TOGAF® and SABSA® Integration

How SABSA and TOGAF complement each other to create better architectures

A White Paper by:

The Open Group TOGAF-SABSA Integration Working Group, comprising leading representatives from the SABSA Institute and members of The Open Group Architecture and Security Forums

October 2011

Copyright © 2011 The Open Group and The SABSA Institute

The Open Group hereby authorizes you to use this document for any purpose, PROVIDED THAT any copy of this document which you make shall retain all copyright and other proprietary notices contained herein.

This document may contain other proprietary notices and copyright information.

Nothing contained herein shall be construed as conferring by implication, estoppel, or otherwise any license or right under any patent or trademark of The Open Group or any third party. Except as expressly provided above, nothing contained herein shall be construed as conferring any license or right under any copyright of The Open Group.

Note that any product, process, or technology in this document may be the subject of other intellectual property rights reserved by The Open Group, and may not be licensed hereunder.

This document is provided "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Any publication of The Open Group may include technical inaccuracies or typographical errors. Changes may be periodically made to these publications; these changes will be incorporated in new editions of these publications. The Open Group may make improvements and/or changes in the products and/or the programs described in these publications at any time without notice.

Should any viewer of this document respond with information including feedback data, such as questions, comments, suggestions, or the like regarding the content of this document, such information shall be deemed to be non-confidential and The Open Group shall have no obligation of any kind with respect to such information and shall be free to reproduce, use, disclose and distribute the information to others without limitation. Further, The Open Group shall be free to use any ideas, concepts, know-how, or techniques contained in such information for any purpose whatsoever including but not limited to developing, manufacturing, and marketing products incorporating such information.

Boundaryless Information Flow™ is a trademark and ArchiMate®, Jericho Forum®, Making Standards Work®, Motif®, OSF/1®, The Open Group®, TOGAF®, UNIX®, and the ``X" device are registered trademarks of The Open Group in the United States and other countries.

COBIT® is a registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute.

ITIL® and M_o_R® are registered trademarks of the Office of Government Commerce in the United Kingdom and other countries.

SABSA® is a registered trademark of the SABSA Institute.

All other brand, company, and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

TOGAF® and SABSA® Integration

Document No.: W117

Published by The Open Group and the SABSA Institute, October 2011.

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

The Open Group, 44 Montgomery St. #960, San Francisco, CA 94104
(ogspecs@opengroup.org)

or to:

The SABSA Institute, 17 Ensign House, Admirals Way, Canary Wharf, London E14 9XQ, UK
(info@sabsa.org)

Table of Contents

Executive Summary	**4**
Introduction	**6**
Overview of TOGAF-SABSA Integration	**7**
Operational Risk and its Relevance to Enterprise Architecture	**17**
A Central Role for Requirements Management	**21**
Creating an Enterprise Architecture with Integrated Security	**29**
Appendix A: Glossary	**48**
Appendix B: TOGAF Benefits for SABSA Practitioners	**51**
References	**56**
About The Open Group	**57**
About the SABSA Institute	**57**
About the SABSA-TOGAF Integration Working Group	**58**

Boundaryless Information Flow ™
achieved through global interoperability
in a secure, reliable, and timely manner

Executive Summary

This White Paper documents an approach to enhance the TOGAF enterprise architecture methodology with the SABSA security architecture approach and thus create one holistic architecture methodology. The following aspects are highlighted:

- Overview of TOGAF and SABSA integration – why bolster TOGAF with security architecture and why use SABSA?
- Operational risk and its relevance to enterprise architecture – why incorporating the concept of operational risk is essential to modern enterprise architecture design.
- A central role for requirements management – how to perform requirements management using SABSA Business Attribute Profiling.
- Creating an enterprise architecture with integrated security – how to align SABSA concepts to the TOGAF ADM.
- TOGAF benefits for SABSA practitioners – how to enhance SABSA-based projects by introducing TOGAF concepts.

This White Paper is intended to guide enterprise and security architects in fully integrating security and risk management into enterprise-level architectures, to stimulate review comments and inform the global architecture community of proposed new content from the SABSA perspective for a future edition of the TOGAF standard.

In December 2005, The Open Group Security Forum submitted a White Paper (W055: Guide to Security Architecture in TOGAF) to the Architecture Forum expressing similar intent regarding integrating security and risk management into TOGAF. This was included in TOGAF 9 but not in the integrated manner that the Security Forum had intended. The Security Forum is revising W055 to submit as complementary to this TOGAF and SABSA Integration White Paper.

