requirements
Part 2-2 Security Program Rating

Figure 5: ISA/IEC 62443 Standards – Hierarchical View

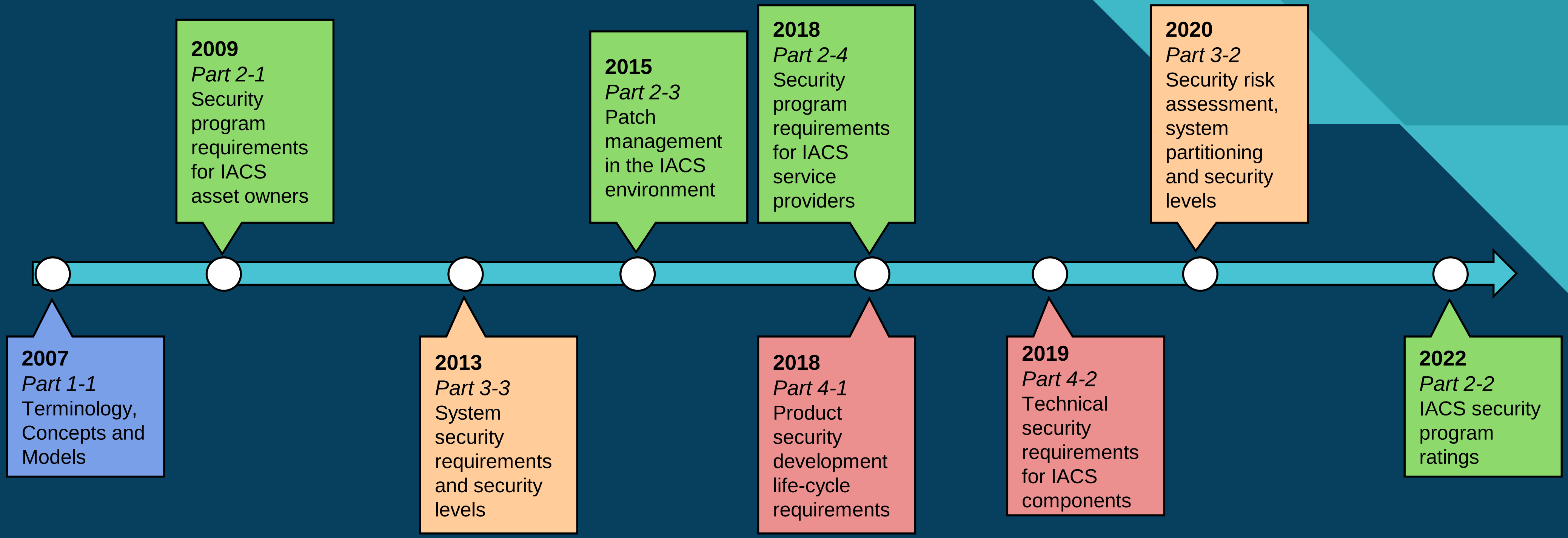


Product Development Lifecycle	Automation Solution Lifecycle	
	Integration	Operation and Maintenance
Part 1-1: Concepts and Models		
	Part 2-1: IACS requirements for Asset Owners	
	Part 2-2: IACS Security Program Rating	
	Part 2-3: IACS Patch management	
	Part 2-4: Security program requirements for IACS 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

Timeline of the Standards Development



2007
Part 1-1
Terminology, Concepts and Models

2009
Part 2-1
Security program requirements for IACS asset owners

2013
Part 3-3
System security requirements and security levels

2015
Part 2-3
Patch management in the IACS environment

2018
Part 2-4
Security program requirements for IACS service providers

2018
Part 4-1
Product security development life-cycle requirements

2019
Part 4-2
Technical security requirements for IACS components

2020
Part 3-2
Security risk assessment, system partitioning and security levels

2022
Part 2-2
IACS security program ratings

ISA/IEC 62443 Part 1-1

Part 1-1 - Concepts and Models

- Definitions (e.g. What is an asset)
- Defines an asset model taxonomy
- Defines a model for Security
- Zones and Conduits
- Defines Security Levels (Target, Achieve, Capability)
- Defines Policies and Procedures Requirements
- and more ...

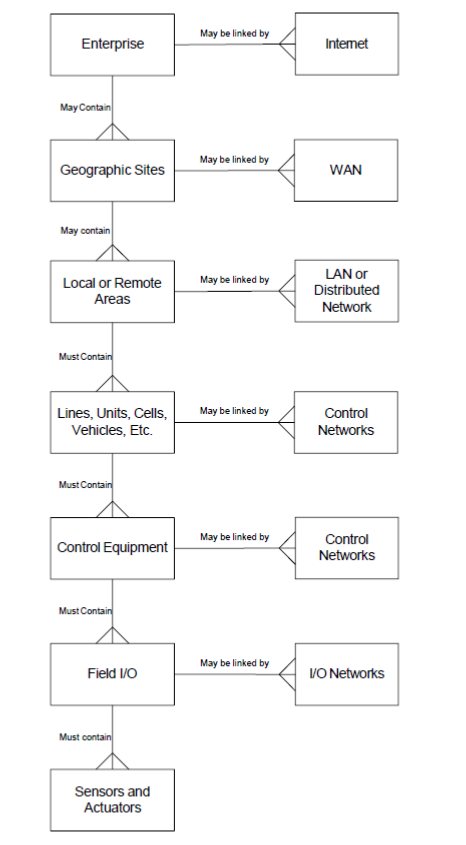


Figure 14 – Process Manufacturing Asset Model Example

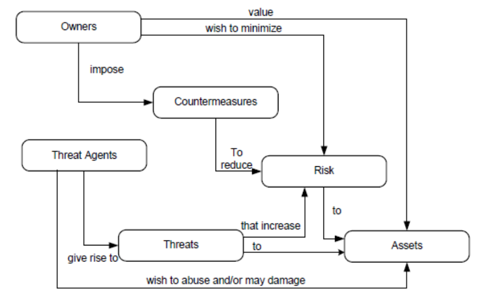


Figure 2 – Context Element Relationships

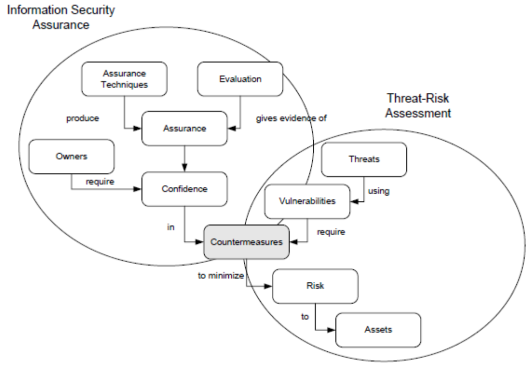


Figure 3 – Context Model

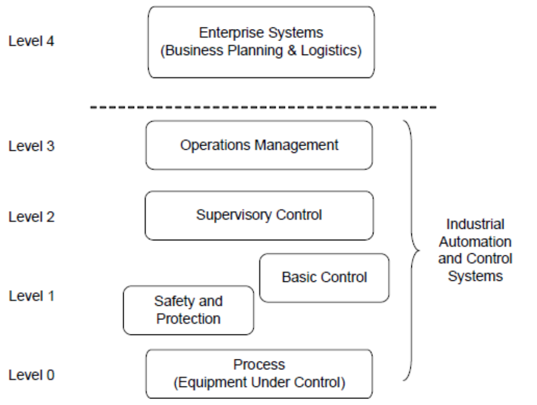

Level 4
Enterprise Systems (Business Planning & Logistics)
Level 3
Operations Management
Level 2
Supervisory Control
Industrial Automation and Control Systems
Basic Control
Level 1
Safety and Protection
Level 0
Process (Equipment Under Control)

Figure 12 – Reference Model for ISA99 Standards

Ref – ISA/IEC 62443 Part 1-1

Part 1-1 – Concepts and Models (cont.)

- Domain
  environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources [11].
- electronic security
  actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets.
- enterprise system
  collection of information technology elements (i.e., hardware, software and services) installed with the intent to facilitate an organization's business process or processes (administrative or project).
- Risk
  expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence.
- Safety
  freedom from unacceptable risk
- Security Architecture
  plan and set of principles that describe the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services, and the performance levels required in the elements to deal with the threat environment .
- 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.

Ref – ISA/IEC 62443 Part 1-1

Part 1-1 – Concepts and Models (cont.)

- Security Zone

  grouping of logical or physical assets that share common security requirements

  NOTE: All unqualified uses of the word "zone" in this standard should be assumed to refer to a security zone.

  NOTE: A zone has a clear border with other zones. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone. Zones can be hierarchical in the sense that they can be comprised of a collection of subzones.

- Conduit

  logical grouping of communication assets that protects the security of the channels it contains.

  NOTE: This is analogous to the way that a physical conduit protects cables from physical damage.

Ref – ISA/IEC 62443 Part 1-1

Part 1-1 – Concepts and Models (cont.)

