W101

Architecting a Secure Digital World

An Overview

Release 1.0

A White Paper published by The SABSA Press™, an imprint of The SABSA Institute™

June 2018

Document Title: Architecting a Secure Digital World: An Overview. (A SABSA White Paper) 2018

Document Number: TSI W101

Published by The SABSA Press, (a trading name of The SABSA Institute C.I.C.) June 2018.

Comments relating to the material contained in this document may be submitted to:

The SABSA Institute C.I.C, 126 Stapley Road, Hove, BN3 7FG, UK

Registered in England and Wales, No. 08439587

Or by electronic mail to:

sabsapress@sabsa.org

Trademarks

This Document

This document is a white paper that introduces SABSA to people who are new to the topic, providing a high-level overview and describing the benefits of adopting the methodology for architecting a secure digital business.

It has been developed and approved by The SABSA Institute C.I.C. Board of Trustees.

Contents

Introducing SABSA

Business Performance is the driver for risk management

With the ever-changing environment both inside and outside organisations and the numerous driving forces these may present, organisations will continue to set performance targets to grasp the opportunities to achieve business objectives. They set these targets despite the threats, because there is the need for survival and growth.

Threats and opportunities exist at all levels in an organisation

Opportunities and threats, affecting business performance, are found on all levels and in all areas in an organisation. They exist in strategy, with regard to reputation, in operations, and in all types of processes, in physical and technological environments, in relation to the people and in change management programmes and projects.

Enterprise Security Architecture is the means to manage cyber risk

All organisations are now leveraging digital technology to improve their businesses. That means they have to operate in cyber space[1]. To have a more complete picture of what to do to grasp digital business opportunities, and what to do against the wide range of related threats, organisations need an Enterprise Security Architecture. This ESA defines the principles, policies, capabilities and standards to set the direction and vision of information systems aligned with and supporting the organisation's needs.

SABSA is the world-leading framework for developing Enterprise Security Architecture

And that is where the SABSA® methodology, with its layered structure, its matrices, models, processes and artefacts can help organisations and individuals to create such an Enterprise Security Architecture.

SABSA views risk as uncertainty of outcome: both opportunities and threats

SABSA offers a strategic balanced view of business risk, in line with ISO 31000[2]. Figure 1 demonstrates the balance to be struck between opportunities and threats, and how risk is merely to do with uncertainty of outcomes. In SABSA thinking, security architecture is as much to do with enabling opportunities as it is about mitigating threats.

[1] For the purposes of this paper we define cyber space as being a complex system of systems comprising the totality of digital computing and communications devices and their functionality over the entire planet. Where satellite communications are in use, this also extends into space. We also include in this system of systems the entire set of people, processes, low-technology support-systems and the environment in which any or all of this system of systems operates. This definition includes such concepts as embedded real-time systems, IoT, industrial controls systems (ICS and SCADA) and any other application of digital computing In summary, if it's related to digital computing and/or communications, it is part of cyber space.

[2] ISO 31000:2018, Risk management – Guidelines, See: https://www.iso.org/iso-31000-risk-management.html.

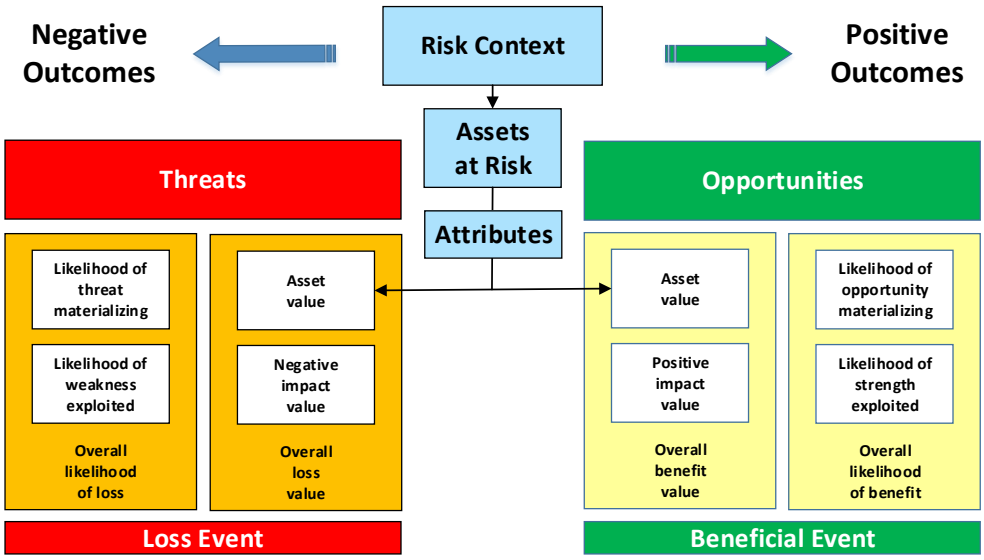

Figure 1: SABSA Balanced Risk Strategy Model

This white paper gives an overview of SABSA

This white paper presents an overview of the core components of the SABSA Methodology; Key Benefits, Features and Advantages; the SABSA Institute C.I.C. (TSI) governing the SABSA Methodology, TSI's Mission and Vision, and the SABSA Certification Roadmap.

Challenges of the Digital Economy

The modern world economy has become digital in its nature

The world economy is turning digital. That is, the spread of digital technology is changing the way that business is done in almost every industry sector and every aspect of government and the delivery of citizen services.

Digital disruption is fundamentally changing many industries

The term 'digital disruption' has been coined to express the magnitude of the changes that are being experienced. In some industries the disruptive transformation to digital products and services is almost complete. Examples of these disrupted industries include: music and entertainment, printing and publishing, photography, banking and to large extent, retailing.

Digital disruption is the driving force for modernisation

Whilst the phrase 'digital disruption' might sound threatening, it is a completely neutral concept. It provides the opportunity for organisations to modernise their business models by leveraging the power of digital technology, and as such is a driving force for business improvement.

