

Security Architectuur in de praktijk

Edwin Vos

3 juni 2026

Introduction Edwin Vos

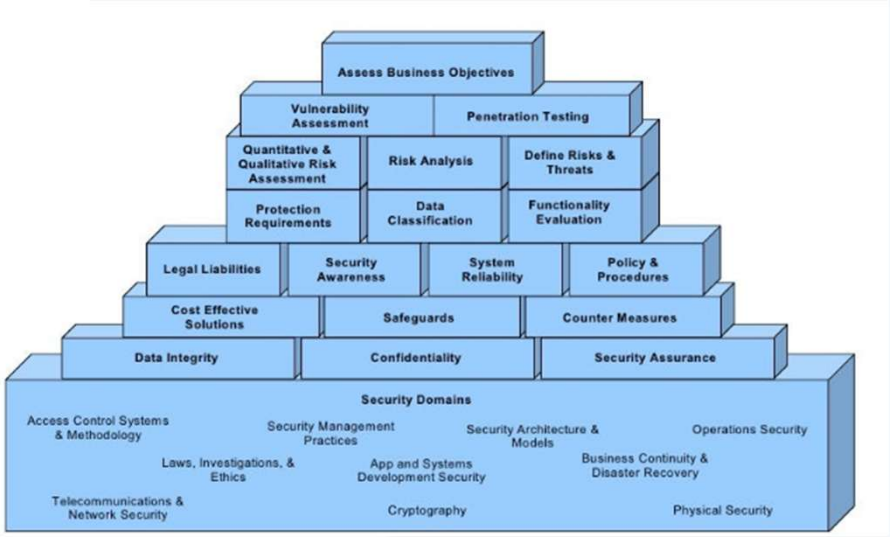
Network Engineer	1989 – 1995
Network Designer	1996 – 2005
Network Architect	2005 – now
Security Consultant	2008 – now
Security Architect	2020 – now




AGENDA
1 Oorsprong
2 Theorie
3 Praktijk

Definitie

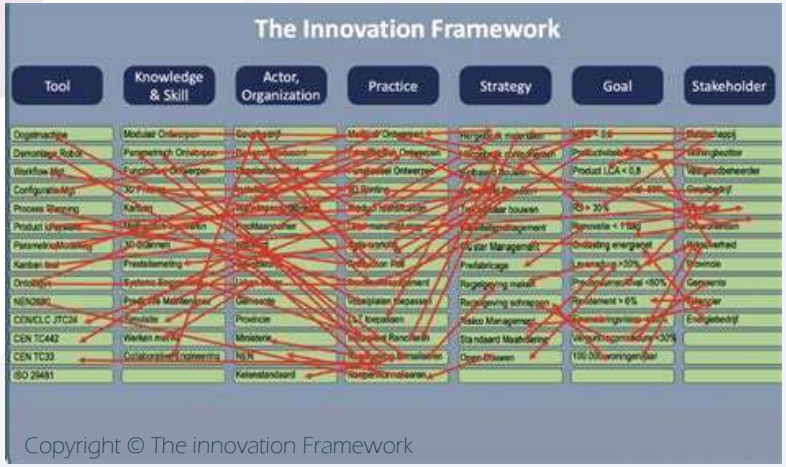
- Wat is Security Architectuur?
- Een model
- Een proces
- Een raamwerk



© ORACLE – CISSP Shone Harris



www.ardoq.com/blog/cybersecurity -architecture

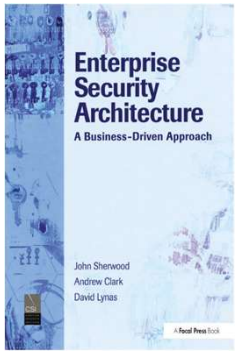


www.nivo.nl

Copyright © The innovation Framework

Terug naar de oorsprong

- ISO 7498-2:1989 Information processing systems - Open Systems Interconnection - Basic Reference Model Part 2: Security Architecture — 1989
- Zachmann framework - 1992 — 1992
- SALSA: A method for developing the enterprise security architecture and strategy - John Sherwood – 1996 — 1996
- SABSA: Enterprise Security Architecture: A Business-Driven Approach
- by John Sherwood, Andrew Clark & David Lynas – 2005 — 2005