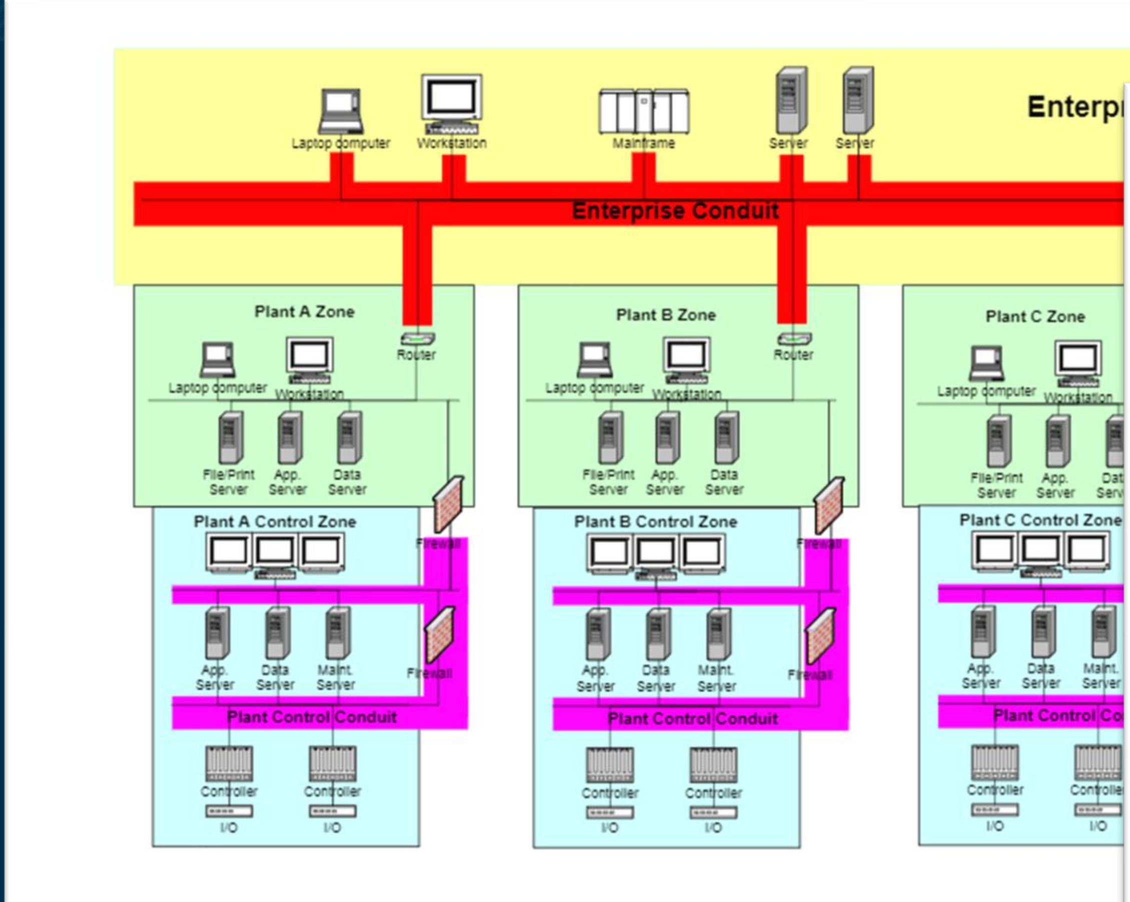


Figure 7 – Conduit Example

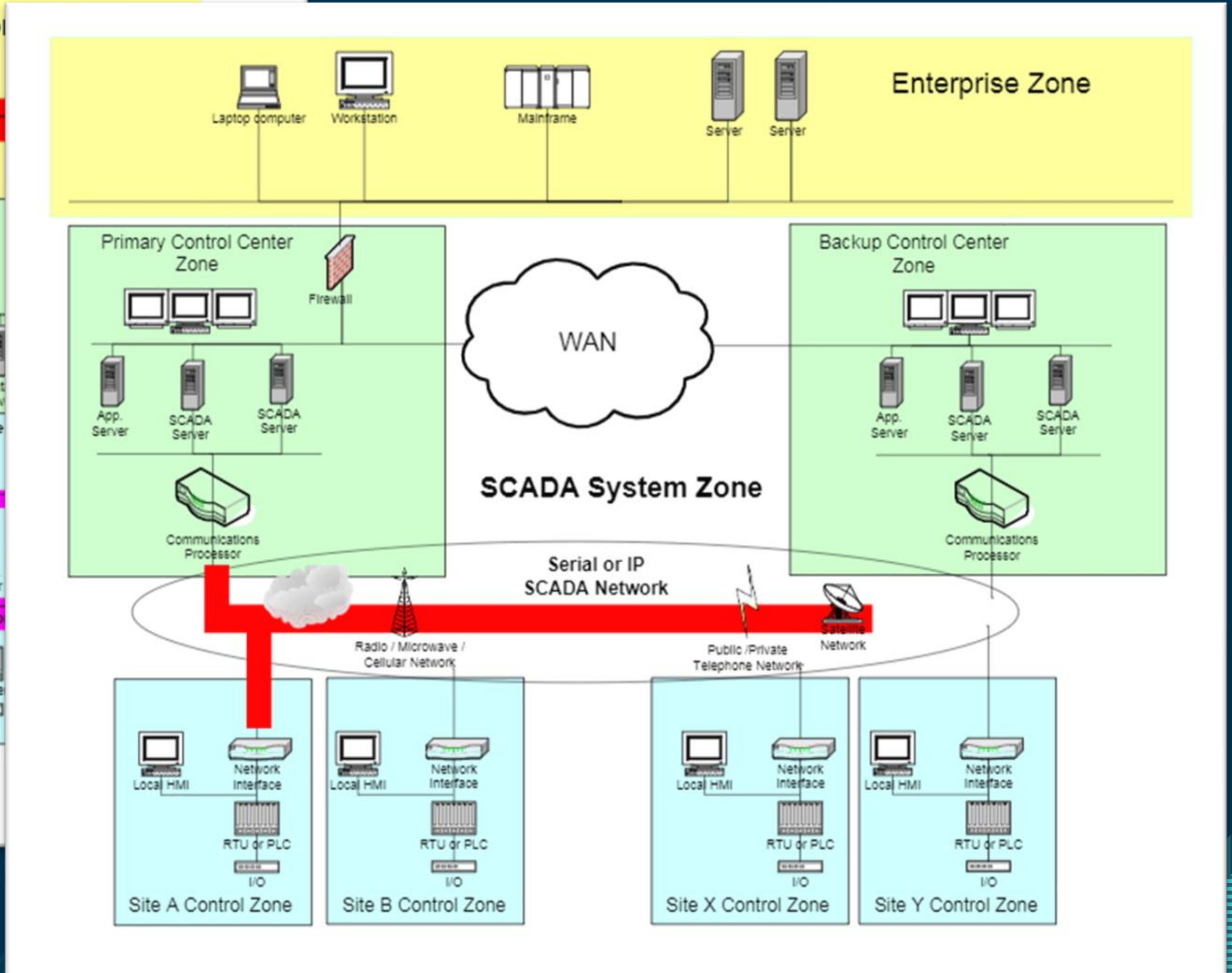


Figure 22 – SCADA Conduit Example

Ref – ISA/IEC 62443 Part 1-1

Part 1-1 – Concepts and Models (cont.)

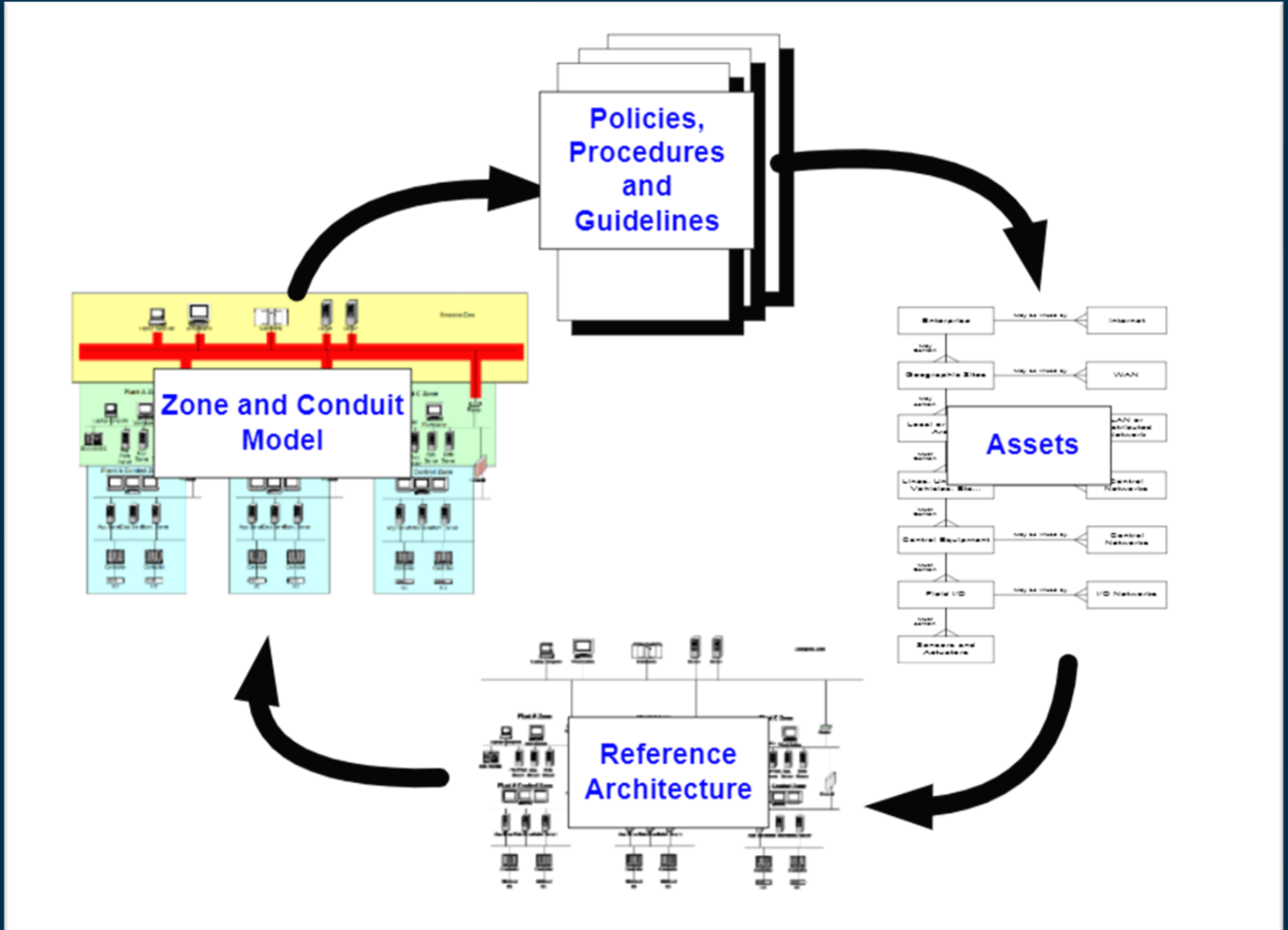


Figure 23 – Model Relationships

Ref – ISA/IEC 62443 Part 1-1

ISA/IEC 62443 Part 2-1

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

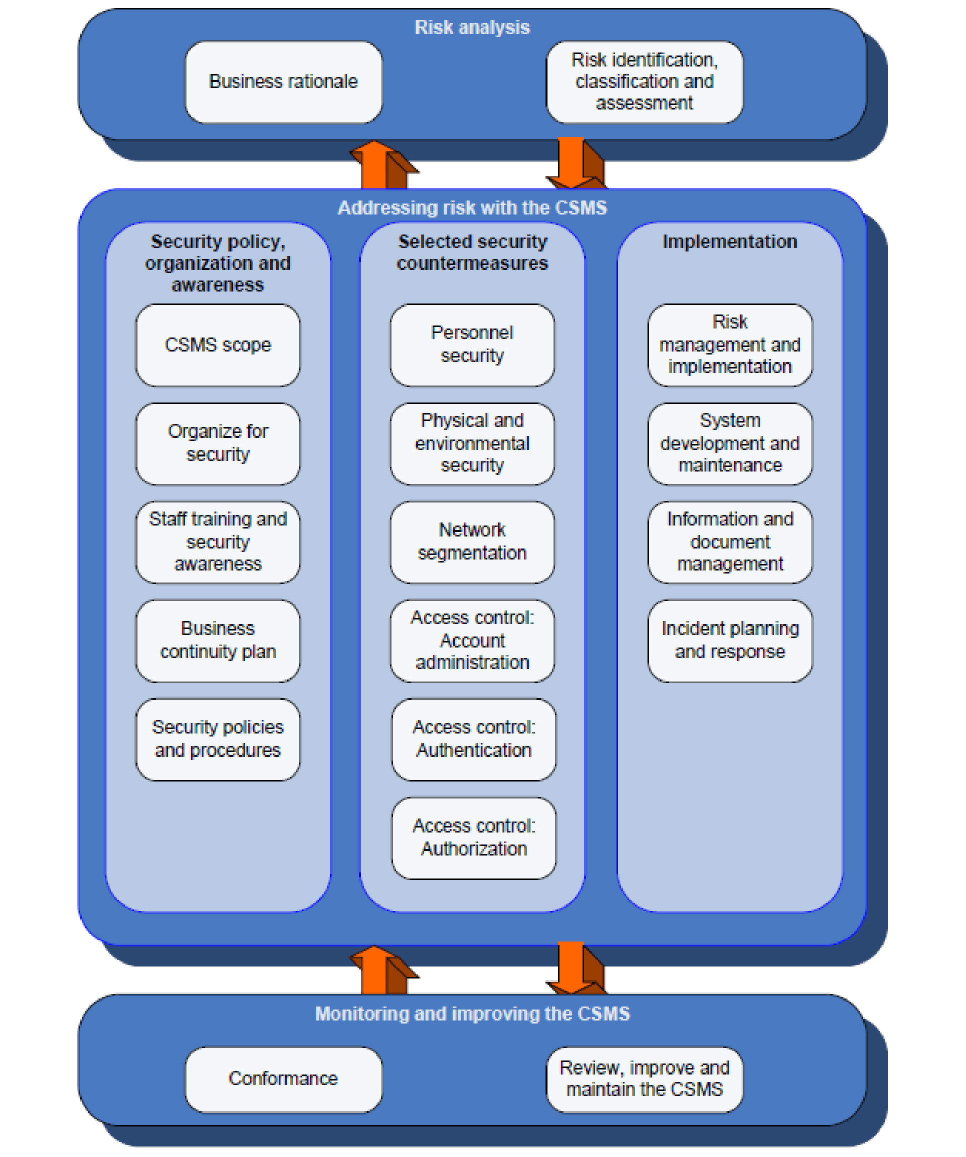

Risk analysis
Business rationale
Risk identification, classification and assessment
Addressing risk with the CSMS
Security policy, organization and awareness
CSMS scope
Organize for security
Staff training and security awareness
Business continuity plan
Security policies and procedures
Selected security countermeasures
Personnel security
Physical and environmental security
Network segmentation
Access control: Account administration
Access control: Authentication
Access control: Authorization
Implementation
Risk management and implementation
System development and maintenance
Information and document management
Incident planning and response
Monitoring and improving the CSMS
Conformance
Review, improve and maintain the CSMS

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

Ref – ISA/IEC 62443 Part 2-1

Part 2-1 – Establishing an IACS Security Program (cont.)

