From the *vest* To the **FLAK** jacket:

How security architecture and architects need to support SecOps

BSIDES

¡!¡ WARNING ¡!¡

- This is general advice and your environment will be **different** and I don’t know how it works – so think before making any changes
- The information presented today has not been obtained from any single one of my previous employers and my views do not represent them
- Please don’t sue me
- Please don’t

TODAY'S AGENDA

1. Why do we need architecture
2. Why System Engineering is a good thing
3. An Overview of SABSA
4. A model of how IT should work
5. What architects should do to support SecOps

/WHOIS

@beLarge

- Cyber Security Specialist who has worked across IT and OT in Network Engineering and Cyber Security roles over the last 10 years
- A cyber security architecture enthusiast & infrastructure tourist
- Soon to be the Operational Technology Security Lead at CyberCX
- Bach Eng (Telecomms) and Master Business (Applied Finance)
- GRID, SCF, CCNP/CCDP(Lapsed), Cyber Security Foundation+Practitioner (ALC)

WHY DO WE NEED ARCHITECTURE?

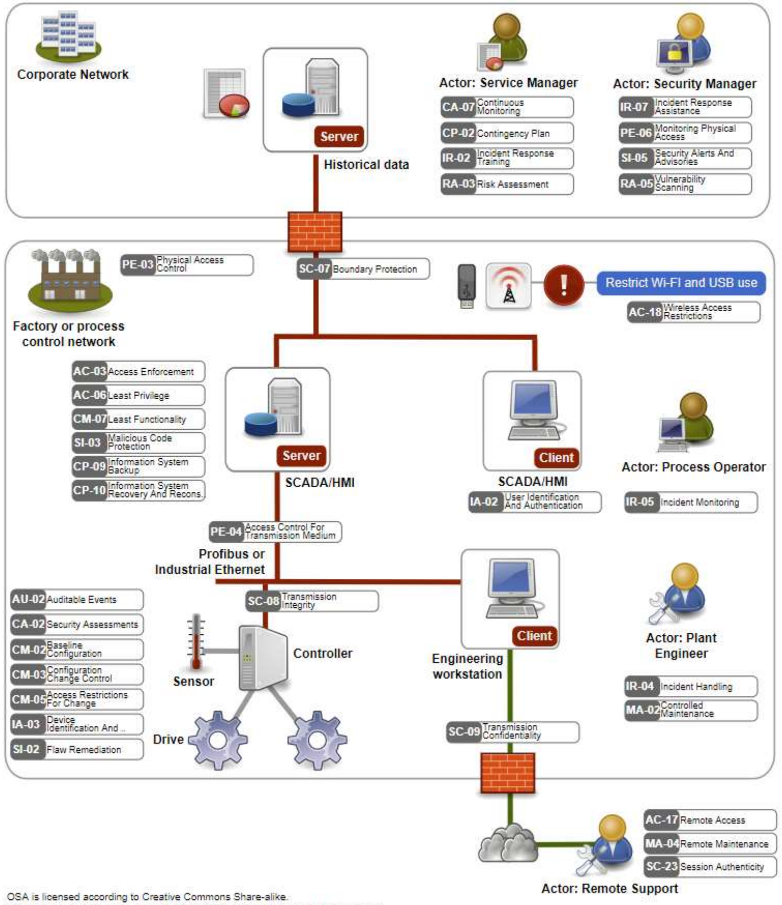
AUDIENCE POLL #1

1. Show of hands – who works in an Internal Security Team (e.g. SOC, Security Engineering, Architect, Security Manager etc)
2. Show of hands – who here is an Architect (either ESA or SA)

COMPLEXITY AND INCONSISTENCY IS THE ENEMY OF CYBER SECURITY

WHY DO WE NEED ARCHITECTURE?

- Architecture enables security teams to approach similar security problems in a consistent manner – it should reduce complexity and encourage reuse of security controls (ideally defined as security patterns)
- Architecture should be expressed at different layers of detail (viewpoints) that are appropriate for the audience – they should guide the logical order of design
- Architectural artefacts should be a communication mechanism between teams


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

Source - http://www.opensecurityarchitecture.org/cms/en/library/patternlandscape/293-draft-sp-023-industrial-control-systems

"ALL MODELS ARE WRONG, BUT SOME ARE USEFUL"

George Box

ARCHITECTURAL VIEWPOINTS

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 probably aligned to projects

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

ROB M. LEE'S SLIDING SCALE OF CYBER SECURITY

Rob M Lee suggests *"Architecture refers to the planning, establishing, and upkeep of systems with security in mind. Ensuring that security is designed into the system provides a foundation upon which all other aspects of cyber security can build."* (p5)

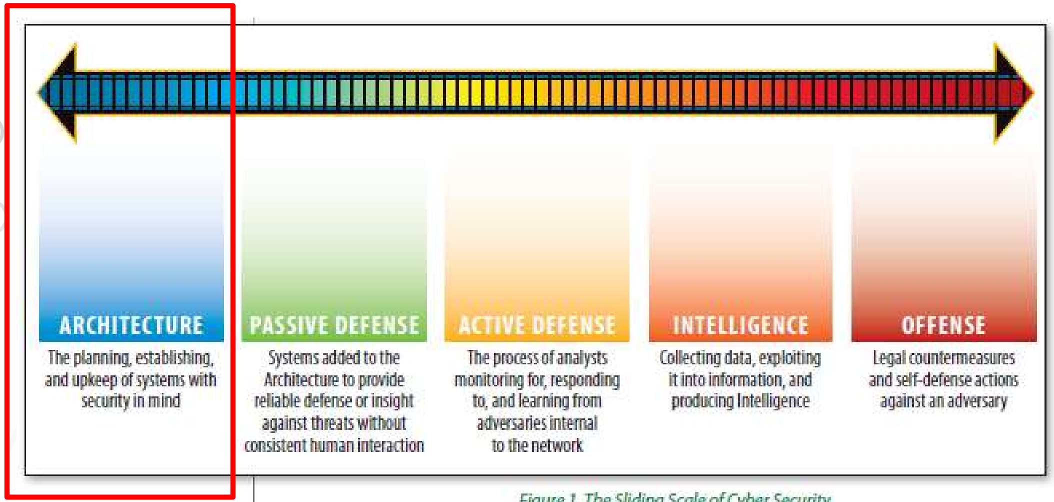

ARCHITECTURE
The planning, establishing, and upkeep of systems with security in mind
PASSIVE DEFENSE
Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction
ACTIVE DEFENSE
The process of analysts monitoring for, responding to, and learning from adversaries internal to the network
INTELLIGENCE
Collecting data, exploiting it into information, and producing Intelligence
OFFENSE
Legal countermeasures and self-defense actions against an adversary