SALSA = Sherwood Associates Limited Security Architecture

SABSA = Sherwood Applied Business Security Architcture

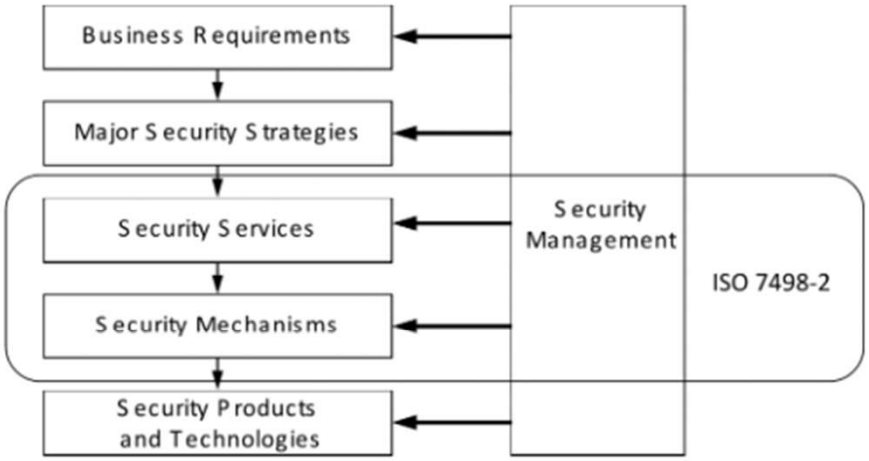
Theorie

- ISO 7498-2:1989

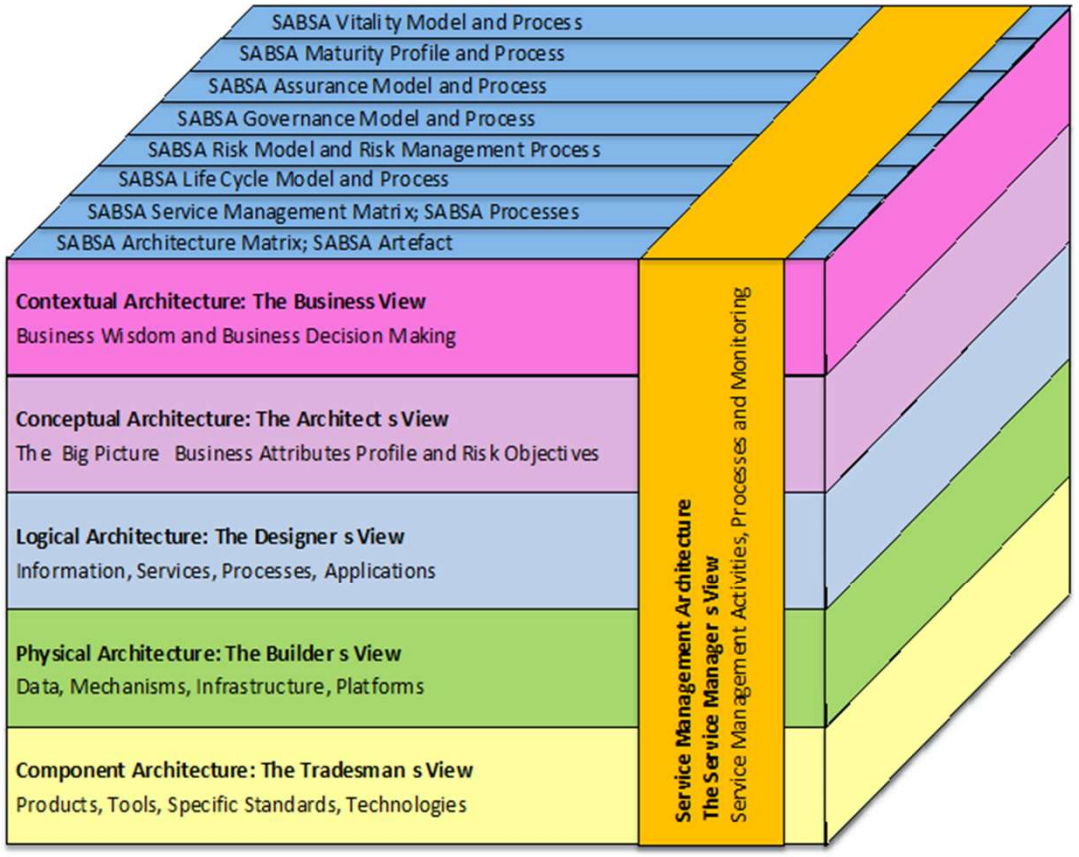
Service \ Mechanism	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer Entity Authentication	Y	Y	•	•	Y	•	•	•
Data Origin Authentication	Y	Y	•	•	•	•	•	•
Access Control Service	•	•	Y	•	•	•	•	•
Connection Confidentiality	Y	•	•	•	•	•	Y	•
Connectionless Confidentiality	Y	•	•	•	•	•	Y	•
Selective Field Confidentiality	Y	•	•	•	•	•	•	•
Traffic Flow Confidentiality	Y	•	•	•	•	Y	Y	•
Connection Integrity with Recovery	Y	•	•	Y	•	•	•	•
Connection Integrity without Recovery	Y	•	•	Y	•	•	•	•
Selective Field Connection Integrity	Y	•	•	Y	•	•	•	•
Connectionless Integrity	Y	Y	•	Y	•	•	•	•
Selective Field Connectionless Integrity	Y	Y	•	Y	•	•	•	•
Non-repudiation, Origin	•	Y	•	Y	•	•	•	Y
Non-repudiation, Delivery	•	Y	•	Y	•	•	•	Y