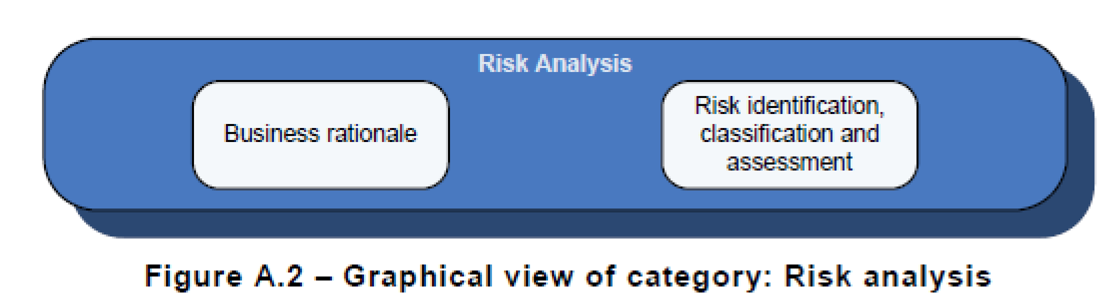
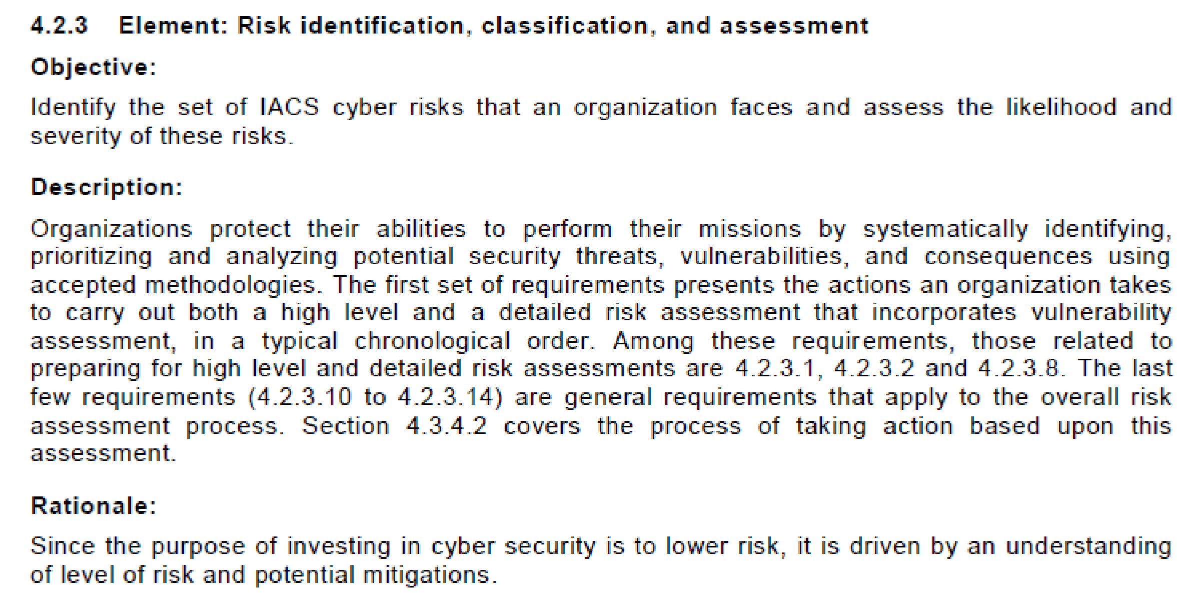


Figure A.2 – Graphical view of category: Risk analysis



4.2.3 Element: Risk identification, classification, and assessment

Objective:

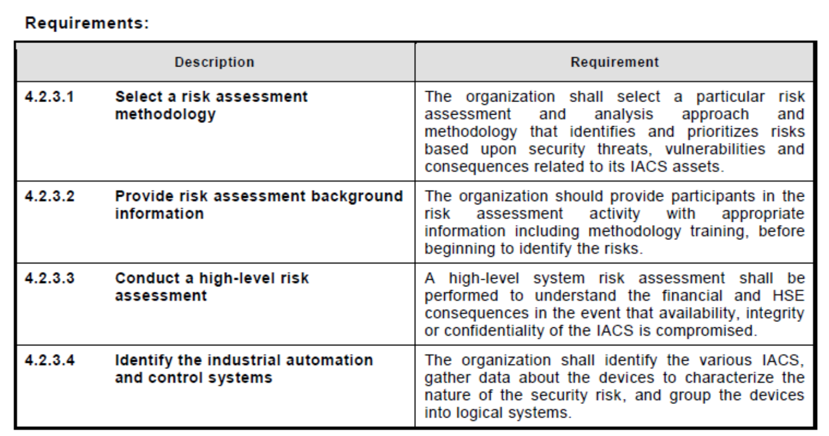
Identify the set of IACS cyber risks that an organization faces and assess the likelihood and severity of these risks.

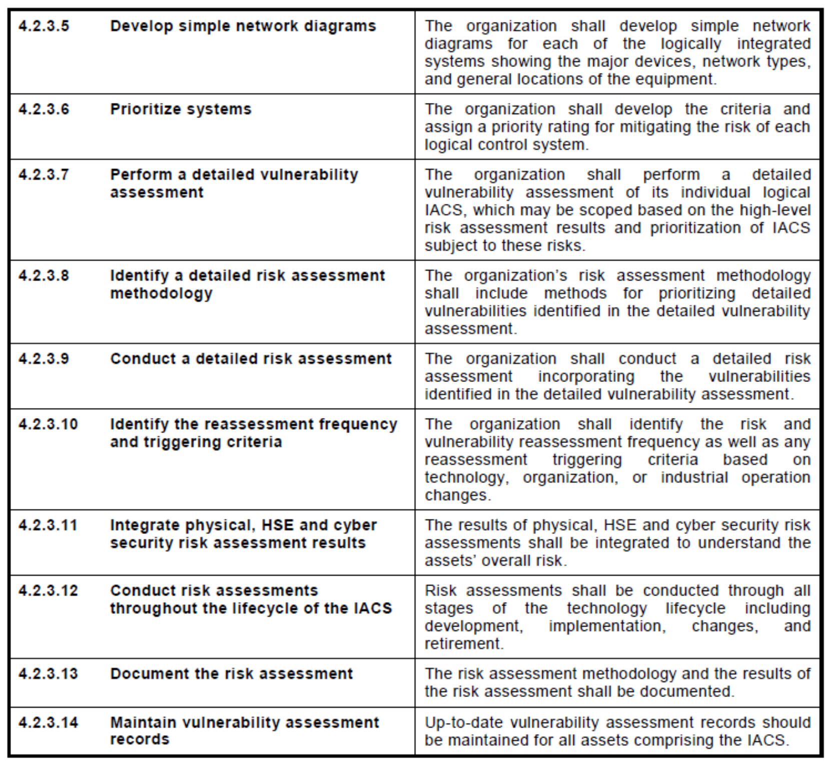
Description:

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.



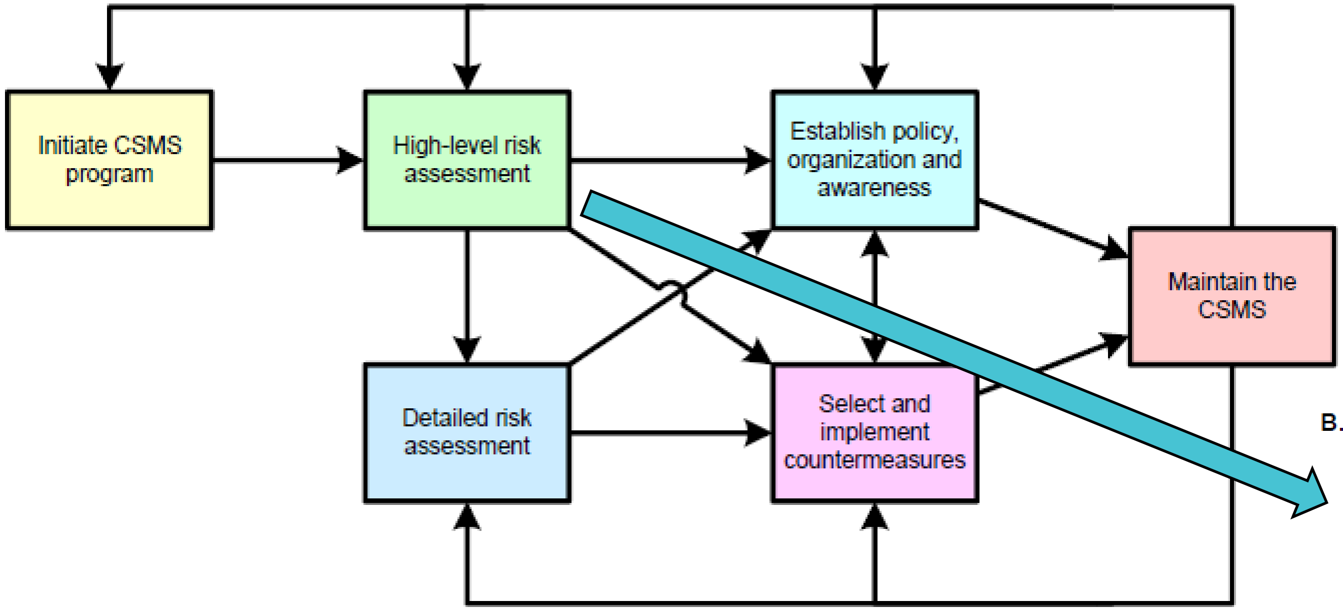


Requirements:

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

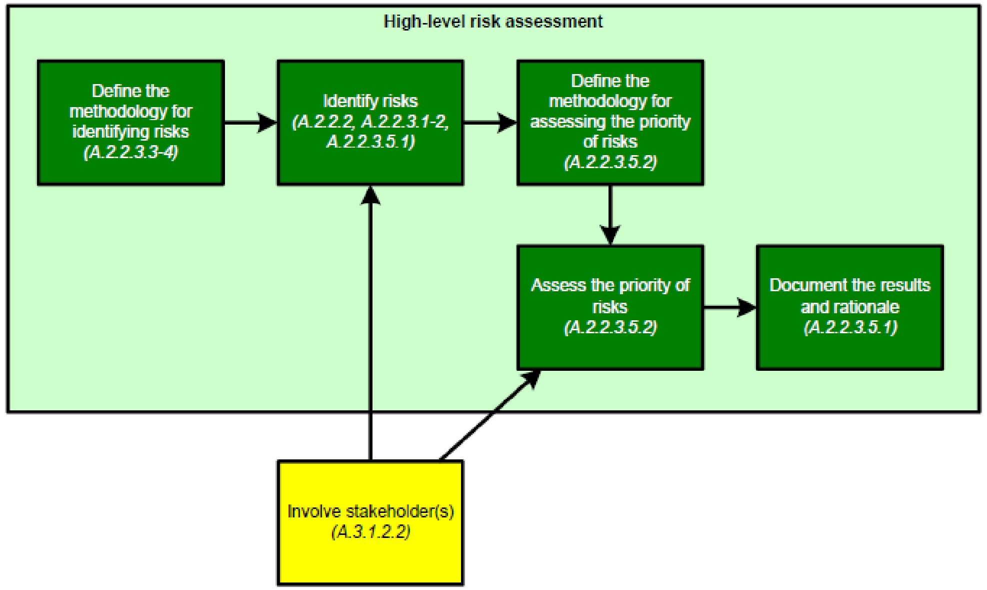
Part 2-1 - Establishing an IACS Security Program (cont.)



