SABSA® Foundation (F1 & F2) – Virtual & In-person Training

1 Introduction

The SABSA® Foundation Modules (F1 & F2) are the SABSA® Institute's official starting point for developing Security Architecture Competencies. They are designed to create a broad-spectrum of knowledge and understanding of the SABSA® method, its frameworks, concepts, models & techniques. Theories and concepts are put to the test in 'proof-of-concept' style case study exercises and workshops so that candidates can understand how SABSA® is best applied to meet the challenges of the real world.

SABSA® Foundation training and examinations are now available as virtual training held online. Hence you can take advantage of this facility and get certified in the only Information Security Governance certification.

2 Course Outline

2.1 Module F1 – Security Strategy & Planning

1. Principles & Objectives of Security Architecture	a. Enterprise Security Architecture b. Guiding Principles c. The Engineer's Complex System & Holistic Approach d. Features, Advantages & Benefits
2. The SABSA® Framework	a. The SABSA® Matrix b. The SABSA® Service Management Matrix c. Traceability Concepts
3. Business Requirements Engineering & Attributes Profiling	a. Business Target Abstraction Technique b. Attributes
4. Risk & Opportunity Modelling	a. Risk Management in Business & Architecture b. Assessing Risk Using Attributes c. The SABSA® Opportunity Model d. Removing Subjectivity & Creating Re-usable Structure
5. Policy Architecture Framework	a. The SABSA® Policy Framework b. SABSA® Domains & Policy c. Creating the Policy Model
6. Systems Engineering & Integrated Compliance	a. Systems Engineering Principles in SABSA® b. SABSA®'s Integrated Compliance Framework
7. Capability-based Defence-in-Depth	a. Control Strategy b. The SABSA® Multi-tiered Control Strategy
8. SABSA® Governance Framework	a. SABSA® Governance Model b. SABSA® Roles & Responsibilities Framework
9. Security Domain Concepts	a. Domain Types b. Domain Models c. Registration & Certification d. Systemic Risk Interactions Between Domains
10 Security Time & Performance Concepts	a. SABSA® Lifecycle

		b. Through-life Risk Management Framework c. Process Improvement Framework d. Performance Management Framework e. Architectural Vitality Framework

2.2 Module F2 – Security Services & Service Management

1.	Information Security & Data Security Architectures	a. The Design Phase – Logical, Physical & Component Layers b. Service Management Overlay for the Design Phase Layers c. Principles of Integration & Alignment d. Start-up Approaches
2.	Risk Treatment Architecture	a. Risk Treatment & Policy Management Architecture b. The SABSA® Assurance Model
3.	Transformation & Service Architecture	a. Top-down Process Analysis in SABSA® b. Securing Information Transformations & Information Flows c. Security Services Definition & Modelling Processes d. Security Service Management Value Proposition
4.	Entity & Trust Modelling	a. Trust & Trust Models b. Decomposing Complex Trust in Solutions Specification
5.	Security Associations Modelling	a. Security Associations Modelling b. Inter-Domain Complexities c. The Extended Domain Concept
6.	Security Service Sequencing & Performance Management	a. Temporal Considerations for Security Architecture b. Security Service Sequencing

3 Competency Development Outcomes

	Module F1 – Security Strategy & Planning	Module F2 – Security Service Management & Design
1.	Define enterprise security architecture, its role, objectives and benefits.	Use SABSA® to create a holistic framework to align and integrate standards
2.	Describe the SABSA® model, architecture matrix, service management matrix and terminology.	Describe roles, responsibilities, decision-making and organisational structure
3.	Describe SABSA® principles, framework, approach and lifecycle.	Explain the integration of SABSA® into a service management environment
4.	Use business goals and objectives to engineer information security requirements.	Define Security Services
5.	Create a business attributes taxonomy.	Describe the placement of security services within IT Infrastructure

	Module F1 – Security Strategy & Planning	Module F2 – Security Service Management & Design
6.	Apply key architectural defence-in-depth concepts.	Create a SABSA® Trust Model
7.	Explain security engineering principles, methods and techniques.	Describe and model security associations intra-domain and inter-domain
8.	Use an architected approach to design an integrated compliance framework.	Explain temporal factors in security and sequence security services
9.	Describe and design appropriate policy architecture.	Determine an appropriate start-up approach for SABSA® Architecture
10.	Define security architecture value proposition, measures and metrics.	Apply SABSA® Foundation level competencies to the benefit of your organisation

