Modeling a SABSA® based Enterprise Security Architecture using Enterprise Architect

By Frank Truyen
frank.truyen@cephascorp.com

October 2018

Trademarks

What is SABSA®?

SABSA (in use since 1995) is:

- A methodology for:
  - developing an enterprise information security architecture.
  - delivering security infrastructure solutions.
- An open standard comprised of models, methods, and processes, with no licensing required for end-User organizations.
- Completely vendor neutral.
- Not specific to any industry sector or organization type.
- Applicable at any level of granularity, from the project scope to the enterprise level.

BEYOND TACTICAL SECURITY CONCERNS

It encompasses not just technical/tactical security issues, but also addresses business goals, as well as all the environmental factors that may impede an organization from reaching those goals. Ultimately it is the **enterprise** and its activities that need to be secured, and the security of its computers and networks is only one means to this end. Unless the architecture can provide **real business support and enablement**, instead of simply focusing on 'security' in the narrow sense, then it is unlikely to deliver what the business needs and expects.

Model Centric and Requirements Driven

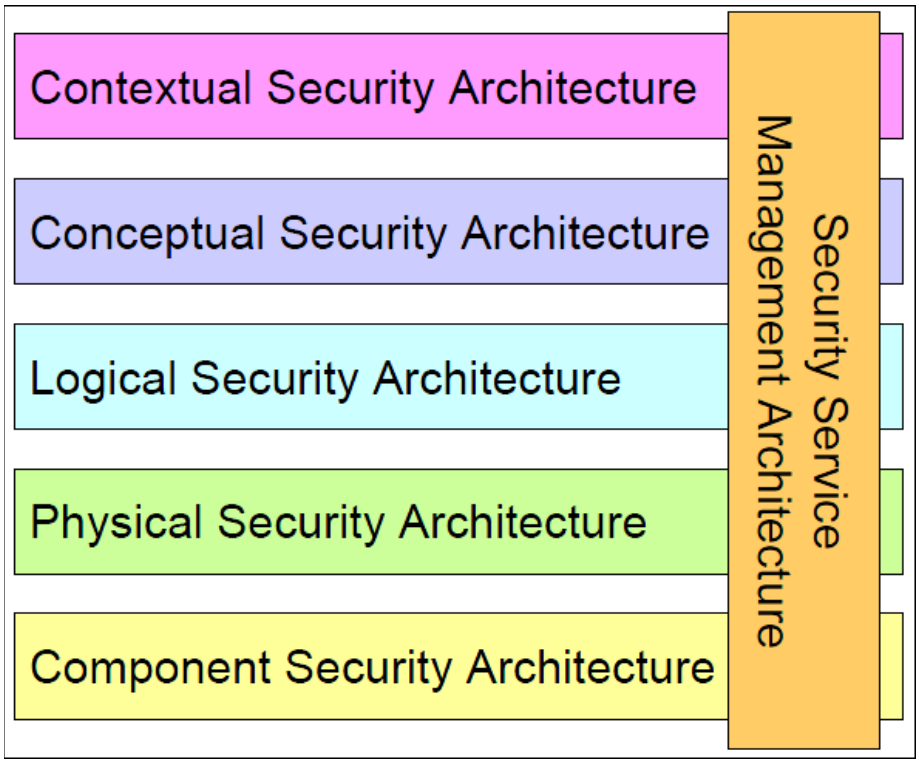
At the core of the SABSA methodology is a **model driven approach** that drives the development process, from analyzing risk-related requirements down to their realization.

Business requirements are the primary driver for developing effective security solutions that protect the business from undue operational risks in a cost-effective manner. These requirements span the areas of information, business continuity, physical, and environmental security.

