Modeling a SABSA® based Enterprise Security Architecture using Enterprise Architect

October 2018

Trademarks
UML™, Unified Modeling Language™, Model Driven Architecture™, MDA™, Business Process Modeling Notation™, BPMN™, UPDM™ and SoaML™ are trademarks of the Object Management Group (OMG). UML® and MDA® are registered trademarks of the OMG. TOGAF® is a registered trademark of The Open Group. Enterprise Architect and MDG Technologies are trademarks of Sparx Systems. All other products or company names mentioned are used for identification purposes only, and may be trademarks of their respective owners.
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.

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.
Layered Architecture

The SABSA model consists of a six layered architecture:

- Contextual Security Architecture
- Conceptual Security Architecture
- Logical Security Architecture
- Physical Security Architecture
- Component Security Architecture
- Management 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:

<table>
<thead>
<tr>
<th>What?</th>
<th>The assets to be protected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why?</td>
<td>The motivation for wanting to apply security, expressed in terms of risk.</td>
</tr>
<tr>
<td>How?</td>
<td>The processes and functions needed to achieve security.</td>
</tr>
<tr>
<td>Who?</td>
<td>The people and organizational aspects of security.</td>
</tr>
<tr>
<td>Where?</td>
<td>The locations where security is applied.</td>
</tr>
<tr>
<td>When?</td>
<td>The time-related aspects of security.</td>
</tr>
</tbody>
</table>
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.

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.

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.

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.

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.
   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).
4. Specialized toolboxes to define security related:


   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 Diagram](image)

   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).

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.


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.

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.

Website: https://enterprisemodelingsolutions.com

General inquiries: contact@enterprisemodelingsolutions.com

Author inquiries: frank.truyen@cephascorp.com