ISO 7498-2:1989

SALSA - SABSA



Copyright © The SABSA Institute 1995



Copyright © The SABSA Institute 1995 - 2016

Uitstapje - TOGAF

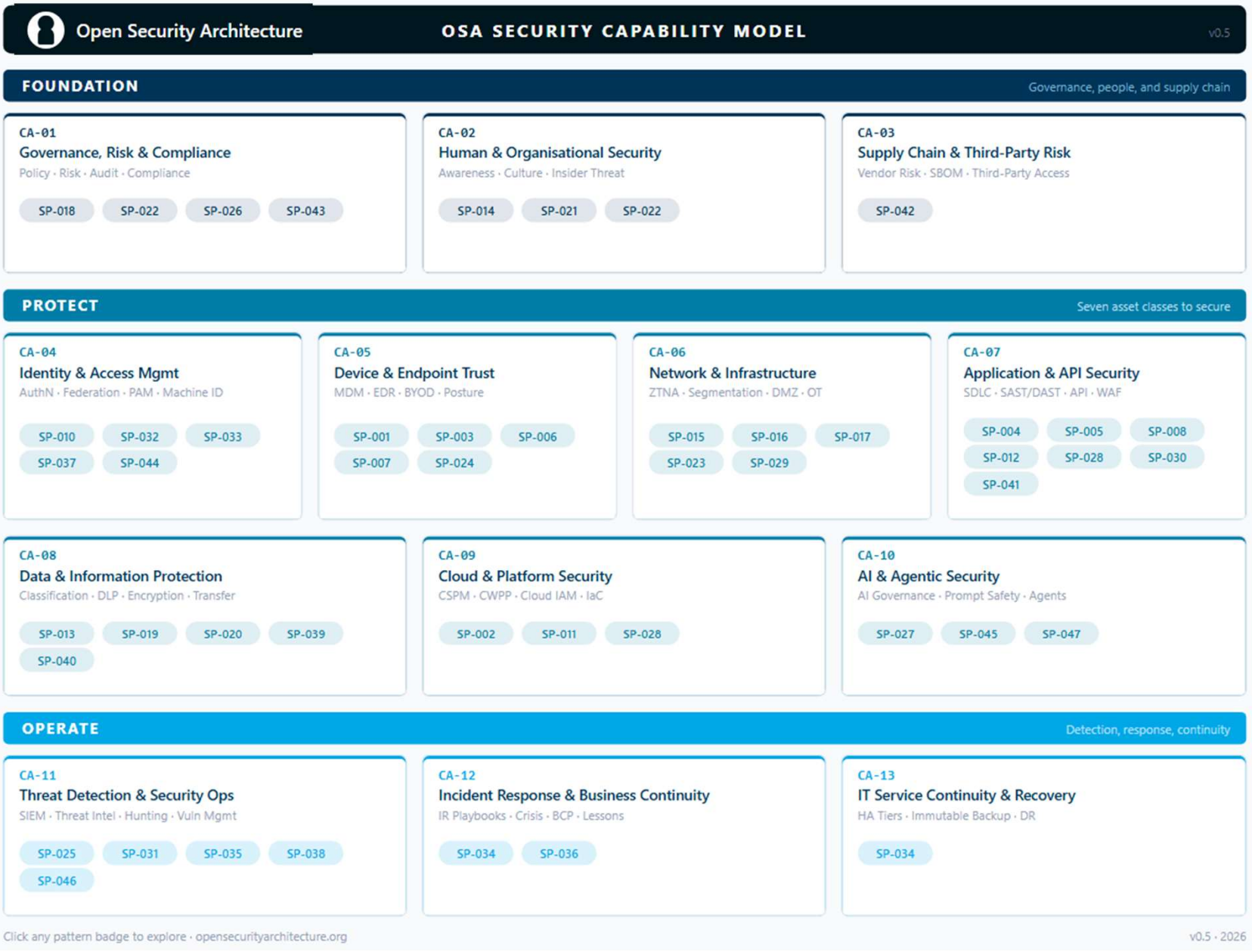
- The Open Group Architecture Framework
- Guide to Security Architecture in TOGAF ADM (2005)



