# Submission to NIST

## Developing a Framework to Improve Critical Infrastructure Cybersecurity

This submission is made by The SABSA Institute CIC. It proposes the adoption of SABSA as the overarching framework for improving critical national infrastructure cybersecurity.

Contact name: John Sherwood
Contact email: john.sherwood@sabsa.org
Contact address: 126 Stapley Road, Hove, East Sussex, UK, BN3 7FG
Contact phone: +44 7769 654466

## About SABSA

SABSA® is a methodology for developing risk-driven enterprise information security architectures, information risk management architectures, and information assurance architectures, and for delivering security solutions that support critical business initiatives through the deployment of ICT infrastructure and applications. These solutions encompass all aspects of operational risk management, including people, processes and technology. It is an open standard, comprising a number of frameworks, models, methods and processes, free for use by all, with no licensing required for end-user organisations that make use of the standard in developing and implementing architectures and solutions.

Originally SABSA was an acronym for Sherwood Applied Business Security Architecture, named after its founder, thought-leader and chief author, John Sherwood. It has been decided that it is no longer desirable to spell out the full acronym, since the word 'SABSA' is in popular use and for reasons of copyright and trademark protection it is legally stronger if SABSA is 'just a word'.

The first SABSA paper was published 1996. Since then SABSA has gained substantial popularity around the world and the body of knowledge has been developed and enhanced. A full-scale training and education programme was launched in 2007 on an international basis through a network of accredited education partners (AEPs) under the brand of 'The SABSA Institute'. At the present time there are AEPs in Europe, Australia/New Zealand, South East Asia, Africa and North America. More than 3,000 people have taken SABSA examinations and been awarded certified SABSA architect status at one of the certification levels available (Foundation, Practitioner or Master). These certified people span 43 different countries around the world.

SABSA is protected by copyright. However, SABSA intellectual property (IP), including SABSA publications and the content of official SABSA training courses, is available to the public. These published copyright materials include the key components of the framework. Any organisation, in its drive to improve its Security Architecture or Security Service Management processes and practices, may use the framework described in these publicly available resources, on condition that proper credit is listed and trademarks are acknowledged. The entire purpose of The SABSA Institute CIC is to own, protect and govern these intellectual property rights (IPR), to ensure that they are owned by the SABSA community for the benefit of the SABSA community, and that the IP will continue to be developed and supported in perpetuity in the hands of the community rather than relying on the individuals who have brought it to this stage of maturity. Anyone may join The SABSA Institute CIC as a member on payment of subscriptions, and the institute will seek corporate sponsorship to finance further research and development. Member and sponsors will be able to participate actively in this research and development activity. Others may also benefit by having access to SABSA materials thus developed and published.

## About The SABSA Institute CIC

The SABSA Institute is a community interest company registered in the UK under UK company law, company number 8439587.

**Vision Statement:**
The SABSA Institute envisions a global business world of the future, leveraging the power of digital technologies, enabled in the management of cyber risk, 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.

**Mission Statement:**
The mission of The SABSA Institute is to:

- Be custodians, guardians and governors of the SABSA IPR in perpetuity;
- Encourage its use by an ever growing SABSA Community comprising both individuals and corporate entities, including national governments;

- Enable governments to adopt SABSA as their framework and methodology of first choice without favouring a particular commercial interest;
- Facilitate, lead and co-ordinate the future development of the SABSA IP;
- Govern the integrity of the IP and its application throughout the SABSA Community.
- Encourage and support the lifelong personal and/or corporate development of members of the SABSA Community;
- Raise the level of competence and qualification of SABSA practitioners;
- Provide thought leadership so as to initiate, develop, evaluate and disseminate SABSA thinking, tools, techniques and practices.