Business models and business architecture are being renewed

The impact of this disruption is that business processes are completely different from those that we knew in the pre-digital age. In many cases product and service development, delivery, consumption and support are changed from existing in a physical world to being carried out in a virtual one. The entire business model and business architecture is new. Even where manual labour is used intensively, the purpose is to maintain employment levels, but the jobs are being de-skilled to fit around the new automation.

Cyber space offers both opportunities and threats to business

Cyber space offers many business opportunities for improved products and services and improved global reach to markets. Businesses need to exploit those opportunities. However, cyber space is also known to harbour agents of a hostile nature, and the need for effective cyber security is of paramount importance in today's business world.

The risks are different and have become an issue for senior management

The operational risks in digital business are new and different, mostly now focused on new opportunities and the potentially hostile nature of cyberspace and the services of the Internet. Cyber security has become an issue for every senior management team. It is no longer considered just a technologist's domain.

Creating a Competitive Edge

Digital disruption is a competitive issue

Digital disruption is the change that occurs when new digital technologies and business models affect the value proposition of existing goods and services. There will be winners and losers, with some incumbents finding themselves overtaken and displaced. McKinsey & Co[3], suggest a progression though four stages:

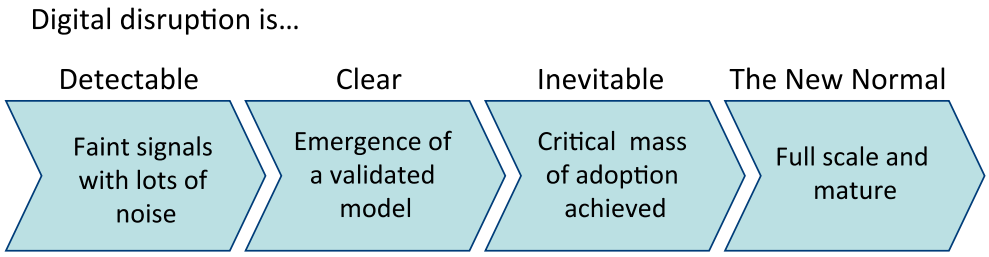

Figure 2: The McKinsey & Co Stages of a Digital Disruption Process

Security is needed to enable new opportunities

Incumbent players in an industry that is undergoing this disruptive transformation need to act quickly if they are not to be left behind by new entrants. It is therefore essential that they address the security issues of cyber space and the deployment of digital infrastructure, services and products. Otherwise they will miss the opportunity.

Security Architecture has become a critical success factor

Without adequate enterprise security architecture they will be unable to meet the challenges and will lose any competitive edge they may have previously had. New agile players will take their place as market leaders in this new digital world. Good security architecture has become a critical success factor in digital business[4]. Adopting SABSA will help those companies to achieve their business goals.

[3] Source: http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/an-incumbents-guide-to-digital-disruption

[4] For example see: https://www.ibm.com/blogs/systems/architecting-for-disruption-a-digital-change-manifesto/

Increasing Value in a Digital Business

All organisations have a 'value proposition'

Every organisation has a goal to create and protect 'value'. For companies that are motivated by profit and shareholder dividends this value is in the form of revenue, earnings, and financial capital value. For others, such as governments and their various agencies, including education services and health care services, the value is expressed in terms of the quality of the services they can deliver to their citizen customers.

SABSA begins by analysing the Value Chain

An enterprise creates value through a series of activities or processes that make up a high-level meta-process, known as the Value Chain. In order to deliver security architecture and security solutions that add true value to the enterprise, SABSA begins its analysis of the business with this value chain.

SABSA traces all security requirements to the their value contribution

Everything in SABSA security architecture is traceable to the value chain. All business requirements for security and risk management can be derived from that analysis. If a security solution or component does not contribute to the creation or protection of business value, why would you want it?

Security should add value, not merely increase costs

Using SABSA as the methodology for creating your security architecture ensures that you are increasing the value proposition of your digital business and not just adding unnecessary costs.

Securing Cyberspace

Cyberspace harbours hostile elements

It is well known that cyber space is a dangerous environment, populated with hostile foreign governments agencies, organised crime gangs, and digital vandals.

Cyberspace is a complex system of systems

Because cyber space is a complex system of systems, of almost infinite complexity, it is not possible to apply simple security solutions and be safe from these various threat agents and their exploits.

SABSA simplifies complexity by applying architectural principles

The way to simplify complexity is through the application of architectural principles to break down the complex structures into simpler building blocks that can be analysed for security requirements. Solutions are then designed to meet those requirements. The pieces then have to be assembled into a holistic framework that provides end-to-end security of all business processes. This is what SABSA does.

What is SABSA?

SABSA is world leading

SABSA is the world's leading free-use Enterprise Security Architecture Framework and Methodology.

SABSA has global market penetration and adoption

Used by Security and Enterprise Architects in more than 60 countries, it delivers a holistic and integrated approach for demonstrably aligning Security with the Business at any level and through-life.

SABSA is business driven and risk-balanced

As a true Enterprise Framework, it enables Architects to define the Business-Driven and Risk-Balanced strategy for Security, the roadmap of programmes and

projects for migrating from current-state to the strategic target-state, and the Security Management Programme to support the entire security lifecycle.

The SABSA Architecture Model

SABSA uses a layered architecture model

SABSA uses a six-layered architecture model, shown on the front face of the cuboid structure in Figure 3. The diagram is the SABSA meta-model, meaning model of models. Other SABSA models are shown as back-planes to the front face. It is beyond the scope of this paper to describe all of these models in detail. More information on these models is available at www.sabsa.org.

