



## **Appendix F1-1**

SABSA White Paper

# Enterprise Security Architecture

John Sherwood, Andrew Clark &amp; David Lynas

[www.sabsa.org](http://www.sabsa.org)

## Executive Summary

SABSA® is a methodology for developing risk-driven enterprise information security and information assurance architectures and for delivering security infrastructure solutions that support critical business initiatives. 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 who make use of the standard in developing and implementing architectures and solutions<sup>1</sup>.

SABSA is unique in that it fulfils ALL of the following criteria:

- It is an open standard, comprising frameworks, models, methods and processes, free for use by all, with no licensing required for end-user organisations who make use of the standard in developing and implementing architectures and solutions;
- The SABSA framework is not related to any IT solutions supplier and is completely vendor-neutral,
- The SABSA framework is scalable, that is, it can be introduced in subsequent areas and systems and implemented incrementally,
- The SABSA framework may be used in any industry sector and in any organisation whether privately or publicly owned, including commercial, industrial, government, military or charitable organisations;
- The SABSA framework can be used for the development of architectures and solutions at any level of granularity of scope, from a project of limited scope to an entire enterprise architectural framework;
- SABSA does not replace or compete with any other information risk or information security standard – rather it provides an overarching framework that enables all other existing standards to be integrated under the single SABSA framework, enabling joined up, end-to-end architectural solutions.
- SABSA fills the gap for ‘security architecture’ and ‘security service management’ by integrating seamlessly with other standards such as TOGAF® and ITIL®.
- The SABSA framework is continually maintained and developed and up-to-date versions are published from time to time,

---

<sup>1</sup> SABSA® is a registered trademark of SABSA Limited which governs and co-ordinates the worldwide development of the SABSA Method. SABSA is protected by copyright and by definition is therefore NOT public domain. However, SABSA intellectual property, 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 reproduced. As with other leading frameworks considered to be publicly available (such as ITIL®) it is NOT true that the contents of official training courses or publications can be appropriated by anyone and everyone for reuse, reproduction or republication without the express permission of SABSA Limited. SABSA Limited owns SABSA, and copyright law protects the SABSA materials. Anyone wishing to reuse, reproduce or republish any part of a SABSA publication, should contact SABSA Limited. Permission to reproduce SABSA property is not normally withheld. All organisations should be aware that SABSA materials and methods obtained without permission, or from any source other than those listed on the official SABSA web sites as being authorised and accredited, are unauthorised and in breach of copyright law.

- Knowledge of SABSA and how to apply it can be obtained and confirmed through an education and certification programme recognised worldwide, the training materials, examinations and certificates being issued by the SABSA Institute;
- SABSA education, training and certification can be obtained through any one of the worldwide network of Accredited Education Partners (AEPs) of the SABSA Institute, by registering for and attending the SABSA Institute courses offered through those AEPs and by sitting the appropriate examinations also offered through the AEP network,
- SABSA may be incorporated into any appropriate computer software tool by a software tool vendor who wishes to offer such a tool to the open market (subject to footnote 1). However, to guarantee support from SABSA Limited in validating and accrediting such a tool, the vendor merely needs to approach SABSA Limited to arrange a commercial agreement under which such support will be offered;

Because of this uniqueness, there is no other certificate or qualification that fulfils the role of a SABSA Chartered Foundation Certificate (SCF), a SABSA Chartered Practitioner Certificate (SCP) or a SABSA Chartered Master Certificate (SCM), and no waivers are offered in respect of other qualifications;

At the heart of the SABSA methodology is the SABSA Model, a top-down approach that drives the SABSA Development Process. This process analyses the business requirements at the outset, and creates a chain of traceability through the SABSA Lifecycle phases of 'Strategy & Planning', 'Design', 'Implement' and ongoing 'Manage and Measure' to ensure that the business mandate is preserved. Framework tools created from practical experience, including the SABSA Matrix and the SABSA Business Attributes Profile, further support the whole methodology.

This white paper explores the advantages of this business-focused approach for creating security architecture. It discusses the pitfalls of a technology-centric approach, and recognises the challenges of integrating the business leadership team with the technology strategists in order to fulfil the potential of the enterprise.

The paper also discusses the SABSA methodology, explaining this approach by comparing it to the classical definition of architecture (i.e., the construction of buildings). By illustrating the contextual, conceptual, logical, physical, component and service management layers of the architectural process, a comprehensive approach unfolds that provides a roadmap for business and ICT (information and communications technology) leadership teams to follow so as to ensure that the technology foundation becomes an enabler of business performance.

## The Origins of Architecture

Architecture has its origins in the building of towns and cities, and everyone understands this sense of the word, so it makes sense to begin by examining the meaning of 'architecture' in this traditional context. Architecture is a set of rules and conventions by which we create buildings that serve the purposes for which we intend them, both functionally and aesthetically. Our concept of architecture is one that supports our needs to live, to work, to do business, to travel, to socialise and to pursue our leisure. The multiplicity and complex interaction of these various activities must be supported, and this includes the relationship between the activities themselves and their integration into a whole lifestyle. Architecture is founded upon an understanding of the needs that it must fulfil.

These needs are expressed in terms of function, aesthetics, culture, government policies and civil priorities. They take into account how we feel about ourselves and about our neighbours, and how they feel about us. In these various ways, architecture must serve all those who will experience it in any way. Architecture is also both driven and constrained by a number of specific factors. These include: the materials available within the locale that can be used for construction; the terrain, the prevailing climate; the technology; and the engineering skills of the people.

As a result, there are fundamentally three major factors that determine what architecture we will create:

- Our goals
- The environment
- Our technical capabilities

## Information Systems Architecture

The concept of 'architecture' in buildings has been adapted to areas of life other than the building of towns and cities. For example one talks about a 'naval architect' being someone that designs and supervises the construction of ships. In more recent times the term has been adopted in the context of designing and building business computer systems, and so the concept of 'information systems architecture' has been born.

In the same way that conventional architecture defines the rules and standards for the design and construction of buildings, information systems architecture addresses these same issues for the design and construction of computers, communications networks and the distributed business systems that are implemented using these technologies.

As with the conventional architecture of buildings, towns and cities, information systems architecture must therefore take account of:

- The goals that we want to achieve through the systems
- The environment in which the systems will be built and used
- The technical capabilities needed to construct and operate the systems and their component sub-systems

If one accepts this analysis then one is already well on the way to recognising that information systems architecture is concerned with much more than mere technical factors. It is concerned with what the enterprise wants to achieve and with the environmental factors that will influence those achievements.

In some organisations this broad view of information systems architecture is not well understood. Technical factors are often the main ones that influence the architecture, and under these conditions the architecture can fail to deliver what the business expects and needs.

This document is mainly concerned only with one aspect of information systems architecture: that is the security, risk management and assurance of business information systems. However, in addressing this specialist area the authors have tried to provide as much advice as possible on how to take the broader view. Thus the focus is on enterprise security architecture, to emphasise that it is the enterprise and its activities that are to be secured, and that the security of computers and networks is only a means to this end.

## The Concept of Enterprise

Using the word 'enterprise' implies that the organisation is much more than the sum of its parts. The concept of enterprise carries the meaning that the organisation is perceived as a single entity rather than as a collection of cooperating units. In particular this concept embraces the notion of end-to-end business processes.

The concept can be applied to organisations of any type, including commercial or industrial businesses, public services, governments and their various departments and charitable trusts. The aims of an enterprise are to optimise all parts of the organisation in a harmonious, coherent way, rather than to achieve local optimisation at business unit level. The benefits of the enterprise approach are: improved overall organisational performance, increased competitiveness in the marketplace and operational excellence in service and product delivery to customers. With specific reference to risk management, the benefit is the optimisation of the basket of risks (the balance between opportunities and threats) by the diversification of risks across the entire enterprise. Thus, when we talk about 'enterprise architecture' or 'enterprise security architecture', it is with this concept of enterprise in mind that we do so.

## Managing Complexity

One of the key functions of 'architecture' as a tool of the architect is to provide a framework within which complexity can be managed successfully. Small, isolated, individual projects do not need 'architecture', because their level of complexity is limited and the chief designer can manage the overall design single-handed. However, as the size and complexity of a project grows, then it is clear that many designers are needed, all working as a team to create something that has the appearance of being designed by a single 'design authority'.

Also, if an individual project is not isolated, but rather is intended to fit harmoniously within a much wider, highly complex set of other projects, then an architecture is needed to act as a 'road-map' within which all of these projects can be brought together into a seamless whole. The result must be as though they were all indeed part of a single, large, complex project. This applies whether the individual projects are designed and implemented simultaneously, or whether they are designed and implemented independently over an extended period of time.

As complexity increases, then a framework is needed within which each designer can work, contributing to the overall design. Each design team member must also be confident that his/her work will be in harmony with that of colleagues and that the overall integrity of the design will not be threatened by the work being split across a large design team.

The role of 'architecture' is to provide the framework that breaks down complexity into apparent simplicity. This is achieved by layering techniques – focusing attention on specific conceptual levels of thinking, and by modularization – breaking the overall design into manageable pieces that have defined functionality and defined interfaces. This process is also known as 'systems engineering'.

