How can cybersecurity architects work within the strategic framework?

Bruce Large

Agenda

1. How does a business work:
   Things that the Technology teams should know
2. How does IT Work (from the Business Team Viewpoint):
   Things that the business should know
3. What’s in the toolbox

¡!¡ WARNING ¡!¡

- These are my views and do not represent the views of my current or former employers
- Please don’t sue me
- Please don’t

/whoami

@beLarge

- Operational Technology (OT) Security Lead at CyberCX
- Cyber Security Specialist who has worked across IT and OT in Network Engineering and Cyber Security roles for just under 15 years
- A cyber security architecture enthusiast & infrastructure tourist
- Bach Eng (Telecomms) and Master Business (Applied Finance)

SABSA FOUNDATION LEVEL SCF

GIAC RESPONSE AND INDUSTRIAL DEFENSE GRID

alc Cyber Security Foundation+Practitioner CERTIFIED

CISCO CERTIFIED CCNP ROUTING & SWITCHING

Lapsed 2017

CISCO CERTIFIED CCDP DESIGN

Lapsed 2017

CISCO CERTIFIED CCNA SECURITY

Lapsed 2017

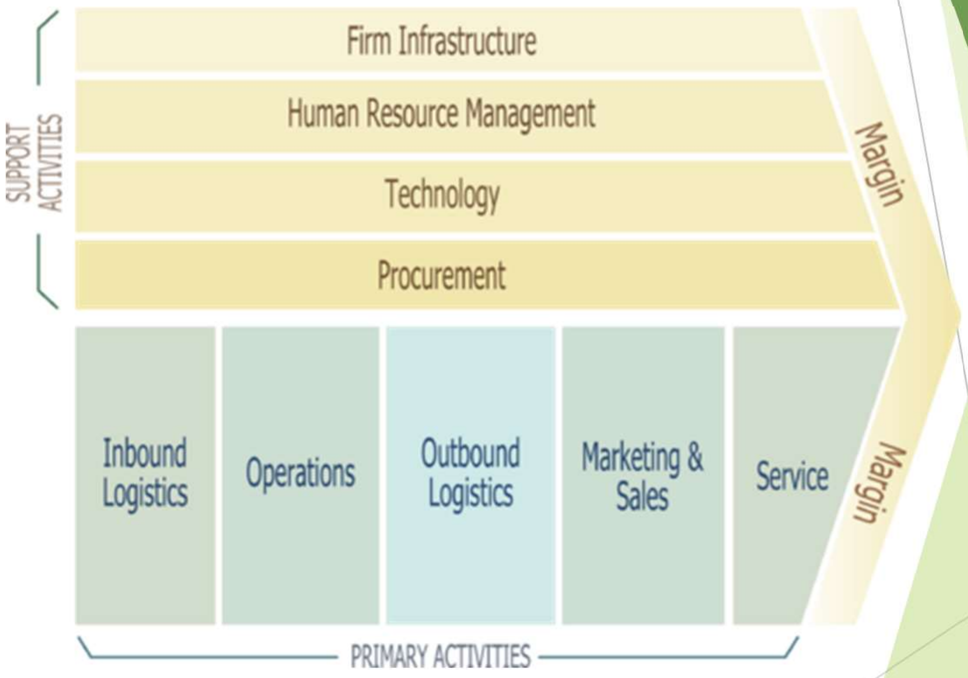
How does a business work?

Things that Technology Teams should know

Think about Value Chains

Introduced by Michael Porter in 1985, a fundamental approach to modelling a business

Enables a business architect to model how value is produced and supported in a business



Source - https://en.wikipedia.org/wiki/Value_chain

Why does everyone care about NPV, ROI, ROA?