Figure 1. The Sliding Scale of Cyber Security

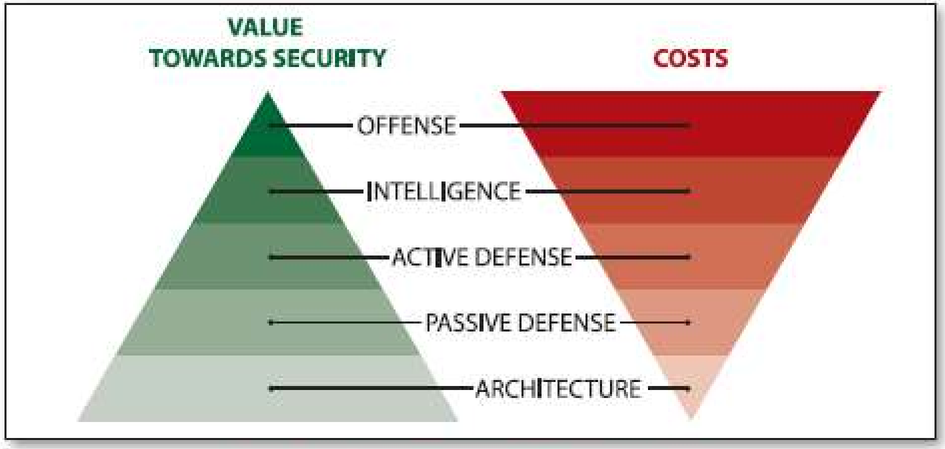


Figure 2. Value Towards Security (Left) vs. Cost (Right)

Source - https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

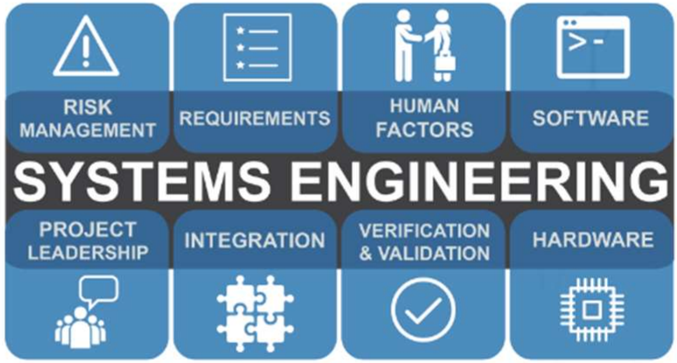
WHY SYSTEM ENGINEERING IS A GOOD THING?

SYSTEM ENGINEERING DEFINITION

"Systems Engineering is a ***transdisciplinary*** *and* ***integrative*** *approach to enable the successful realization, use, and retirement of* ***engineered systems****, using* ***systems principles and concepts,*** *and scientific, technological, and management methods."*

We use the terms "engineering" and "engineered" in their ***widest sense****: "the action of working artfully to bring something about".*

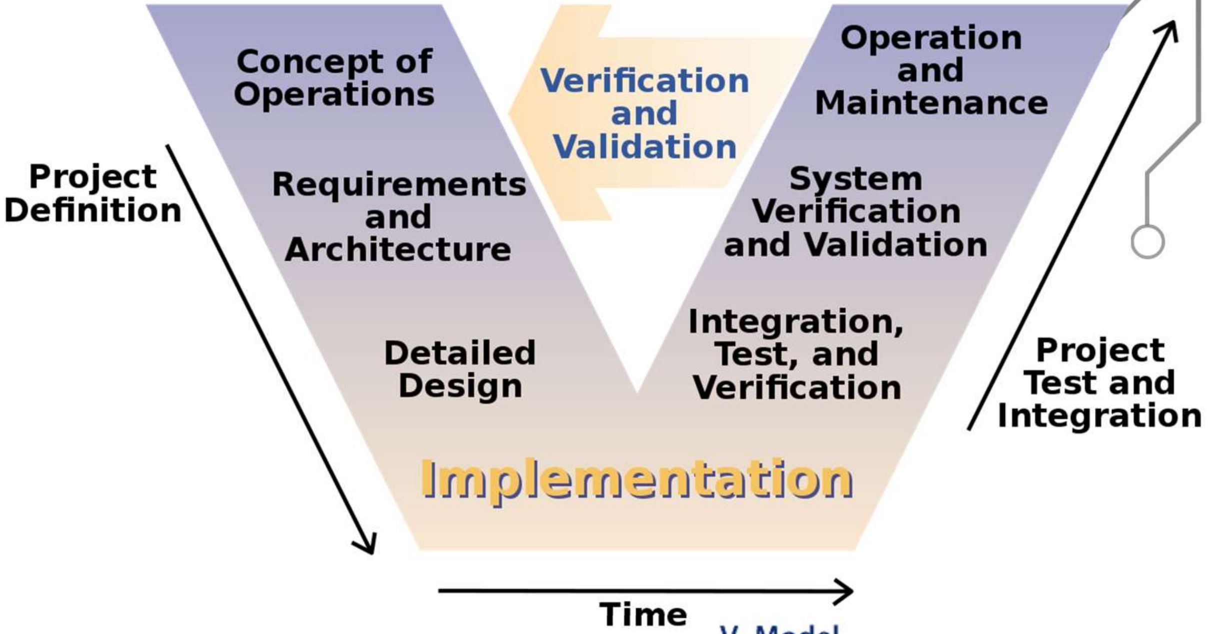
*"****Engineered systems****" may be composed of any or all of people, products, services, information, processes, and natural elements."*