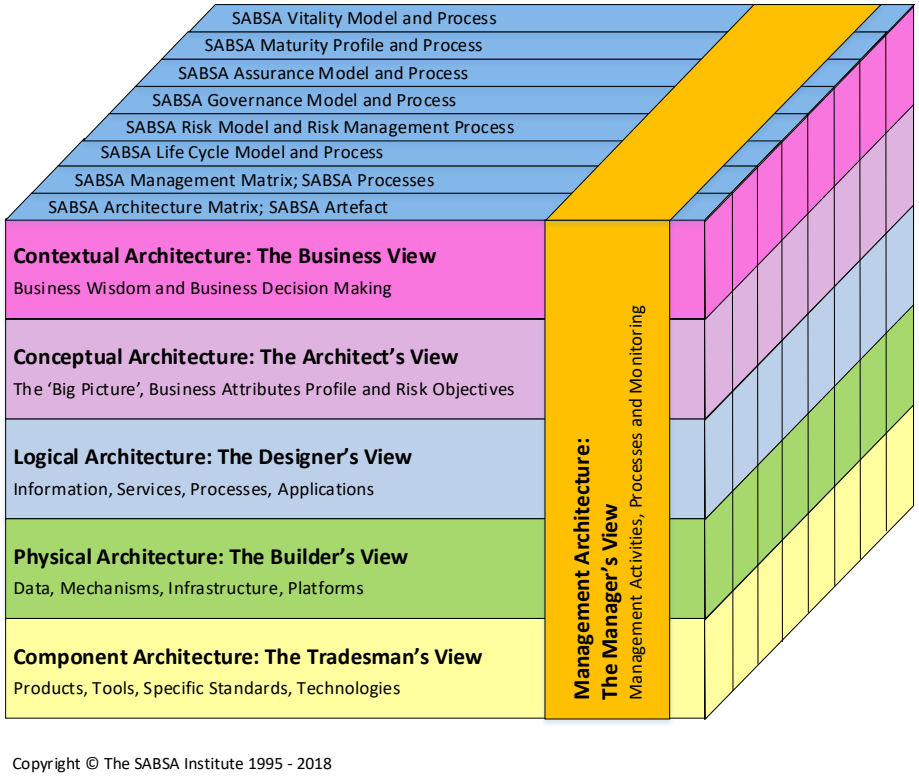

Figure 3: The SABSA Meta-Model (Model of Models)

SABSA architecture layers are mapped to stakeholder views

The layers of the SABSA Architecture Model represent the views of different stakeholders who operate at different levels within the organisation. The viewpoints and views are summarised here:

- **The Business View**: Also known as the Contextual Security Architecture (or simply Contextual Architecture) because it is concerned with the business context.

  This is the view seen from the viewpoint of the business owner or executive business manager. These are the people with the business wisdom and experience for directing the business, determining business strategy and making business decisions at the highest level of significance.

Many of these people are entrepreneurs with an appetite for taking business risks in order to create more business value. They determine the type of business in which the enterprise will engage, its markets, its products and services and its goals and objectives. Ultimately business risk-taking is the responsibility of this group of people. Without input from this group of stakeholders it is doubtful that security architecture could adequately serve the needs of the business.

- **The Architect's Vision:** An architect is a creative person with a grand vision. Architects thrive on meeting challenging and complex business requirements. They create impressionistic visions and high-level descriptions. The pictures are painted with broad brushes and sweeping strokes. They prepare the way for more detailed work later on, when other people with different types of expertise and skill will fill in the gaps with fine brush strokes.

  The architect's view is the overall *concept* by which the business requirements of the enterprise may be met. Thus, this layer of the SABSA Model is referred to as the Conceptual Security Architecture (or simply Conceptual Architecture). It defines principles and fundamental concepts that guide the selection and organisation of the logical and physical elements at the lower layers of abstraction.

- **The Designer's View**: Also known as the Logical Security Architecture (or simply Logical Architecture) because it is concerned with the logical elements of architecture such as information, services, processes or application functions. These are things that do not imply physicality. They are to do with a virtual view of the world.

  The designer takes over from the architect. The designer has to interpret the architect's conceptual vision and turn it into a logical structure that can be engineered to create a real system. This design process is often called systems engineering. This view models the business as a system, with system components that are themselves sub-systems. It shows the major architectural security elements in terms of logical security services, and describes the logical flow of control and the relationships between these logical elements.

  The architect is an artist and visionary, but the designer is an engineer.

- **The Builder's / Constructor's View**: The designer hands over the development process to the builder or constructor. The builder is someone who can take the logical descriptions and drawings and turn these into a technology model that can be used to construct the system. The builder's role is to choose and assemble the physical elements that will make the logical design come to life as a real construction. This view is therefore also referred to as the Physical Security architecture (or simply Physical Architecture).

- **The Technician's View**: The builder assembles and installs a series of products from specialist vendors, and employs a team of technicians with the

integration skills to configure and join these products together during an implementation of the design.

Each of the installers and integrators has specialist technical knowledge and skills of the various components to be assembled. Some are hardware-related, some are software-related, and some are service oriented, working with interface specifications and standards. This layer of the architectural model is also called the Component Security Architecture (or simply the Component Architecture).

- **The Managers' View**: When the system construction is finished, those who architected, designed and built it move out, but someone has to run the system during its lifetime. Such a person is often called the facilities manager, service manager, or operations manager. Security management is a sub-task within this overall role.

  The job of the manager is to deal with the operation of the system and its various services, maintaining it in good working order, and monitoring how well it is performing in meeting the requirements and reporting this to senior management. The framework for doing this is called the Management Architecture.

  The Management Architecture is relevant across all the other architecture layers and is shown in Figure 3 as cutting vertically through those other layers. It also has a Life-Cycle View (visible as a backplane in Figure 3) shown in Figure 4.

  The Strategy & Planning phase maps to the Contextual and Conceptual Architecture layers; the Design phase maps to the Logical, Physical and Component layers; and the Implement and Manage & Measure phases map to the Management Architecture itself.

