avolution

Try ABACUS Login

SABSA Framework for Enterprise Architects

Updated on 16th April 2024

SABSA Framework Overview

SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for creating business-driven security architectures: security is viewed as an enabler for business functions, not just a set of restrictions.

SABSA is made up of a series of integrated frameworks, models, methods and processes, used independently or as a holistic integrated enterprise solution, including:

- Business Requirements Engineering Framework (known as Attributes Profiling)
- Risk and Opportunity Management Framework
- Policy Architecture Framework
- Security Services-Oriented Architecture Framework
- Governance Framework
- Security Domain Framework
- Through-life Security Service Management & Performance Management Framework

Benefits of SABSA

The SABSA framework focuses on addressing security risks relevant to the business. It can be used alongside popular enterprise architecture frameworks and integrates well with TOGAF, ArchiMate and ITIL.

SABSA also provides tools for aligning security with standards like ISO 27001 .

Who Uses SABSA?

SABSA is widely used by architects across all industries globally, including commercial enterprises, Government Services and Defence & Intelligence communities.

Data Exchange: Architects can import & export data relevant to security architecture development using ABACUS integrations and API

Collaboration: Architects, security teams, and business stakeholders can collaborate on security data and models

Reporting and Visualization: ABACUS users can generate reports and visualizations that clearly illustrate the security architecture aligned with SABSA principles

Robust Security: ABACUS provides best-in-class access management and security to ensure the integrity of sensitive security architecture data

SABSA Security Architecture

Using SABSA in ABACUS allows architects to incorporate SABSA's structured approach to security architecture within the ABACUS architecture modeling environment.

This enables organizations to:

Define and document security requirements: Use SABSA principles to identify and specify security requirements at different levels of the enterprise architecture, ensuring that security considerations are systematically addressed

Map security controls: Use SABSA's framework to map security controls to specific architectural components within the ABACUS model, enabling organizations to understand how security measures are implemented across the enterprise

Analyze security posture: Leverage analytics and visualizations in ABACUS to assess the effectiveness of security controls and identify potential gaps or vulnerabilities in the architecture. SABSA provides a structured methodology for conducting security risk assessments and improving the overall security posture

Communicate security concerns: Use dashboards and visualization in ABACUS to communicate security-related information effectively to stakeholders. Employ SABSA's terminology and concepts to ensure clarity and alignment with industry standards

By integrating SABSA in ABACUS, organizations can strengthen their security architecture practices, improve risk management capabilities, and ensure that security considerations are integrated seamlessly into the broader enterprise architecture. This integration streamlines decision-making and enables organizations to mitigate security risks more effectively while supporting business objectives.

SABSA Tools & Techniques

Using SABSA in ABACUS provides:

Business Alignment: Mapping security controls to business objectives

Communicating Security Architectures

Using a tool which supports the SABSA methodology can significantly enhance communication for security architects, providing:

Clear Documentation and Templates: ABACUS can provide pre-built templates and consistent documentation across security architecture projects

Visualizations and Layered Models: Visual representations like diagrams and layered models (which break down security considerations from different stakeholder perspectives) can be generated by the tool. This supports clear communication with both technical and non-technical audiences

SABSA Matrix

In the architecture model, each horizontal layer undergoes vertical segmentation, addressing inquiries such as what, why, how, who, where, and when. This segmentation, known as the SABSA Matrix, forms the basis of the SABSA content framework. A distinct matrix is also available for service management.

SABSA SERVICE MANAGEMENT MATRIX (Aligned with ITIL v3)

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	The row above is a repeat of Layer 6 of the main SABSA Matrix. The five rows below are an exploded overlay of how this Layer 6 relates to each of these other Layers					
CONTEXTUAL ARCHITECURE	Business Driver Development	Business Risk Assessment	Service Management	Relationship Management	Point-of-Supply Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Service Capabilities for Providing Value to Customers	Managing Service Providers & Service Customers; Contract Man'ment	Demand Man'ment; Service Supply; Deployment & Consumption	Defining Business-Driven Performance Targets
CONCEPTUAL ARCHITECTURE	Proxy Asset Development	Developing ORM Objectives	Service Delivery Planning	Service Management Roles	Service Portfolio	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Risk Analysis on Business Attributes Proxy Assets	SLA Planning; BCP; Financial Planning & ROI; Transition Planning	Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Service Catalogue	Managing Service Performance Criteria and Targets
LOGICAL ARCHITECTURE	Asset Management	Policy Management	Service Delivery Management	Service Customer Support	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management; Test & Validation Management	Policy Development; Policy Compliance Auditing	SLA Management; Supplier Management; BCM; Cost Management; Transition Management	Access Management; User Privileges, Account Administration & Provisioning	Configuration Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
PHYSICAL ARCHITECTURE	Asset Security & Protection	Operational Risk Data Collection	Operations Management	User Support	Service Resources Protection	Service Performance Data Collection
	Change Management; Software & Data Integrity Protection	Operational Risk Management Architecture	Job Scheduling; Incident & Event Management; Disaster Recovery	Service Desk; Problem Man'ment; Request Man'ment	Physical & Environmental Security Management	Systems and Service Monitoring Architecture
COMPONENT ARCHITECTURE	Tool Protection	ORM Tools	Tool Deployment	Personnel Deployment	Security Management Tools	Service Monitoring Tools
	Product & Tool Security & Integrity; Product & Tool Maintenance	ORM Analysis, Monitoring and Reporting Tools & Display Systems	Product & Tool Selection and Procurement; Project Management	Recruitment Process Disciplinary Process Training & Awareness Tools	Products & Tools for Managing Physical & Logical Security of Installations	Service Analysis, Monitoring and Reporting Tools & Display Systems

architecture development process outlined by TOGAF. This integration involves identifying security requirements, risks, and controls at each phase of the TOGAF Architecture Development Method (ADM).