## Enterprise Security Architecture

It is the common experience of many corporate organisations that information security solutions are often designed, acquired and installed on a tactical basis. A requirement is identified, a specification is developed and a solution is sought to meet that situation. In this process there is no opportunity to consider the strategic dimension, and the result is that the organisation builds up a mixture of technical solutions on an *ad hoc* basis, each independently designed and specified and with no guarantee that they will be compatible and interoperable. There is often no analysis of the long-term costs, especially the operational costs which make up a large proportion of the total cost of ownership, and there is no strategy that can be identifiably said to support the goals of the business.

An approach that avoids these piecemeal problems is the development of an enterprise security architecture which is business-driven and which describes a structured inter-relationship between the technical and procedural solutions to support the long-term needs of the business. If the architecture is to be successful, then it must provide a rational framework within which decisions can be made upon the selection of security solutions. The decision criteria should be derived from a thorough understanding of the business requirements, including:

- The need for cost reduction
- Modularity
- Scalability
- Ease of component re-use
- Operability
- Usability
- Inter-operability both internally and externally
- Integration with the enterprise IT architecture and its legacy systems.

Furthermore, information systems security is only a small part of information security, information assurance or information risk management (these terms have a certain amount of inter-changeability), which in turn is but one part of a wider topic: business security. Business security embraces three major areas: information security; business continuity; physical and environmental security. Broader still is the view that business security is concerned with all aspects of operational risk management. Only through an integrated approach to these broad aspects of business security will it be possible for the enterprise to make the most cost-effective and beneficial decisions with regard to the management of operational risk. The enterprise security architecture and the security management process should therefore embrace all of these areas.

The team at SABSA Limited has been working since 1995 with a model and a methodology for developing enterprise security architecture. This SABSA Model is the basis used for major consulting assignments with clients, and over the years the methodology has been reviewed and refined in the light of experience and in response to new inputs of ideas from various sources, and continues to be updated as new ideas evolve.

The primary characteristic of the SABSA Model is that everything must be derived from an analysis of the business requirements for security and risk management, especially those in which security has an enabling function through which new business opportunities can be developed and exploited. The risk management focus of SABSA embraces both the notion of opportunity and the notion of threat, and the balance that must exist between these two concepts. The model is layered, with the top layer being the business requirements definition stage. At each lower layer a new level of abstraction is developed, going through the definition of the conceptual architecture, logical architecture, physical architecture and finally at the lowest layer, the selection of technologies and products (component architecture) - in other words, the shopping list (in the building trade known as the 'bill of materials'). In addition the whole area of security service management, administration and operations is addressed through the operational or 'service management' architecture. In this respect SABSA aligns closely with ITIL v3.

The SABSA Model itself is generic and can be the starting point for any organisation, but by going through the process of analysis and decision-making implied by its structure, the output becomes specific to the enterprise, and is finally highly customised to a unique business model. It becomes in reality the *enterprise security architecture*, and it is central to the success of a strategic programme of information security management within the organisation. Readers should note at this point that SABSA is not a recipe book – it is a methodology and framework by which unique and highly customised recipes (solutions) can be developed, but SABSA is not itself pre-loaded with any recipes

## Why Architectures Sometimes Fail to Deliver Benefit

### Historical Background

Many corporate organisations implement technical solutions to business security requirements on a very tactical basis. Usually a requirement is identified and a product is sought and acquired to meet that requirement without regard to the broader implications. A point solution is implemented which is often effective in providing some security, but frequently no-one is really sure that the security is appropriate to the risk, or that the cost is commensurate with the benefit, or that it meets a wide variety of other business requirements which are not specifically or obviously security-related (although they are risk-related, in the broader sense). Security is often the last thing to be considered in business information system design, and often gets relegated to the status of a few add-on fixes when all other design decisions have been frozen.

This can lead to many problems. The security solutions are often isolated and incapable of being integrated together or of inter-operating with one another. The variety of security solutions leads to increased complexity and cost of support, and in particular can lead to an exploding workload with regard to administration and management. Worst of all, because there has been inadequate attention paid to the business requirements, the "solution" can sometimes hinder the business process rather than helping it, and the reputation of "security" among the business community gets worse and worse.

Appropriate 'business security' is that which protects the business from undue operational risks in a cost-effective way. If 'business security' is to be effective in enhancing the business process and achieving business goals (and what other possible use could it have?) then the approach described above must be avoided. A much more strategic view should be developed, in which the business requirements are the primary driver for developing effective information security solutions.

### The Wider Business Requirements

Consider again the issue of information security, using it as an example, whilst remembering that the requirements for business assurance and operational risk management also span the areas of business continuity and physical and environmental security. The same principles developed below can be applied across the entire area of business assurance.

The primary business requirements for information security are business-specific. They will usually be expressed in terms of protecting the availability, integrity, authenticity and confidentiality of business information, and providing accountability and auditability in information systems. To understand these requirements, a detailed analysis of the business processes is required, using as source data information gathered by direct interviews with operational business managers.



However, there is much more to the business requirements than pure “security and control”. Information security (or information assurance) provides for the *confident use of information for business purposes across the entire organisation*. The generic business requirements for an information security solution often include the following:

### **Usability**

Is the solution appropriate to the technical competence of the intended users and will it be ergonomically acceptable to those users?

### **Inter-Operability**

Will the solution provide for the long-term requirements for inter-operability between communicating information systems and applications?

### **Integration**

Will the solution integrate with the wide range of computer applications and platforms for which it might be required in the long term?

### **Supportability**

Will the solution be capable of being supported in the environment<sup>2</sup> within which it has been designed to be used?

### **Low Cost Development**

Is the solution of modular design and hence capable of being integrated into a development programme at minimal cost?

### **Fast Time to Market**

Is the solution capable of being integrated into a development programme with minimal delay so as to meet the timeframes associated with windows of business opportunity?

### **Scalability of Platforms**

Will the solution fit with the range of computing platforms<sup>3</sup> with which it might be required to integrate?

### **Scalability of Cost**

Is the entry-level cost appropriate to the range of business applications for which the solution is intended?

### **Scalability of Security Level**

Does the solution support the range of cryptographic and other techniques that will be needed to implement the required range of security strengths and assurance levels?

### **Scalability of Use**

Is the solution capable of being scaled to meet future numbers of business users and/or future capacity requirements for throughput and storage of information and transaction volumes?

### **Re-Usability**

Is the solution re-usable in a wide variety of similar situations to get the best return on the investment in its acquisition and development?

### **Operations Costs**

Will the cost impact on systems operations be minimised?

---

<sup>2</sup> Including the number of end-users and service-delivery points, their geographical location and their distribution.

<sup>3</sup> Potential platforms range from high-end mainframes, through mid-range servers, down to PCs, workstations, laptops and mobile devices.

### **Administration Costs**

Will the solution provide an efficient means for security administration to minimise the costs of this activity?

### **Risk-Based Cost/Benefit Effectiveness**

Is the reduction of risk (the benefit) appropriate to the costs of acquisition, development, installation, administration and operation?

### **Enabling Business**

Finally there are usually a number of business-specific requirements that influence the security strategy. These include requirements where security has an important role in generating the appropriate level of confidence so as to enable new ways of doing business using the latest advances in information technology, such as:

- Exploiting the global reach of the Internet;
- Using global e-mail;
- Outsourcing the operational management of networks and computer systems;
- Providing remote access to third parties;
- Developing on-line business services;
- Delivery of digital entertainment products (video, music, etc)
- Improving customer service through integration of information and consistent presentation of a user interface
- Obtaining software upgrades and system support through remote access by vendors;
- Tele-working, 'mobile computing', 'road warriors' and the 'virtual office'.

## **Being a Successful Security Architect**

Unless the security architecture can address this wide range of operational requirements and provide real business support and business enablement, rather than just focusing upon 'security', then it is likely that it will fail to deliver what the business expects and needs.

This type of failure is a common phenomenon throughout the information systems industry, not just in the realm of information systems security. In SABSA the whole emphasis is on the need to avoid this mistake, by keeping in mind at all times the real needs of the business. It is not sufficient to compile a set of business requirements, document them and put them on the shelf, and then proceed to design a security architecture driven by technical thinking alone.

Being a successful security architect means thinking in business terms at all times, even when you get down to the real detail and the nuts and bolts of the construction. You always need to have in mind the questions: Why are you doing this? What are you trying to achieve in business terms here? Otherwise you will lose the thread and finish up making all the classic mistakes.

It will also be difficult to battle against the numerous other people around you who do not understand strategic architecture, and who think that it is all to do with technology. These people will constantly challenge you, attack you and ridicule you. You have to be ready to deal with this. You have to realise that being a successful architect is also about being a successful communicator who can sell the ideas and the benefits to others in the enterprise who need to be educated about these issues.