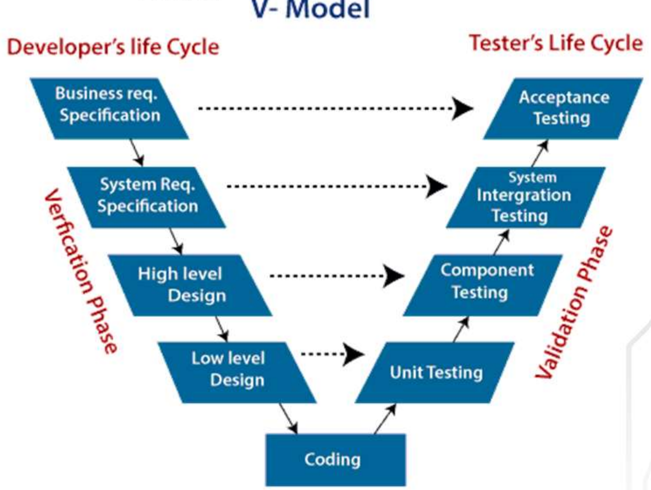
Source - https://www.incose.org/systems-engineering

THE "V" MODEL

- A graphical representation of the Systems Development Life Cycle
- Also introduces the two important concepts of:
  - Verification – "Are you building it right?"
  - Validation – "are you building the right thing"
- As architects, what are we doing to ensure V&V?



Project Definition
Concept of Operations
Requirements and Architecture
Detailed Design
Verification and Validation
Operation and Maintenance
System Verification and Validation
Integration, Test, and Verification
Project Test and Integration
Implementation
Time



Source - https://en.wikipedia.org/wiki/V-Model & https://www.javatpoint.com/software-engineering-v-model

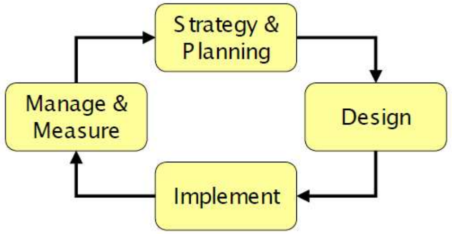
AN OVERVIEW OF SABSA

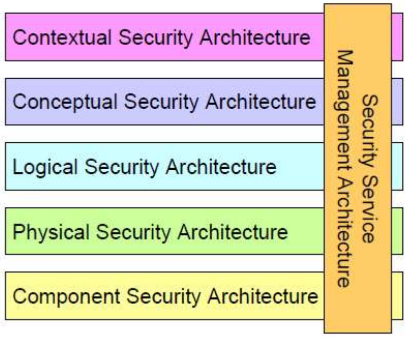
AUDIENCE POLL #2

1. Show of hands – who has heard of SABSA before?
2. Show of hands – who here is a (SCF|SCP|SCM)?
3. Show of hands – who has attended COSAC or COSAC Connect this year?

SHERWOOD APPLIED BUSINESS SECURITY ARCHITECTURE (SABSA)

- Developed by Sherwood, Clark and Lynas; SABSA has it's origins in the development of the SWIFT payments system
- It is the application of System Engineering Concepts to address Cyber Security Problems through the use of Enterprise Security Architecture
- Links Business Objectives to Cyber Security activities through Attributes
- Great starting point of the SABSA White Paper – W100