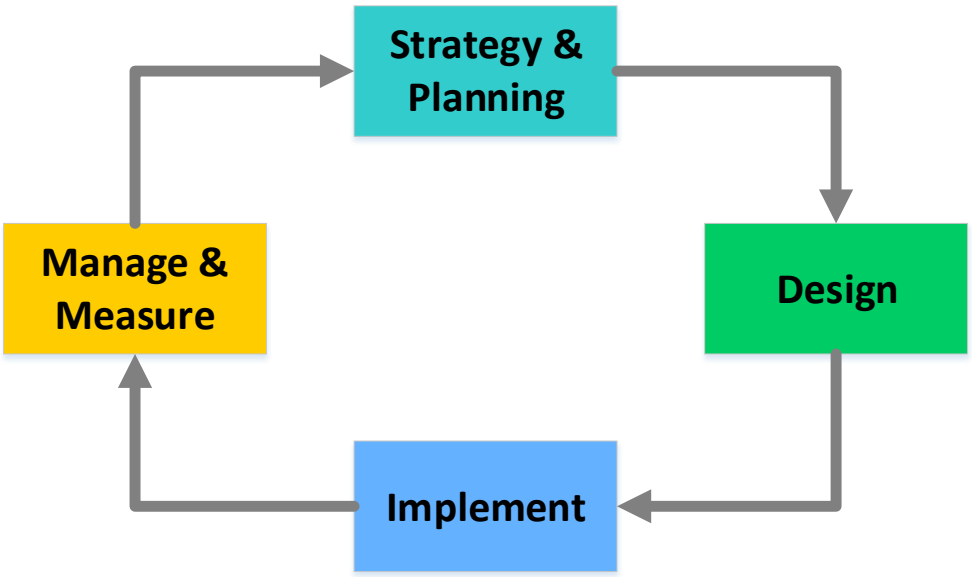

Figure 4: The SABSA Life Cycle

There are two more stakeholder pervasive views

There are two more viewpoints not shown in the architecture layering. These views are pervasive across the entire enterprise security architecture and do not fit into a single layer:

- **The Governor's View**: The governors are the owners and senior management. SABSA has a governance model that is an overlay of the SABSA Lifecycle and visible as a backplane in Figure 3. Figure 5 shows this model in greater detail. In any given business domain there are operational staff carrying out the day-to-day work and a senior manager overseeing, directing and governing them. The governor sets performance targets and the staff report back on the actual performance achieved. SABSA is highly focused on performance management. Notice that all the verbs in the various boxes of the governance framework are behavioural – they are action verbs shown in italics in the diagram.

SABSA Governance Model

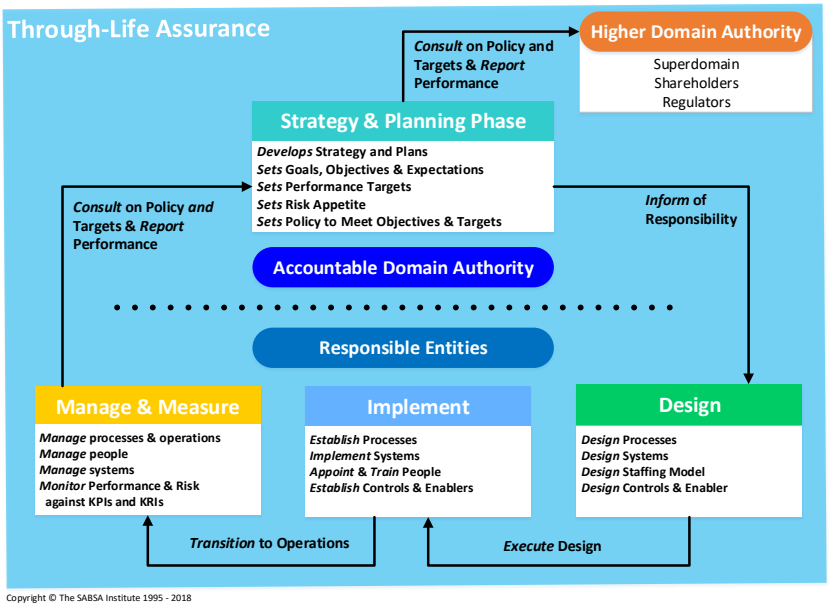

Figure 5: The SABSA Governance Model

- **The Inspector's View**: SABSA also incorporates an Assurance Framework. This can be seen as one of the backplanes of the SABSA Meta-Model in Figure 3. An inspector is someone such as an auditor or a regulatory supervisor who takes an independent view of the performance of the business against targets and reports to the governors.

  The Through-Life Assurance process is also shown as a backplane of the SABSA Governance Model in Figure 5.

The SABSA Matrices

The SABSA Matrices provide a detailed analysis of each architectural layer

The layered views of the SABSA Architecture Model are further analysed in detail in two table structures known as the SABSA Matrices. The analysis applied is to pose six questions against each layer and to use these questions to explore the detail of what is to be done in that layer. The questions are: What? (Assets); Why? (Motivation); How? (Process); Who? (People); Where? (Location); and When? (Time).

The SABSA Architecture Matrix™ is presented in Figure 6, shows how these six analytical questions are used to define the range of architectural artefacts that can be produced using SABSA.[5] Figure 7 shows the SABSA Management Matrix™ in which the analysis is applied to show the range of management activities and processes that will be needed to make the architecture work operationally.