- According to Shareholder theory, a business exists to maximise returns for their shareholders
- This means that every dollar invested must meet an investment criteria – some of these criteria are:
  - Net Present Value (NPV)

$$NPV = \sum_{t=1}^{n} \frac{R_t}{(1+i)^t}$$

where:

R_t = Net cash inflow-outflows during a single period t

i = Discount rate or return that could be earned in alternative investments

t = Number of timer periods

  - Return on Investment (ROI)

$$\text{ROI} = \frac{\text{Current Value of Investment} - \text{Cost of Investment}}{\text{Cost of Investment}}$$

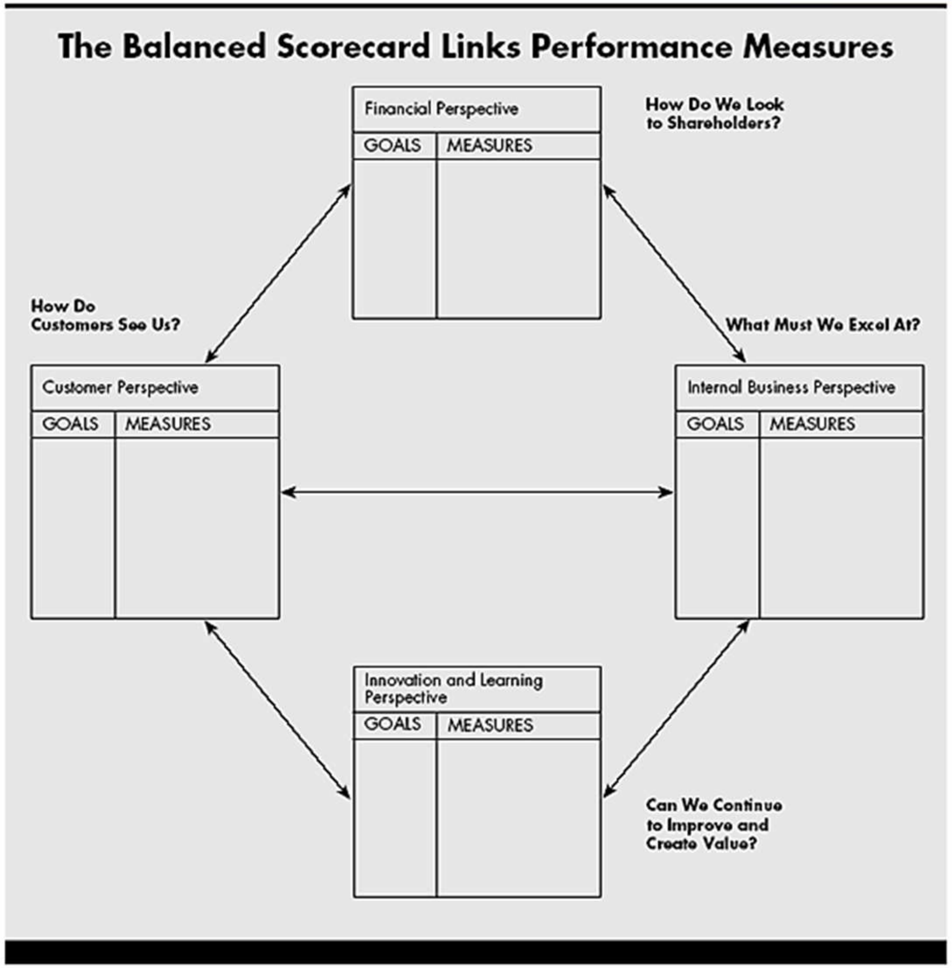
  - Return on Assets (ROA)

$$Return\ on\ Assets = \frac{Net\ Income}{Total\ Assets}$$

Source and for more information- https://www.investopedia.com

What’s a Balanced Score Card

- From Kaplan and Norton (1992) Balance Score Cards are a way to understand what Key Performance Indicators (KPI) are important for a business as well as how different KPIs interact



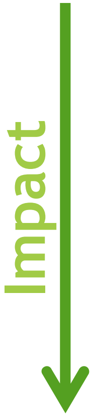
The Balanced Scorecard Links Performance Measures

Financial Perspective
GOALS
MEASURES
How Do We Look to Shareholders?
How Do Customers See Us?
Customer Perspective
GOALS
MEASURES
What Must We Excel At?
Internal Business Perspective
GOALS
MEASURES
Innovation and Learning Perspective
GOALS
MEASURES
Can We Continue to Improve and Create Value?

Source - https://hbr.org/1992/01/the-balanced-scorecard-measures-that-drive-performance-2

Why do we care about business disruption?