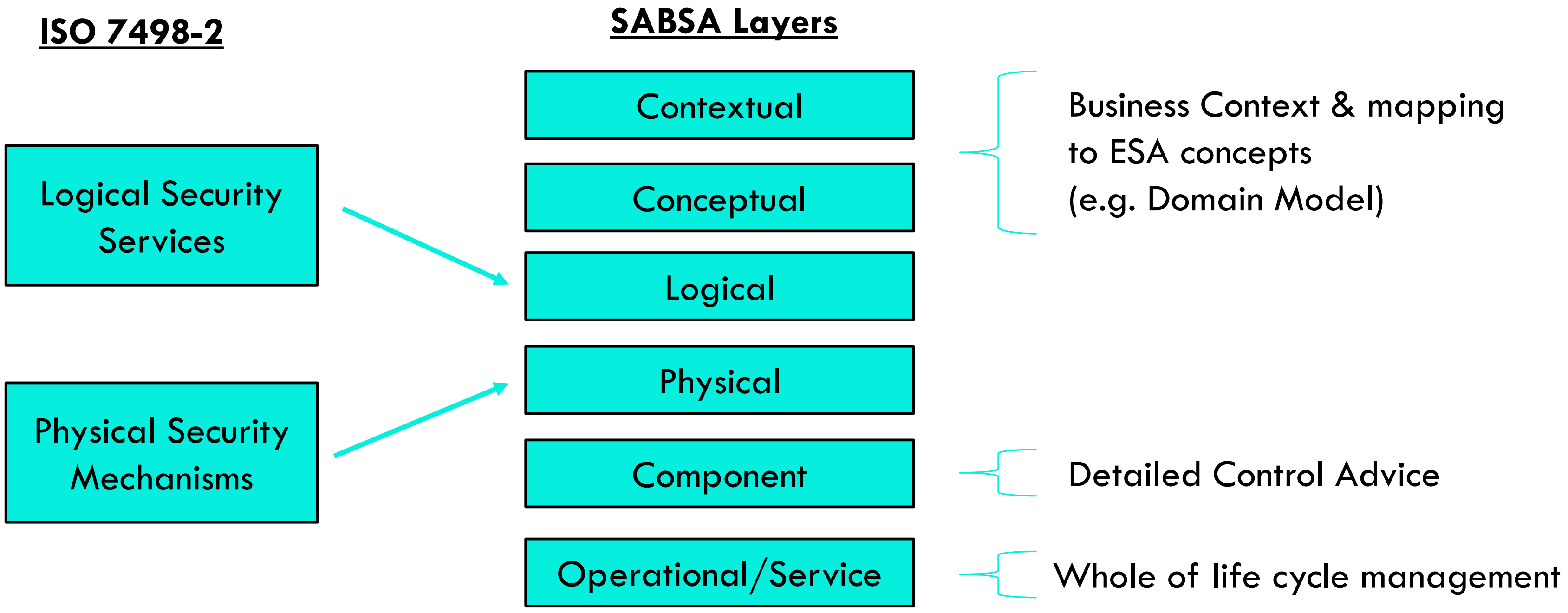


Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Management Architecture

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

HOW DID THEY GET TO THE 6 LAYERS

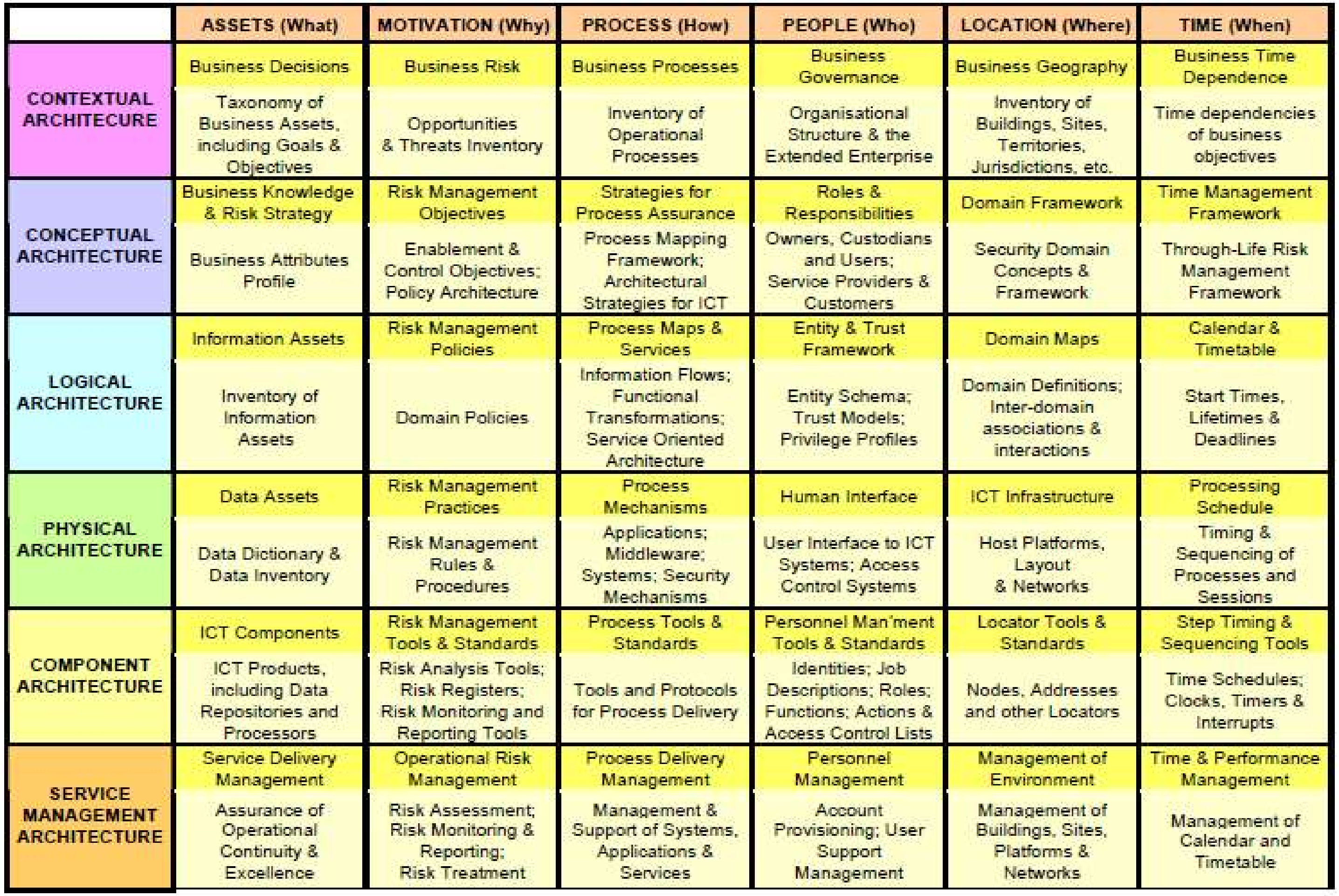
- Began with ISO 7498-2 which defined Logical Security Services and Physical Security Mechanisms and added layers above for context, layers before for detailed specification and a Service Operations Layer


ISO 7498-2
SABSA Layers
Logical Security Services
Physical Security Mechanisms
Contextual
Conceptual
Logical
Physical
Component
Operational/Service
Business Context & mapping to ESA concepts (e.g. Domain Model)
Detailed Control Advice
Whole of life cycle management