Zachmann model

	DATA *What*	FUNCTION *How*	NETWORK *Where*	PEOPLE *Who*	TIME *When*	MOTIVATION *Why*
Objective/Scope (contextual) *Role: Planner*	List of things important in the business	List of Business Processes	List of Business Locations	List of important Organizations	List of Events	List of Business Goal & Strategies
Enterprise Model (conceptual) *Role: Owner*	Conceptual Data/ Object Model	Business Process Model	Business Logistics System	Work Flow Model	Master Schedule	Business Plan
System Model (logical) *Role:Designer*	Logical Data Model	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Technology Model (physical) *Role:Builder*	Physical Data/Class Model	Technology Design Model	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Detailed Reprentation (out of context) *Role: Programmer*	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Speculation
Functioning Enterprise *Role: User*	Usable Data	Working Function	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy

Marcel Douwe Dekker based on earlier work of Phogg2 et al. - self-made, combination of File:Zachman Framework Basics.jpg and File:Zachman Framework.jpg


Open Security Architecture
OSA SECURITY CAPABILITY MODEL
v0.5
FOUNDATION
Governance, people, and supply chain
CA-01
Governance, Risk & Compliance
Policy · Risk · Audit · Compliance
SP-018 SP-022 SP-026 SP-043
CA-02
Human & Organisational Security
Awareness · Culture · Insider Threat
SP-014 SP-021 SP-022
CA-03
Supply Chain & Third-Party Risk
Vendor Risk · SBOM · Third-Party Access
SP-042
PROTECT
Seven asset classes to secure
CA-04
Identity & Access Mgmt
AuthN · Federation · PAM · Machine ID
SP-010 SP-032 SP-033 SP-037 SP-044
CA-05
Device & Endpoint Trust
MDM · EDR · BYOD · Posture
SP-001 SP-003 SP-006 SP-007 SP-024
CA-06
Network & Infrastructure
ZTNA · Segmentation · DMZ · OT
SP-015 SP-016 SP-017 SP-023 SP-029
CA-07
Application & API Security
SDLC · SAST/DAST · API · WAF
SP-004 SP-005 SP-008 SP-012 SP-028 SP-030 SP-041
CA-08
Data & Information Protection
Classification · DLP · Encryption · Transfer
SP-013 SP-019 SP-020 SP-039 SP-040
CA-09
Cloud & Platform Security
CSPM · CWPP · Cloud IAM · IaC
SP-002 SP-011 SP-028
CA-10
AI & Agentic Security
AI Governance · Prompt Safety · Agents
SP-027 SP-045 SP-047
OPERATE
Detection, response, continuity
CA-11
Threat Detection & Security Ops
SIEM · Threat Intel · Hunting · Vuln Mgmt
SP-025 SP-031 SP-035 SP-038 SP-046
CA-12
Incident Response & Business Continuity
IR Playbooks · Crisis · BCP · Lessons
SP-034 SP-036
CA-13
IT Service Continuity & Recovery
HA Tiers · Immutable Backup · DR
SP-034
Click any pattern badge to explore · opensecurityarchitecture.org
v0.5 · 2026