- Disruption is a critical market force which an organisation has to respond to
- From a technology viewpoint, this response could be:



Impact

  - The investment in new technology
  - The investment of new process and people
  - The divesture of a part of the business
  - The investment in the creation of a new line of a business
  - Could lead to broader Merger and Acquisition Activity

Why the need for Business Strategy

- A business Strategy is how a business plans to respond to the system in which it exists and should consider -
  - The Mission
    - Why does the business exist?
    - What Motivates it?
  - The Vision
    - Where does it want to be?
  - The Approach
    - Goals – To get to the vision, what are the goals that should be achieved
      - And what Objectives – these are the waypoints on the way to achieving a goal

What is business governance

- The Governance institute of Australia defines governance as
  - *"Governance encompasses the system by which an organisation is controlled and operates, and the mechanisms by which it, and its people, are held to account. Ethics,* ***risk management****,* ***compliance*** *and administration are all elements of governance."*
- The interest in governance has increased following the high-profile corporate collapses in the 2000s, for example Enron Corporation
- Cyber Security functions should think how they can support the governance of the organisaton by working with Internal Audit

Source - https://www.governanceinstitute.com.au/resources/what-is-governance/

How does IT work from the Business Team Viewpoint

Things that the business should know

The *As-Is* Plan, Build, Run

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?

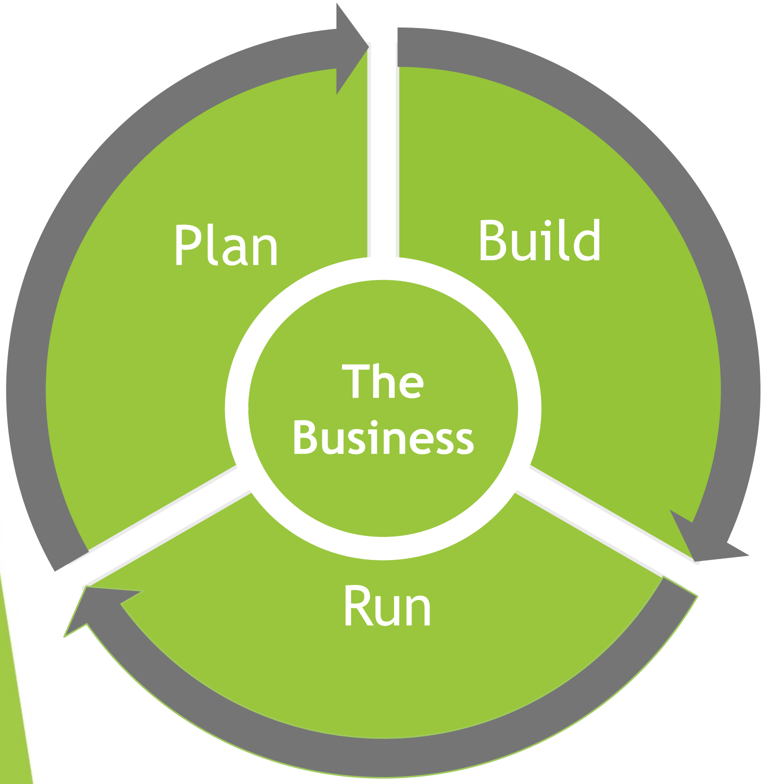
Why are none of our systems integrated?

Why does no one talk to me?