Reference from SABSA F1 & F2 Material

THE WHAT, WHY, HOW, WHO, WHERE AND WHEN OF SABSA

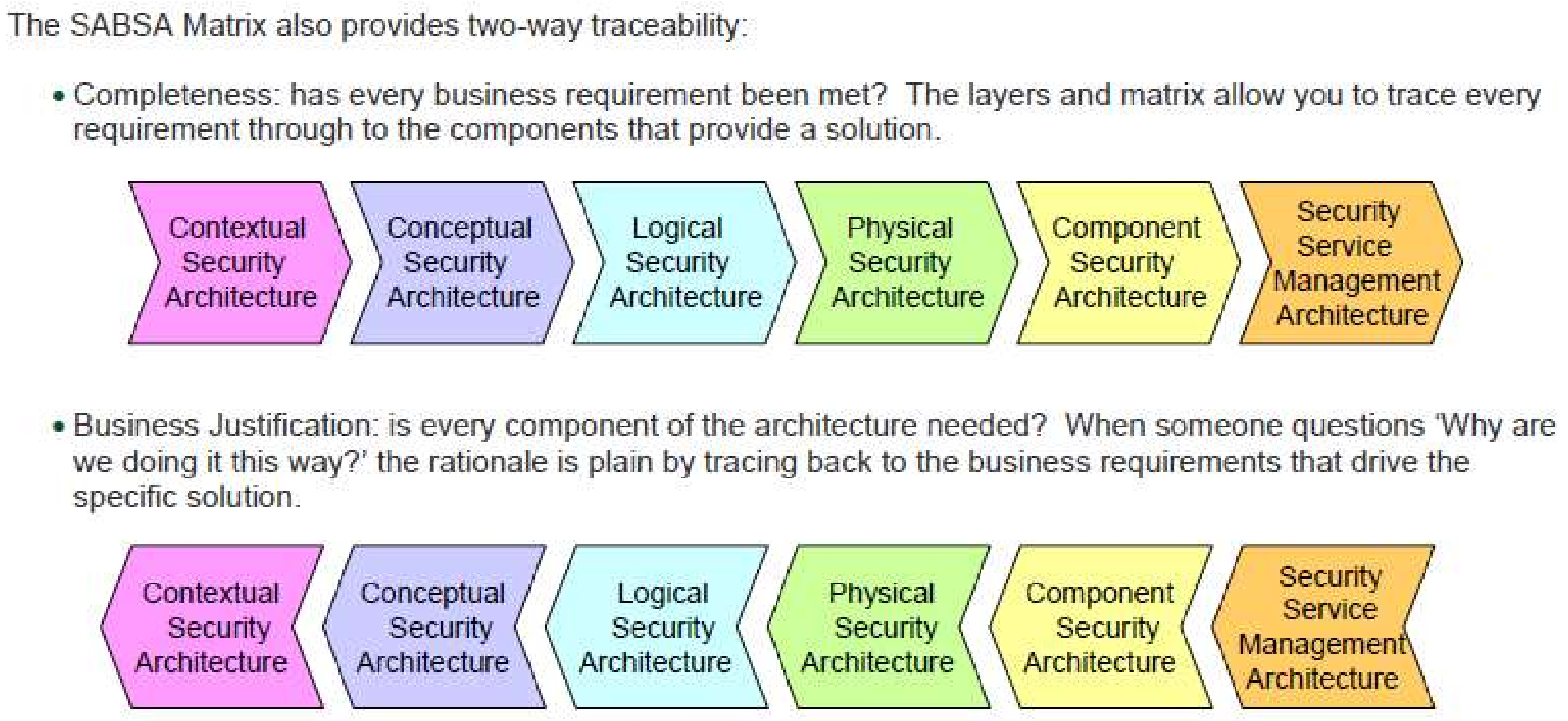
Table 3: SABSA MATRIX



	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions Taxonomy of Business Assets, including Goals & Objectives	Business Risk Opportunities & Threats Inventory	Business Processes Inventory of Operational Processes	Business Governance Organisational Structure & the Extended Enterprise	Business Geography Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Business Time Dependence Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy Business Attributes Profile	Risk Management Objectives Enablement & Control Objectives; Policy Architecture	Strategies for Process Assurance Process Mapping Framework; Architectural Strategies for ICT	Roles & Responsibilities Owners, Custodians and Users; Service Providers & Customers	Domain Framework Security Domain Concepts & Framework	Time Management Framework Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets Inventory of Information Assets	Risk Management Policies Domain Policies	Process Maps & Services Information Flows; Functional Transformations; Service Oriented Architecture	Entity & Trust Framework Entity Schema; Trust Models; Privilege Profiles	Domain Maps Domain Definitions; Inter-domain associations & interactions	Calendar & Timetable Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets Data Dictionary & Data Inventory	Risk Management Practices Risk Management Rules & Procedures	Process Mechanisms Applications; Middleware; Systems; Security Mechanisms	Human Interface User Interface to ICT Systems; Access Control Systems	ICT Infrastructure Host Platforms, Layout & Networks	Processing Schedule Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components ICT Products, including Data Repositories and Processors	Risk Management Tools & Standards Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Process Tools & Standards Tools and Protocols for Process Delivery	Personnel Man'ment Tools & Standards Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Locator Tools & Standards Nodes, Addresses and other Locators	Step Timing & Sequencing Tools Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management Assurance of Operational Continuity & Excellence	Operational Risk Management Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Process Delivery Management Management & Support of Systems, Applications & Services	Personnel Management Account Provisioning; User Support Management	Management of Environment Management of Buildings, Sites, Platforms & Networks	Time & Performance Management Management of Calendar and Timetable

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

TRACEABILITY



The SABSA Matrix also provides two-way traceability:

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

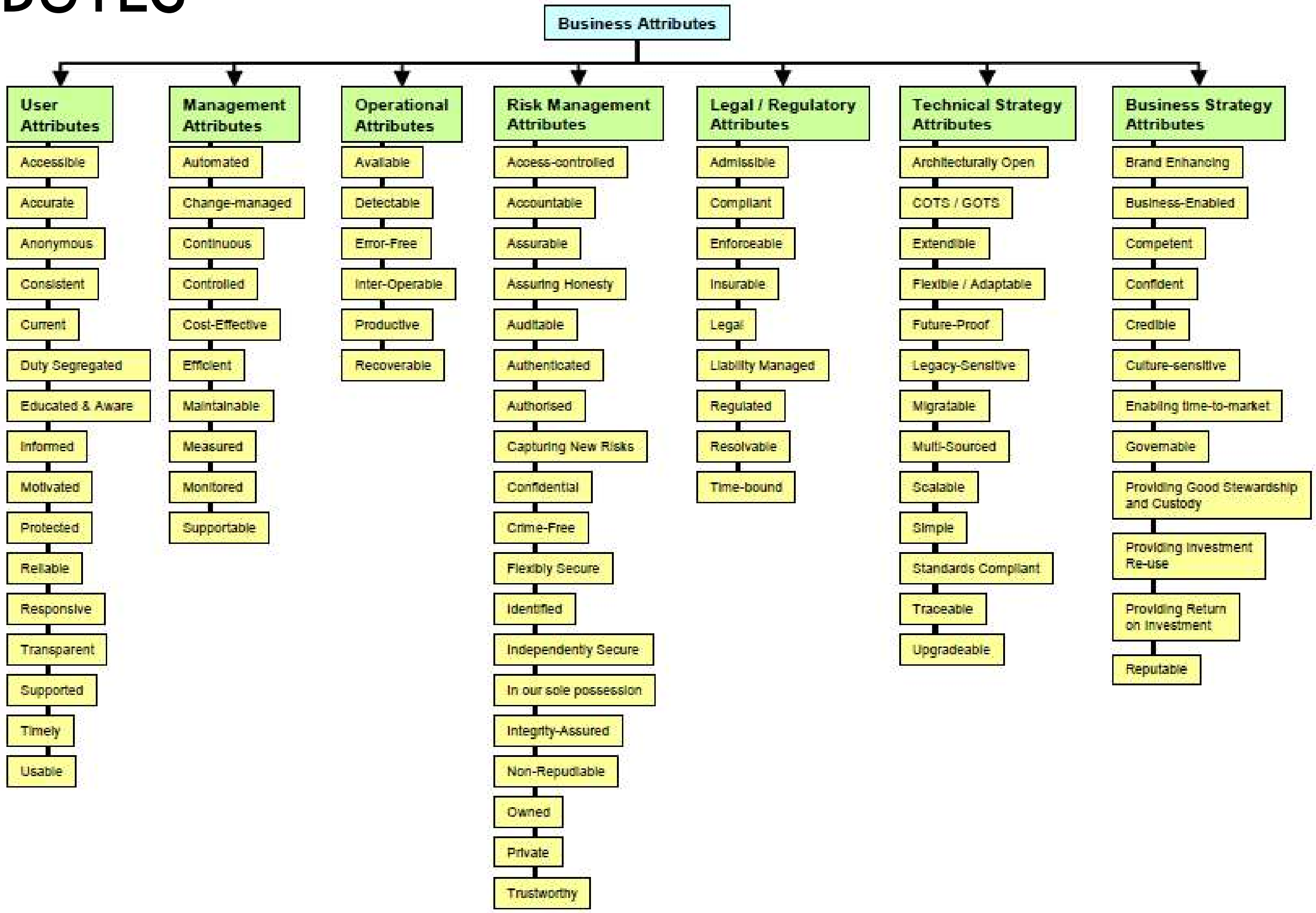
Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Management Architecture