[5] The SABSA Architecture Matrix and SABSA Management Matrix presented here are the updated, 2018 versions. For an analysis of changes since the 2009 version of the matrices, see TSI R101 SABSA Matrices 2018, Release Notes: Analysis of Changes in 2018. The SABSA Institute, May 2018.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Goals & Decisions	Business Risk	Business Meta-Processes	Business Governance	Business Geography	Business Time Dependence
	Business Value; Taxonomy of Business Assets, including Goals & Objectives , Success Factors, Targets	Opportunities & Threats Inventory	Business Value Chain; Business Capabilities	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of Business Goals and Value Creation
CONCEPTUAL ARCHITECTURE	Business Value & Knowledge Strategy	Risk Management Strategy & Objectives	Strategies for Process Assurance	Security & Risk Governance; Trust Framework	Domain Framework	Time Management Framework
	Business Attributes Taxonomy & Profile (with integrated performance targets)	Enablement & Control Objectives; Policy Architecture; Risk Categories; Risk Management Strategies; Risk Architecture; Risk Modelling Framework; Assurance Framework.	Inventory of all Operational Processes (IT, industrial, & manual); Process Mapping Framework; Architectural Strategies for IT used in process support.	Owners, Custodians and Users; Service Providers & Customers; Trust Modelling Framework	Security Domain Concepts & Framework	Through-Life Risk Management Framework; Attribute Performance Targets
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Trust Relationships	Domain Maps	Calendar & Timetable
	Inventory of Information Assets; Information Model of the Business	Risk Models; Domain Policies; Assurance Criteria (populated Assurance Framework).	Information Flows; Functional Transformations; Service Oriented Architecture; Services Catalogue; Application Functionality and Services	Domain Authorities; Entity Schema; Privilege Profiles; Trust Relationship Models	Domain Definitions; Inter-domain Associations & Interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	Infrastructure	Processing Schedule
	Data Dictionary & Data Storage Devices Inventory	Risk Management Rules & Procedures; Risk Metadata	Working Procedures; Application Software; Middleware; Systems; Security Mechanisms; Process Control Points	User Interface to Business Systems; Identity & Access Control Systems	Workspaces; Host Platforms, Layout of Devices & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	Component Assets	Risk Management Components & Standards	Process Components & Standards	Human Entities: Components & Standards	Locator Components & Standards	Step Timing & Sequencing Components and Standards
	Products and Tools, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery; Application Products	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators; Component Configuration	Time Schedules; Clocks, Timers & Interrupts
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	Assurance of Operational Excellence & Continuity	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Management & Support of Enterprise-wide and Extended Enterprise Relationships	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Figure 6: The SABSA Architecture Matrix

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	Assurance of Operational Excellence & Continuity	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Management & Support of Enterprise-wide and Extended Enterprise Relationships	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable
	The row above is a repeat of Layer 6 of the main SABSA Matrix. The five rows below are an exploded overlay of how this Layer 6 relates to each of these other Layers					
CONTEXTUAL ARCHITECTURE	Business Driver Development	Business Risk Assessment	Capability Management	Relationship Management	Supply Chain Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Processes and Capabilities for Providing Value to Stakeholders	Managing Suppliers, Service Providers, Customers; Business Partners & Employees. Contract Management	Demand & Supply Management (upstream and downstream); Deployment & Consumption	Defining Business-Driven Performance Targets
CONCEPTUAL ARCHITECTURE	Proxy Asset Development	Developing Risk Objectives	Delivery Planning	Role Management	Business Portfolio Management	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Maintaining Risk Modelling Framework; Risk Analysis on Business Attributes Profile	SLA Planning; BCP; Financial Planning; Transition Planning. Planning and Maintaining the Inventory of Processes and Services Catalogue	Maintaining Trust Modelling Framework; Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Business Footprint: Points of Supply and Access	Managing Performance Criteria and Targets; Abstracting Attribute Performance Targets
LOGICAL ARCHITECTURE	Logical Asset Management	Policy Management	Delivery Management	Enterprise-wide User Management	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management	Risk Modelling; Management of Policy Development & Maintenance. Policy Publication & Compliance Management	SLA Management; Supply Chain Management; BCM; Financial Management; Transition Management	Trust Modelling; Identity & Access Management; Management of User Privileges, Account Administration & Provisioning	Configuration (CMDB) Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
PHYSICAL ARCHITECTURE	Physical Asset Management	Risk Data Management	Operations Management	User Support	Resources Management	Performance Data Collection
	Change Management; Platform & Data Storage Management	Risk Procedure Management; Risk Metadata Management	Job, Incident, Event, and Disaster Recovery Management	Service Desk, Problem, and Request Management	Physical & Environmental Security Management; Real Estate and Facilities Management	Business Systems Monitoring Procedure Management
COMPONENT ARCHITECTURE	Component Management	Risk Management Components	Component Deployment	Personnel Component Management	Component Environment Management	Monitoring Components
	Product & Component Standards Management	Risk Analysis, Monitoring & Reporting Components, Systems and Standards Management	Product & Component Selection, Procurement. Project and Standards Management	Recruitment, Disciplinary, Training & Awareness Delivery. Component and Standards Management	Physical and Environmental Security Component and Standards Management	Analysis, Monitoring & Reporting Component and Standards Management

Figure 7: The SABSA Management Matrix

Why is SABSA the Security Architecture Method-of-Choice?

SABSA is a proven framework of choice

SABSA is the global pre-eminent method of choice for delivering Security end-to-end and top-to-bottom of the Enterprise with proven techniques that:

- Enable the change of security landscape from a Business-inhibiting 'control' culture to a Business-driven Value Creation and Enablement culture;
- Focus Security on benefits realisation and risk and resource optimisation;
- Use a method fully compatible and seamlessly aligned with Enterprise Goals, Methods and Principles at every level of the organisation;
- Can align and seamlessly integrate Security Principles to communicate and prove that Security is working to the same business objectives as overall Enterprise Governance, Risk & Compliance functions and that they collectively are driven by and focused on meeting Business Stakeholder needs;
- Leverage not just the theoretical models, but also the techniques, mechanisms, tools and taxonomies to execute and operationalise Security from a Business perspective;
- Can extend the application of the principles beyond Security for IT on a truly Enterprise Risk and Enablement basis;
- Can demonstrate in measurable terms the contribution of Security to the Organisation at all levels and in all business domains;
- Embrace and embed the principles of a true Enterprise Framework, providing a holistic approach, creating positions of security strength and business enablement, and integrating and aligning Security end-to-end and through-life;
- Realise opportunities to integrate Security with any combination of approaches including Enterprise Architecture, Policy, Quality, Governance, Risk, Compliance, Service Management, Performance Management, Business Continuity, Business Process Engineering, Project Management and Physical Security;
- Improve security communication and understanding amongst all internal and external stakeholders due to the common and sustainable globally accepted framework and language for relating Security to over-arching business goals;
- Create the capability to derive and distribute Security risk appetite from Business objectives and to aggregate security performance into Business terms;
- Embed into organisational culture a logical and systematic method by which Security and Risk Management supports Enterprise Goals
- Ensure Enterprise Security Architecture decisions are informed and driven by the Business Goals and provides traceability and assurance of Architectural artefacts and Business Requirements;

- Meet the need to separate Security Governance from Security Management and executes traceability methods to achieve clarity of Security risk ownership and accountability.