Even terug naar SABSA

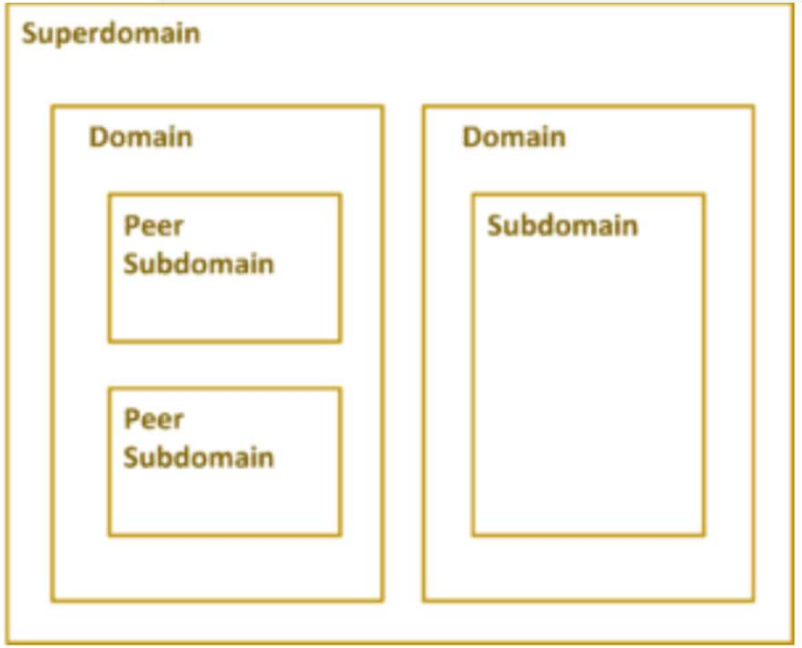
- Filosofie: Information Security as the Enabler of Business

Definitie volgens SABSA:

Security architecture is the art and science of designing and supervising the construction of business systems, usually business information systems, which are: free from danger, damage, etc.; free from fear care etc.; in safe custody; not likely to fail; able to be relied upon; safe from attack.

Security domein

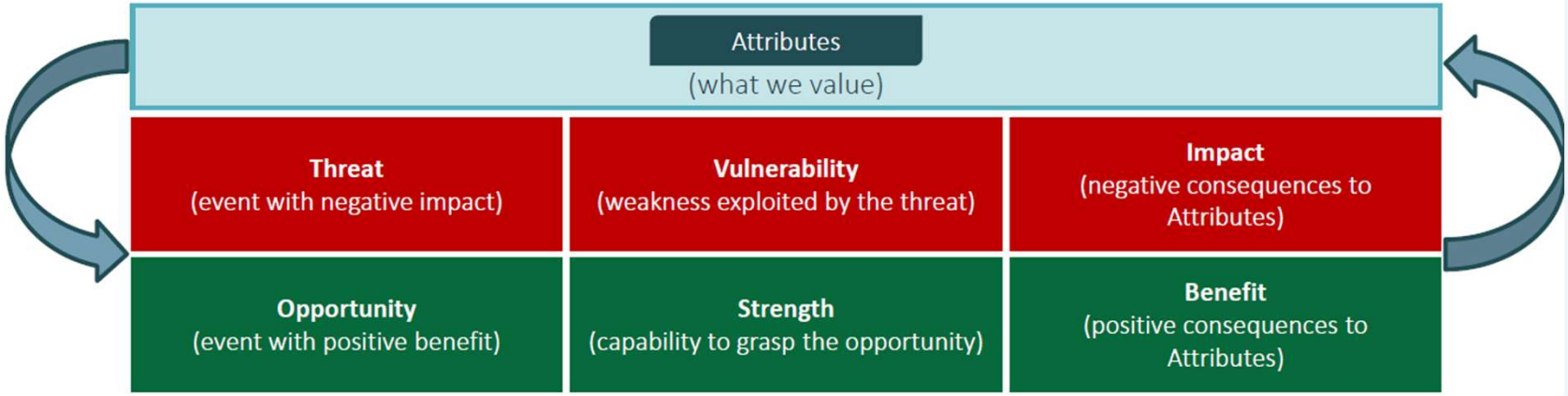
- Volgens SABSA: Deel van de organisatie waar een eigen policy geldt met een eigen verantwoordelijkheid.
- Volgens IT: afgebakende security techniek