## Core Values

The core values of The SABSA Institute are:

> **Benefit for Stakeholders:** We focus on meeting the emerging needs of all our stakeholders in the SABSA Community;
>
> **Inclusive Culture:** We have an inclusive culture and positive attitude towards the SABSA Community; all those with a professional or personal interest in the activities and goals of the SABSA Institute are welcome in the SABSA Community;
>
> **Collaborative Approach:** We encourage sharing and collaboration between all members of the SABSA Community for the overall benefit of all, whether or not these members are formal, informal, *de facto* or future joiners;
>
> **Global Business Enablement:** We facilitate and encourage change towards a business-enabled, risk-driven, trusted, assured and secured digital society and economy on a global basis.

## Business Objectives

The business objectives of The SABSA Institute are to:

- Grow the overall membership base and achieve a critical mass of the membership of the Institute, both individual members and corporate sponsors;
- Win support for, engagement with, and financial sponsorship for the Institute from corporate entities across all industry sectors and nations;
- Increase awareness of the Institute, and achieve recognition for its contribution to better information assurance, security and risk management practice;
- Increase the uptake of SABSA personal development and education through Institute programmes and qualifications;
- Develop relevant revenue streams to support the business operations of the Institute and for investment in further development of the SABSA IP;
- Develop the Institute's structure, systems, intellectual capital and financial strength so as to enable the organisation to fulfil its mission and to realise its vision.

## Stakeholders

We see the stakeholders as belonging to the following major groups:

### Th SABSA Community at Large

The community includes all persons and corporate organisations with a professional or personal interest in the activities and goals of The SABSA Institute.

### Individual Members of the Institute

Those individuals who choose to become registered as Members and to pay annual subscriptions.

### Chartered Members

Individual Members who have chosen to enter and pass The SABSA Institute examinations and thus become qualified at Foundation, Practitioner or Master level.

### Corporate Sponsors of the Institute

Corporate bodies from industry, commerce, education, government, military and charitable work that have a sufficient interest to invest either financial support, or human resources, or both, in the development of the SABSA IP for the benefit of the entire community, including the benefits to them.

### Corporate and Governmental Users of SABSA

Corporate bodies, especially large publicly owned companies quoted on stock exchanges and governments and their agencies whose internal governance requires them to be fair, equitable and duly diligent in the expenditure of their funds, and who cannot choose to adopt SABSA without a high level of assurance as to its provenance, longevity and freedom from commercial exploitation.

### Regulators

Initially these include the UK Secretary of State for Business, Innovation and Skills and the UK Community Interest Companies Regulator who will regulate The SABSA Institute to create the assurance referred to in the previous section.

However, many corporate users of SABSA are (and/or will in the future be) regulated firms in industries such as banking, insurance, civil aviation, energy provision, pharmaceuticals, road and rail transport, telecommunications and critical national infrastructure in general. Part of the regulation of these industries is to set requirements for risk management, including information risk management, and to supervise the implementation of solutions that are compliant with the regulations. We propose SABSA as a tool that will assist with this regulatory process, enabling regulated firms better to demonstrate their levels of compliance.

## Benefits of Adopting SABSA for Developing a Framework to Improve Critical Infrastructure Cybersecurity

**Economic Advantage**

SABSA is a world-leading approach to the development and deployment of solutions to manage cyber risk, assurance and security in a globally accelerating digital business environment. All national governments need to be able to position themselves at the heart of such developments so as to leverage the best economic advantage for the country and to support investment in its digital economy. By adopting SABSA a government will be recognizing the importance of advanced thought leadership in risk management and the economic benefits it can bring.

**Cyber Security**

There are many standards out in the world that suggest solution approaches to cyber security. The problem is that none of these really relate back in a traceable way to the business risks in the specific environment in which the organisation operates, an environment in which the threat landscape and the available solutions are constantly changing. SABSA is quite different inasmuch as it is a process-based architectural approach that does not anticipate specific threats or mitigating solutions but instead embraces all possible threat scenarios and solutions known at the time of the solution development. In allows for all other standards and approaches to be embraced and thus is completely open minded and divergent in its thinking, rather than a convergent approach that lacks flexibility and agility to deal with an ever changing cyber risk environment.