Delivering an Integrated Approach

SABSA provides a holistic approach

The principles of any good Enterprise Framework include the enablement of a holistic approach. To provide true business value to the organisation, any model or framework claiming to be Enterprise-wide must contain the models, tools and techniques to align with, integrate with, and incorporate all other approaches, models and frameworks utilised by the organisation, whatever they are and whatever they may become.

SABSA is a superior approach because it serves the business

If it cannot do so in a demonstrable, transparent fashion it cannot be operationalised or deployed effectively on an Enterprise basis: it fails to meet the needs of Enterprise stakeholders to provide business value and manage risk; and it fails to embrace the organisational culture end-to-end leading to resistance and lack of adoption. In short - it fails to be an Enterprise Framework and it fails to serve the Business. That is why SABSA is so superior in its approach, because it does all the things that avoid such failures.

SABSA aligns with enterprise-wide and through life requirements

SABSA was authored as an Engineering-style holistic framework and fully-embraces the principles and (perhaps more importantly) provides the techniques to ensure that Information Security is fully aligned and integrated on an Enterprise-wide and through-life basis.

Meeting Business Stakeholder Needs

SABSA aligns with stakeholder needs

The SABSA Enterprise Security Architecture Framework creates a consistent set of principles, policies, capabilities and standards that sets the direction and vision for the development and operation of the organisation's business information security to ensure alignment with and support for the business needs. SABSA-developed security architectures are specifically driven by business needs for managing Enterprise Risk and enabling Enterprise Goals and Objectives to meet the needs of stakeholders throughout the enterprise, including risk owners and impacted internal and external domains.

Fit for purpose

The Architectural framework provides predictability, consistency, efficiency, effectiveness and vitality of fit-for-purpose risk treatments traceable to business appetites.

Supporting risk appetite

The SABSA model provides mechanisms for supporting Enterprise GRC needs through a logical and systematic method with demonstrable Business Risk Appetite Distribution and Performance Aggregation.

End-to-End & Through-Life Coverage

Traceability, ownership and accountability

SABSA's traceability methods add support to achieving clarity of risk ownership & accountability ensuring that the Enterprise risk structures are fully reflected in Architectural approaches and solutions through-life and end-to-end of business processes.

Through-life risk management

As a true Enterprise Framework for Security, the 'Through-life' nature of SABSA models and techniques ensure alignment and compliance between the Architecture and Enterprise Risk structures at every phase:

- Strategic Risk Management is embedded and reflected in the Architectural strategy, planning and concepts;
- Programme, Project and Change Risk Management is embedded and reflected in the progressive road-map for establishing Architectural solutions and at every step of migration from 'current-state architecture' to 'target-state architecture';
- Operational Risk Management is embedded and reflected in the SABSA Management structures that ensure Architecture solutions are continuously managed, monitored and measured traceably to the risk appetites of Business Stakeholders.
- This approach ensures that an Enterprise has a clearly articulated, Business-driven, risk and enablement focused understanding of:
  - 'Current-state' risk exposures and enablement opportunities;
  - 'Target-state' appetite-driven risk exposures and enablement opportunities;
  - The Enterprise-wide strategic roadmap to migrate from current-state to target-state.

A Single Integrated & Aligned Framework

Practical capabilities

Security, like risk, is ultimately a property of real business assets, objectives, processes and infrastructure. For Security Architecture to succeed it must therefore create and operate the capabilities, policies, standards and principles required to definitively support those of the business that it serves.

Practical modelling tools

For an Enterprise-wide framework to be successful it must be accompanied by a methodology – not just the conceptual theory but the models, tools and techniques that operationalise the alignment, and integration and incorporation of all other approaches, models and frameworks utilised by the organisation.

Prioritisation of needs

SABSA provides organisations not just with the descriptive 'What does security need to do?' and 'Why do we need to do it?' but the prescriptive collateral and work product for 'How do we do what is needed most?'

Enabling a Holistic Approach

SABSA embeds a holistic approach

The SABSA Framework for Enterprise Security Architecture fully embeds the principles of a holistic approach. Indeed, since it was established in 1995 its ability to seamlessly and holistically align and integrate security strategies, processes, solutions and cultures to Business Objectives in a truly Enterprise fashion has led to it being the reference approach of choice for many independent organisations and framework developers.

Living in the real world

One of the drivers for SABSA's worldwide adoption is that it provides the means for Security to bring about reality from the theoretical models and frameworks such that the risk appetite of the business stakeholders can be articulated. The performance of the mitigations and enablers can be monitored and reported in terms that the real owners of business assets, objectives, processes and infrastructure understand.

All-of-business: not just IT

The single integrated business-driven framework can be applied holistically from an 'all-of-business' perspective (not just an IT perspective) to ensure that security aligns and integrates seamlessly with any Enterprise function or dimension, including:

- Business & IT Architecture
- Information Assurance
- Policy Framework
- Performance Management
- Service Management
- Risk Management
- Governance & Compliance

Separating Governance from Execution

SABSA Governance model

SABSA and the SABSA Governance Model (Figure 5) are widely referenced as a method for defining Governance taxonomies and operationalising the principles, policies and communication frameworks that drive processes, organisational structures, culture, ethics and behaviours.