Integrating security and risk management in enterprise architecture strongly supports The Open Group vision of Boundaryless Information Flow, by informing well justified design decisions which maximize business opportunity whilst minimizing business risk.

Where appropriate, this White Paper includes excerpts from the SABSA Blue Book and SABSA White Paper update, with the full approval and permission of the SABSA Institute.

Introduction

Purpose

Enterprise architecture (including security architecture) is all about aligning business systems and supporting information systems to realize business goals in an effective and efficient manner (systems being the combination of processes, people, and technology). One of the important quality aspects of an enterprise architecture is risk regarding information security and the way this can be managed. For too long, information security has been considered a separate discipline, isolated from the enterprise architecture. This White Paper documents an approach to enhance the TOGAF enterprise architecture methodology with the SABSA security architecture approach and thus create one holistic architecture methodology.

The vision is to support enterprise architects who need to take operational risk management into account, by providing guidance describing how TOGAF and SABSA can be combined such that the SABSA business risk and opportunity-driven security architecture approach can be seamlessly integrated into the TOGAF business strategy-driven approach to develop a richer, more complete enterprise architecture.

There are two main focal points in this White Paper. The first is to describe how SABSA can best be used in TOGAF-based architecture engagements. Unlike regarding security as a separate product, this White Paper gives a practical approach that makes the SABSA security requirements and services available as common TOGAF artifacts.

The second focal point is to show how the requirements management processes in TOGAF can be fulfilled in their widest generic sense (i.e., not only with regard to security architecture) by application of the SABSA concept of Business Attribute Profiling to the entire ADM process.

Furthermore, TOGAF also offers significant benefits for a pure SABSA-based architecture project and these are described in Appendix B: TOGAF Benefits for SABSA Practitioners as guidance for SABSA practitioners.

Project background

The TOGAF-SABSA integration project started in May 2010 as a joint initiative of both the Architecture Forum and the Security Forum of The Open Group, and the SABSA Institute. With the publication of this White Paper the project ends.

Next steps

This White Paper intends to communicate current thinking and to elicit comments from the architecture and security communities. The project results and received comments are submitted via this White Paper to The Open Group Architecture Forum for their use to create the new security and risk management content for a scheduled revision of the TOGAF standard and, in particular, the content currently in Chapter 21 regarding security architecture.

Overview of TOGAF-SABSA Integration

It is the common experience of many corporate organizations 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 organization 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.

An enterprise security architecture does not exist in isolation. It is part of the enterprise. It builds on enterprise information that is already available in the enterprise architecture, and it also produces information that should be used by the enterprise architecture. This is why a close integration of security architecture in the enterprise architecture is beneficial. In the end, doing it right the first time saves costs and increases effectiveness compared to bolting on security afterwards. This is why security architects are seeking ways to align with enterprise architects, and this alignment will be easier if both speak the same language. That language is provided in this White Paper.

What is TOGAF?

TOGAF [1] is an architecture framework which provides the methods and tools for assisting in the acceptance, production, use, and maintenance of enterprise architecture. It is based on an iterative process model supported by best practices and a re-usable set of existing architecture assets.

Why does TOGAF need an update on security architecture aspects?

TOGAF has treated security and risk either implicitly through stakeholder requirements or through a limited set of techniques in Chapter 21 (Security Architecture and the ADM). The Open Group Architecture Forum and Security Forum agree that the coverage of security and risk can be updated and improved. Specific objectives envisaged in this White Paper include:

- Guidance on producing business and risk management-based security architectures, which is increasingly seen as an essential element of enterprise architecture
- Guidance on developing secure architectures to support business outcomes by enabling exploitation of business opportunities
- Guidance on producing architectures that enable the efficient management of security

Why include SABSA in TOGAF security architecture?

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 organizations that make use of the standard in developing and implementing architectures and solutions.

SABSA is business outcome-based. The fundamental idea behind SABSA is that the security architecture is there to facilitate the business. This is in line with TOGAF concepts.

At the heart of the SABSA methodology is the SABSA Model, a top-down approach that drives the SABSA Development Process. This process analyzes 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 & Measure to ensure that the business mandate is preserved.

SABSA contains framework tools created from practical experience, including the SABSA Matrix and the SABSA Business Attribute Profile that further support the whole methodology.

SABSA is well described in the "Blue Book" [2]. In addition, new SABSA thinking is published at www.sabsa.org.

