What is SABSA?

SABSA is a proven framework and methodology for Enterprise Security Architecture and Service Management used successfully by numerous organisations around the world. Now used globally to meet a wide variety of Enterprise needs including Risk Management, Information Assurance, Governance, and Continuity Management, SABSA has evolved since 1995 to be the ‘approach of choice’ for commercial organisations and Government alike.

SABSA ensures that the needs of your enterprise are met completely and that security services are designed, delivered and supported as an integral part of your business and IT management infrastructure.

Although copyright protected, SABSA is an open-use methodology, not a commercial product.

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 framework available.

SABSA is based on an idea first developed by John Sherwood in 1995 and published in 1996 as ‘SABSA: A Method for Developing the Enterprise Security Architecture and Strategy’. SABSA was originally an acronym for ‘Sherwood Applied Business Security Architecture’ and was the basis on which the Sherwood team (including David Lynas and Andy Clark the leading players in the ongoing development of the methodology and in its use in delivering client consulting assignments) built their world-wide reputation for thought leadership in the area of 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).

Unknown to Sherwood at the time, this work was closely related to work being carried out in the USA on the wider context of overall enterprise architectures, authored by John Zachman, published by the Zachman Institute for Framework Advancement and known as the ‘Zachman Framework’.

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. As part of that activity he was fortunate enough to visit a conference entitled ‘Enterprise Architecture’ in San Francisco, and 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.

Since then the methodology has been promoted in many seminars and applied in a number of client situations in several countries and in several regions, where it has been enthusiastically received. To meet the ever-increasing demands of the global market and provide more extensive support for increased use of the method on a global scale, the methodology was launched on a major scale, partly through the publication of the SABSA book ‘Enterprise Security Architecture: A Business Driven Approach’ (by Sherwood, Clark and Lynas), partly through the continued training and education seminars on the subject, and partly through the creation of the SABSA Institute and this web site. Initiatives to support the world-wide growth in the use of SABSA include the world-wide launch of the SABSA Certification programme to provide assurance to employers and peers over competency of professionals and service providers to use SABSA.

The SABSA Model comprises six layers, the summary of which is in the table below. It follows closely 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.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Security Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Business View</td>
<td>Contextual Security Architecture</td>
</tr>
<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

There is another configuration of these six layers which is perhaps more helpful, shown in the next figure. In this diagram 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 Model for Security Architecture Development]

The SABSA Model for Security Architecture Development

**SABSA Matrix**

For detailed analysis of each of the six layers, the SABSA Matrix also uses the same six questions that are used in the Zachman Framework and which were so eloquently articulated by Rudyard Kipling in his poem ‘I Keep Six Honest Serving Men’: 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 summarised for all six horizontal layers. This gives a 6 x 6 matrix of cells, which represents the whole model for the enterprise security architecture. It 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. The process of developing an enterprise security architecture is a process of populating all of these thirty-six cells.

<table>
<thead>
<tr>
<th>Assets (What)</th>
<th>Motivation (Why)</th>
<th>Process (How)</th>
<th>People (Who)</th>
<th>Location (Where)</th>
<th>Time (When)</th>
</tr>
</thead>
</table>

The SABSA Matrix for Security Architecture Development

**SABSA Framework for Security Service Management**

The area of security service management, administration and operations is addressed through the SABSA operational architecture layer. This layer of the framework is applied vertically across all of the other five providing enormous flexibility to ensure seamless and holistic integration with the standards & operational frameworks of your choice. SABSA not only ensures Information Security compliance with frameworks such as ITIL, BS15000 / AS8018, ISO 17799, and CobIT, but where these state what needs to be done SABSA delivers the invaluable roadmap to determine how it should be done in your business context.
The SABSA Framework for Security Service Management

SABSA Development Process

The SABSA Model provides the basis for an architecture development process, since it is clear that through understanding the business requirements, the architect can create the initial vision. This is used by the designers to create the detailed design, which in turn is used by the builder to construct the systems, with components of various sorts provided by specialists. Finally, the facilities manager operates the finished system, but unless the earlier phases take account of the operational needs, this phase in the lifetime of the system will be fraught with difficulty. The development process itself is shown, at a high level, in the following diagram.
The SABSA Development Process

The high-level development process (see diagram above) indicates that there is a natural break after the first two phases. Once the Contextual Architecture and the Conceptual Architecture are agreed and signed off, then work on the later phases can begin, with considerable parallel working. However, it is difficult to make useful progress on the later stages until these first two are fairly fully defined. The temptation to go straight to an implementation of certain products and tools should be avoided, since this is the source of so many severe problems during the operational phase.

It is also important not to be confused by the positioning of the sub-process ‘Define Operational Security Architecture’. The Operational Security Architecture itself cuts across all of the other five layers, but the development process for that Operational Security Architecture is best delayed until after the Contextual and Conceptual Security Architectures have been defined and signed off.

SABSA Lifecycle

The SABSA Lifecycle is designed to align with your IT Lifecycle. Whatever your scope, the SABSA Framework provides a structured approach for successful delivery. Whether you are facing the challenges of service management, enterprise-wide architecture, designing the infrastructure for a new business initiative, implementing a single IT project, or complying with governance and compliance directives, the SABSA Lifecycle will give you the roadmap for success.
In the SABSA Lifecycle, the first two phases of the SABSA Development Process are grouped into an activity called ‘Strategy & Concept’. This is followed by an activity called ‘Design’, which embraces the design of the logical, physical, component and operational architectures. The third activity is ‘Implement’, followed by ‘Manage and Measure’. The significance of the ‘Measure’ activity is that early in the process you set target performance metrics (see the discussion of the SABSA Business Attributes Profile). Once the system is operational, it is essential to measure actual performance against targets, and to manage any deviations observed. Such management may simply involve the manipulation of operational parameters, but it may also feed back into a new cycle of development.

**SABSA Attributes**

A further refinement is the use of SABSA Business Attributes. These attributes are compiled from extensive experience with numerous clients in many countries and industry sectors. Over the course of that work it became apparent that although every business is unique, there are commonly recurring themes. This experience has been used to create a taxonomy of SABSA Business Attributes, shown in the next figure. These are organised under seven group headings.
The SABSA Taxonomy of Business Attributes

Each SABSA Business Attribute is an abstraction of a real business requirement previously encountered in client work, most of them encountered many times over. Each SABSA Business Attribute has a detailed definition and some suggested guidelines for applying metrics to that attribute, not included in this overview.

This is a very powerful tool that allows any unique business to be translated and ‘normalised’ into a SABSA Business Attributes Profile. This profile selects only those SABSA Business Attributes that apply to this specific business (creating new attributes if there are found to be gaps). The taxonomy provides a check-list of possible attributes and the business analysts can decide whether or not a given attribute should be included in this specific profile. The SABSA Business Attributes Profile is an important conceptualisation of the real business and has many additional powerful applications in areas such as Risk Management, Assurance, Governance, Continuity and Service Management. It forms a core part of the ‘Conceptual Architecture’. It can be seen on row 2, column 1 of the SABSA Matrix.

More information see: www.sabsa.org