Supporting business value creation

SABSA provides the techniques and models to define the roles, activities and relationships required to enable and scope Governance from a security perspective to achieve benefits-realisation and risk-optimisation. It delivers 'Value Creation' structures from a Security perspective that are derived from the Value Chain of the Business. It also provides techniques to enhance the traditional roles and responsibilities modelling approaches to:

- Model security roles and responsibilities on an Enterprise-wide basis;
- Define and articulate security ownership in business terms;
- Clearly delineate between ownership, liability, accountability, and responsibility;
- Enable implementation of communication structures that traceably:
  - Delegate and translate business-level risk appetites and performance targets to adoptable, consumable and executable execution;
  - Aggregate risk and opportunity performance of security and IT related operations to demonstrate contribution to value-creation and business targets.

Who Uses SABSA?

Global market penetration of SABSA

Architects from more than 60 countries and every imaginable sector from Nuclear Power to Charities have had their SABSA competency assessed and certified by The SABSA Institute at Foundation (SCF), Practitioner (SCP) or Master (SCM) level, although there are many others who leverage SABSA as a free-use method for demonstrating business benefit but who have not yet registered their use.

Referenced by other leading certification bodies

Independent professional bodies including The Open Group, ISACA, The IT Governance Institute and ISC^2 either recommend the SABSA Approach or reference it within their guidance and method documents or training and certification programmes. Security Interest Groups and Associations worldwide also regularly reference SABSA.

Popular in government and defence

Government and Defence organisations in multiple countries have opted to make SABSA a reference model of choice, a *de facto* or formal standard. Many are researching how SABSA can be adapted and integrated into their existing risk management security frameworks to enhance their existing investments in methods, processes and models.

Popular in financial services

Numerous influential organisations in the Finance sector worldwide now not only embed the SABSA approach, but also mandate it into functions beyond security, and financial regulators are increasingly mandating formal Enterprise Security Architecture for the Financial Sector.

A benchmark for recruitment of security architects

Employers throughout the world now regularly require job applicants to have obtained SABSA certification to demonstrate competence and capability prior to employment in the Security and Architecture fields.

A new paradigm for tackling cyber security and cyber defence

As the world moves into the new era of digital business and cyber security, the old security methods developed in the 1980s and 1990's are running out of power to confront the threat landscape and enable the wide range of new business opportunities. Cyberspace is a complex, almost infinite, eco-system that requires sound, solid systems engineering approaches and a holistic view of the challenges. The world needs to adopt new thinking and new tools to meet these challenges. This is what the SABSA framework delivers.

Developing Economic Advantage

SABSA underpins the development of economic advantage in all regions of the world

SABSA is a world-leading approach to the development and deployment of solutions to manage information risk, assurance, and security in a globally accelerating digital business environment. All centres of economic power need to position themselves at the heart of such developments to leverage the best economic advantage for their country and region and to support investment in the digital economy. SABSA provides advanced thought leadership in risk management and the economic benefits it can bring.

Promoting Social Responsibility

SABSA makes the world a better place to live

The SABSA community comprises individuals, corporations and universities who use SABSA to advance their professional aims, ambitions and objectives in the digital business world. In doing this it enhances both their personal and professional lives, improves their sense of self-worth and makes them feel good about their contributions to a better society

Leadership in Innovation

SABSA promotes innovation leadership

In this age of digital business, those who lead innovation gain the most social and economic benefit. This applies at every level, including regional governments (such as the EU), national governments, local governments, and all sizes and types of private and public enterprise.

Social and economic advantage through innovation

SABSA provides the business risk-driven framework that will enable all these organisations to manage their digital business risks to maximise both social and economic advantage through innovation.

Getting the right Skills

A worldwide education, training and certification programme supports SABSA

In order to meet the challenges we have set out above, an organisation needs to be able to recruit and train a team of security architects who have the requisite, fit-for-purpose professional skills. The SABSA Institute offers a worldwide programme of education, training and certification in security architecture theory and practice. No other similar programme exists at the present time.

Skills Development

The SABSA Institute leads the way in developing skills for the new digital age

New skills, competencies, and tools are essential to both national and international economic success in the digital age. SABSA is itself a tool-kit and the SABSA Education Programme develops professional competencies to support its deployment. Those who adopt SABSA and participate in The SABSA Institute are placing themselves in a leadership position for skills and competencies development with regard to managing business risks in a digital age.

Value for Employers

SABSA professional certification programme

The SABSA Institute provides an international SABSA Training and Certification programme. This leads to certification of individual security architects at three levels: Foundation (SCF), Practitioner (SCP) and Master (SCM).

Providing industry with qualified security architects

As interest in cyber security develops, employers are increasingly seeking highly qualified security architects to address the issues and to build enterprise and solution security architectures that are fit for purpose.

Supporting recruitment of security architects

To recruit the right set of skills and competencies there is a need for qualified, certified people to meet this demand. The SABSA training and certification programme meets this need and provides business value to employers, who can use these qualifications as a benchmark for suitability of the candidate for the job.

Value for Employees

Career enhancement for security architects

As employers develop greater appetite for recruiting qualified, certified security architects, the SABSA training and certification programme provides a means for individual security architects to increase their market value as potential employees, and thus increase their employability.

SABSA's unique certification offering

The SABSA programme is the only enterprise security architecture scheme to offer the full range of qualification levels (Foundation / Practitioner / Master) that enables a security architect to develop a full, career-aligned series of certifications.

SABSA Education and Training

A comprehensive education, training and certification programme

Awareness and knowledge of SABSA for competency development is provided through certification course programmes offered and facilitated through Accredited Education Partners (AEP's).

A competency framework based on Bloom's Taxonomy

The courses are created according to a professional competency framework derived from Bloom's Taxonomy of Cognitive Levels. The levels cover basic knowledge of theory and concepts to advanced levels of demonstrable application of competence.

Courses offered at two levels

SABSA certification course programmes are currently offered at two levels, Foundation and Advanced.