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

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

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

ATTRIBUTES

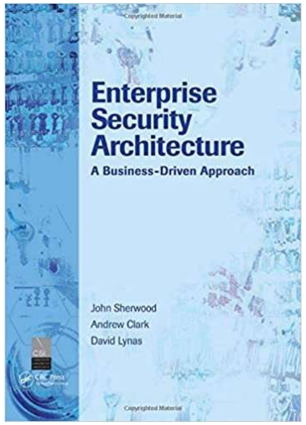


Business Attributes

- User Attributes
  - Accessible
  - Accurate
  - Anonymous
  - Consistent
  - Current
  - Duty Segregated
  - Educated & Aware
  - Informed
  - Motivated
  - Protected
  - Reliable
  - Responsive
  - Transparent
  - Supported
  - Timely
  - Usable
- Management Attributes
  - Automated
  - Change-managed
  - Continuous
  - Controlled
  - Cost-Effective
  - Efficient
  - Maintainable
  - Measured
  - Monitored
  - Supportable
- Operational Attributes
  - Available
  - Detectable
  - Error-Free
  - Inter-Operable
  - Productive
  - Recoverable
- Risk Management Attributes
  - Access-controlled
  - Accountable
  - Assurable
  - Assuring Honesty
  - Auditable
  - Authenticated
  - Authorised
  - Capturing New Risks
  - Confidential
  - Crime-Free
  - Flexibly Secure
  - Identified
  - Independently Secure
  - In our sole possession
  - Integrity-Assured
  - Non-Repudiable
  - Owned
  - Private
  - Trustworthy
- Legal / Regulatory Attributes
  - Admissible
  - Compliant
  - Enforceable
  - Insurable
  - Legal
  - Liability Managed
  - Regulated
  - Resolvable
  - Time-bound
- Technical Strategy Attributes
  - Architecturally Open
  - COTS / GOTS
  - Extendible
  - Flexible / Adaptable
  - Future-Proof
  - Legacy-Sensitive
  - Migratable
  - Multi-Sourced
  - Scalable
  - Simple
  - Standards Compliant
  - Traceable
  - Upgradeable
- Business Strategy Attributes
  - Brand Enhancing
  - Business-Enabled
  - Competent
  - Confident
  - Credible
  - Culture-sensitive
  - Enabling time-to-market
  - Governable
  - Providing Good Stewardship and Custody
  - Providing Investment Re-use
  - Providing Return on Investment
  - Reputable

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

DO YOU WANT TO KNOW MORE?



Enterprise Security Architecture

A Business-Driven Approach

John Sherwood
Andrew Clark
David Lynas

https://www.amazon.com.au/Enterprise-Security-Architecture-Business-Driven-Approach/dp/157820318X

SABSA®

alc 26 Years

https://www.alctraining.com.au/course/sabsa-foundation/

SABSA® INSTITUTE

The SABSA Institute
https://sabsa.org
@SABSA_Institute

COSAC

https://www.cosac.net/

A MODEL OF HOW IT SHOULD WORK

PLAN, BUILD, RUN … & SHADOW IT

Plan

What direction is the business going and how does IT need to plan to deliver?
How do we engage with the business?
How does the IT Team integrate new technologies?
How do we do IT differently?
Why is everything so expensive?

Build

Alright, let's build it!!
Project Managers and Engineers
What are these EAs thinking?
"Ops can figure it out"
"its OK we will do the doco at the end"
"its OK we can fix in production"