Initiate CSMS program
High-level risk assessment
Establish policy, organization and awareness
Maintain the CSMS
Detailed risk assessment
Select and implement countermeasures

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

B.4 Activity: High-level risk assessment



High-level risk assessment
Define the methodology for identifying risks (A.2.2.3.3-4)
Identify risks (A.2.2.2, A.2.2.3.1-2, A.2.2.3.5.1)
Define the methodology for assessing the priority of risks (A.2.2.3.5.2)
Assess the priority of risks (A.2.2.3.5.2)
Document the results and rationale (A.2.2.3.5.1)
Involve stakeholder(s) (A.3.1.2.2)

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

Ref – ISA/IEC 62443 Part 2-1

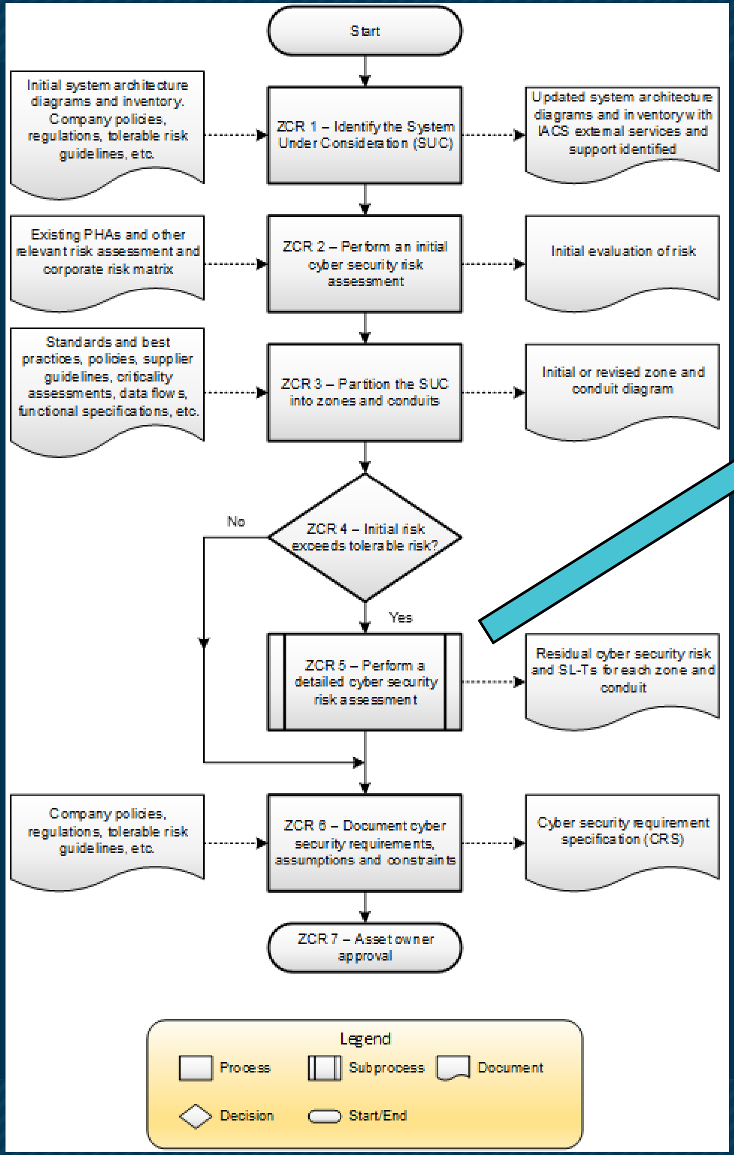
ISA/IEC 62443 Part 3-2

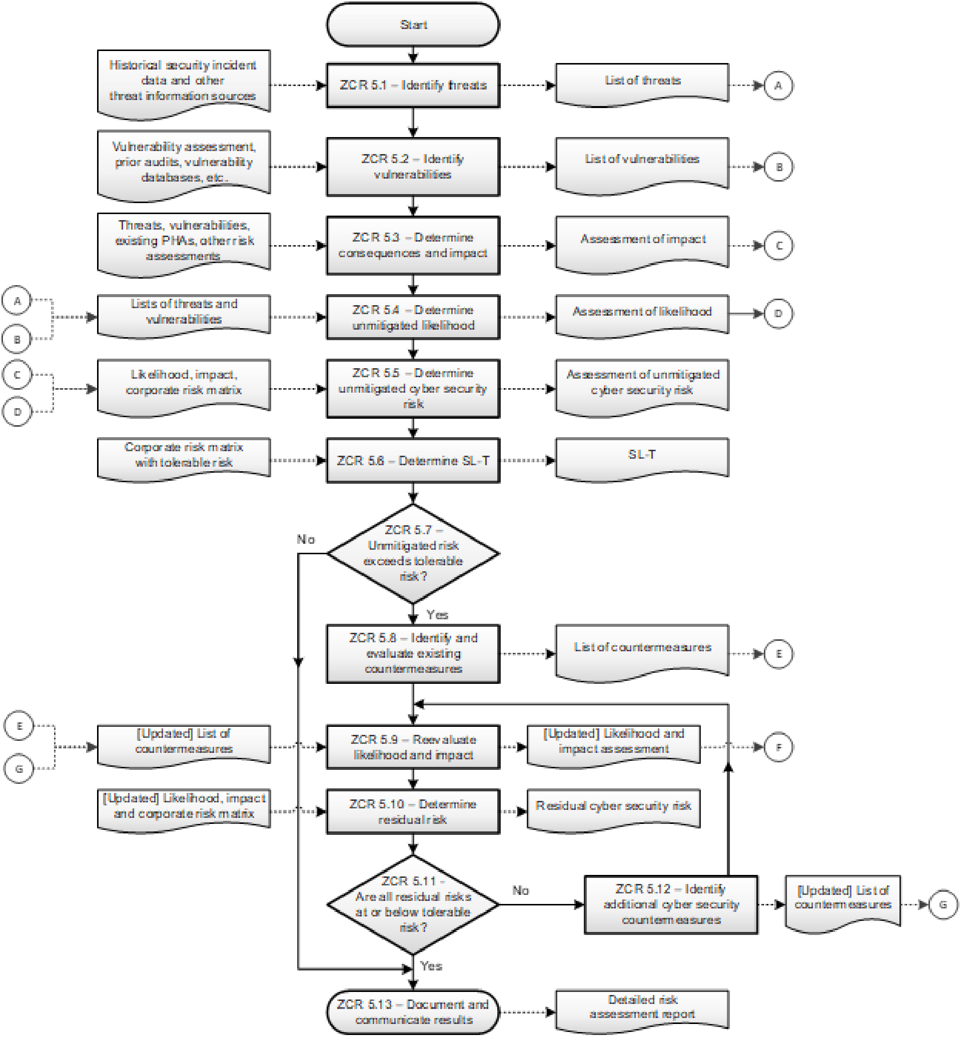
Part 3-2 - Security risk assessment, system partitioning and security levels

- Defines Cyber Vulnerability Assessments (CVA), Cyber Risk Assessment (CRA) and the Cyber Security Risk Assessment
- Types of CVAs:
  - 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

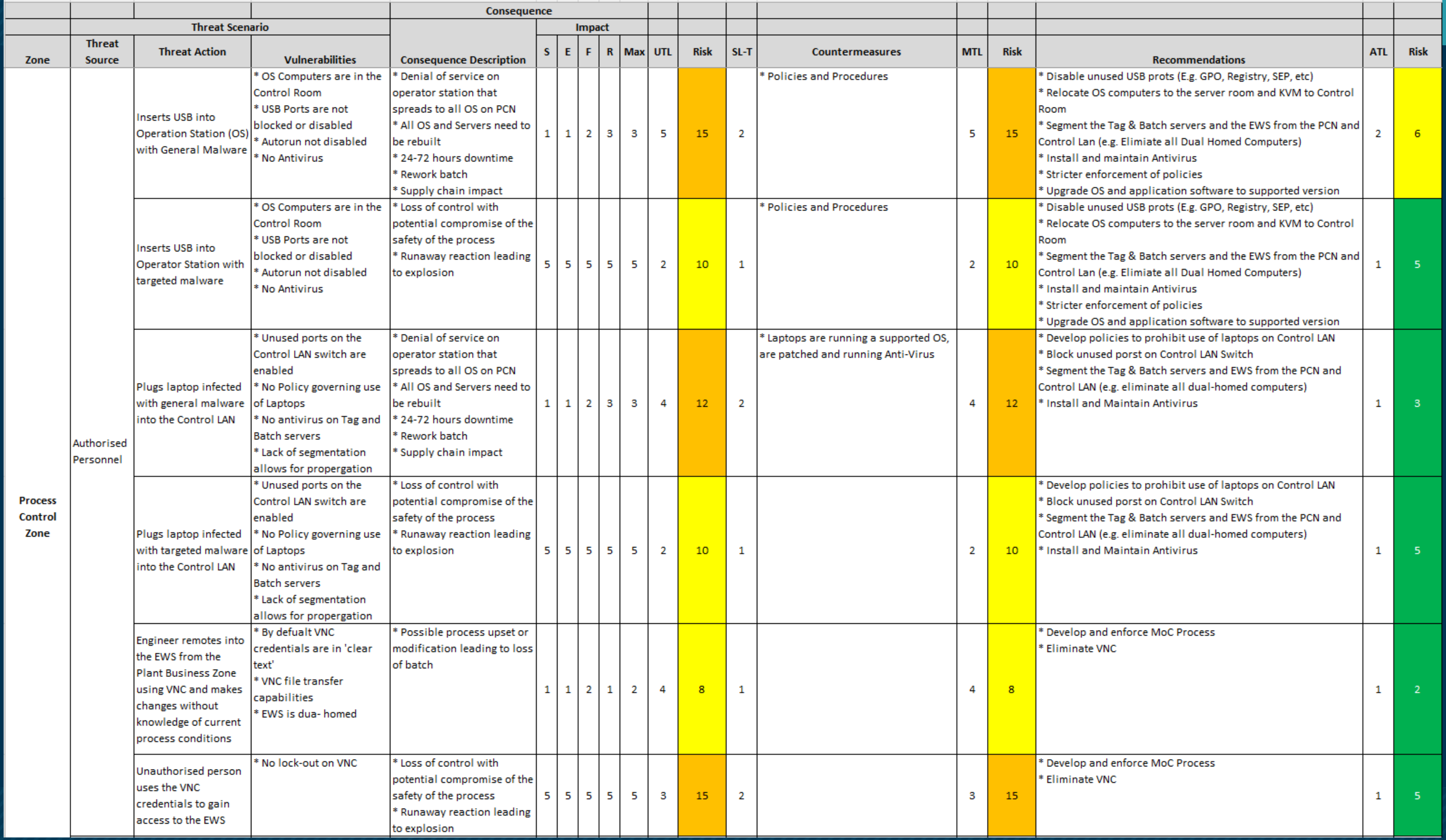
Part 3-2 – cont.