4 Examination Format

No. of Exams: 2

Duration: Each exam is of 1 hours duration

No. of Questions: 48 MCQs each

Coverage: Equally distributed through 6 knowledge domains (the columns of the SABSA® Matrix)

Passing Score: 75% and above in BOTH modules (F1&F2)

Examinations are available online

5 Who Should Attend?

6 Course Information

Certification: SABSA® Chartered Architect – Foundation Level (SCF) (no expiry or CPEs)

Duration: 5-days

Venue: Online

Training Fees: <Please contact us to enable us to give an attractive training proposal>

7 Terms & Conditions

1. Full payment to be received 2 weeks prior to the commencement of the training
2. If a nominated person cannot attend a substitute can attend. If a person cannot be nominated 40% of the course fee is levied to cover the costs.
3. If the minimum number of attendees is not available, the training maybe cancelled, and the payment shall be refunded (after the deduction of any bank charges)

8 Contact Details

For any enquiries related to the training please contact Ms. Shereen Mahmood, at Sysprove Consulting on:

Email shereen@sysprove.com or Mobile: +973 3963 0392, +966 56 329 8240

9 Benefits of SABSA®

Feature	Advantage	Benefits							
		Chairman & Board	CEO	CFO	COO	CRO	CIO	CISO	CTO & Architects
Business driven	Value-assured	Protects shareholder value	Protects corporate reputation	Ensures efficient return on investment	Focuses on performance management	Enables flexible fit with industry regulations	Enables a digital information-age business	Facilitates alignment of security strategy with business goals	Leverages the full power of information technology
Risk focused	Prioritised and proportional responses	Optimises shareholder risk and aligns with risk appetite	Meets corporate governance requirements	Improves predictability and consistency	Enables process improvement	Supports enterprise risk management	Identifies information exploitation opportunities	Facilitates prioritisation of security and risk control solutions	Manages Information system risk
Comprehensive	Scalable scope	Addresses all shareholder concerns	Meets enterprise wide requirements	Supports scalable, granular budgeting	Provides end-to-end process coverage	Enables a fully integrated risk control strategy	Sustains through-life information architecture	Ensures all business concerns regarding security and control are addressed	Applies at any level of project size or complexity
Modular	Apply for ease of implementation and management	Enables flexibility to meet dynamic market and economic conditions	Enables fast time to market with business solutions	Facilitates effective management of both development and operational costs	Integrates with legacy environments	Enables incrementally increasing maturity	Enables technology neutral information management strategies	Enables a project focused approach to security and control development	Provides a holistic architectural approach

Feature	Advantage	Benefits							
		Chairman & Board	CEO	CFO	COO	CRO	CIO	CISO	CTO & Architects
Open Source (protected by UK Government-approved Institute)	Free use, open source, global standard	Guarantees 'escrow' and perpetuity of return on investment	Provides assurance through industry standard	Eliminates expensive on-going licence fees	Simplifies recruitment and training	Provides global acceptability for auditors and regulatory supervisors	Provides a futureproof strategic framework for information security and assurance management	Provides a sustainable framework for integration of other security standards	Avoids vendor dependence and lock-in
Auditable	Demonstrates compliance to relevant authorities	Demonstrates compliance to regulators and external auditors	Ensures a smooth and successful external and regulatory audit process	Minimises costs of management time dealing with audit processes	Minimises adverse effect of audits on performance targets	Ensures that compliance risk is effectively managed	Facilitates smooth and successful internal audits of information systems and processes	Supports security and risk review processes	Improves relationship and interactions with auditors and security reviewers
Transparent	Two-way traceability	Supports market transparency and disclosure	Provides a clear view of where expenditure is made and what value is returned	Enables full audit ability for effectiveness of expenditure	Measures efficiency and effectiveness of processes and resource deployment	Demonstrates 'current state' and 'desired state' of compliance levels	Encourages fully integrated people - process - technology solutions	Provides traceability of implementation of business-aligned security requirements	Verifies justification and completeness of technical solutions