SABSA Foundation Module

SABSA Foundation Module for beginners

The SABSA Foundation Module is The SABSA Institute's official starting point for developing security architecture competencies. It is 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 Advanced Modules

SABSA Advanced for existing practitioners

The SABSA Advanced Module programme is oriented toward further development and demonstration of competence in applying SABSA that benefit both the organisation and an individual.

Extending professional competence

The Advanced Module programme aims to provide confidence and assurance that a successful candidate has demonstrated in practical terms the real competence and ability to:

- Analyse and assess business problems and business-driven requirements;
- Apply, modify and adapt the SABSA method to satisfy the unique requirements of their organisation, culture and sector contexts;
- Design and create the work-products required to establish and operationalise SABSA for security solution strategies unique to an organizations environment;

- Assess, evaluate and test concepts and theories by populating the work-products designed for real-world applications;

A choice of specialisms

The SABSA advanced modules cover dimensions of Risk and Governance as well as advanced SABSA Architecture and Design. Other advanced modules will be offered in the future according to demand from the SABSA Community.

Certification Levels

Progressive certification levels

Passing the SABSA Foundation certificate enables the candidate to adopt the designation of SABSA Chartered Architect (SCF). A person who is Foundation certified and has passed one advanced module can adopt the designation of SABSA Chartered Practitioner (SCP). By passing a second advanced module and by submitting a successful thesis on original SABSA work the candidate may become a SABSA Chartered Master (SCM).

SABSA Institute Members

The SABSA Institute Membership Scheme

Members of the SABSA Institute are key stakeholders in the SABSA Community and The SABSA Institute. The goals of our membership services are to:

- Encourage and support the lifelong personal and/or corporate development of professional members of the SABSA Community;
- Raise the level of competence and qualification of SABSA practitioners;
- Provide thought leadership to initiate, develop, evaluate and disseminate SABSA Thinking™, tools, techniques and practices;
- Offer participation in the development of new SABSA Intellectual Property.

By registering for Membership you will be able to:

- Share with and learn from others about the application of SABSA;
- Participate in discussions regarding the development of SABSA and work along on new white papers, reports, guides, project charters, standards and the development of the SABSA Intellectual Property;
- Have early access to new white papers before those are released to the public;
- Presentations from Local Chapters where those have been released for publication by the author;
- Have access to the repository we are currently building up with you and other members.

There are three types of Membership available: General Membership, Chartered Membership, and Founding Membership. For additional information on Institute membership, please visit https://www.sabsa.org/membership-benefits.

The Elevator Pitch

The table below analyses the various views that might be taken by Chief Officers in a commercial enterprise. For those who find themselves in the classic situation of having a few moments with a C-level executive and the opportunity to make a case for using SABSA as the security architecture framework of choice, these points will help to frame the content of that short conversation during the encounter, whether or not it occurs in the elevator. However, this is just an example that may or may not fit your organisation for business type and senior role definitions. If it doesn't, consider developing your own version of it, customised to your business.

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	Agility 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
Open Source (protected by UK Government-approved Institute / CIC)	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 future-proof 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

Figure 8: The C-Level Executive View of SABSA Value: Features, Advantages & Benefits

Things you can do Next

So, if you have an interest in promoting these SABSA ideas in your organisation, here's what you can do:

- Share this paper with other colleagues in your organisation (or with friends in other organisations).
- Read and learn more about SABSA in publications (papers, blogs and web articles) on the web site (see www.sabsa.org).
- Start to use SABSA as a framework for structuring your own work.
- When people admire your work tell them how you achieved the results using SABSA.
- Share your SABSA ideas with work colleagues (but try to avoid selling them 'another framework' when they already have a cupboard full of those).
- Find a senior level champion who will promote these ideas in senior management circles of the organisation.
- Learn an elevator pitch main points and use them whenever you get a chance to speak to a senior executive whose support you want to gain. The one on the previous page will give you ideas but it is only one example and will not apply to all organisations. You can make your own elevator pitch customised to your business and its senior roles.
- Attend a formal SABSA Foundation training course and become certified as a SABSA Architect.
- Attend SABSAWorld events in your region (see http://www.sabsaworld.org).
- Attend one of the COSAC Conference / SABSA World Congress events in either the Republic of Ireland or Australia (see https://www.cosac.net).
- Join The SABSA Institute as a Member and get access to member services including new SABSA publications and discussion forums.
- Encourage other colleagues to read SABSA blogs, articles and papers and attend these events.
- Encourage other colleagues to become Members of The SABSA Institute.
- Become a SABSA evangelist and spread the word.

The SABSA Institute C.I.C.

SABSA IP is available licence-free for end users

The intellectual property of SABSA is licence-free for use by all end user organisations in the development of their information security and cyber security architecture. It is owned, governed and maintained by The SABSA Institute™.

Only official SABSA training leads to certification

Official SABSA training and certification is only available through Accredited Education Partners (AEPs) of The SABSA Institute. Beware of unofficial training programmes that will not give certification.

The SABSA Institute is the professional governing body for SABSA

The SABSA Institute is the professional member and certification body for Enterprise Security Architects of all specialisms and at all career levels. It is incorporated in England and Wales as a Community Interest Company. It governs the on-going development and management of SABSA intellectual property and the associated certification and education programs worldwide. This on-going development and support guarantees the longevity of the framework and provides confidence in the SABSA Community (those who use the methodology) that it will continue to be developed and supported to meet the needs of that community.

The SABSA Institute Vision

The SABSA Institute envisions a globally connected world of the future, leveraging the power of digital technologies, enabled in the management of information risk, information assurance, and information security through the adoption of SABSA as the framework and methodology of first choice for commercial, industrial, educational, government, military, and charitable enterprises, regardless of industry sector, nationality, size, or socio-economic status, and leading to enhancements in social well-being and economic success.

Further Information

Further information on The SABSA Institute can be found at www.sabsa.org.