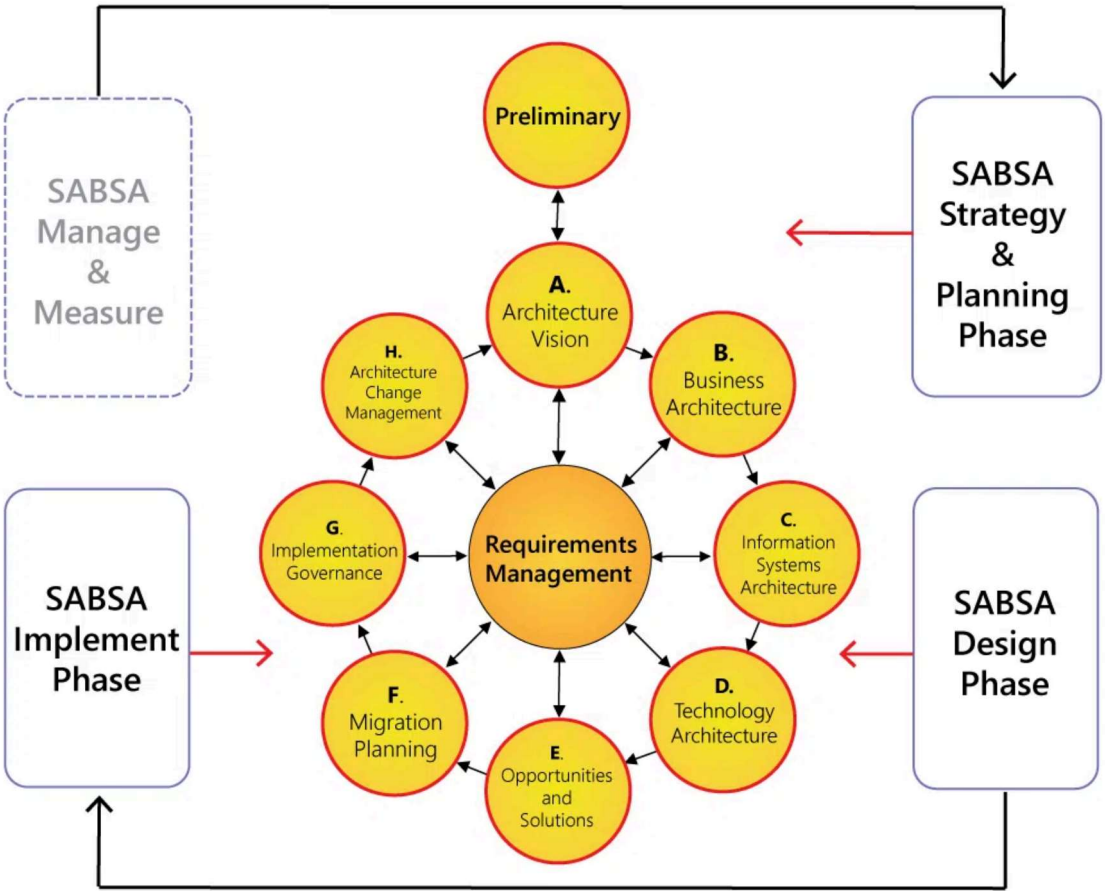
The TOGAF – SABSA integration is based on three foundations:

Risk Management

Requirements Management

The TOGAF ADM (Architecture Development Method)

By aligning SABSA principles with TOGAF's structured approach, architects can ensure that security concerns are integrated well into the overall architecture. This improves the organizations' ability to manage risk and support business objectives. This integration can also support better coordination between security architects and enterprise architects.



SABSA Lifecycle Phases Mapped to the TOGAF ADM (Image Source: SABSA Institute)

ABACUS is a TOGAF certified tool by The Open Group, providing conformance with all the TOGAF Framework requirements. ABACUS is also certified for ArchiMate.

ArchiMate provides a rich set of elements and relationships that can map to the key concepts of SABSA.

For instance, ArchiMate's business processes can represent activities within the organization. Application components can depict the IT systems delivering those services. Data objects within ArchiMate can be used to model the information flowing through the processes. This allows for a comprehensive view of the security posture of business services, enabling architects to identify potential vulnerabilities and design more secure systems.

By using ArchiMate's visual representation with SABSA stakeholders across business services, enabling architects to identify potential vulnerabilities and design more secure systems.

Combining SABSA with ArchiMate involves integrating security concerns into the broader enterprise architecture using ArchiMate's notation and framework. This integration allows organizations to depict security requirements, controls, and policies alongside other architectural elements such as business processes, applications, and infrastructure components. By utilizing ArchiMate's standardized symbols and relationships, SABSA principles can be effectively communicated and aligned with broader enterprise objectives, facilitating better decision-making and risk management.

SABSA Resources:

The SABSA Institute

SABSA Training and Certification For Architects

avolution

Try ABACUS Login

Subscribe now