Copyright © The SABSA Institute

Attribute

- Een genormaliseerde, meetbare, binnen context definitie van hetgeen belangrijk is (Business Value).



SABSA Risk

The positive or negative effect of uncertain events on Attributes

Copyright © The SABSA Institute - SABSA-A1-Risk-Assurance-Governance-v2.1

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	Assurance of Operational Excellence & Continuity	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Management & Support of Enterprise-wide and Extended Enterprise Relationships	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable
	The row above is a repeat of Layer 6 of the main SABSA Matrix. The five rows below are an exploded overlay of how this Layer 6 relates to each of these other Layers					
CONTEXTUAL ARCHITECTURE	Business Driver Development	Business Risk Assessment	Capability Management	Relationship Management	Supply Chain Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Processes and Capabilities for Providing Value to Stakeholders	Managing Suppliers, Service Providers, Customers; Business Partners & Employees. Contract Management	Demand & Supply Management (upstream and downstream); Deployment & Consumption	Defining Business-Driven Performance Targets
CONCEPTUAL ARCHITECTURE	Proxy Asset Development	Developing Risk Objectives	Delivery Planning	Role Management	Business Portfolio Management	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Maintaining Risk Modelling Framework; Risk Analysis on Business Attributes Profile	SLA Planning; BCP; Financial Planning; Transition Planning. Planning and Maintaining the Inventory of Processes and Services Catalogue	Maintaining Trust Modelling Framework; Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Business Footprint: Points of Supply and Access	Managing Performance Criteria and Targets; Abstracting Attribute Performance Targets
LOGICAL ARCHITECTURE	Logical Asset Management	Policy Management	Delivery Management	Enterprise-wide User Management	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management	Risk Modelling; Management of Policy Development & Maintenance. Policy Publication & Compliance Management	SLA Management; Supply Chain Management; BCM; Financial Management; Transition Management	Trust Modelling; Identity & Access Management; Management of User Privileges, Account Administration & Provisioning	Configuration (CMDB) Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
PHYSICAL ARCHITECTURE	Physical Asset Management	Risk Data Management	Operations Management	User Support	Resources Management	Performance Data Collection
	Change Management; Platform & Data Storage Management	Risk Procedure Management; Risk Metadata Management	Job, Incident, Event, and Disaster Recovery Management	Service Desk, Problem, and Request Management	Physical & Environmental Security Management; Real Estate and Facilities Management	Business Systems Monitoring Procedure Management
COMPONENT ARCHITECTURE	Component Management	Risk Management Components	Component Deployment	Personnel Component Management	Component Environment Management	Monitoring Components
	Product & Component Standards Management	Risk Analysis, Monitoring & Reporting Components, Systems and Standards Management	Product & Component Selection, Procurement. Project and Standards Management	Recruitment, Disciplinary, Training & Awareness Delivery. Component and Standards Management	Physical and Environmental Security Component and Standards Management	Analysis, Monitoring & Reporting Component and Standards Management

Copyright © The SABSA Institute 1995—2018. All rights reserved.