One of the most important factors for success is to have buy-in and sponsorship from senior management levels within the enterprise. Enterprise architecture cannot be achieved unless the most senior decision-makers are on your side. The fruits of the architectural work will be enjoyed throughout the enterprise, but only if the enterprise as a whole can begin to think and act in a strategic way. Creating this environment of acceptance and support is probably one of the most difficult tasks that you will face in the early stages of your work.



## Security Architecture Needs a Holistic Approach

Many people make the mistake of believing that building security into information systems is simply a matter of referring to a checklist of technical and procedural controls and applying the appropriate security measures on the list. However, security has an important property that most people know about but few pay any real heed to it: it is like a chain, made up of many links, and the strength and suitability of the chain is only as good as that of its weakest link. At worst, if one link is missing altogether, the rest of chain is valueless.

The checklist approach also fails because many people focus on checking that the links in the chain exist but do not test that the links actually fit together to form a secure chain. The chain is a reasonably good analogy, but the problem is actually much worse than this. Imagine a checklist that has the following items: engine block; pistons; piston rings; piston rods, bearings, valves; cam shaft, wheels, chassis, body, seats, steering wheel, gearbox, etc. Suppose that this list comprehensively itemises every single component that would be needed to build a car. If you go through the checklist and make sure that you have all of these components, does it mean that you have a car? Not exactly!

A car is a good example of a complex system. It has many sub-systems, which in turn have sub-systems, and eventually a very large number of components. Designing and building a car needs a 'systems-engineering' approach. Some of the key questions not addressed by the checklist approach to car construction are:

- Do you understand the requirements?
- Do you have a design philosophy?
- Do you have all of the components?
- Do these components work together?
- Do they form an integrated system?
- Does the system run smoothly
- Are you assured that it is properly assembled?
- Is the system properly tuned?
- Do you operate the system correctly
- Do you maintain the system?

The analogy of the car as a complex machine that needs a holistic architectural design is much more powerful than the idea of a chain. Security architecture is more like the car, not so much like the chain.

## The SABSA Model

### A Layered Model of Architecture

To establish a layered model of how security architecture is created, it is useful to return for a moment to the use of the word in its conventional sense: the construction of buildings.

The SABSA Model comprises six layers, the summary of which is in Table 1. It follows closely the work done by John A. Zachman<sup>4</sup> in developing a model for enterprise architecture, although it has been adapted somewhat to a security view of the world. Each layer represents the view of a different player in the process of specifying, designing, constructing and using the building.

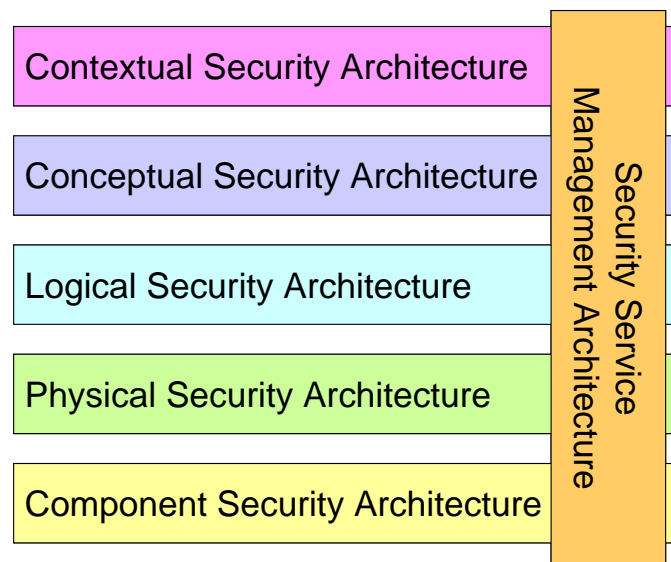
There is another configuration of these six layers which is perhaps more helpful, shown in Figure 1. In this diagram the 'security service management architecture' has been placed vertically across the other five layers. This is because security service management issues arise at each and every one of the other five layers. Security service management has a meaning in the context of each of these other layers.

---

<sup>4</sup> Published through the Zachman Institute for Framework Advancement. Reference: <http://www.zifa.com>

**Table 1: Layered Architecture Views**

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Service Manager's View	Security Service Management Architecture



**Figure 1: The SABSA Model for Security Architecture**

### ***The Business View***

When a new building is commissioned, the owner has a set of business requirements that must be met by the architecture. At the highest level this is expressed by the descriptive name of the building: it is a domestic house; a factory; an office block; a sports centre; a school; a hospital; a warehouse; a theatre; a shopping centre; an airport terminal; a railway station; or whatever. Each one of these business uses immediately implies an architecture that will be different from all the others, an architecture that will fulfil expectations for the function of the building in business terms.

Having stated *what* sort of building is needed the owner must then decide some more detail about its use:

- *Why* do you want this building? The goals that you want to achieve.
- *How* will it be used? The detailed functional description.
- *Who* will use the building, including the types of people, their physical mobility, the numbers of them expected, and so on?
- *Where* should it be located, and what is its geographical relationship to other buildings and to the infrastructure (such as roads, railways etc)?
- *When* will it be used? The times of day / week / year, and the pattern of usage over time.

This type of analysis is essential before any type of design work is done. It is through this process that the requirements of the building are established, and understanding the requirements is a pre-requisite to designing a building that will meet those requirements. When you design a secure business system, the same applies. There are many possible architectural approaches that you could take, but the one that will be the most suitable will be driven from a clear understanding of the business requirements for the system.

- *What* type of system is it and for what will it be used?
- *Why* will it be used?
- *How* will it be used?
- *Who* will use it?
- *Where* will it be used?
- *When* will it be used?

These are the characteristic questions that you must ask. From the analysis of the replies you receive, you should be able to gain an understanding of the business requirements for the secure system. From those you should be able to synthesise a system architecture and a security architecture that meets those requirements.

In the SABSA Model this business view is called the *contextual security architecture*. It is a description of the business context in which your secure system must be designed, built and operated.

Any attempt to define an architecture that takes a short cut and avoids this essential step is very unlikely to be successful. Even so, simple observation reveals that many enterprises undertaking architectural work do not take this stage seriously. It is very common for systems architecture work to begin from a technical perspective, looking at technologies and solutions whilst ignoring the requirements.

It seems to be such obvious common sense that one must first understand the requirements, and yet so few people seem to know how to approach architecture development in the information systems arena. Unfortunately many technologists and technicians believe that they already know the requirements, even though they have a poor relationship with those who might express these requirements.

The results of taking a short cut in the requirements definition stages of an architecture development are abundantly clear. When one looks around at many large corporate enterprises and at their information systems infrastructure managers or applications teams, the relationship with the business community is often strained. For many years the 'business people' have been complaining that the 'information systems people' are unable to deliver what the business needs, and that ICT is a serious source of cost with very little tangible benefit to show for it. The reason is simple: the business people are right. ICT vendor interests and technical innovations often drive business systems development strategy, rather than it being driven by business needs. Those with responsibility for architecture and technical strategy often fail to understand the business requirements because they do not know how to do otherwise. Ignorance of architectural principles is commonplace.

We describe here how to take a layered approach to security architecture development. Many of you will be tempted to flip the pages to get to the end sections where some of the solutions can be found. You are in a hurry, and whilst you know that this step-wise approach is correct, you simply do not have the time to linger on the appetisers and starters – you need to get to the meat course. Well, be warned. There simply is no substitute for doing architecture work the proper way. You may try to take short cuts, but your efforts will most likely result in failure, which costs the business more money, delivers less benefit, and destroys the confidence that business people may have in information and communications technology as the means to enable business development.

In the model presented here, the contextual architecture is concerned with:

- *What?* The business, its assets to be protected (brand, reputation, etc.) and the business needs for information security (security as a business enabler, secure electronic business, operational continuity and stability, compliance with the law, etc.). In terms of the highest level of information architecture this is expressed as 'business decisions', along with business goals and objectives.

- **Why?** The business risks expressed in terms of business opportunities and the threats to business assets. These business risks drive the need for business security (enabling eBusiness, brand enhancement and protection, fraud prevention, loss prevention, fulfilling legal obligations, achieving business continuity, etc.).
- **How?** The business processes that require security (business interactions and transactions, business communications, etc.).
- **Who?** The organisational aspects of business security (governance and management structures, supply chain structures, out-sourcing relationships, strategic partnerships), including a definition of the 'extended enterprise', which includes all business partners and external relationships.
- **Where?** The business geography and location-related aspects of business security (the global village market place, distributed corporate sites, remote working, jurisdictions, etc.).
- **When?** The business time-dependencies and time-related aspects of business security in terms of both performance and sequence (business transaction throughput, lifetimes and deadlines, just-in-time operations, time-to-market, etc.).

## ***The Architect's View***

An architect is a creative person with a grand vision. Architects thrive on challenging business requirements. They marshal their skill, experience and expertise to create an inspired picture of what the building will look like. They create impressionistic drawings 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*. It defines principles and fundamental concepts that guide the selection and organisation of the logical and physical elements at the lower layers of abstraction.