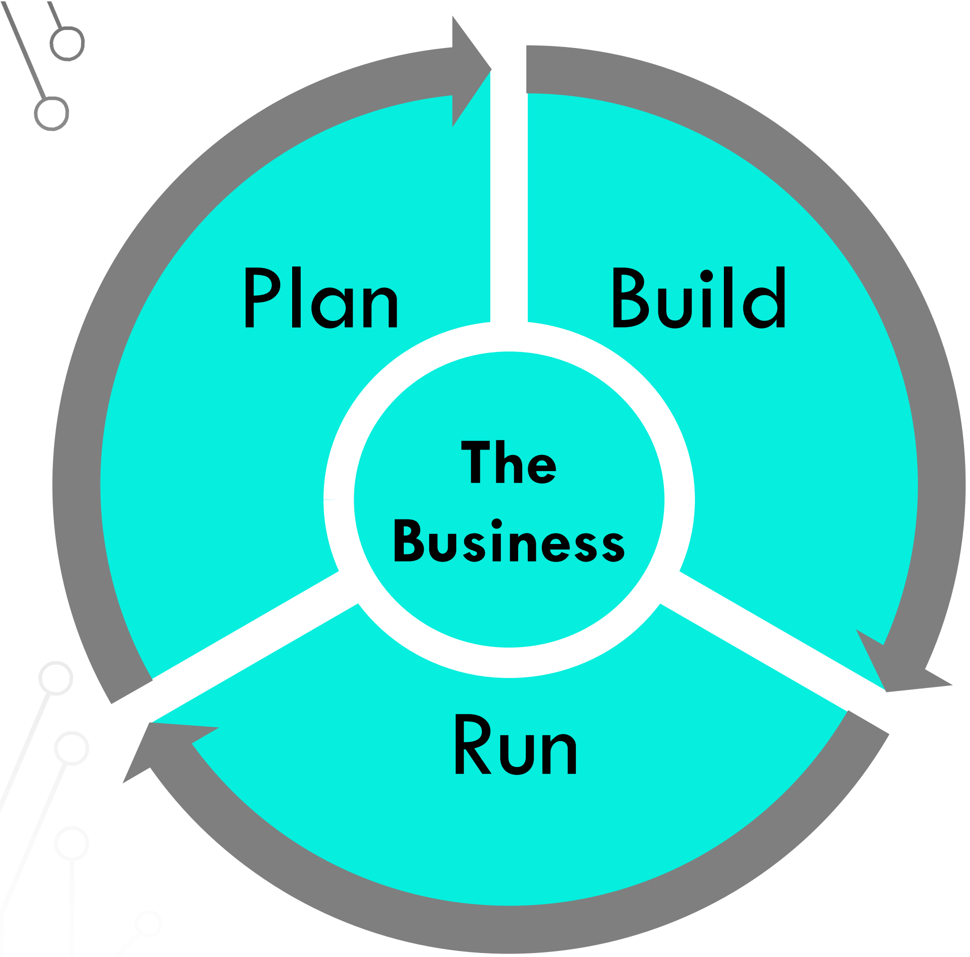
Run

What is this?
Why is everything on fire?
What do you mean everything is End of Life?
Is this another point solution?
Why are none of our systems integrated?
Why does no one talk to me?

Shadow IT

Haha get in losers I have a credit card

WHAT IT SHOULD BE



- A cyclical system where there is one team that aims to support the business
- Reduce hand offs and someone else's problem
- Pull the right stakeholders into projects as soon as possible in the engagement
- Encourage secondments and ride-alongs
- Not waiting to deliver perfection – incremental delivery!
- No need for shadow IT because you are delivering!

WHAT SHOULD ARCHITECTS DO TO SUPPORT SECOPS

LISTEN TO AND WORK WITH YOUR SECOPS TEAM

- Listen to your SecOps Team!
- Help get what's in your SecOps team's heads onto paper – develop a cyber security tools landscape drawing
- Work through the Cyber Security Risk Register with the SecOps team (you do have a cyber security risk register?)
- Facilitate table tops and exercises

BUILD A SECURITY TOOLS LANDSCAPE

- I like the CAESARS and NIST 800-137 as references
- Use the categories from Security Automation Domains and then consider the integration of tools – also can use this as a view for determining your SecOps team capabilities

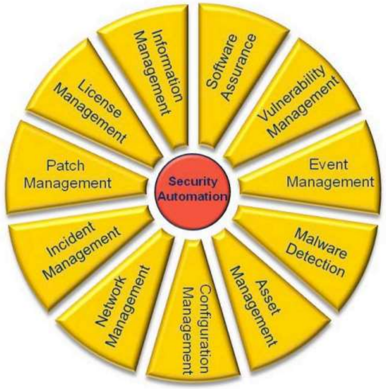
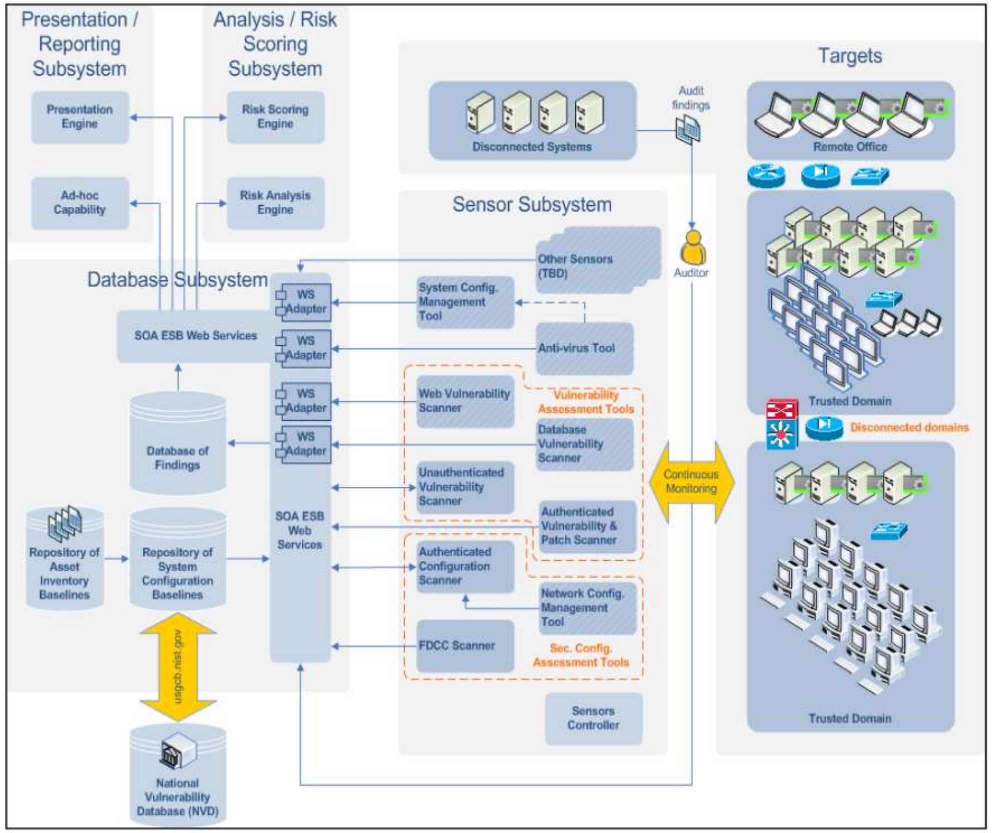