Shadow IT

Haha get in losers I have a credit card

The *To-Be* Plan, Build, Run

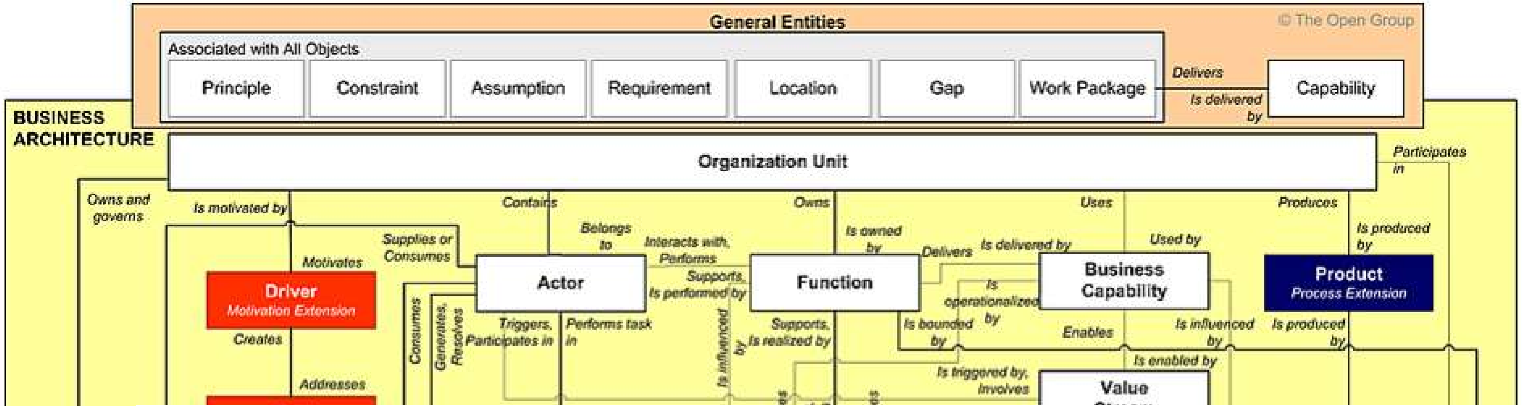


- A cyclical system where there is one team that aims to support the business
- Reduce hand offs and someone else's problem
- Pull the right stakeholders into projects as soon as possible in the engagement
- Encourage secondments and ride-alongs
- Not waiting to deliver perfection – incremental delivery!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

What is Business Architecture

- Business Architecture is how IT models the business so that it can define the interactions and requirements of different business functions and capabilities
- This is the work of Business Analysts and Enterprise & Enterprise Security Architects
- Beware the terminology and jargon may switch off key business stakeholders
- In EA and ESA Frameworks
  - TOGAF – The Business Architecture
  - SABSA – The Contextual and Conceptual Layers

What is Business Architecture (cont.)



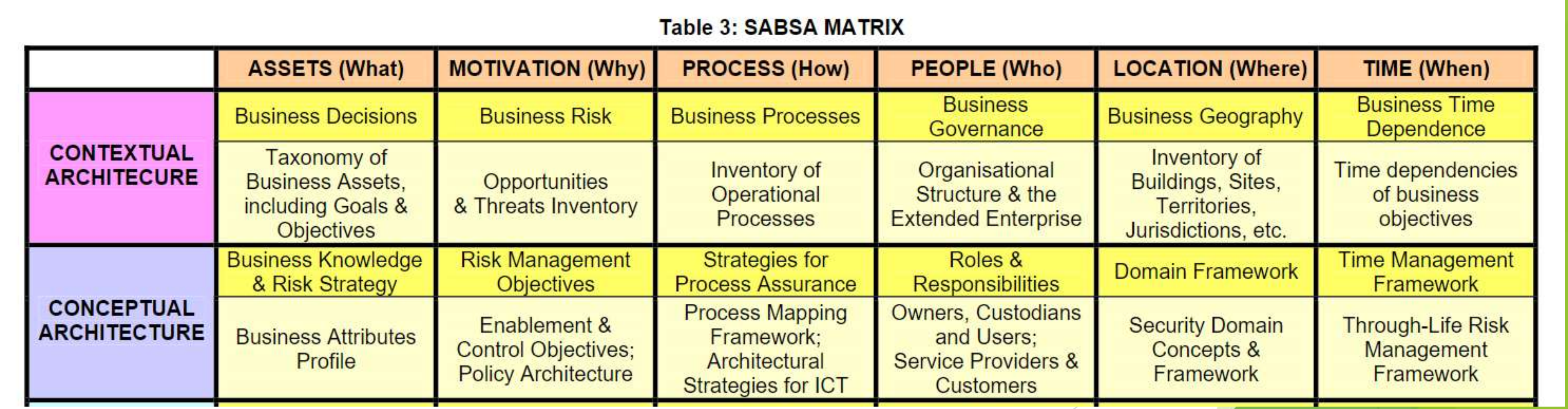


Table 3: SABSA MATRIX

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain 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

Source - https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap30.html
& The SABSA White Paper https://sabsa.org/sabsa-white-paper-download-request

What’s in the toolbox

So now we have some background, what do we do?