When describing the enterprise security architecture, this is the place to describe the security concepts and principles that will be used. These include:

- **What** you want to protect, expressed in the SABSA framework in terms of Business Attributes.  
SABSA Business Attributes Profiling is explained in more detail later in this paper. This profile provides the primary 'requirements engineering' tool by which business requirements can be captured in a normalised, standardised form. The SABSA Business Attributes Profile is then used as a set of proxy assets against which the SABSA risk assessment is carried out. .
- **Why** the protection is important, in terms of control and enablement objectives.  
Control and enablement objectives are derived directly from an analysis of business operational risks (this risk assessment being made against the Business Attributes Profile – the proxy assets) and are a conceptualisation of business motivation for security.
- **How** you want to achieve the protection, in terms of high-level technical and management security strategies and a process-mapping framework through which to describe business processes.  
These strategies set out the conceptual layered framework for integrating individual tactical elements at the lower levels, ensuring that these fit together in a meaningful way to fulfil the overall strategic goals of the business. Such strategies may include: the strategy for applications security; the network security strategy; the public key infrastructure (PKI) strategy; the role-based access control (RBAC) strategy; and so on. For every major area of the business requirements identified in the contextual security architecture, there will be a security strategy (or group of strategies) that supports it.
- **Who** is involved in security management, in terms of roles and responsibilities and the type of business trust that exists between the parties, including asset owners, custodians and users, and service providers and service customers.

The important trust concepts are concerned with the various policy authorities that govern trust within a domain, the policies that they set to govern behaviour of entities in each of those domains, and the inter-domain trust relationships.

- *Where* you want to achieve the protection conceptualised in terms of a security domains framework.

The important concepts here are security domains (both logical and physical), domain boundaries and security associations.

- *When* is the protection relevant, expressed in terms of a business time-management framework.

The important concept is the through-life risk management framework.

## ***The Designer's View***

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

In the world of business computing and data communications, this design process is often called *systems engineering*. It involves the identification and specification of the logical architectural elements of an overall system. 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. It is therefore also known as the *logical security architecture*.

In terms of architectural decomposition down through the layers, the logical security architecture should reflect and represent all of the major security strategies in the conceptual security architecture. At this logical level, everything from the higher layers is transformed into a series of logical abstractions.

The logical security architecture is concerned with:

- *What?* Business information is a logical representation of the real business. It is this business information that needs to be secured.
- *Why?* Specifying the security and risk management policy requirements (high-level security policy, registration authority policy, certification authority policy, physical domain policies, logical domain policies, etc.) for securing business information.
- *How?* Specifying the logical security services (entity authentication, confidentiality protection, integrity protection, non-repudiation, system assurance, etc.) and how they fit together as common re-usable building blocks into a complex security system that meets the overall business requirements. The logical flow of security services is also specified in terms of process maps and a functional specification describes the required functionality.
- *Who?* Specifying the entities (users, security administrators, auditors, etc.) and their inter-relationships, attributes, authorised roles and privilege profiles in the form of a 'schema', and the trust that exists between them in the form of a trust framework.
- *Where?* Specifying the security domains and inter-domain relationships (logical security domains, physical security domains, security associations).
- *When?* Specifying the security-related calendar and timetable in terms of start times, deadlines and lifetimes (such as for registration, certification, login, session management, etc.).

## ***The Builder's View***

The designer of the building hands over the work 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 building. It is the builder's role 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*.

In the world of business information systems, the designer produces a set of logical abstractions that describe the system to be built. These need to be turned into a physical security architecture model that describes the actual technology model and specifies the detailed design of the various system components. The logical security services are now expressed in terms of the physical security mechanisms and servers that will be used to deliver these services. In total, the physical security architecture is concerned with:

- *What?* Specifying the business data model and the security-related data structures (tables, messages, pointers, certificates, signatures, etc.)
- *Why?* Specifying rules that drive logical decision-making within the system (conditions, practices, procedures and actions).
- *How?* Specifying security mechanisms (encryption, access control, digital signatures, virus scanning, etc.) and the physical applications, middleware and servers upon which these mechanisms will be hosted.
- *Who?* Specifying the people dependency in the form of the human interface (screen formats and user interactions) and the access control systems.
- *Where?* Specifying security technology infrastructure in the form of the host platforms and the networks (physical layout of the hardware, software and communications lines).
- *When?* Specifying the physical time management in terms of the timing and sequencing of processes and sessions (sequences, events, lifetimes and time intervals).

### ***The Tradesman's View***

When the builder plans the construction process, s/he needs to assemble a team of experts in each of the building trades that will be needed: the bricklayer, the plasterer, the electrician, the plumber, the carpenter, and so on. Each one of these brings some very specific production skills and some very specific products to the overall construction process.

So it is in the construction of information systems. The builder needs to assemble and install a series of products from specialist vendors, and a team with the integration skills to join these products together during an implementation of the design.

Each of the installers and integrators is the equivalent of a tradesman, working with specialist products and system components that are the equivalent of building materials and components. Some of these 'trades' are hardware-related, some are software-related, and some are service oriented. The 'tradesmen' work with a series of components that are hardware items, software items, and interface specifications and standards. Hence this layer of the architectural model is also called the *component security architecture*.

The component architecture is concerned with:

- *What?* ICT components such as ICT products, including data repositories and processors.
- *Why?* The risk management-related tools and products such as risk analysis tools, risk registers, risk monitoring and reporting tools.
- *How?* Process tools and standards (tools and protocols for process delivery - both hardware and software).
- *Who?* Personnel management tools and products (identities, job descriptions, roles, functions, actions and access control lists).
- *Where?* Locator tools and standards (nodes, addresses, and other locators).
- *When?* Step timings and sequencing tools (time schedules, clocks, timers and interrupts).

### ***The Service Manager's View***

When the building is finished, those who architected, designed and constructed it move out, but someone has to run the building during its lifetime. Such a person is often called the facilities manager or service manager. The job of the service manager is to deal with the operation of the building and its various services, maintaining it in good working order, and monitoring how well it is performing in meeting the requirements. The framework for doing this is called the *service management security architecture*.



In the realm of business information systems the service management architecture is concerned with classical systems operations and service management work. Here the focus of attention is only on the security-related parts of that work. The security service management architecture is concerned with the following:

- *What?* Service delivery management (assurance of operational continuity and excellence of the business systems and information processing, and maintaining the security of operational business data and information).
- *Why?* Operational risk management (risk assessment, risk monitoring and reporting, and risk treatment so as to minimise operational failures and disruptions).
- *How?* Process delivery management (management and support of systems, applications and services, performing specialised security-related operations such as user security administration, system security administration, data back-ups, security monitoring, emergency response procedures, etc.).
- *Who?* Personnel management (account provisioning and user support management for the security-related needs of all users and their applications, including business users, operators, administrators, etc.).
- *Where?* Management of the environment (management of buildings, sites, platforms and networks).
- *When?* Management schedule (managing the security-related calendar and timetable).

However, referring back to Figure 1, there is another dimension to the security service management architecture – its vertical relationship with the other five layers of the model. Thus the security service management architecture needs to be interpreted in detail at each and every one of the other five layers. This is shown in Table 2, with some examples of the type of operational activity that is implied with regard to each of the layers.

**Table 2: The Security Service Management Architecture**

Contextual Layer	Business driver development, business risk assessment, service management, relationship management, point-of-supply management and performance management.
Conceptual Layer	Developing the Business Attributes Profile, developing operational risk management objectives through risk assessment, service delivery planning, defining service management roles, responsibilities, liabilities and cultural values, service portfolio management, planning and maintaining the service catalogue and managing service performance criteria and targets (service level definition).
Logical Layer	Asset management, policy management, service delivery management, service customer support, service catalogue management, and service evaluation management.
Physical Layer	Asset security and protection, operational risk data collection, operations management, user support, service resources protection, and service performance data collection.
Component Layer	Tool protection, operational risk management tools, tool deployment, personnel deployment, security management tools and service monitoring tools.

### ***The Inspector's View***

There is another view of security in business information systems, the Inspector's View, which is concerned with providing assurance that the architecture is complete, consistent, robust and 'fit-for-purpose' in every way. In the realm of information systems security this is the process of 'security auditing' carried out by 'computer auditors' or 'systems quality assurance' personnel.

However, the SABSA framework does not recognise this as a separate architectural view. The SABSA approach to audit and assurance is that the architecture model as a whole supports these needs. The existence of such architecture is one of the ways in which the auditors will establish that security is being applied in a systematic and appropriate way. The framework itself can provide a means by which to structure the audit process. In addition, security audit and review is addressed as one of the major strategic programmes within the security service management architecture associated with the conceptual layer (see Table 1 above).

## The Governor's View

Another view of information security management is the Governor's View. This has similarities with the Inspector's View in that it is pervasive throughout the SABSA framework, all of which needs to be governed. However, there are two focal points for this view that will become clear as you read further and discover more about the detailed columns that are the vertical cuts through of the SABSA Matrix. These are the 'people' column, which deals directly with governance and management, and the 'motivation' column that deals specifically with risk management, policy-making and monitoring and reporting compliance with policy. These two areas of the SABSA Matrix are the main thrust of the Governor's influence over the information security management programme as a whole. Later in this paper is described a governance process by which this governance role is achieved in the SABSA framework.

