

Advanced Module A3

SABSA Architecture & Design Master Class

Overview

The SABSA A3 Course module covers the architecture and design of:

- Identity and access management
- Network security
- Application and web security
- Cryptographic sub-systems

Identity and Access Management Strategy & Architecture

Identity and access management (I&AM) is arguably the most important and most pervasive concept in the entire field of information security architecture. It applies to both network and applications architecture and design and addresses a wide range of issues, including:

- Naming schemes for unique identification of entities to which information access privileges are to be granted;
- Entity relationships and trust;
- Security domains and their information access policies;
- Authorisation of entities for future access to selected information resources;
- Authentication of an entity as a pre-requisite to granting a real-time information access request;
- Checking authorisations in real time to support access control decisions;
- Contextual considerations (such as time of day and entity location) in making access control decisions;
- Creating and managing event logs of information access activities for audit, forensic and diagnostic purposes;
- Administering entity registrations and authorisation profiles;
- The application of cryptography for securing remote authentication handshaking protocols;
- Directory services for managing entity-related information such as names, aliases, authorisations and authentication information.

I&AM strategy and architecture are major considerations for a SABSA-based enterprise security programmes. The pervasiveness of this topic is evident in the SABSA framework inasmuch as various aspects appear in many different cells of the SABSA Matrices. This topic is the key overarching design discipline for anyone involved in security architecture and design.

Network Security Architecture & Design

The job of the network is information transfer. Think of it as a postal or courier service, collecting letters and parcels from some locations and delivering them to others. It is not the concern of the courier to know what is inside the packages, other than perhaps to put some size and weight restrictions on them for convenience of transfer. A data communications network is very like this – concerned with transferring packages of information between applications without having any knowledge of the contents of the packages.

Once you grasp this concept, understanding the purpose and scope of network security is clear. Network security is concerned with protecting the transfer service – making sure all the packages get collected and delivered to the right places, at the right time, in the correct sequence, that none get damaged, lost or stolen, and that the network customers – the applications – pay the proper rates for the service. By contrast, application security deals with the protection of the contents of the packages.

This distinction is at its most obvious when the network owner and the application owner are completely separate organisations. The network service provider needs security to protect the network services, but the application owner needs to ensure that the contents of the packages sent through the network are securely wrapped for confidentiality purposes, and that if the network service allows a package to be damaged, lost or stolen, this can be detected.

The SABSA A3 course module is based upon this clear distinction between the network security strategy and the application security strategy, a distinction and a decoupling that is key to developing appropriate enterprise security architectures.

Application and Web Architecture & Design

The distinction between applications and networks with regard to security strategy and architecture has been made above in the section on networks. The SABSA A3 course module addresses the use of SABSA to develop a strategy and architecture for the design of applications, including web-based applications.

Cryptographic Techniques

Every level and every part of information system security architecture and design, including network security, application and web security and identity &

access management, requires the application of cryptography. The SABSA A3 course module addresses the use of SABSA to select and apply these techniques as a part of the overall architecture and design of the systems.

Course Overview

This 5-day course provides participants with a practical guide on how to design and implement strategies and architectures in the wider context of a SABSA-based enterprise information security architecture and risk management programme. This course is not a technical detail course; it is a course on how to apply SABSA models and processes to developing a systems strategy, policy and architecture.

High-Level Learning Objectives

After attending this course a course attendee will be able to:

- Apply the SABSA framework to define the business requirements for architecture and design within a given enterprise;
- Analyse the business requirements to build a SABSA Business Attributes Profile that reflects the needs of the enterprise for systems architecture and design;
- Use the SABSA Business Attributes Profile to create a set of focused enablement and control objectives covering all aspects of systems architecture and design;
- Plan, design, implement and manage an information systems strategy and architecture within the SABSA framework;
- Plan, design, implement and manage information systems and sub-systems at the conceptual, logical, physical and component layers of the SABSA framework;
- Develop and implement SABSA-aligned operational processes for managing information systems;
- Apply the SABSA framework as a template against which to audit designs and implementations of information systems and processes.

Pre-Requisite Knowledge

There are no pre-requisites for attending this course or for sitting the SABSA Institute A3 examinations on completion of the course. However, attendees will probably benefit most if they have some previous knowledge of the SABSA framework. For those wishing to be awarded the SABSA Chartered Practitioner Certificate or the SABSA Chartered Master Certificate, they will need to complete the SABSA Chartered Foundation Certificate before the Practitioner award can be made, which in turn is a prerequisite for the award of the Master certificate.

What a Course Attendee will take away

- A comprehensive knowledge of the principles and practice of information systems architecture and design within the SABSA framework;
- The skill and knowledge to plan, design, implement and manage an information systems strategy and architecture within the SABSA framework;
- A practical SABSA-based approach to managing business processes for providing secure information services that are aligned with the needs of the business.

Who Should Attend

- CIO / CISO / CTO / CIRO
- IT Strategists and Planners
- IT Architects
- IT Development Managers and Project Leaders
- Designers and Developers of Information Systems
- Software Managers and Architects
- Network Managers and Architects
- Computer / Application / Web / Network / Information Security Managers, Advisors, Consultants & Practitioners
- IT Line Managers
- IT Service Delivery Managers
- Internal and External Auditors

Methodology

The course consists of lectures and workshop sessions, supplemented by case studies drawn from a combination of published real life examples and/or practical experience. In the workshops attendees will work in small groups to synthesise ideas and strategies and to apply the material in the context of case studies and simulations. Open forum discussions will also feature where appropriate.

Lecture content is naturally less intense than in Foundation classes, with more emphasis on practical work. The course focuses heavily on developing the skills and knowledge for a practitioner or master through hands-on workshop sessions and discussions, so as to provide the appropriate balance and emphasis on practice rather than theory.

During the course many references will be made to *Enterprise Security Architecture: A Business Driven Approach* (Sherwood, Clark and Lynas, ISBN 1-57820-318-X) for technical details that cannot be covered in full during the lecture programme. Every course attendee will therefore need to have a copy of this book. If you already own one, please bring it with you. If you would like to purchase one from us then please order your copy along with the course.

Course Outline

1. Basic Risk and Security Concepts and Components for Information Systems Architecture and Design from the SABSA Matrices.
2. Information System Security Strategy Development using SABSA.
3. SABSA Entity Relationships and SABSA Trust Models and their use in Information Systems Architecture and Design.
4. SABSA Information System Security Domains and Policy Management.
5. SABSA Conceptual, Logical and Physical Information System Architectures.
6. SABSA Information System Management Strategy, Architecture and Design.
7. Auditing the Architecture and Design of Information Systems using the SABSA Framework.