Start
Initial system architecture diagrams and inventory. Company policies, regulations, tolerable risk guidelines, etc.
ZCR 1 – Identify the System Under Consideration (SUC)
Updated system architecture diagrams and inventory with IACS external services and support identified
Existing PHAs and other relevant risk assessment and corporate risk matrix
ZCR 2 – Perform an initial cyber security risk assessment
Initial evaluation of risk
Standards and best practices, policies, supplier guidelines, criticality assessments, data flows, functional specifications, etc.
ZCR 3 – Partition the SUC into zones and conduits
Initial or revised zone and conduit diagram
No
ZCR 4 – Initial risk exceeds tolerable risk?
Yes
ZCR 5 – Perform a detailed cyber security risk assessment
Residual cyber security risk and SL-Ts for each zone and conduit
Company policies, regulations, tolerable risk guidelines, etc.
ZCR 6 – Document cyber security requirements, assumptions and constraints
Cyber security requirement specification (CRS)
ZCR 7 – Asset owner approval
Legend
Process
Subprocess
Document
Decision
Start/End


Start
Historical security incident data and other threat information sources
ZCR 5.1 – Identify threats
List of threats
A
Vulnerability assessment, prior audits, vulnerability databases, etc.
ZCR 5.2 – Identify vulnerabilities
List of vulnerabilities
B
Threats, vulnerabilities, existing PHAs, other risk assessments
ZCR 5.3 – Determine consequences and impact
Assessment of impact
C
A
B
Lists of threats and vulnerabilities
ZCR 5.4 – Determine unmitigated likelihood
Assessment of likelihood
D
C
D
Likelihood, impact, corporate risk matrix
ZCR 5.5 – Determine unmitigated cyber security risk
Assessment of unmitigated cyber security risk
Corporate risk matrix with tolerable risk
ZCR 5.6 – Determine SL-T
SL-T
No
ZCR 5.7 – Unmitigated risk exceeds tolerable risk?
Yes
ZCR 5.8 – Identify and evaluate existing countermeasures
List of countermeasures
E
E
G
[Updated] List of countermeasures
ZCR 5.9 – Reevaluate likelihood and impact
[Updated] Likelihood and impact assessment
F
[Updated] Likelihood, impact and corporate risk matrix
ZCR 5.10 – Determine residual risk
Residual cyber security risk
ZCR 5.11 – Are all residual risks at or below tolerable risk?
No
ZCR 5.12 – Identify additional cyber security countermeasures
[Updated] List of countermeasures
G
Yes
ZCR 5.13 – Document and communicate results
Detailed risk assessment report

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

ISA/IEC 62443 Part 3-3

Part 3-3 - Controls

- Defines 100 Security 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

Part 3-3 - Controls (cont.)

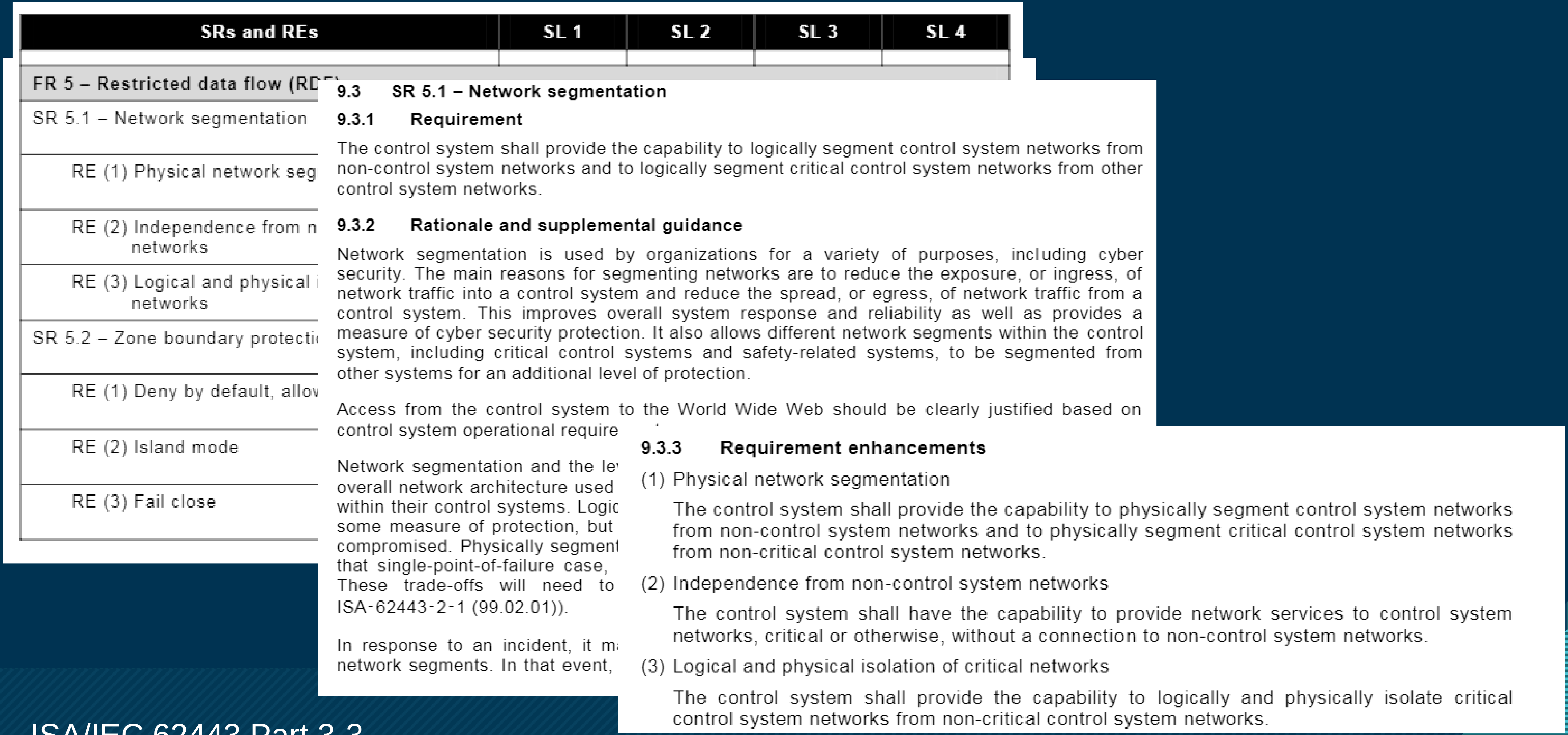
The 100 Requirements are assigned to Security Levels 1 to 4:

- 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

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 i 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

ISA/IEC 62443 Part 4-1

Part 4-1 - Secure Product Development Lifecycle Requirements

- Primary goal of the framework to produce a secure-by- design, defense-in-depth approach to designing, building, maintaining and retiring products in use in Industrial Automation and Control Systems
- Defines requirements per Practice:
  - Practice 1 - Security Management
  - Practice 2 - Specification of Security Requirements
  - Practice 3 - Secure by Design
  - Practice 4 - Secure Implementation
  - Practice 5 - Security Verification and Validation testing activities
  - Practice 6 - Management of security-related issues
  - Practice 7 - Security Update Management
  - Practice 8 - Security Guidance

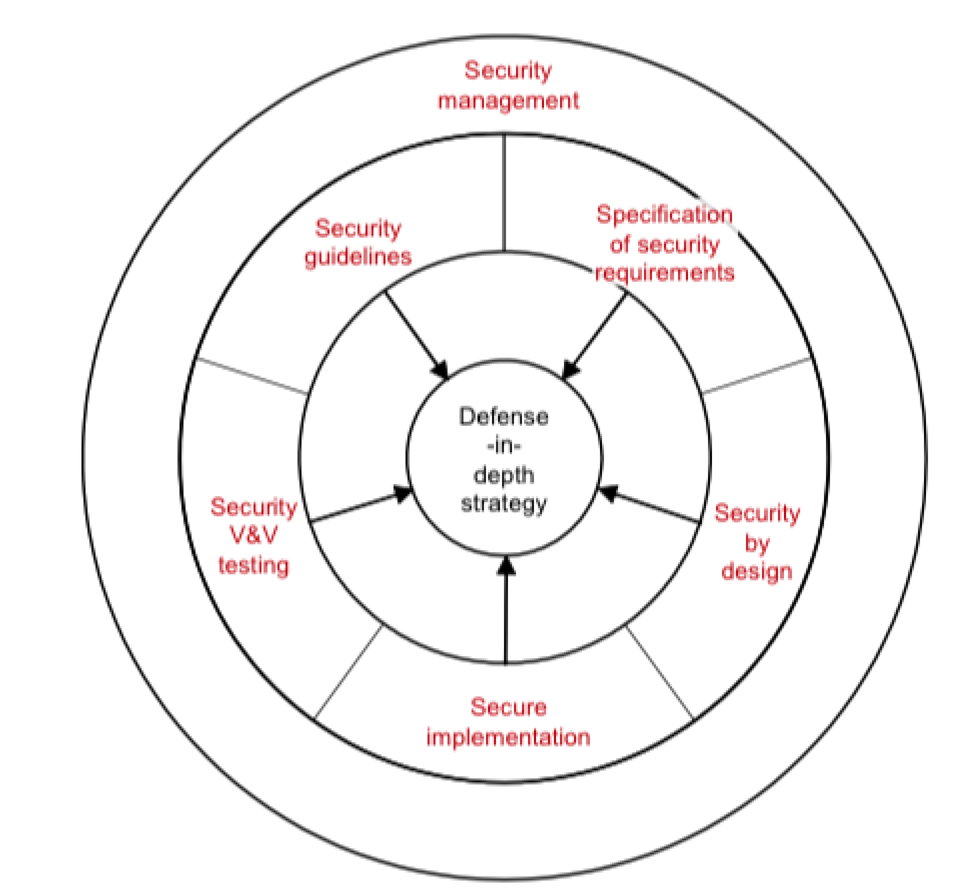


Image Source - https://blogs.grammatech.com/the-role-of-static-analysis-in-isa/iec-62443-secure-product-development-lifecycle

ISA/IEC 62443
Part 4-2

Part 4-2 - Technical Security requirements for IACS components

- Provides Component Requirements (CRs) to meet Security Level Capabilities for Foundational Requirements from Part 3-3 along with Rationale and Guidance
- Defines four component types:
  - Software Application
  - Embedded Device
  - Host Device
  - Network Device
- Defines representative Device Categories in Appendix A

Questions?

