SABSA Overview

SABSA is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives. The primary characteristic of the SABSA model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited.

The process analyses the business requirements at the outset, and creates a chain of traceability through the strategy and concept, design, implementation, and ongoing ‘manage and measure’ phases of the lifecycle to ensure that the business mandate is preserved. Framework tools created from practical experience further support the whole methodology.

The model is layered, with the top layer being the business requirements definition stage. At each lower layer a new level of abstraction and detail is developed, going through the definition of the conceptual architecture, logical services architecture, physical infrastructure architecture and finally at the lowest layer, the selection of technologies and products (component architecture).

The SABSA model itself is generic and can be the starting point for any organisation, but by going through the process of analysis and decision-making implied by its structure, it becomes specific to the enterprise, and is finally highly customised to a unique business model. It becomes in reality the enterprise security architecture, and it is central to the success of a strategic programme of information security management within the organisation.

SABSA History

SABSA is a six-layer model for security architecture widely accepted today as the most mature and most comprehensive security architecture

SABSA was originally an acronym for ‘Sherwood Applied Business Security Architecture’. The starting point for this work was ISO 7498-2 1989: ‘Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture’. This standard is relatively unsophisticated in terms of business drivers, but it sets out an important framework in terms of ‘security services’ – the logical architecture, ‘security mechanisms’ – the physical architecture, and ‘security management’ – the operational architecture. The Sherwood team added two upper layers to provide a business-driven approach (contextual and conceptual architectures), and a lower layer to map onto real tools and products (component architecture).

John Sherwood presented the SABSA work at COMPSEC 96 in London and published the follow-up paper on it later that year. At that time he had never heard of Zachman’s work. In April 1998 Sherwood was working for an international client as the security architect on a team engaged in developing entirely new global infrastructure architecture was fortunate enough to visit a conference entitled ‘Enterprise Architecture’ in San Francisco, where one of the key note speakers at that conference was John Zachman.

The Sherwood team was able to re-work SABSA to incorporate some of the language and ideas that Zachman had talked about in his presentation. However, the original concepts of SABSA remained pretty much unchanged.

**SABSA Model**

The SABSA Model comprises six layers, as shown in the table below. It follows the work done by John A. Zachman in developing a model for enterprise architecture, although it has been adapted somewhat to a security view of the world.
Each layer represents the view of a different player in the process of specifying, designing, constructing and using the business system. These six layers are similar to the rows of the Zachman matrix.

<table>
<thead>
<tr>
<th>The Business View</th>
<th>Contextual Security Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Architect’s View</td>
<td>Conceptual Security Architecture</td>
</tr>
<tr>
<td>The Designer’s View</td>
<td>Logical Security Architecture</td>
</tr>
<tr>
<td>The Builder’s View</td>
<td>Physical Security Architecture</td>
</tr>
<tr>
<td>The Tradesman’s View</td>
<td>Component Security Architecture</td>
</tr>
<tr>
<td>The Facilities Manager’s View</td>
<td>Operational Security Architecture</td>
</tr>
</tbody>
</table>

The SABSA Model for Security Architecture Development

Another configuration of these six layers which is perhaps more helpful, shown in the next figure. Here, the ‘operational security architecture’ has been placed vertically across the other five layers. This is because operational security issues arise at each and every one of the other five layers. Operational security has a meaning in the context of each of these other layers.
SABSA Matrix and SABSA Method

For detailed analysis of each of the six layers, the SABSA Matrix also uses the same six questions that are represented by columns in the Zachman Framework: What, Why and When, How, Where and Who? For each horizontal layer there is a vertical analysis as follows:

- **What** are you trying to do at this layer? – The assets to be protected by your security architecture.
- **Why** are you doing it? – The motivation for wanting to apply security, expressed in the terms of this layer.
- **How** are you trying to do it? – The functions needed to achieve security at this layer.
- **Who** is involved? – The people and organisational aspects of security at this layer.
- **Where** are you doing it? – The locations where you apply your security, relevant to this layer.
- **When** are you doing it? – The time-related aspects of security relevant to this layer.

These six vertical architectural elements are now summarized for all six horizontal layers. This gives a 6 x 6 matrix of cells, which represents the whole model for the enterprise security architecture. This arrangement is called the SABSA Matrix (see below).

If you can address the issues raised by each and every one of these cells, then you will have covered the entire range of questions to be answered, and you can have a high level of confidence that your security architecture is complete.

According to the SABSA team approach, “The process of developing an enterprise security architecture is a process of populating all of these thirty-six cells.”
The SABSA Matrix for Security Architecture Development

A final Question for you:

1) How is the SABSA model different from the Zachman model? List at least three items. Only one of these answers can come from the above model diagram.