In particular SABSA has at its heart the Business Attributes Profiling method that allows requirements definition in business risk related terms and puts measurable performance indicators and measurable key risk indicators in place that can be used in scorecards and dashboards to report the on-going performance of deployed solutions against the business requirements. It is this approach that has led to close cooperation between The SABSA Institute and The Open Group in the development of Next generation TOGAF. This joint development puts SABSA Business Attributes Profiling (BAP) at the heart of the TOGAF Architecture Development Method (ADM) for requirements management – not just for security, but also for all aspects of business requirements definition. Both the Architecture Forum and the Security Forum of The Open Group embrace this approach as the leading edge of requirement management methodology. The method is broad ranging and allows all possible requirements to be addressed. In particular it emphasises the relationship between the architecture of business operational capabilities and the management of operational risk. Unless business capabilities are designed and built with downstream operational risk in mind they are unlikely to be fit for purpose in managing those risks. It is this disconnect that gives so much trouble in our current environments and one that is a major cause of some of the inadequacies of some current approaches to cyber risk management. SABSA addresses this issue more thoroughly than any other methodology currently available.

**Innovation Leadership**

In this age of digital business those who lead innovation gain the most social and economic benefit. Any national government that adopts the SABSA approach to protecting critical national infrastructure (CNI) and to managing cyber risk will have an immediate advantage over those that do not.

**Social Responsibility**

The SABSA community comprises individuals, corporations, governments and universities who use SABSA to advance their professional aims, ambitions and objectives in the digital business world. When they do 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.

**Skills Development**

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. See below for more information on the SABSA Education, Training and Certification programme.

## SABSA Education Programme

**The SABSA Body of Knowledge**

SABSA is a body of academic knowledge and an associated set of competencies for practitioners of SABSA. It comprises a methodology for developing risk-driven enterprise information security architectures, information and cyber risk management architectures, and information assurance architectures, and for delivering security solutions that support critical business initiatives through the deployment of ICT infrastructure and applications. These solutions encompass all aspects of operational risk management, including people, processes and technology. It is an open standard, comprising a number of frameworks, models, methods and processes, free for use by all, with no licensing required for end-user organizations that make use of the standard frtamework in developing and implementing architectures and solutions.

**The SABSA Community**

There exists de facto a SABSA community. This comprises people, corporate organizations, governments and educational institutions that have adopted SABSA as their method of choice for developing security architectures. They find that SABSA's business-driven approach, its risk-focus and its neutrality to all other standards and methods make SABSA a unique framework that adds huge value to their work. They have been vociferous in their demands for The SABSA Institute to be established to support the further development of the SABSA intellectual property (IP), to guarantee its integrity and longevity, and to provide a formal framework for education and certification in all things SABSA. Many of them wish to contribute by participating in a series of working groups that will focus on specific aspects of future research and development, and they see the SABSA Institute as the vehicle by which this participation and co-ordination can be achieved. The establishment of The SABSA Institute as a high-level research, development and teaching body has been in response to heavy public demand from all over the world.

**SABSA Education and Certification**

The key to the continuing successful adoption of SABSA on a global basis is the competency-based education and certification programme. The SABSA education and certification programme has accredited providers (AEPs) in ten countries (United Kingdom, Netherlands, Poland, United States, Canada, Australia, New Zealand, Singapore, Malaysia and South Africa) and receives additional applications and enquiries regularly. At the date of writing, those in progress include preliminary applications for the territories of Latin America and the whole African continent. The demand for further expansion and the appeal of SABSA to the global community is highlighted by candidate demographics. In addition to the ten countries in which SABSA AEPs currently operate live, candidates have travelled internationally to obtain SABSA education. Currently the certified SABSA community spans 43 different countries.

The role of The SABSA Institute is to provide the solid institutional foundations upon which this education and certification programme can be developed further and deployed in many more countries around the world. The Institute will launch an online SABSA training programme later this year in three languages: English, Chinese and Dutch. French, Spanish and German language versions will follow.

There are on-going discussions with The Open Group on ways in which the SABSA Education, Training and Certification programme can be integrated and aligned with a similar programme operated by The Open Group.