## The SABSA Matrix

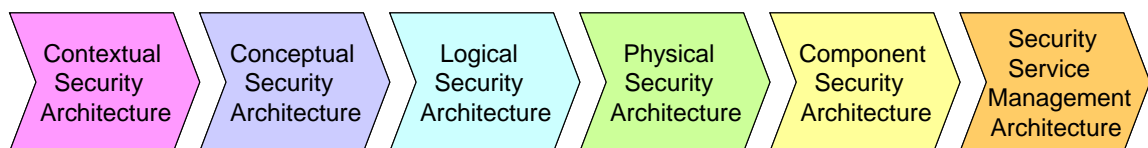
In the above sections, each of the six horizontal layers of abstraction of the architecture model (contextual, conceptual, logical, physical, component and service management) has been examined. Each of the sections has also introduced a series of vertical cuts through each of these horizontal layers, answering the questions:

- *What* are you trying to do at this layer? – The assets to be protected by your security architecture.
- *Why* are you doing it? – The motivation for wanting to apply security, expressed in the terms of risk.
- *How* are you trying to do it? – The processes and functions needed to achieve security.
- *Who* is involved? – The people and organisational aspects of security.
- *Where* are you doing it? – The locations where you apply your security.
- *When* are you doing it? – The time-related aspects of security.

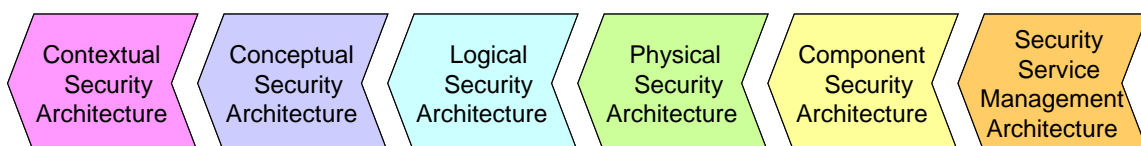
These six vertical architectural elements are now summarised for all six horizontal layers. This gives a 6 x 6 matrix of cells, which represents the whole model for the enterprise security architecture. It is called the SABSA Matrix (see Table 3). If you can address the issues raised by each and every one of these cells, then you will have covered the entire range of questions to be answered, and you can have a high level of confidence that your security architecture will be complete. The SABSA process of developing enterprise security architecture is a process of populating all of these thirty-six cells.

The SABSA Matrix also provides two-way traceability:

- **Completeness:** has every business requirement been met? The layers and matrix allow you to trace every requirement through to the components that provide a solution.



- **Business Justification:** is every component of the architecture needed? When someone questions 'Why are we doing it this way?' the rationale is plain by tracing back to the business requirements that drive the specific solution.



**Table 3: SABSA MATRIX**

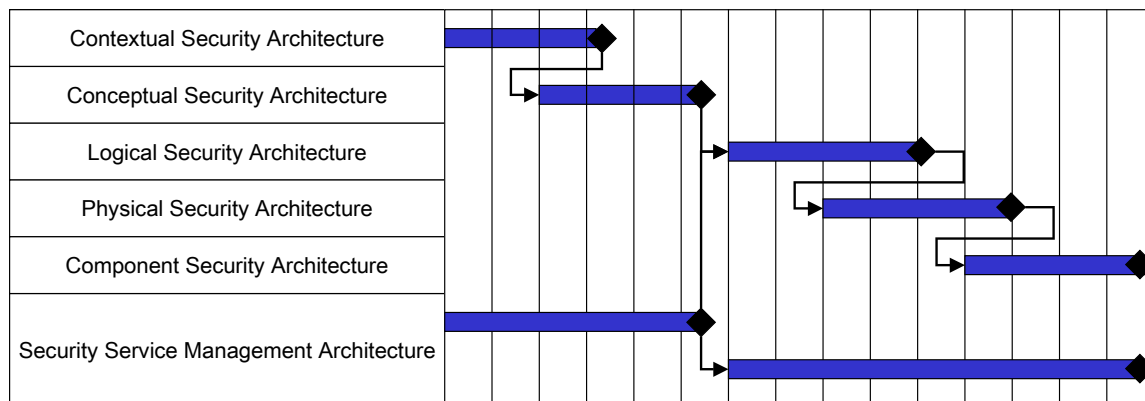
	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
<b>CONTEXTUAL ARCHITECTURE</b>	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
<b>CONCEPTUAL ARCHITECTURE</b>	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
<b>LOGICAL ARCHITECTURE</b>	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
<b>PHYSICAL ARCHITECTURE</b>	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
<b>COMPONENT ARCHITECTURE</b>	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
<b>SERVICE MANAGEMENT ARCHITECTURE</b>	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

**Table 4: SABSA SERVICE MANAGEMENT MATRIX (Aligned with ITIL v3)**

	<b>ASSETS (What)</b>	<b>MOTIVATION (Why)</b>	<b>PROCESS (How)</b>	<b>PEOPLE (Who)</b>	<b>LOCATION (Where)</b>	<b>TIME (When)</b>
	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	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					
<b>CONTEXTUAL ARCHITECTURE</b>	Business Driver Development	Business Risk Assessment	Service Management	Relationship Management	Point-of-Supply Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Service Capabilities for Providing Value to Customers	Managing Service Providers & Service Customers; Contract Man'ment	Demand Man'ment; Service Supply, Deployment & Consumption	Defining Business-Driven Performance Targets
<b>CONCEPTUAL ARCHITECTURE</b>	Proxy Asset Development	Developing ORM Objectives	Service Delivery Planning	Service Management Roles	Service Portfolio	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Risk Analysis on Business Attributes Proxy Assets	SLA Planning; BCP; Financial Planning & ROI; Transition Planning	Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Service Catalogue	Managing Service Performance Criteria and Targets
<b>LOGICAL ARCHITECTURE</b>	Asset Management	Policy Management	Service Delivery Management	Service Customer Support	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management; Test & Validation Management	Policy Development; Policy Compliance Auditing	SLA Management; Supplier Management; BCM; Cost Management; Transition Management	Access Management; User Privileges, Account Administration & Provisioning	Configuration Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
<b>PHYSICAL ARCHITECTURE</b>	Asset Security & Protection	Operational Risk Data Collection	Operations Management	User Support	Service Resources Protection	Service Performance Data Collection
	Change Management; Software & Data Integrity Protection	Operational Risk Management Architecture	Job Scheduling; Incident & Event Management; Disaster Recovery	Service Desk; Problem Man'ment; Request Man'ment	Physical & Environmental Security Management	Systems and Service Monitoring Architecture
<b>COMPONENT ARCHITECTURE</b>	Tool Protection	ORM Tools	Tool Deployment	Personnel Deployment	Security Management Tools	Service Monitoring Tools
	Product & Tool Security & Integrity; Product & Tool Maintenance	ORM Analysis, Monitoring and Reporting Tools & Display Systems	Product & Tool Selection and Procurement; Project Management	Recruitment Process Disciplinary Process Training & Awareness Tools	Products & Tools for Managing Physical & Logical Security of Installations	Service Analysis, Monitoring and Reporting Tools & Display Systems

## The SABSA Development Process

The SABSA model provides the basis for an architecture development process, since it is clear that through understanding the business requirements, the architect can create the initial vision. This is used by the designers to create the detailed design, which in turn is used by the builder to construct the systems, with components of various sorts provided by specialists. Finally, the facilities manager operates the finished system, but unless the earlier phases take account of the operational and service management needs, this phase in the lifetime of the system will be fraught with difficulty. The development process itself is shown, at a high level, in Figure 2.



**Figure 2: The SABSA Development Process**

The high-level development process in Figure 2 indicates that there is a natural break after the first two phases. Once the Contextual Security Architecture and the Conceptual Security Architecture are agreed and signed off, then work on the later phases can begin, with considerable parallel working. However, it is difficult to make useful progress on the later stages until these first two are fairly fully defined. The temptation to go straight to an implementation of certain products and tools should be avoided, since this is the source of so many severe problems during the operational phase.

The development of the Security Service Management Architecture sub-process needs to be started right at the beginning of the process, since aspects of this are required for the development of the Contextual and Conceptual Security Architectures. Once again, there is a natural break while the first two phases are signed off, after which development of the Security Service Management Architecture can be resumed.