Alignment and integration with SABSA

Layer by Layer

Alignment at a high level

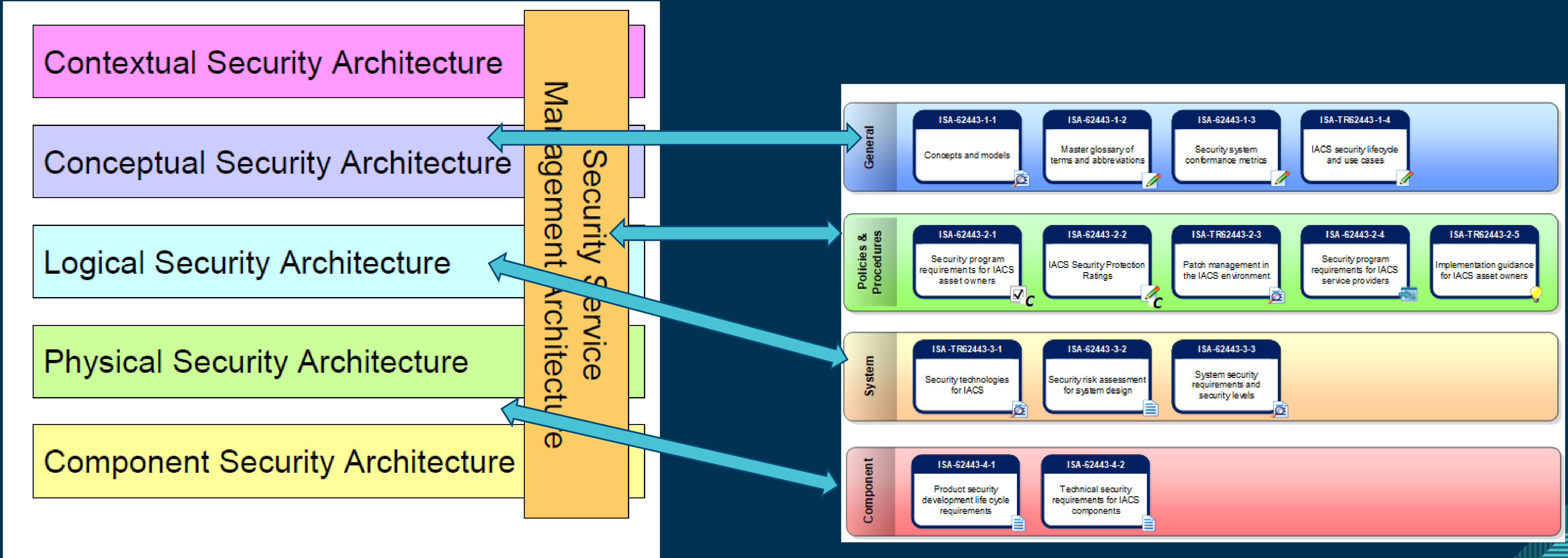
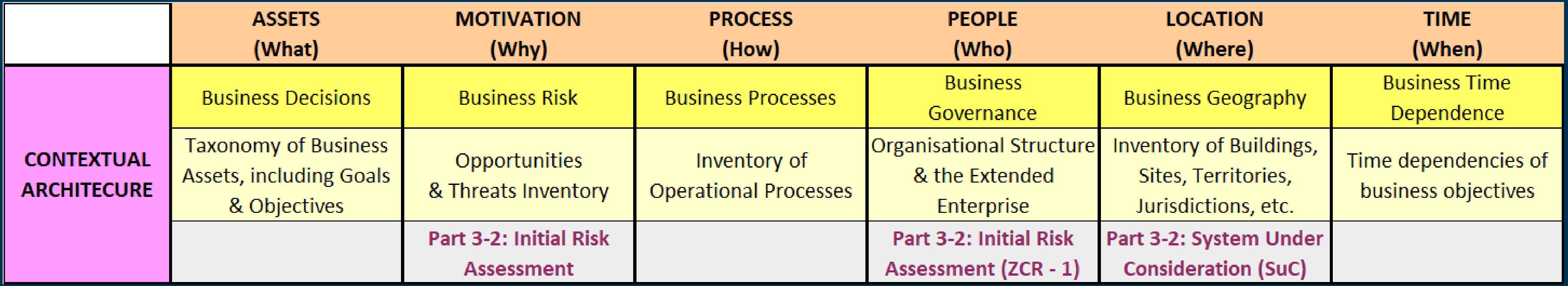
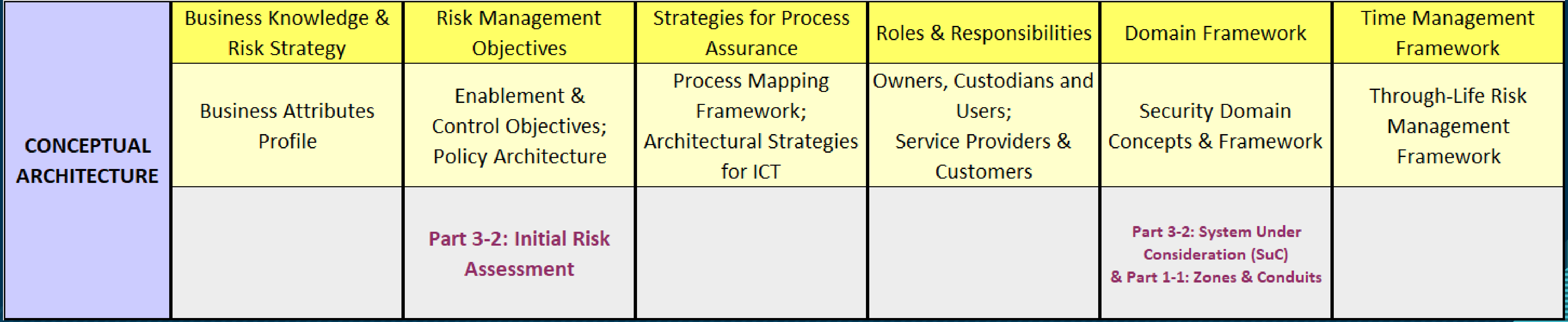

Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Management Architecture
General
ISA-62443-1-1
Concepts and models
ISA-62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
Security system conformance metrics
ISA-TR62443-1-4
IACS security lifecycle and use cases
Policies & Procedures
ISA-62443-2-1
Security program requirements for IACS asset owners
ISA-62443-2-2
IACS Security Protection Ratings
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Security program requirements for IACS service providers
ISA-TR62443-2-5
Implementation guidance for IACS asset owners
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security risk assessment for system design
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Product security development life cycle requirements
ISA-62443-4-2
Technical security requirements for IACS components

Figure 1: The SABSA Model for Security Architecture

SABSA Matrix - Contextual & Conceptual Layer

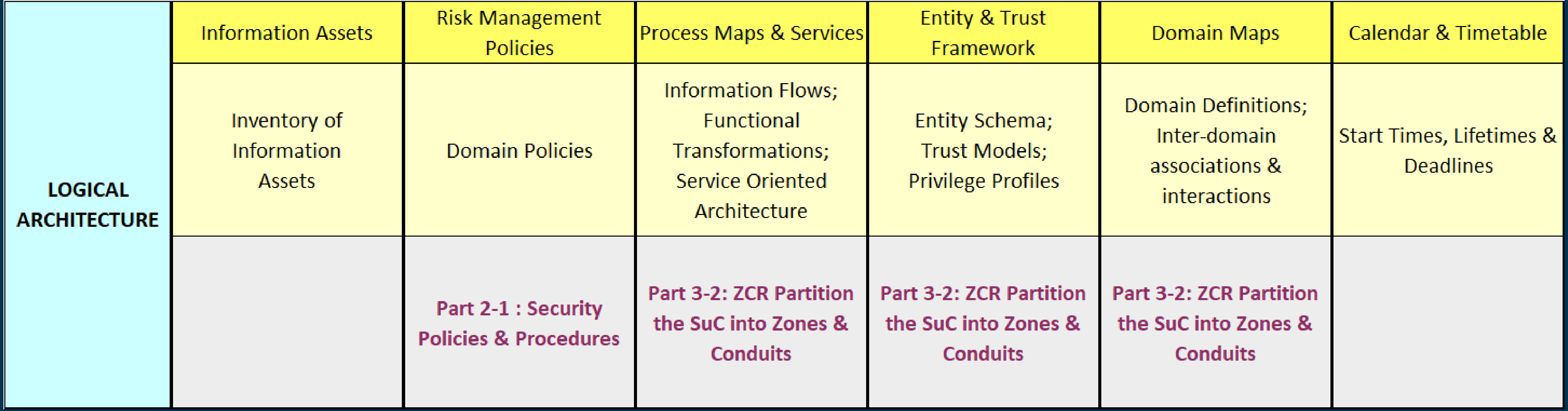


	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & 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



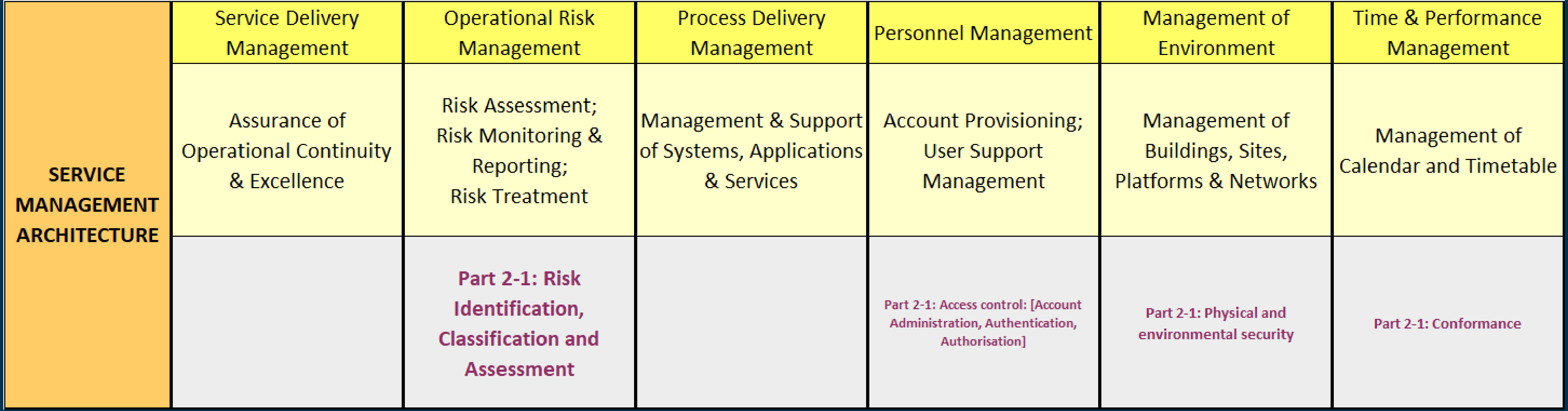
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; 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