SABSA ARCHITECTURE

Layered Architecture

The SABSA model consists of a six layered architecture:



Matrix

To facilitate the classification and organizational structure of the different viewpoints that make up each layer of the security architecture, a SABSA Matrix has been defined, derived from the Zachman Framework, to address six interrogatives:

What?	**The assets to be protected.**
Why?	**The motivation for wanting to apply security, expressed in terms of risk.**
How?	**The processes and functions needed to achieve security.**
Who?	**The people and organizational aspects of security.**
Where?	**The locations where security is applied.**
When?	**The time-related aspects of security.**

The resulting 6 X 6 matrix covers the entire range of questions to be answered, enabling a high level of confidence that the security architecture will be complete.

SABSA MATRIX

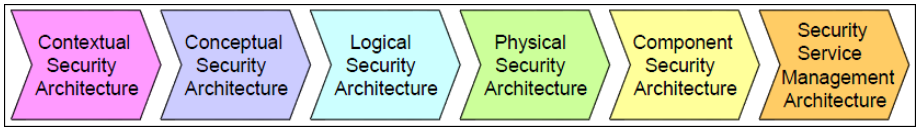
	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & 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
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
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
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment 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
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

Two-way Traceability

Completeness – has every business requirement been met?

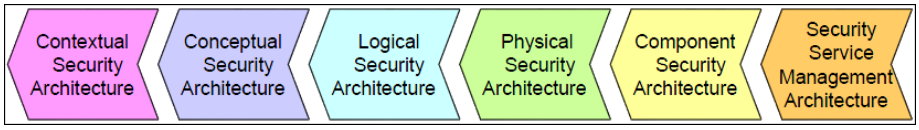
The matrix allows every requirement to be traced down to the component providing the solution.

SABSA TRACEABILITY



Business Justification – is every component in the architecture needed?

Every aspect of the solution can be traced back to the related business requirement/s.



Business Attributes Profile

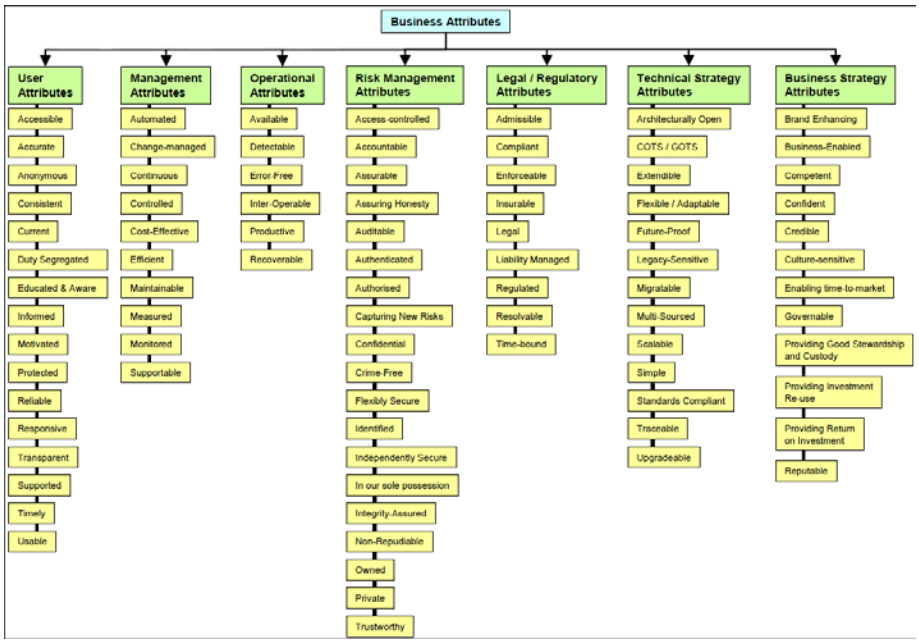
At the heart of the SABSA methodology, the Business Attributes profile provides a **requirements engineering technique** that enables the creation of links between the business requirements and the security architecture design.