Risk Management

- Cyber security is the application of risk management
- You need to be able to communicate cyber security risk in the same risk language as the rest of the business
- You need to understand the business's cyber security risk appetite
- You need to make sure the business is aware and has accepted the cyber security risk it is currently holding
- Hubbard's *The Failure of Risk Management* and *How to Measure Anything in Cyber Security* are fantastic resources

Project and Programme Management (PPM)

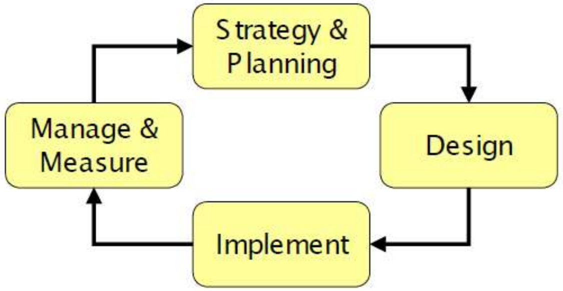
- The Project Management Office (PMO) should use a Project and Programme Management (PPM) approach
- Cyber Security Architects should be key stakeholders of the PMO
- The PMO should also have project gates to control spend and execution as well as assurance capabilities
- Security can *shift left* through the PMO!

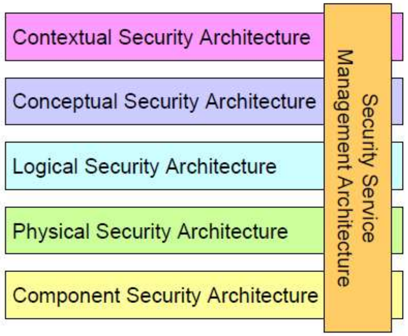
Information Security Management Systems (ISMS)

- The ISMS is the system to manage information security risk consistently across the company
- Can mean many different things
  - From just being a compliance tick for a suite of documents
  - An integrated management system that balances risk and opportunity across the organisation and defines a cyber security strategy for the business
  - And everything in between
- A key capability for managing cyber security for the organisation

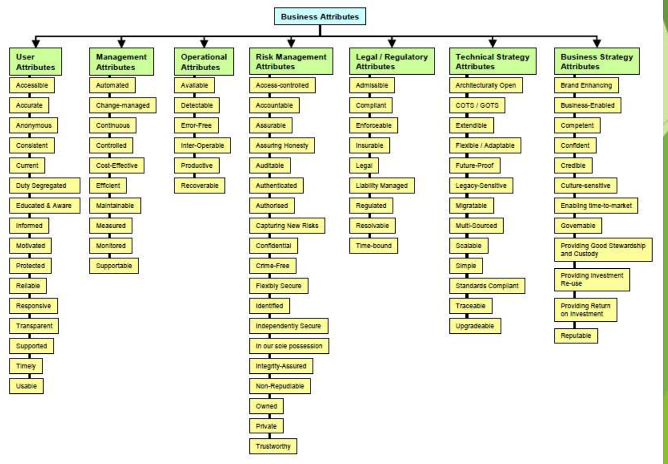
SABSA

- 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 (ESA)
- Links Business Objectives to Cyber Security activities through Attributes