Security Architectuur in de Praktijk

- Verzameling security services
- Proces rond het goedkeuren van projecten
- Security by design i.p.v. achteraf maatregelen implementeren
- Security architectuur document
- Vertaling van een maatregelenkader naar concrete maatregelen

- Agile → security adviseur rol in teams

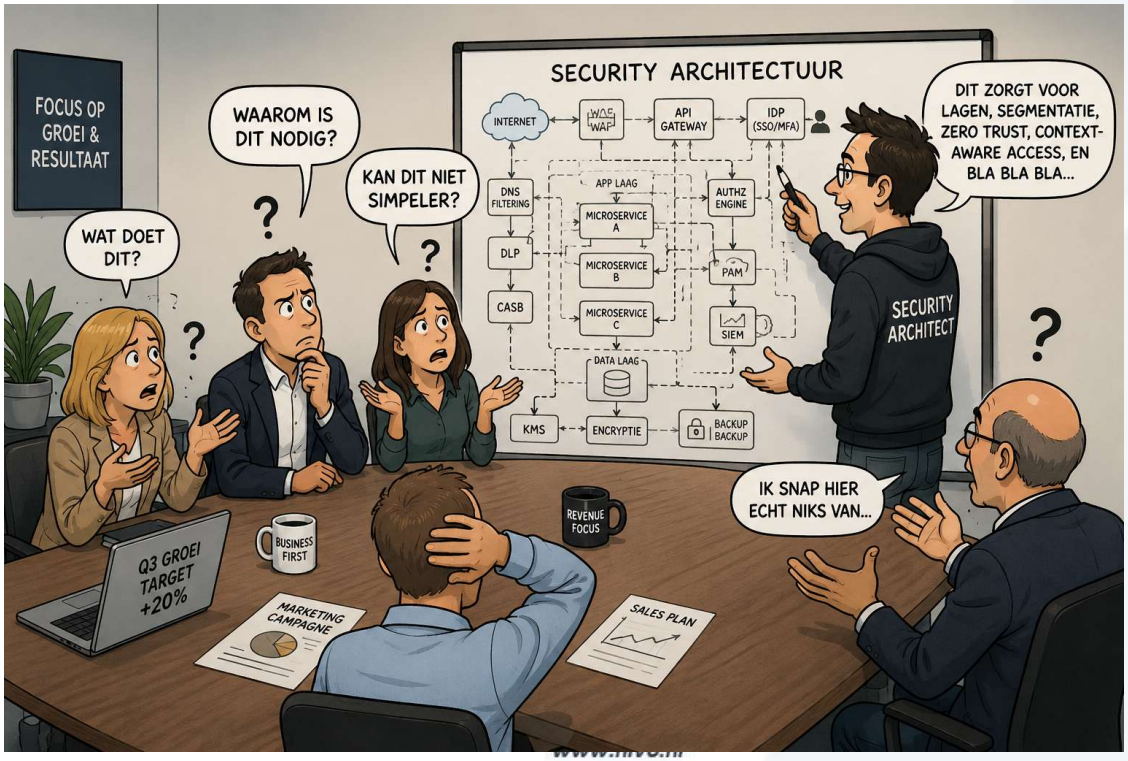
Valkuil 1:

- Betrek management er maar niet in.
- Ze hebben toch geen idee/kennis.



Valkuil 2:

- Business snapt niets van architectuur.



Valkuil 3:

- Wanneer is het klaar?



Valkuil 4:

- Security is een IT-feestje



Hoe dan wel?