The Business Attributes taxonomy has been compiled over many years by the team of security architects at the SABSA Institute, as a result of working with numerous customers in various industries. Each Business Attribute:

- is an abstraction of a real business requirement encountered in actual organizations,
- has a detailed definition, as well as suggested guidelines for applying it.

BUSINESS ATTRIBUTES

Consider the following subset of these Attributes:



When adopting SABSA, end Users can customize and/or extend this set of Attributes to meet their particular needs. Note also that not all the Attributes are applicable to a given organization. However the taxonomy can be used as a checklist of possible Attributes to be applied.

SABSA Integration with Enterprise Architect

MDG Technology for SABSA Security Architecture

The integration is provided by means of an MDG Technology extension (plugin) to the Enterprise Architect modeling tool from Sparx Systems. The integration covers:

1. The five horizontal layers of the SABSA Security Architecture, but not the Management Architecture, the artifacts of which are typically maintained outside of a modeling tool.
2. Consequently the five top rows of the SABSA Matrix, provided as a diagram index page in Enterprise Architect.
3. Two-way traceability using the built-in features of Enterprise Architect.
4. The complete (default) set of Business Attributes, including definition and guidance notes.

SABSA MDG TECHNOLOGY FEATURES

The Technology extension comes predefined with:

1. A template folder structure containing a Package and child diagram for each cell of the Matrix. Any number of instances of the structure can be created within a single repository, using the tool's Model Wizard.
2. Catalogs (libraries) containing default sets of:
    a. Business Attributes.
    b. Business Impact Types.
    c. Requirement Types.
    d. Security Mechanisms.
    e. Security Services.
    f. Tool and Product Types.
    g. Threat Categories and Threat Agents.
3. Specialized diagrams and toolboxes to define the:
    a. Business requirements.
    b. Contextual architecture.
    c. Conceptual architecture.
    d. Logical architecture.
    e. Physical architecture.
    f. Component architecture.

    Where applicable the extension leverages existing diagram types such as:

    - UML (for Class models).
    - ERD (for conceptual data models).
    - BPMN 2.0 (for business process models).
    - Business Motivation Model (BMM).
    - Org Charts, Business Logistics, and Database Schema.

4. Specialized toolboxes to define security related:

   a. **Element types**: Business Requirement, Risk, Threat Agent, Threat Category, Business Impact, Impact Type, Vulnerability, Time-based-measurement, Control Objective, Architectural Layer, Security Strategy, Security Service, Security API, Registry, Role, Authorized Role, Resource, Rule, Entity, Entity Schema, Schema Rule, Trust Broker, Directory, Certificate, Logical/Physical Security Domain, Logical Domain Service, Logical Domain Function, Application, Application Function, Access Control, Firewall, Security Policy, Policy Authority, Privilege Profile, Security Object, Security Lifetime, Security Guideline, Security Practice, Security Procedure, Security Mechanism, Access Mechanism, Bastion Host, LAN, Laptop, Mobile Device, Router, Server, Product, Standard, Tool, Protocol, Protocol Stack, User.

   b. **Connector types**: Communication, Persisted In, Issues, Trusts, Governs, Protects, Rules, Relates To, Flows To, Interacts With, Role Assignment, Authorized For, Certifies, Stored In, Accesses, Connection, and more.

   Many of these element and connector types are augmented with custom properties and graphics.