The SABSA artifacts described in this paper mainly refer to the Blue Book; however, it is recommended that to reflect current thinking which has moved on considerably since the Blue Book was published, users of this White Paper should refer to the most recently published SABSA materials available at www.sabsa.org [3].

Brief description of the concepts used

This section gives a short background description of the TOGAF and SABSA concepts relevant for this White Paper.

TOGAF Architecture Development Method (ADM)

The TOGAF Architecture Development Method (ADM) provides a tested and repeatable process for developing architectures.

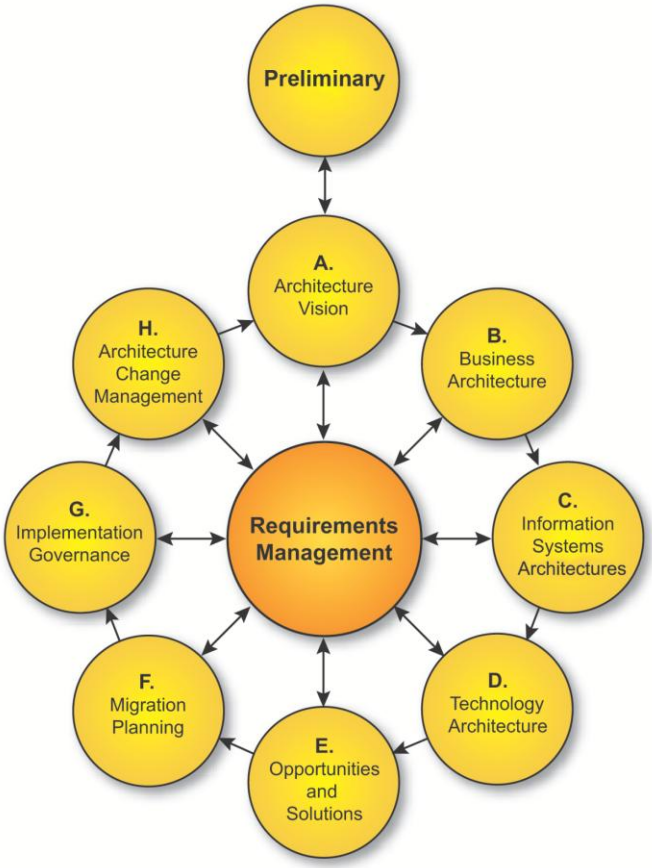

Figure 1: TOGAF Architecture Development Method (ADM)

The ADM includes activities related to establishing an architecture framework, developing architecture content, transitioning, and governing the realization of architectures. All of these activities are carried out within an iterative cycle of continuous architecture definition and realization that allows organizations to transform their enterprises in a controlled manner in response to often changing business goals and opportunities. See Chapter 5 of TOGAF 9.

TOGAF Content Metamodel

The content metamodel provides a definition of all the types of building blocks that may exist within an architecture, showing how these building blocks can be described and related to one another.