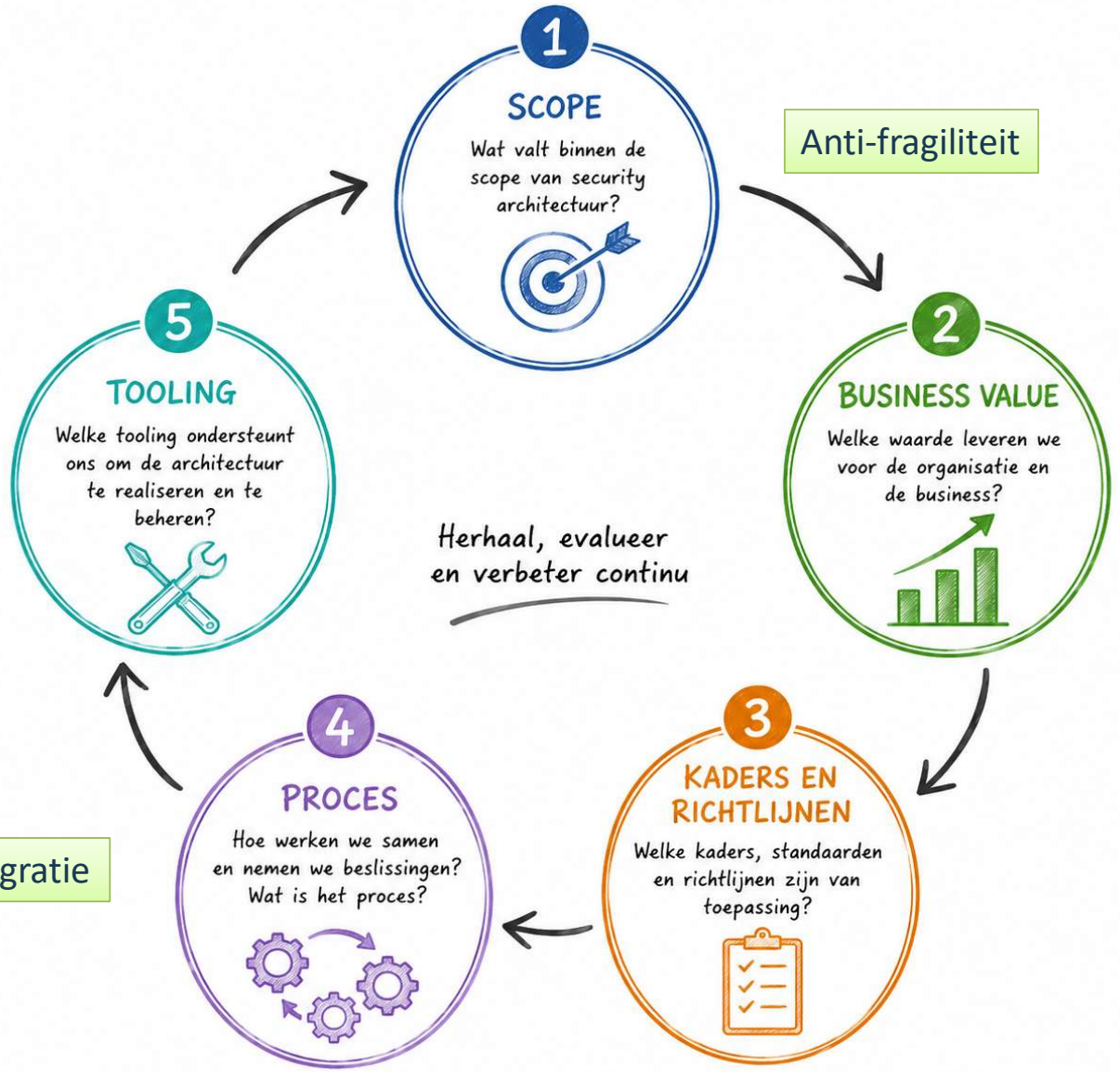
- Identificeer stakeholders en business vertegenwoordigers.
- Bepaal domeinen en verantwoordelijke personen
- Spreek met hen in hun eigen taal.
- Vraag wat zij belangrijk vinden en waar security hun kan helpen.
- Achterhaal attributes, zonder dit te benoemen.
- Stel een plan op en deel dit met de stakeholders.

Vervolgstappen

- Documenteer welke zaken belangrijk zijn voor de business
- Geef kaders en richtlijnen hoe de organisatie de beschikbaarheid, integriteit en exclusiviteit gaat invullen van de informatie en systemen.
- Richt processen in (b.v. risico management proces).
- Adviseer tooling (b.v. GRC-tool) te gebruiken.

- Evalueer de stappen en stel bij waar nodig.

Anti-fragiliteit



Post-Quantum migratie

Copyright © Edwin Vos