SABSA® FOUNDATION

DURATION: 5 DAYS

CYBER SECURITY

SABSA® is the world's leading open security architecture framework and methodology. SABSA is a top-to-bottom framework and methodology to conceive, conceptualise, design, implement and manage security in a business-driven model.

The term 'business-driven' is the key to SABSA's power, and its acceptance. SABSA is all about empowering the organisation to do business as it needs and wants to do, while ensuring that it is secured and fully enabled. SABSA is an open and inclusive standard that readily integrates with other frameworks and tools such as ITIL, 17799/27000 series, COBIT and the like. It can be used as a compliance and governance framework for complex sets of standards.

SABSA is used commonly as the security parallel and tool set for organisations using the world's leading IT Architecture Framework – Zachman.

SABSA ROADMAP

The SABSA Certification Program is structured into three areas – Foundation (the mandatory base for all certification), Advanced Modules (counting towards Practitioner and Masters certification), and Topical Master Classes (two-day non- exam events covering specialty areas and offering credits towards certification).

SABSA® is a registered trademark of The SABSA Institute

COURSE CONTENTS

MODULE F1: SECURITY STRATEGY & PLANNING

1. THE SABSA FRAMEWORK

- Information Security Strategy, Benefits and Objectives
- Introduction to SABSA Best Practice

2. INFORMATION SECURITY STRATEGY

- Business Requirements & How To Define Them
- Strategic Concepts & How To Apply Them

3. SABSA PRACTITIONER GUIDE

- The Strategy Programme & Architecture Delivery
- Managing The Strategic Programme

MODULE F2: SECURITY SERVICE MANAGEMENT

4. THE SABSA SECURITY MANAGEMENT FRAMEWORK

- The SABSA Security Management Framework

5. THE SABSA SECURITY POLICY AND RISK MANAGEMENT FRAMEWORK

- Security Policy Management
- Operational Risk Management

6. THE SABSA INTEGRATED ASSURANCE MANAGEMENT FRAMEWORK

- Security Organisation & Responsibilities
- Assurance of Operational Continuity
- Systems Assurance

7. SECURITY SERVICES DESIGN

- Security Services Architecture
- Security Infrastructure Services

8. SECURITY SERVICES DELIVERY & SUPPORT

- Operational Security Services
- Security Administration & Management

9. SECURITY SERVICES PERFORMANCE MEASUREMENT

- Return on Investment & Return of Value
- Security Measures & Metrics
- SABSA Architecture
- Apply SABSA Foundation level competencies to your own environment

WHO SHOULD ATTEND

This course is designed for: CIO / CISO / CRO / CIRO, IT Strategists and Planners, IT Architects, IT Development Managers and Project Leaders, Software Managers and Architects, Computer / Information Security Managers, Advisors, Consultants & Practitioners, IT Line Managers, IT Service Delivery Managers, Risk Managers, Internal and External Auditors

EXAMINATION PROCEDURE

The SABSA Foundation exam comprises 2 modules, F1 & F2. Each exam is of one-hour duration and contains 48 multiple choice questions. The SABSA Foundation Certificate is issued to candidates who pass both Foundation Level exams.

LEARNING OUTCOMES

F1 – Security Strategy and Planning

This module provides participants with a comprehensive understanding of how the SABSA framework delivers successful security strategy and architecture. Through a series of innovative presentations, case studies and workshops, you will develop the skills to use the most proven security architecture design and management processes and find out how to develop a comprehensive strategy for the creation of a security architecture that genuinely meets the needs of your organisation.

The top ten competencies developed on this course are:

- Define enterprise security architecture, its role, objectives and benefits
- Describe the SABSA model, architecture matrix, service management matrix and terminology
- Describe SABSA principles, framework, approach and lifecycle
- Use business goals and objectives to engineer information security requirements
- Create a business attributes taxonomy
- Apply key architectural defence-in-depth concepts
- Explain security engineering principles, methods and techniques
- Use an architected approach to design an integrated compliance framework
- Describe and design appropriate policy architecture
- Define security architecture value proposition, measures and metrics

F2 – Security Service Management and Design

This module leverages the strategy defined in Foundation Module One to create the roadmap to design, deliver and support a set of consistent and high-quality security services.

Covering the good practice lifecycle, participants will find out how to design, deliver and support a comprehensive security services architecture that integrates fully and seamlessly with their existing IT management and business infrastructure and practices.

The top ten competencies developed on this course are:

- Use SABSA to create an holistic framework to align and integrate standards
- Describe roles, responsibilities, decision-making and organisational structure
- Explain the integration of SABSA into a service management environment
- Define Security Services
- Describe the placement of security services within ICT Infrastructure
- Create a SABSA Trust Model
- Describe and model security associations intra-domain and inter-domain
- Explain temporal factors in security and sequence security services
- Determine an appropriate start-up approach for