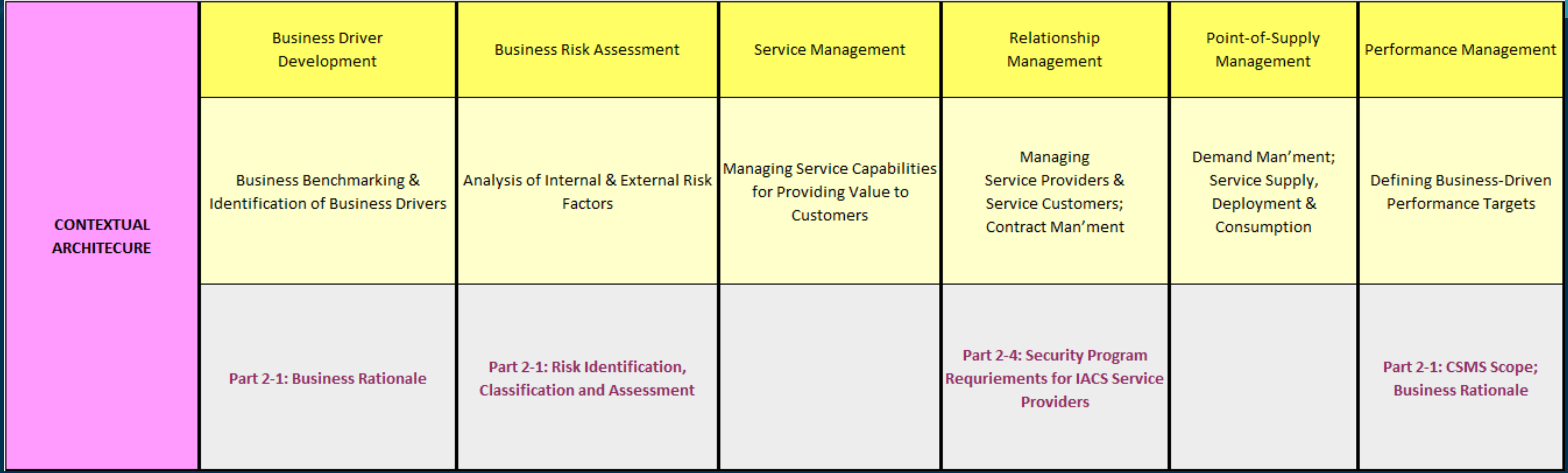


SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management

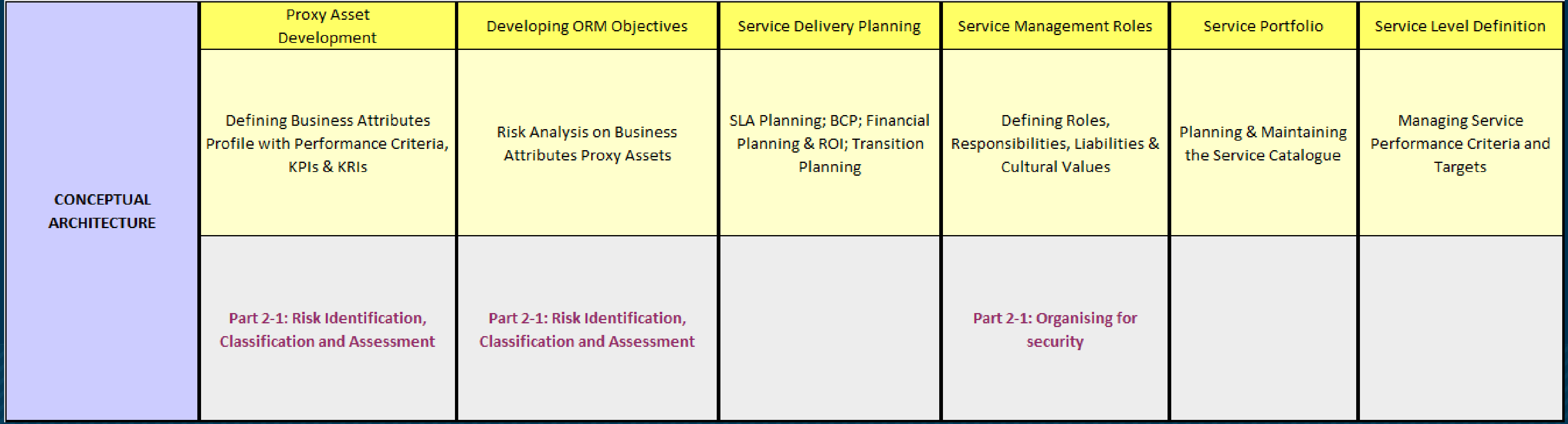
	Assurance of Operational Continuity & Excellence	Risk Assessment;
		Risk Monitoring & Reporting;
		Risk Treatment
			Management & Support of Systems, Applications & Services	Account Provisioning;
				User Support Management
					Management of Buildings, Sites, Platforms & Networks	Management of Calendar 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

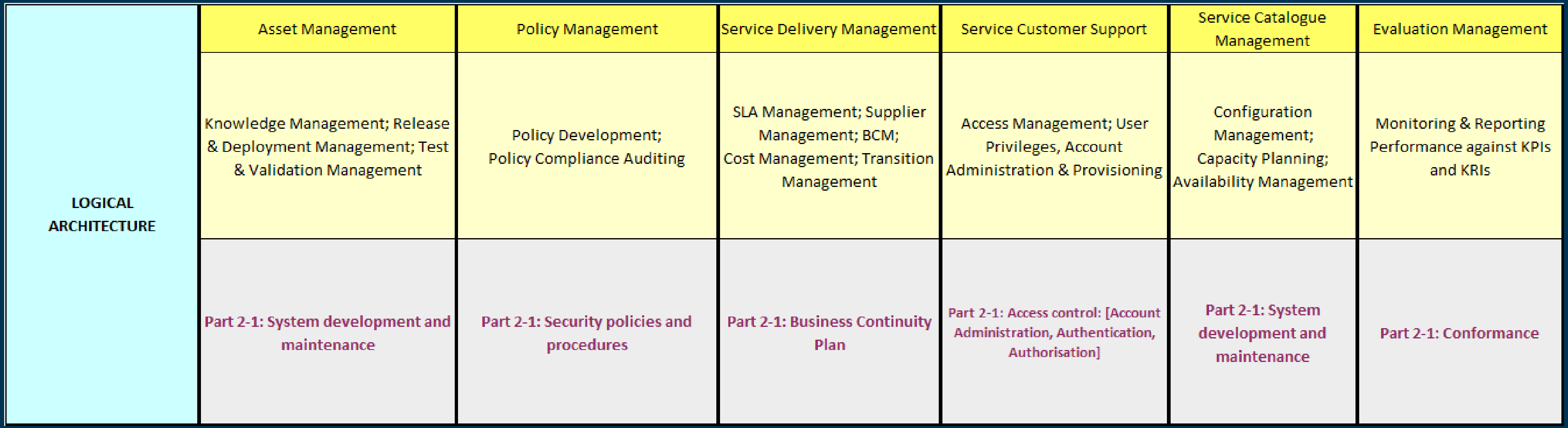


CONTEXTUAL ARCHITECURE	Business Driver Development	Business Risk Assessment	Service Management	Relationship Management	Point-of-Supply Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Service Capabilities 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

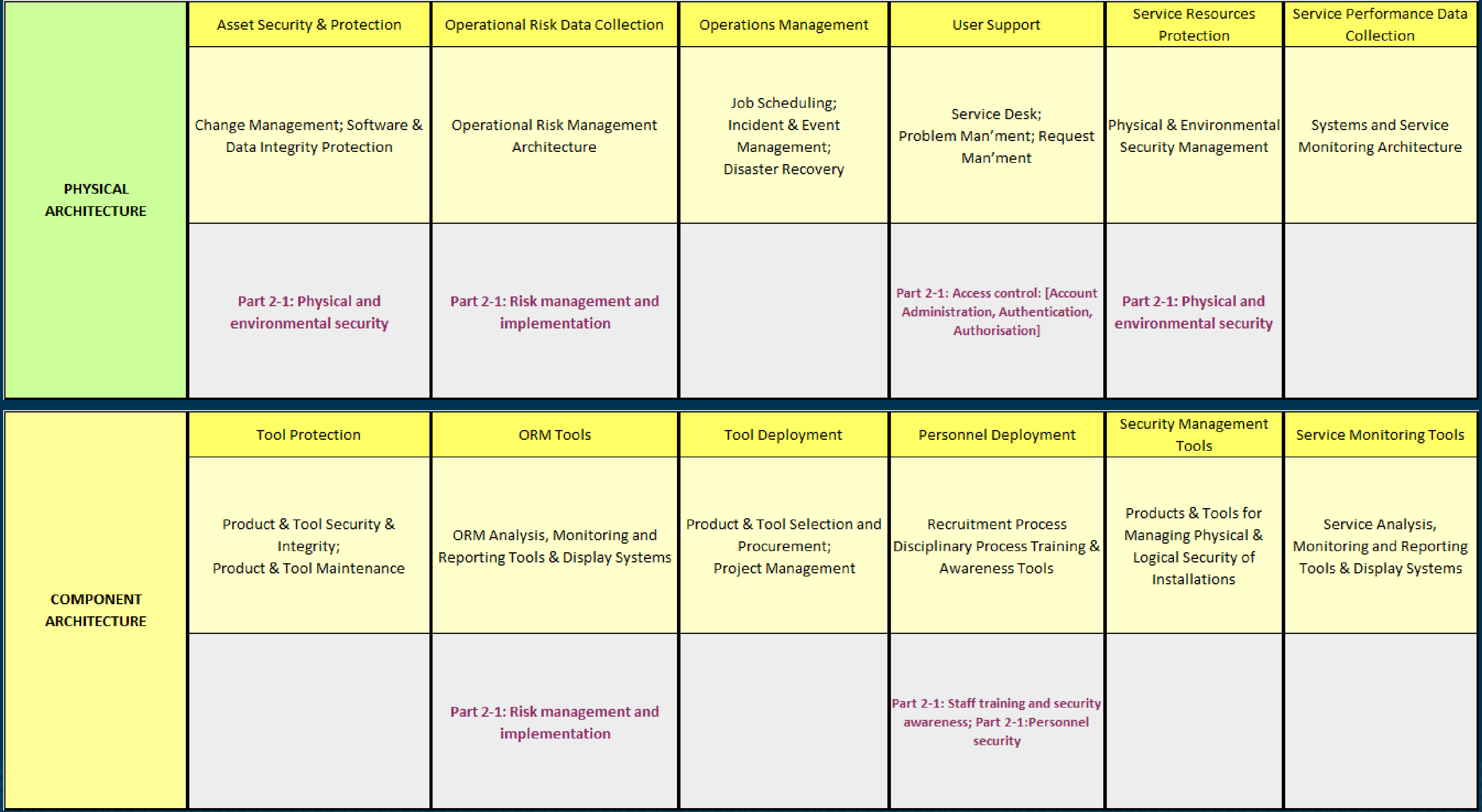


	Asset Management	Policy Management	Service Delivery Management	Service Customer Support	Service Catalogue Management	Evaluation Management

LOGICAL ARCHITECTURE	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		

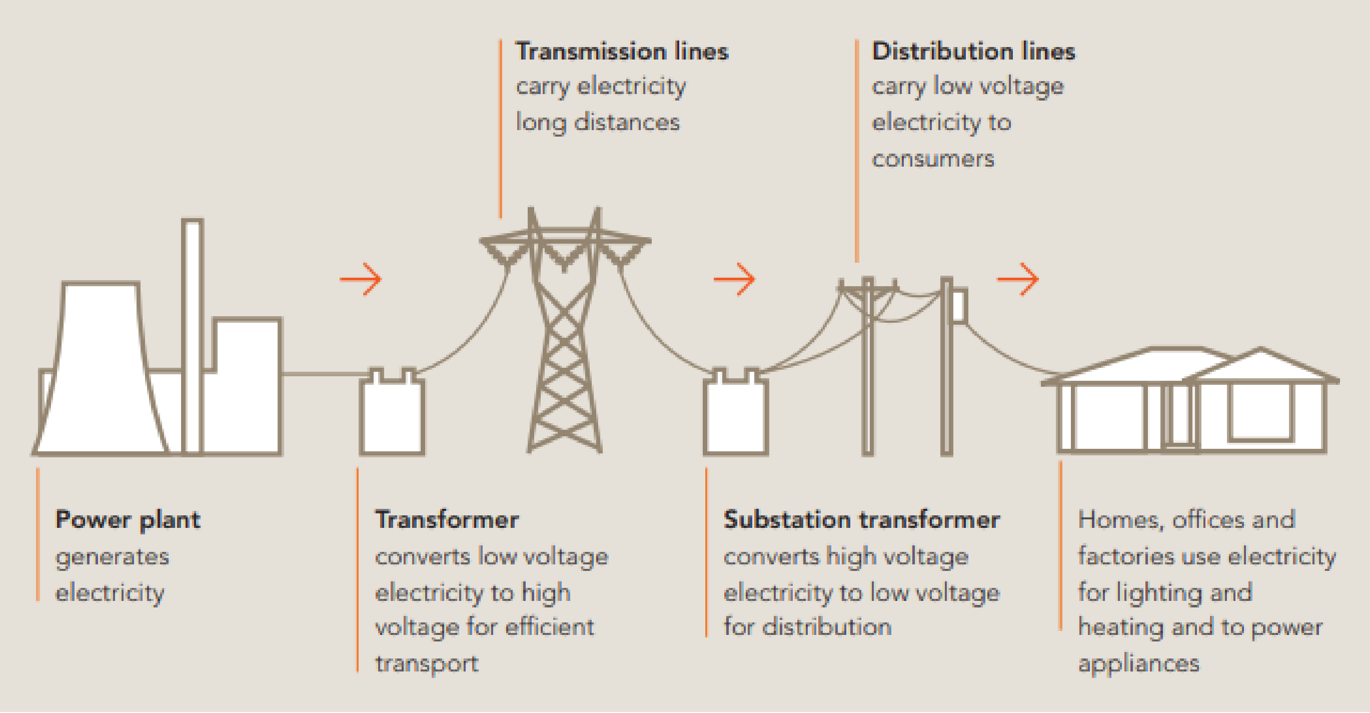
Alignment of FRs and Sample Security Services