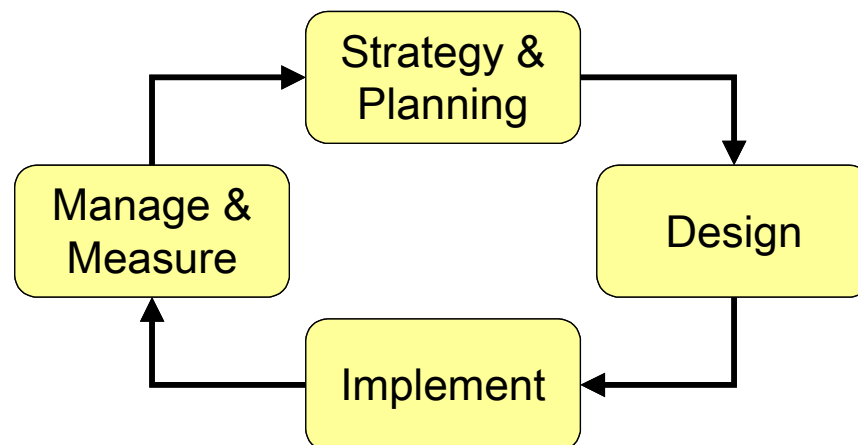
## The SABSA Lifecycle

The SABSA Development Process can be seen in the context of an overall SABSA Lifecycle for the security architecture, shown in Figure 3. In this SABSA Lifecycle, the first two phases of the process are grouped into an activity called 'Strategy and Planning'. This is followed by an activity called 'Design', which embraces the design of the logical, physical, component and service management architectures. The third activity is 'Implement', followed by 'Manage and Measure'.

The significance of the 'Manage and Measure' activity is that early in the process you set target performance metrics (see the discussion of the SABSA Business Attributes Profile below). Once the system is operational, it is essential to measure actual performance against targets, and to manage any deviations observed. Such management may simply involve the manipulation of operational parameters, but it may also feed back into a new cycle of development.

Failure to meet the performance goals is a risk event. Thus the performance goals (or key performance indicators – KPIs) are also capable as being viewed from the opposite perspective as key risk indicators (KRIs). It is usual in the SABSA framework to set two performance or risk indicators. The primary indicator is the actual target threshold that represents the limit of acceptable performance (also an expression of the risk appetite), but another secondary indicator can be used as an early warning mechanism to provide the opportunity to manage risks back within the comfort zone of the organisation before this risk appetite is exceeded. This lends itself to 'traffic light reporting' on scorecards and dashboards, using green, yellow and red colour coding.





**Figure 3: The SABSA Lifecycle**

## The SABSA Business Attributes Profile

The SABSA Business Attributes Profile is at the heart of the SABSA methodology. It is this 'requirements engineering' technique that makes SABSA truly unique and provides the linkage between business requirements and technology / process design.

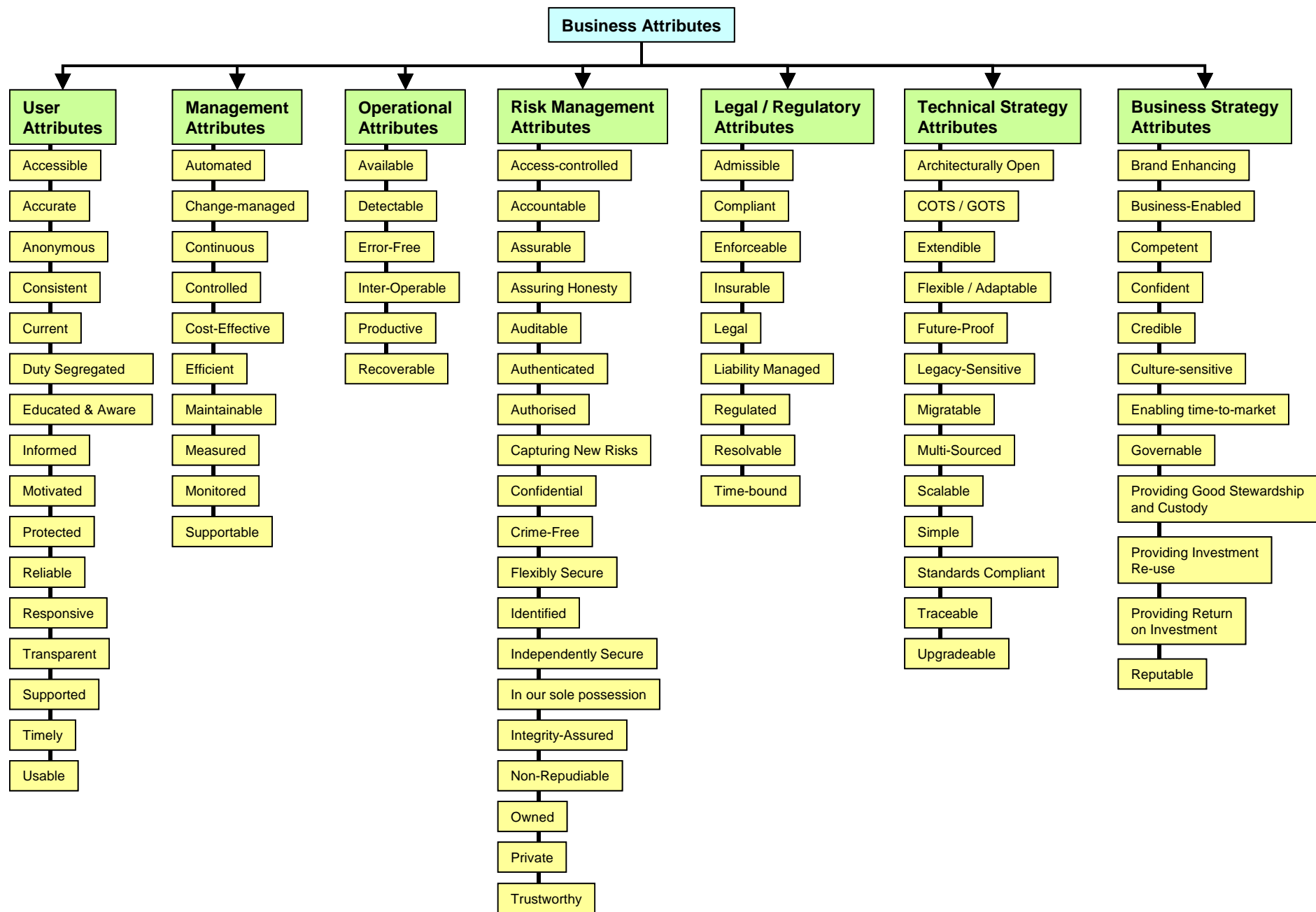
These Business Attributes are compiled from extensive experience with numerous organisations in many countries and various industry sectors. Over the course of that work it became apparent that although every business is unique, there are commonly recurring themes. This experience has been used to create a taxonomy of SABSA Business Attributes, shown in Figures 4 and 5. Figure 4 shows the original SABSA Business Attributes Taxonomy focused specifically on ICT systems and their environment. These are organised under seven group headings. Each SABSA Business Attribute is an abstraction of a real business requirement previously encountered in several organisations; most of them encountered many times over. Each SABSA Business Attribute has a detailed definition and some suggested guidelines for applying metrics to that attribute, not included in this overview. Figure 5 is a more recent development, after the success of the Business Attributes Profiling technique across the information security industry, raising the level of abstraction from ICT-focused to pure business-focused. In both cases these taxonomies should be seen as examples only. They are not comprehensive or definitive and are capable of being expanded to embrace new attributes almost without limit. In some cases, organisations with special business needs have diversified some of these attributes into a lower level of granularity to suit their specific businesses. Nor should the lists be seen as mandatory, because not all of the attributes listed here will necessarily be applicable to a given organisation. Both taxonomies are designed to be customised so as to describe a unique organisation with a unique set of business requirements.

Business Attributes Profiling is a very powerful tool that allows any unique set of business requirements to be translated, standardised and 'normalised' into a SABSA format. Each profile selects only those SABSA Business Attributes that apply to the specific business of the organisation (creating new attributes if there are found to be gaps). The taxonomy provides a checklist of possible attributes and the business analysts can decide whether or not a given attribute should be included in this specific profile. The SABSA Business Attributes Profile is an important conceptualisation of the real business, and forms a core part of the 'Conceptual Security Architecture'. It can be seen on row 2, column 1 of the SABSA Matrix in Table 3.

It also allows the selection of metrics that are used to set performance targets as an integral part of the SABSA Business Attributes Profile that can later be measured (did you hit the target?). This too is at the choice of the business analysts, using either the suggested metrics in the detailed definitions of the attributes, or creating new metrics if it seems more appropriate.

Thus the 'Manage & Measure' activity in the SABSA Lifecycle is based upon the SABSA Business Attributes Profile that was set out during the 'Strategy & Planning' activity, and which has been customised specifically to conceptualise the business of this unique organisation.