Figure D-1. Security Automation Domains



Presentation / Reporting Subsystem
Presentation Engine
Ad-hoc Capability
Analysis / Risk Scoring Subsystem
Risk Scoring Engine
Risk Analysis Engine
Database Subsystem
SOA ESB Web Services
WS Adapter
WS Adapter
WS Adapter
WS Adapter
Database of Findings
SOA ESB Web Services
Repository of Asset Inventory Baselines
Repository of System Configuration Baselines
usgcb.nist.gov
National Vulnerability Database (NVD)
Disconnected Systems
Audit findings
Sensor Subsystem
Other Sensors (TBD)
System Config. Management Tool
Anti-virus Tool
Web Vulnerability Scanner
Vulnerability Assessment Tools
Database Vulnerability Scanner
Unauthenticated Vulnerability Scanner
Authenticated Vulnerability & Patch Scanner
Authenticated Configuration Scanner
Network Config. Management Tool
FDCC Scanner
Sec. Config. Assessment Tools
Sensors Controller
Auditor
Continuous Monitoring
Targets
Remote Office
Trusted Domain
Disconnected domains
Trusted Domain

Figure 3. Contextual Description of the CAESARS System

Source - https://csrc.nist.gov/csrc/media/publications/nistir/7756/draft/documents/draft-nistir-7756_second-public-draft.pdf & https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

THE RISK REGISTER

- The AESCSF has practices that involve the risk register which are a good starting point to consider

Risk Register (RM-2J)

- TVM-1j – *Threat information is added to the risk register*
- TVM-2m – *Cyber Security Vulnerability information is added to the risk register*
- SA-2j* – *Risk Register content is used to identify indicators of anomalous activity*
- IR-1g – *Cyber Security event detection activities are adjusted based on information from the organisation's risk register (RM-2j) and threat profile (TVM-1d) to help detect known threats and monitor for identified risks*
- IR-2g – *Criteria for Cyber Security event escalation, including Cyber Security incident declaration criteria, are adjusted according to information from the organisation's risk register (RM-2j) and threat profile (TVM-1d)*
- EDM-2c – *Identified Cyber Security dependency risks are entered into the risk register (RM-2j)*

Source - https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources

WORK WITH THE BUILD TEAM

- Encourage the build team to produce useful* documentation for the ops team
- How do project risks get transferred to the risk register (!!!)
- How does the project test and commission their systems
- How do the SecOps team accept systems?
- How do projects deliver training and knowledge transfer
- How does the project team champion the SecOps team
- Get good at running workshops and identifying requirements – absolutely critical to how you then build test plans

HOW TO SUPPORT SECOPS IN THE PLAN TEAM

- As architects – we must be excellent communicators
- Understand the business, understand the business drivers and understand the business strategy
- Talk in the language of business – finance and risk
- Enable the traceability between security and the business
- Don’t try and make artifacts that are everything to everyone – you need to choose the correct viewpoint for your audience
- Understand existing cyber security frameworks and how to use them to improve your security program

MISC. TOOLS AND TIPS

VISIO & POWERPOINT ARE YOUR FRIENDS

- We are going to spend a lot of time in Visio and Powerpoint – I suggest you have a look at the below resources I have found useful
  - https://networkdiagram101.com/
  - https://breakingintowallstreet.com/biws/powerpoint-pro/ (https://www.youtube.com/watch?v=wWdwicGLWGE&list=PL5hdd9oiuWS8LWdrxu5k4P0K2AJ2IremU)

… BUT FORMAL MODELLING IS WHERE IT'S AT

- Early days for me but I was impressed by the below video discussing modelling SABSA with Archimate
- https://www.youtube.com/watch?v=Bt1xRZQ5T58 But I recommend you look at the SABSA institute resources - https://sabsa.org/modelling-sabsa-with-archimate/

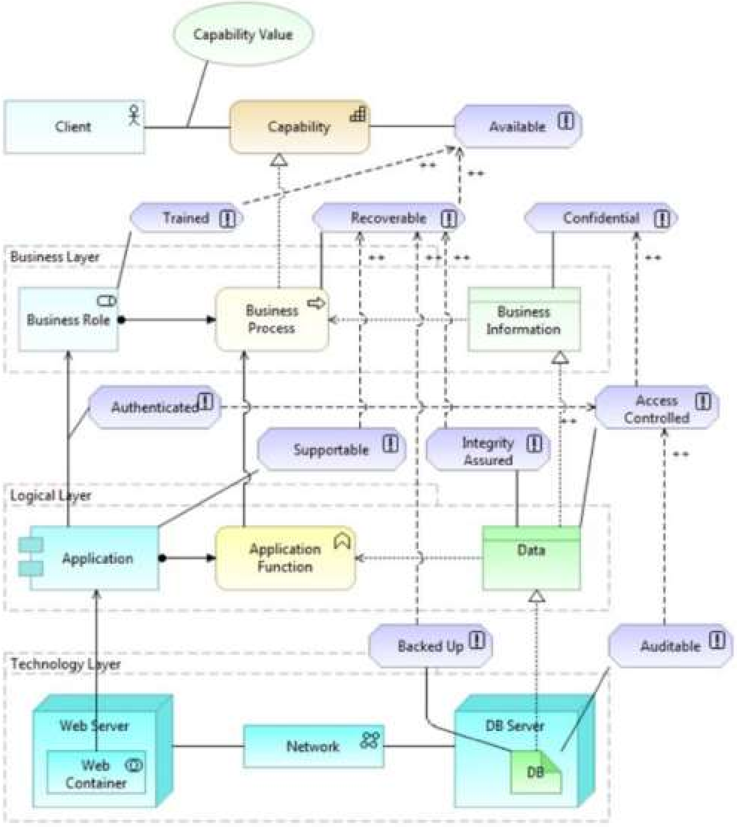


Figure 19: Attribute Traceability across Layers

NEXT STEPS

NEXT STEPS FOR YOU AS AN ARCHITECT

Next Week

1. Organise time to ride along in the SOC
2. Review Existing System Landscape documents
3. Organise a whiteboard brain dump session with the SecOps team

Next Month*

1. Get familiar with your corporate strategy
2. Review the Cyber Security Risk Register and work with the SecOps team on what is missing
3. Build an architectural repository and share with them your draft landscape view

Next 6 Months

1. Make sure you can align your key cyber security initiatives with your corporate strategy (two way traceability)
2. Update the Cyber Security Risk Register
3. Find ways to update the process to engage the SecOps team earlier in the project life cycle

THANK YOU AND Q&A

- Thank you for your time today – this deck will be uploaded to my GitHub – https://github.com/beLarge/
- Follow me on Twitter @beLarge