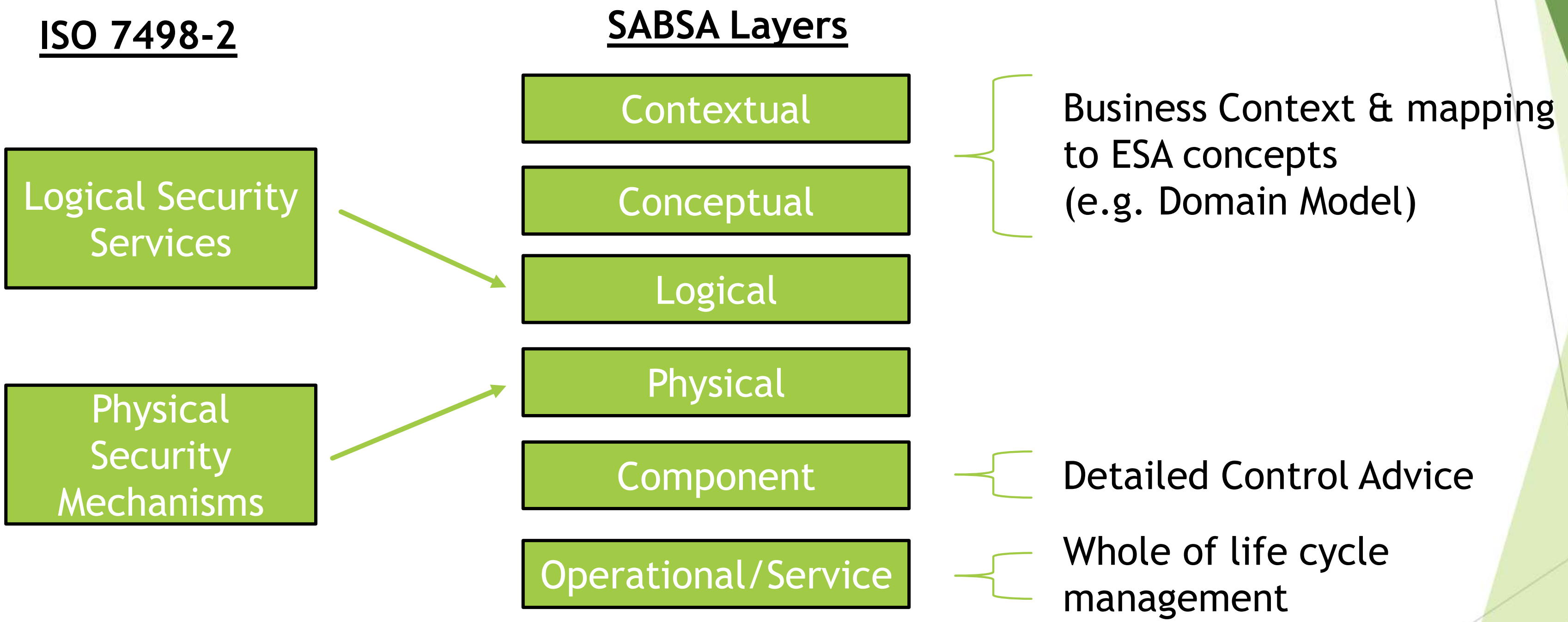


Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Management Architecture



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

SABSA (cont.) – Why 6 Layers?



ISO 7498-2

Logical Security Services

Physical Security Mechanisms

SABSA Layers

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

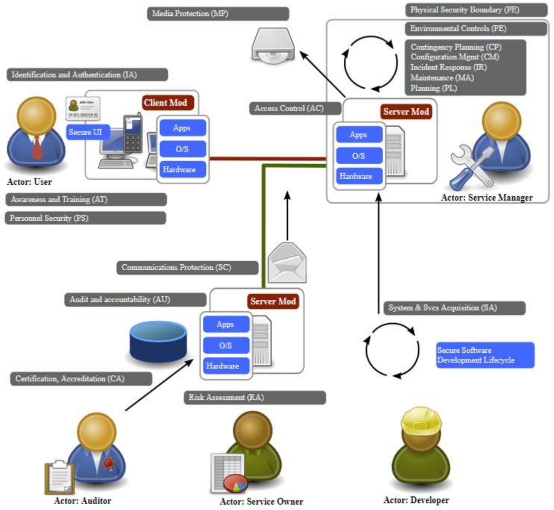
Security Patterns

- To scale the effort of the Security Team, Security Patterns are a fantastic way of sharing preferred cyber security standards to the broader technology team
- Think of them as a fast path for security design and review processes
- Should also evolve over time and be a standard reference as opposed to “let’s just copy the last one”
- Great starting point is Open Security Architecture (https://www.opensecurityarchitecture.org/)

Security Patterns (cont.)

SP-009: Generic Pattern

Diagram:



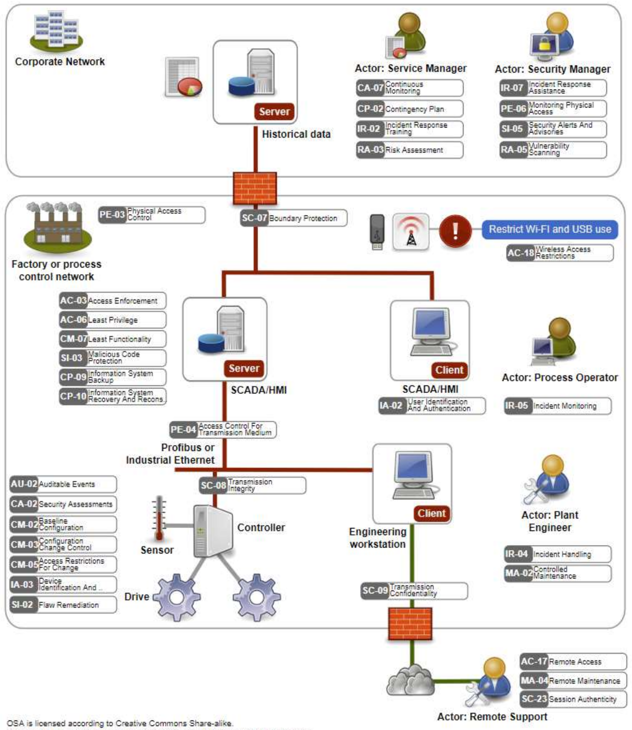
Media Protection (MP)
Physical Security Boundary (PE)
Environmental Controls (PE)
Contingency Planning (CP)
Configuration Mgmt (CM)
Incident Response (IR)
Maintenance (MA)
Planning (PL)
Identification and Authentication (IA)
Client Mod
Secure UI
Apps
O/S
Hardware
Access Control (AC)
Server Mod
Actor: User
Actor: Service Manager
Awareness and Training (AT)
Personnel Security (PS)
Communications Protection (SC)
Audit and accountability (AU)
System & Svcs Acquisition (SA)
Secure Software Development Lifecycle
Certification, Accreditation (CA)
Risk Assessment (RA)
Actor: Auditor
Actor: Service Owner
Actor: Developer

08_02_Pattern_009_02_Generic_Control_Families.svg
Depiction of generic security pattern that indicates the relationship and application of the main NIST control families.

SP-023: Industrial Control Systems

Industrial Control Systems Pattern

Diagram:



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

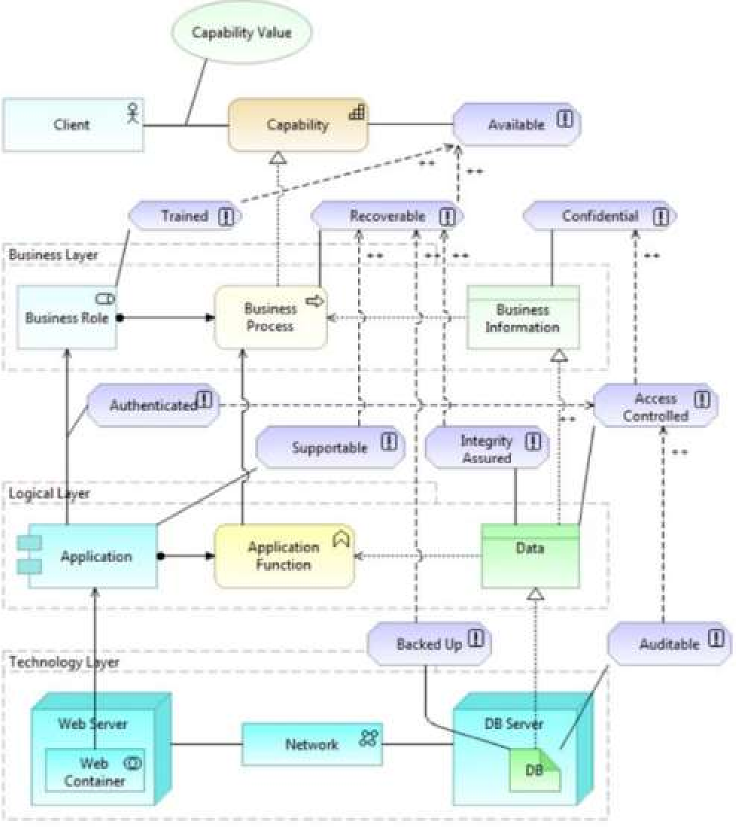


Figure 19: Attribute Traceability across Layers

Source - https://www.opensecurityarchitecture.org/
& https://sabsa.org/modelling-sabsa-with-archimate/

Some homework for you …

Next Week

1. Review the materials in the slide deck
2. Say hi to your cyber security architecture team
3. Understand what IT and Business forums you have (e.g. quarterly Steer Co meetings etc) – Is Security on the Agenda?

In the next 3 months

1. Review your Business Strategy and make sure your security strategy is aligned
2. Review your Risk Registers and ISMS documentation and identify the pain points between you and the business – brain storm new approaches with your team
3. Road Show to the business on your architecture function
4. Road Show to the technology teams your architecture function

Questions?

https://linkedin.com/in/blargeau

https://github.com/beLarge

@beLarge