**Figure 4: The SABSA Taxonomy of ICT Business Attributes**

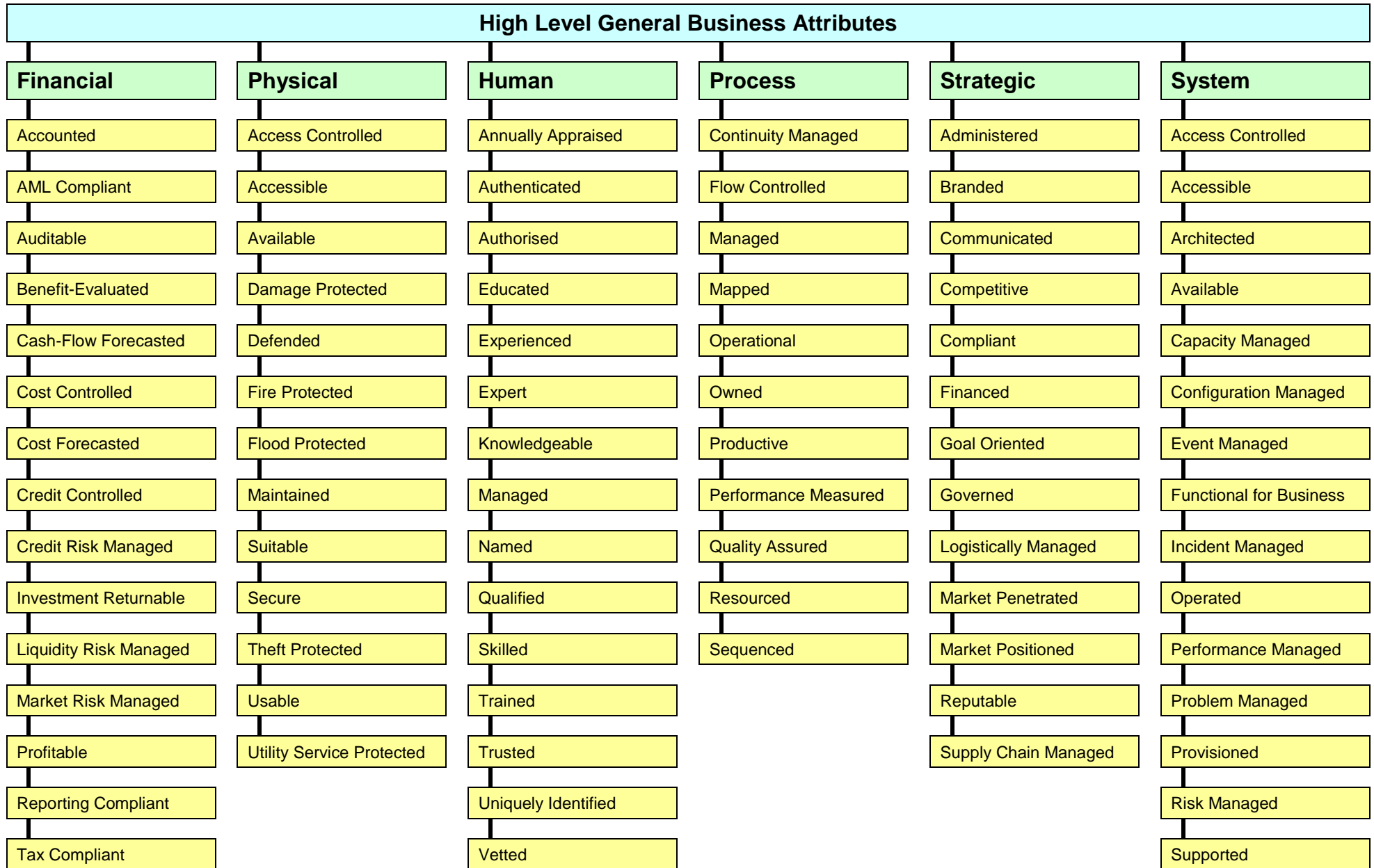


Figure 5: The SABSA Taxonomy of High Level General Business Attributes

## SABSA Risk Management

In the SABSA framework there is heavy emphasis on the duality of risk – the balance between opportunity and threat. Many definitions of ‘operational risk’ miss this important point and focus only on the downside risks or potential loss events. This is unfortunate, because operational risk management provides many opportunities to develop operational excellence and improved service and product delivery to customers. It can also contribute significantly to meeting the performance goals of the enterprise and assisting individual line managers to achieve their personal target KPIs. SABSA embraces fully this ‘opportunity’ aspect of operational risk management in general and information risk management in particular. Figure 6 shows this in diagrammatic format.

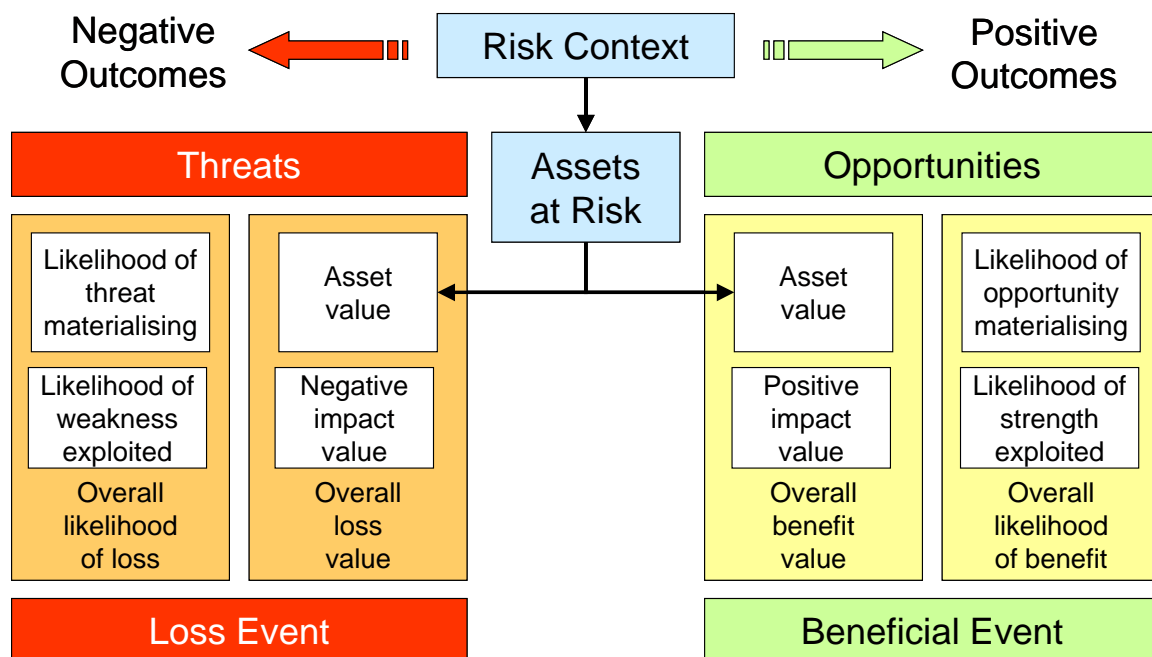


Figure 6: SABSA Model of Operational Risk

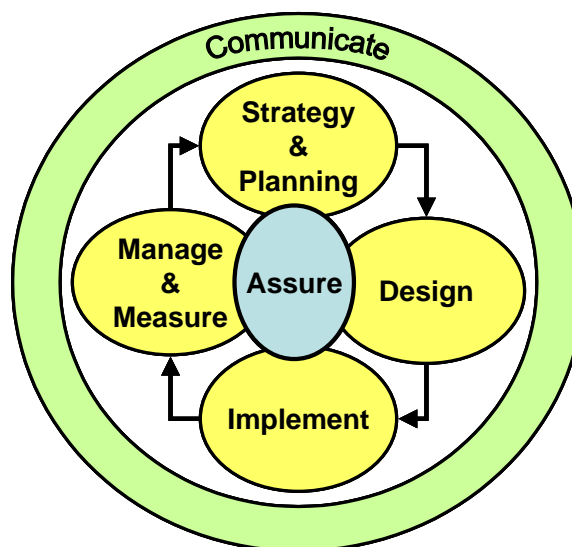


Figure 7: SABSA Risk Management Process

Based upon the SABSA Model of Operational Risk with its recognition of both opportunities and threats, the SABSA framework also provides a fully end-to-end SABSA Risk Management Process that covers every stage of the SABSA Lifecycle in detail. Figure 7 gives a summary overview of this risk management process and Figure 8 shows the next level of detail. The full details of this process are described in the SABSA standard.