5. A Matrix diagram.

SABSA MATRIX IN ENTERPRISE ARCHITECT

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

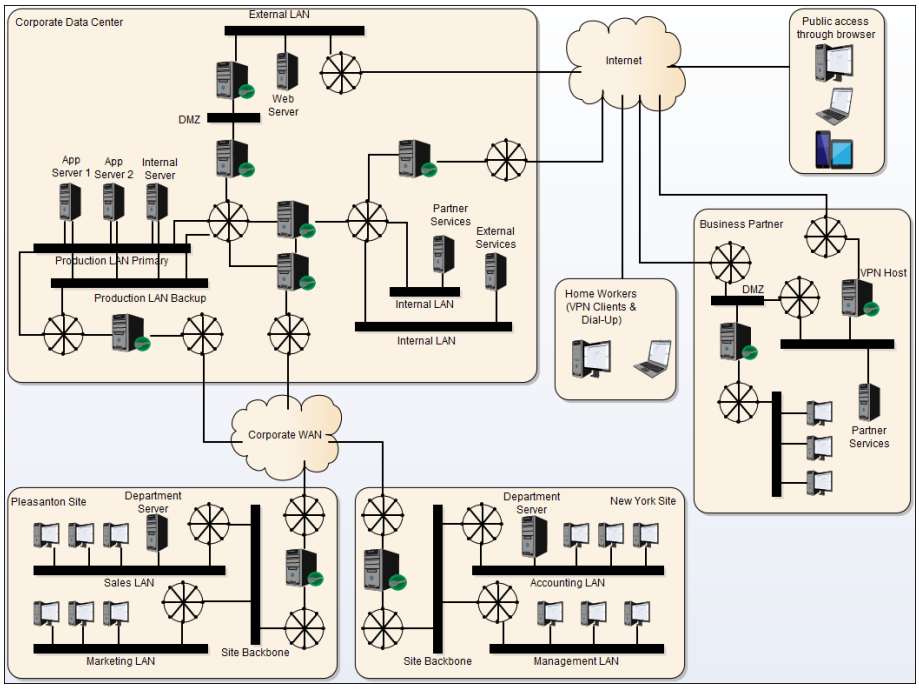
Each cell hyperlinks to the corresponding diagram in the aforementioned Package/folder structure.

6. Database queries and Relationship Matrix definitions.

Example Diagram

The following diagram illustrates a network topology, part of the Physical Architecture – Location viewpoint (row 4, column 5 of the Matrix).

NETWORK TOPOLOGY EXAMPLE DIAGRAM



Integration with Existing Architecture Models

The SABSA Security Architecture extension integrates seamlessly into existing architectural models, be they based on TOGAF®, UPDM™, Zachman, or a homegrown methodology, by adding an extra dimension to the framework.

The security architecture can be modeled as one perspective (with its own set of viewpoints) of a multi-dimensional framework, with other possible dimensions corresponding to traditional non-functional perspectives such as availability, extensibility, fault tolerance, interoperability, performance, reliability, reusability, and scalability.

The security specific model elements can then be traced effortlessly inside the other dimensions of the framework to the objects that are affected, constrained, or otherwise relevant to security considerations (e.g. UML Class/Interface operations, Use Case Actors, Activity nodes, database tables or columns, business capabilities, etc.).

References and Links

SABSA White Paper – an executive summary of its methods, techniques, and concepts.

Enterprise Security Architecture: A Business Driven Approach, by John Sherwood, Andrew Clark, and David Lynas.

A free trial of the SABSA Security Architecture extension to Enterprise Architect (version 13.x or later) is available for download.

A SABSA specific one-day (in-person, web-based) training class can be scheduled.

About Cephas Consulting Corp.

COMPANY BACKGROUND

Since 2001 Cephas Consulting Corp. has been helping its clients introduce state of the art modeling practices in their organization. We offer expertise in the areas of:

. Training Users on modeling with the UML®, BPMN™, SysML™, SoaML®, ArchiMate®, and other notations.

. Training on the use of the Enterprise Architect tool from Sparx Systems.

. Installation, configuration, and customization of the tool.

. Migrating data out of other (legacy) tools such as Microsoft Visio.

. Converting development organizations into using Model Driven Architecture (MDA).

. Providing advanced consulting and mentoring services around all aspects of modeling.

CONTACT DETAILS

Website : https://enterprisemodelingsolutions.com

General inquiries: contact@enterprisemodelingsolutions.com

Author inquiries: frank.truyen@cephascorp.com