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	*???*

A Practical Application

For an OT Scenario

A quick primer on Electricity Systems



Transmission lines carry electricity long distances

Distribution lines carry low voltage electricity to consumers

Power plant generates electricity

Transformer converts low voltage electricity to high voltage for efficient transport

Substation transformer converts high voltage electricity to low voltage for distribution

Homes, offices and factories use electricity for lighting and heating and to power appliances

TRANSPORT OF ELECTRICITY

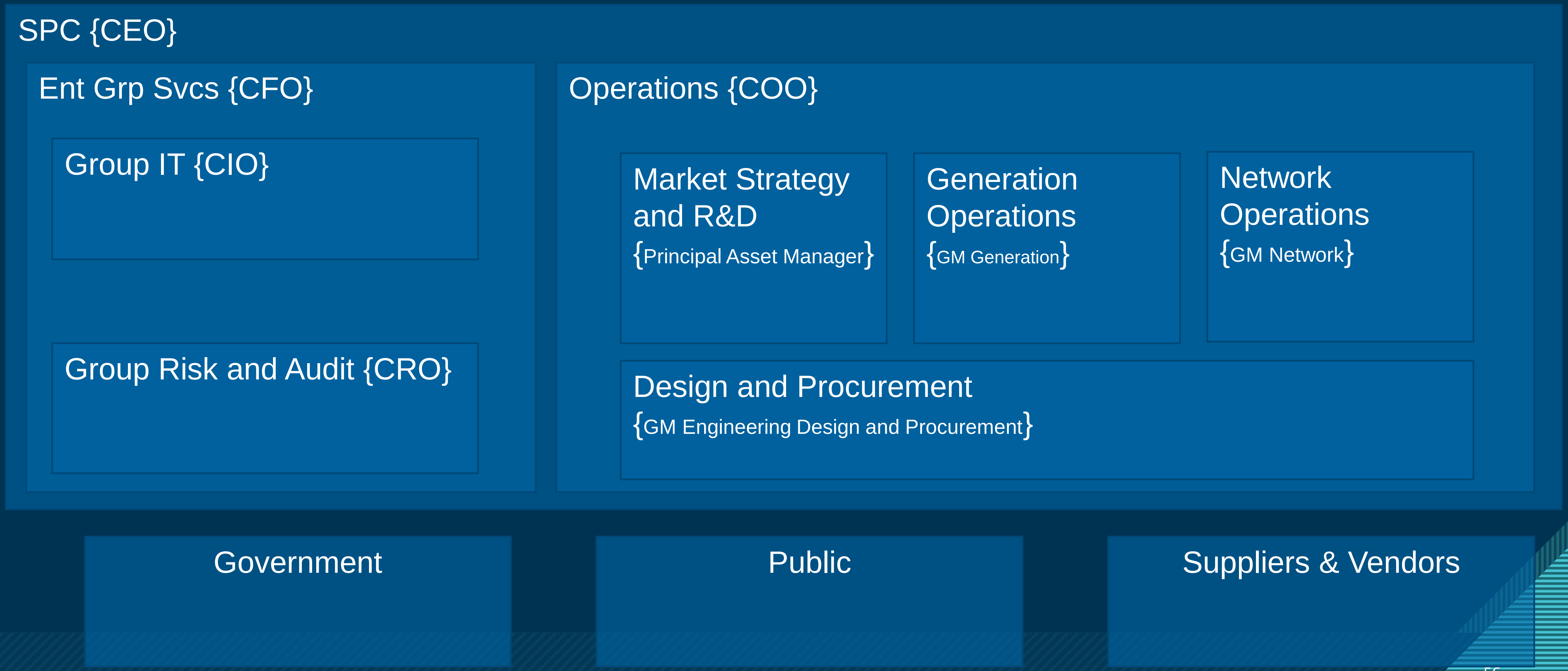
An Overview of State Power Corporation

- *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



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}

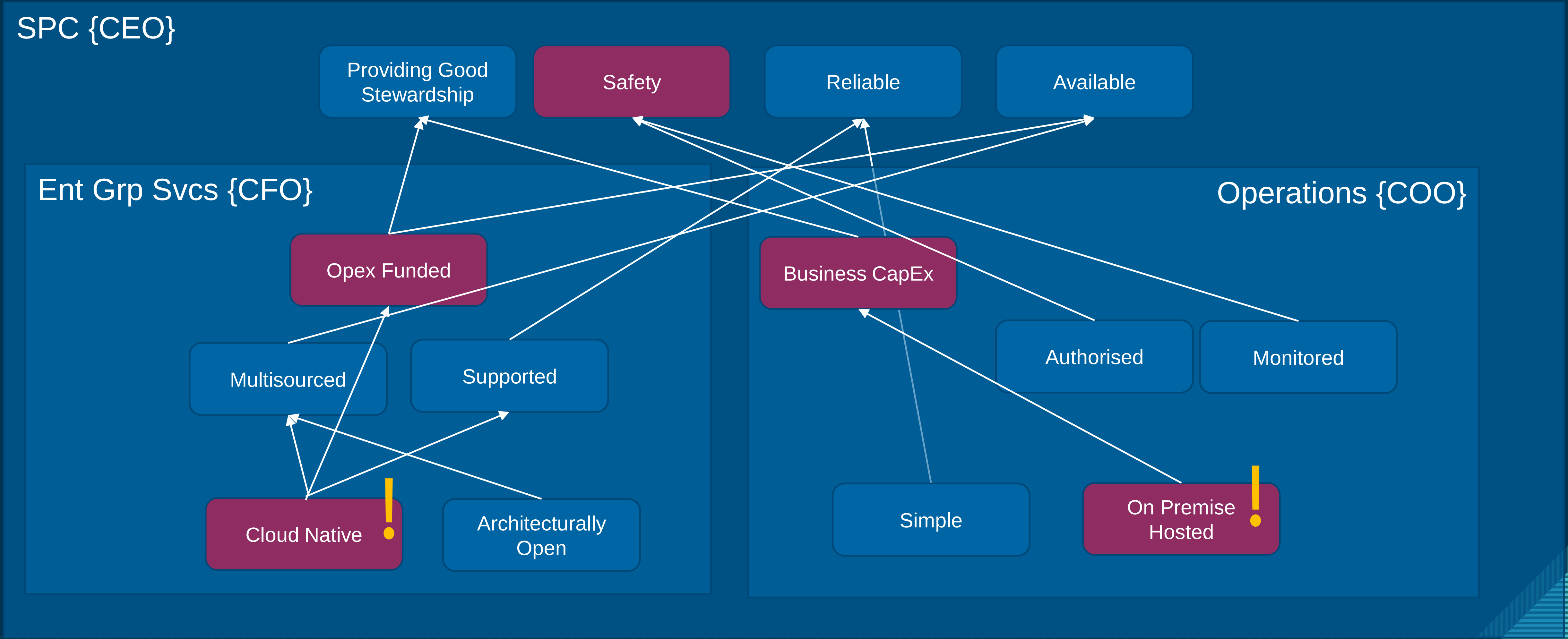
Design and Procurement {GM Engineering Design and Procurement}

Government

Public

Suppliers & Vendors

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

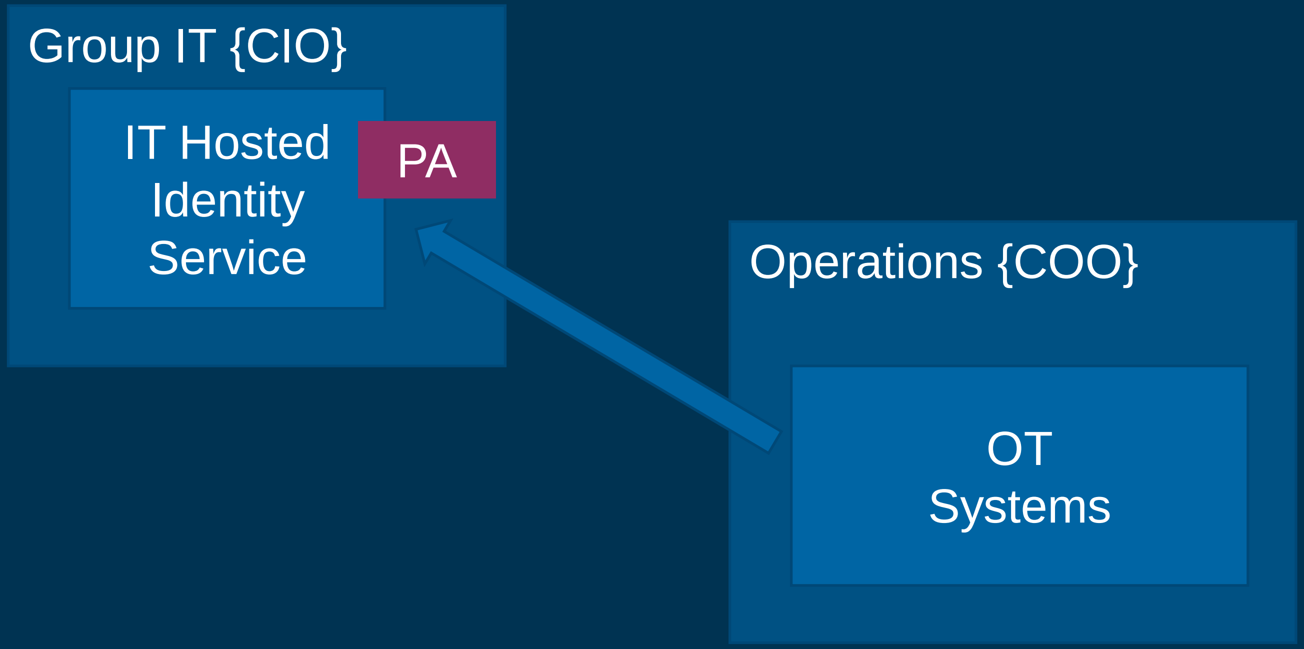
Technical

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



Questions?

Tips & References for working with your OT Stakeholders

Tips for working with OT

1. Take time to learn the physical process, visit the sites and genuinely learn the environment
2. SANS have awesome ICS posters including an ICS Site Visit Plan
3. Establish joint cyber security forums for IT and OT
4. Understand the context for why decisions have been made – they usually have been made for a real reason and understanding the context goes a long way!
5. Help them with the IT Systems Security and Security Automation tasks

Useful References

- SANS Five ICS Cybersecurity Critical Controls
- ACSC Protecting Industrial Control Systems
- NCSC OT Security Design Principles
- SANS ICS Youtube Channel
- Improving ICS Security Defense in Depth & ICS-CERT recommended Practices
- S4 OnRamp and S4 Highway Sessions
- Dragos Year in Review
- ICS CERT VLP
- Knapp and Langill – Industrial Network Security 2nd Ed

Useful IEC/ISA 62443 References

- Read the Quick Start Guide
- Read the other ISAGCA ISA/IEC 62443 Resources
- Join the ISA and View the Standards as a Member Benefit and join a branch
- Take the ISA/IEC 62443 Training Courses
- Exida - Implementing 62443 – A pragmatic Approach to Cybersecurity

Summary & Homework

What to do when you get back to work

Homework

1 Week

- Read the SANS 5 ICS Critical Security Controls
- Read the ISAGCA Quick Start Guide for 62443
- Watch the S4 Onramp and Highway videos

1 Month

- Establish IT and OT Security Forums
- Share the ICS-CERT Materials with your site team
- Organise a site visit and “walk the process”
- Do some OSINT and have an onsite Cyber Security workshop
- Start defining your OT Domain Models

6 Months

- Work with OT to build a training plan
- Work with OT to build a CSMS
- Start extending and integrating your ESA to OT (Security Patterns!)

Thank You, Questions?

https://linkedin.com/in/blargeau

https://github.com/beLarge

@beLarge