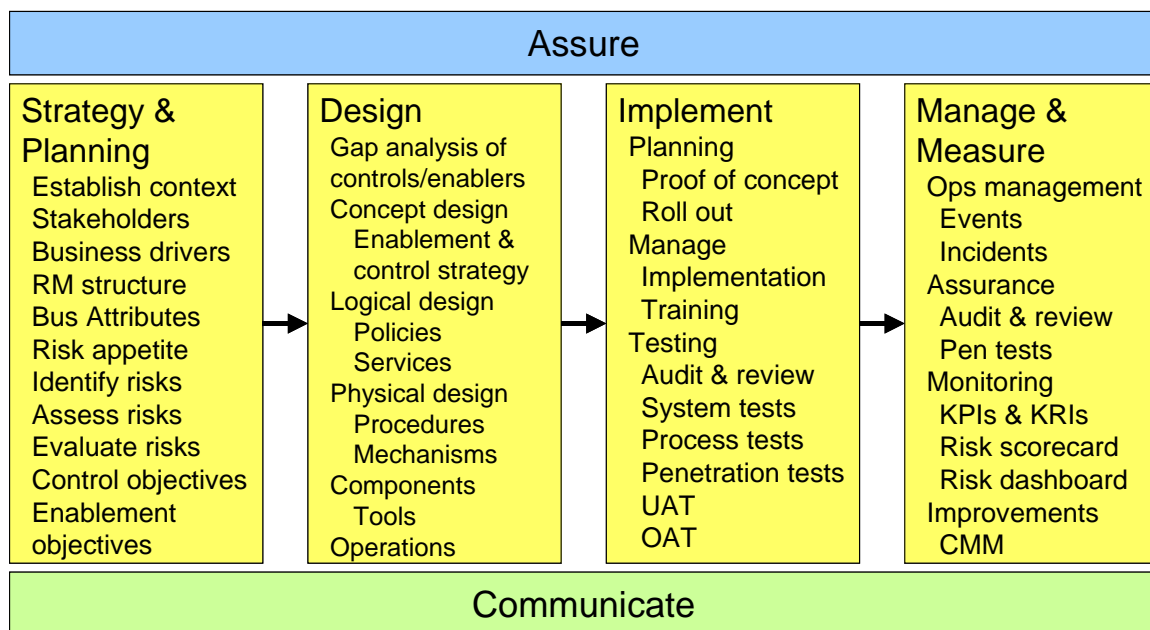


Figure 8: Details of the SABSA Risk Management Process

## SABSA Assurance

The 'Assure' component of the SABSA Risk Management process also has its own SABSA Assurance Framework shown in Figure 9, offering the possibility of different levels of assurance for different business requirements. It may also be applied at each column of the SABSA Matrix and for each of the stages of the SABSA Lifecycle. The full details of how this model is used are described in the SABSA standard.

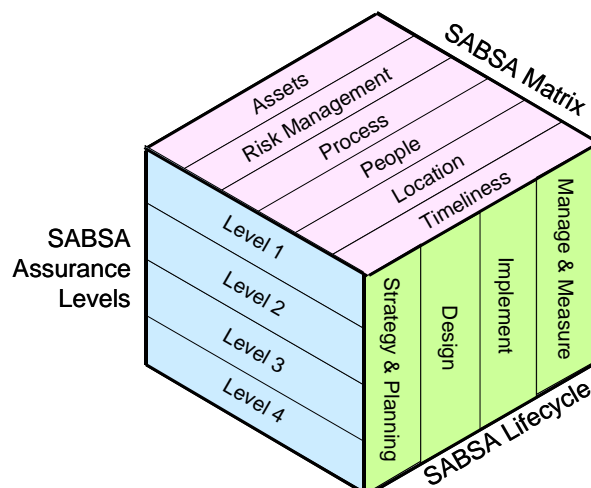


Figure 9: SABSA Assurance Framework

## SABSA Governance

Figure 10 shows the overview of the SABSA Governance Process, again mapped onto the four stages of the SABSA Lifecycle.

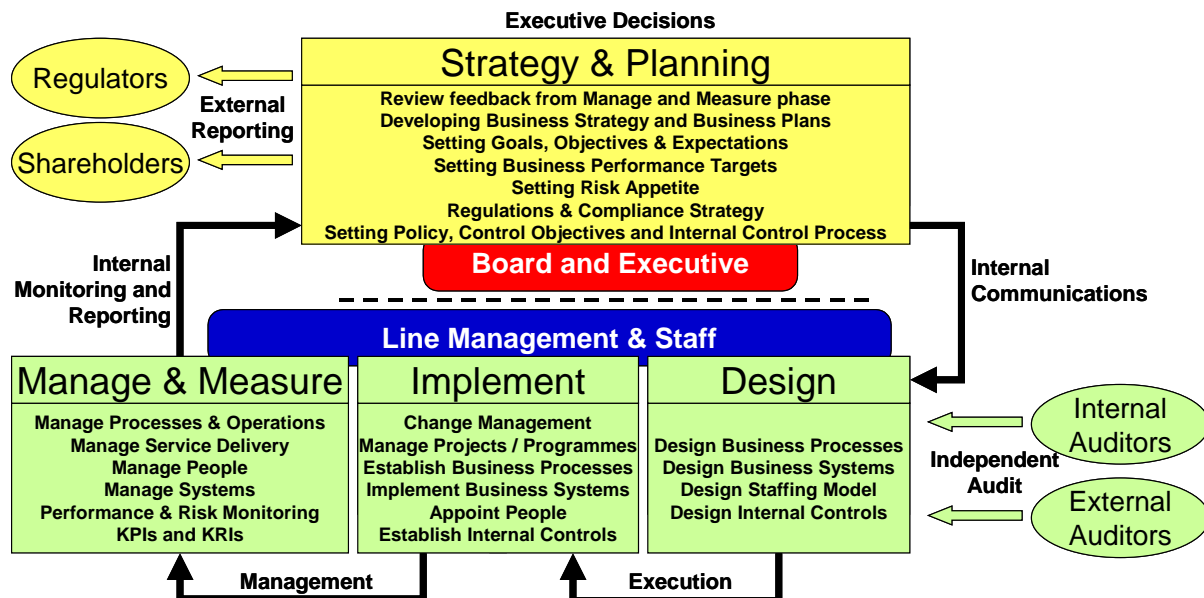


Figure 10: SABSA Governance Process

## SABSA Maturity Profile

The SABSA Maturity Profile (SMP) enables an organisation to benchmark the level of maturity of its SABSA management processes, using conventional capability maturity modelling techniques, but applied specifically to the SABSA Framework.

## SABSA Implementation

The SABSA Lifecycle contains an activity called 'Implement'. However, it is unlikely that a major strategic enterprise-wide security architecture will ever be implemented as a single project. What is more likely is that the architecture provides a blue-print and a road-map that guides a whole series of separate implementation projects, each of which is driven by a specific business initiative and funded by a budget associated with that initiative. Some of these projects may themselves be 'infrastructure projects', such as building an integrated, enterprise wide, unified directory service.

The reality is that implementation will usually be fragmented in this way. Thus the main purpose of the security architecture is to ensure that this fragmentation does not lead to a piecemeal approach to design. Despite the fragmented projects, the overall systems environment should maintain its architectural integrity – provided that the architecture has been created and documented, and provided that project teams refer to it and are guided by it. Individual projects should therefore be subject to architectural governance and approval by an Architecture Board.

## Architecture Maintenance

A security architecture developed using the SABSA Methodology is not shelf-ware – it is a living, breathing thing that needs to be maintained and applied constantly. Certainly it is a reference document that should be used by project teams as they design and implement their specific business-led projects (see above under 'Implementation'). However, the world is constantly changing. The business requirements evolve over time.

Sometimes they experience a step change as when a major acquisition or divestment occurs, or in the case of a sudden economic downturn, but sometimes they evolve slowly in response to a changing marketplace.

Whatever the case, the front end of the architecture – the contextual architecture – needs to be reviewed and updated from time to time. The question then arises – at what point do the contextual changes create sufficient pressure to change the underlying conceptual architecture and other layers?

Technology also changes. New solutions become available. Again this raises a question – at what point should you change decisions in the component architecture from one strategic technology or product to another? All of this suggests some kind of continual architecture review process, governed by an Architecture Board.

## Summary and Conclusion

Unless the security architecture can address a wide range of operational requirements and provide real business support and enablement, rather than just focusing upon short-term point solutions, then it will likely fail to deliver what the business expects. This type of failure is a common phenomenon throughout the information systems industry, not just in the realm of security architecture. Yet it is not sufficient to compile a set of business requirements, document them and then put them on the shelf, and proceed to design a security architecture driven by technical thinking alone. Being a successful security architect means thinking in business terms at all times, and setting up quantifiable success metrics that are developed in business terms around business performance parameters, not technical ones.

Another challenge is the sheer number of other people who do not understand strategic architecture, and who think only in terms of technology. To overcome their objections, you must be a good communicator who can sell these ideas and these benefits to others in the enterprise. One of the most important factors for success is gaining buy-in and sponsorship from senior management within the enterprise. Enterprise security architecture cannot be achieved unless the most senior decision-makers are on your side. To achieve this level of backing, senior management must feel that their success is directly tied to the success of the architecture. Creating this environment of acceptance and support is probably one of the most difficult tasks, since it may force the enterprise as a whole to begin to think and act in a very different way. However, if a business-driven approach is utilized, the fruits of the architectural work will be enjoyed throughout the enterprise.

## Further Information

For those who would like greater detail on this subject, there is a major reference work (587 pages) affectionately known as the 'Book of SABSA' and entitled:

'Enterprise Security Architecture: A Business Driven Approach'; ISBN 1-57820-318-X

To purchase the book directly from the publisher, or to read reviews by prominent professionals, visit the Elsevier web site:

<http://www.elsevierdirect.com/index.jsp>

The 'Book of SABSA' (ESA – see above) is also available from all major bookstores and on-line booksellers. Probably the quickest access is via Amazon:

<http://www.amazon.com/Enterprise-Security-Architecture-Business-Driven-Approach/dp/157820318X>

Updates to the SABSA Standard are published electronically at regularly intervals on SABSA web sites.

## SABSA Institute Education and Certification

For details on the SABSA Institute's comprehensive education and certification programme please visit <http://www.sabsa.org>