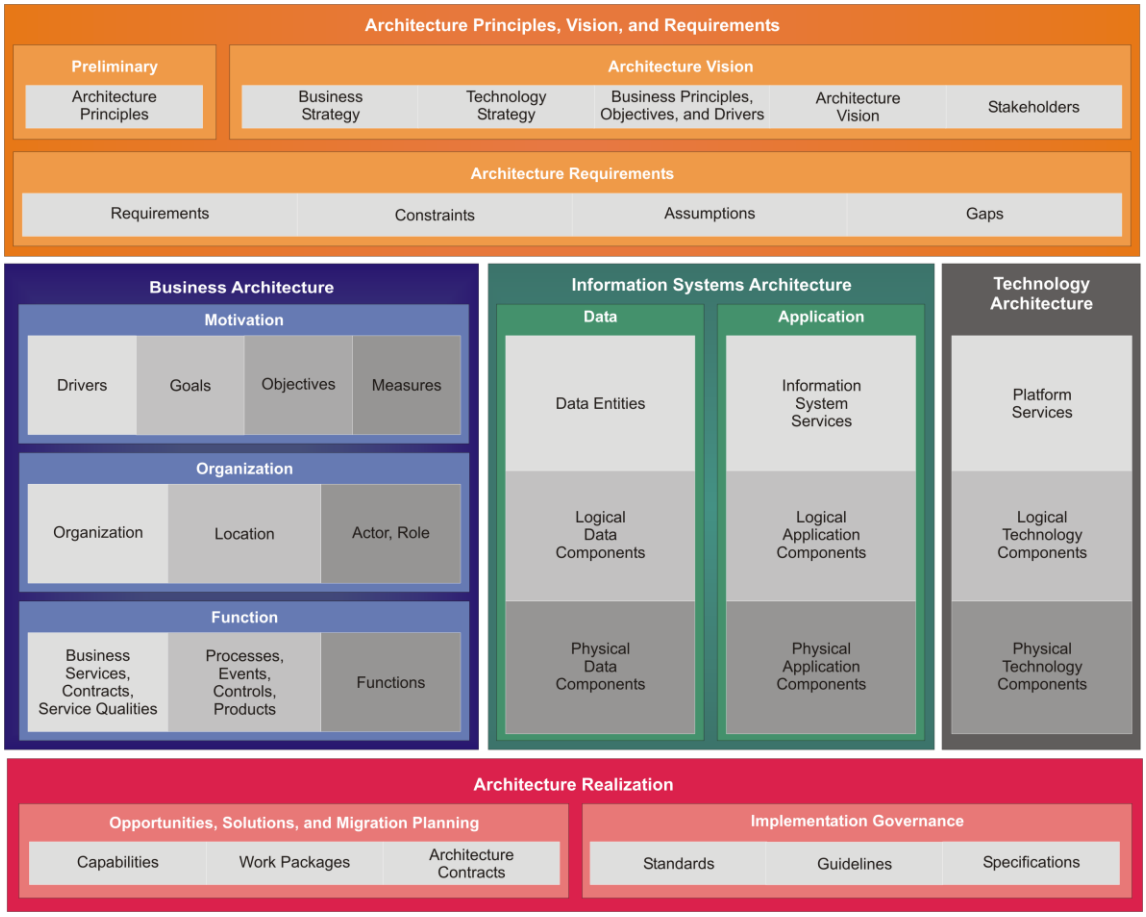

Figure 2: TOGAF Content Metamodel

For example, an architect could identify applications, the data entities processed, and the technologies that implement those applications. These applications will in turn support particular groups of business user or actor, and will be used to support business services. See Chapter 34 of TOGAF 9.

SABSA Model

The SABSA Model comprises six layers. It is based on the well-known Zachman framework[1] for developing a model for enterprise architecture, although it has been adapted somewhat to a security view of the world.

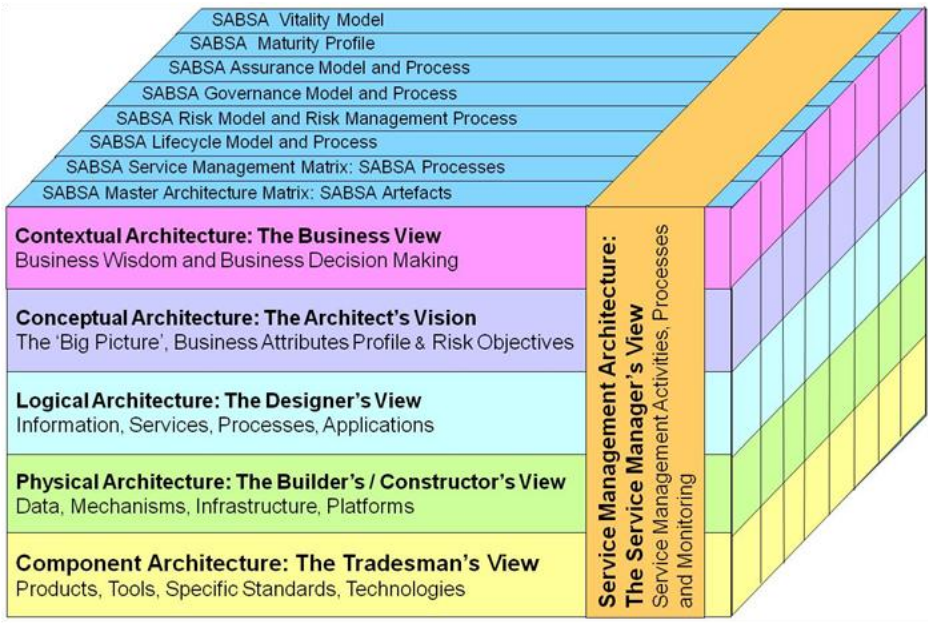

Figure 3: The SABSA Metamodel

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. See Chapter 3 (pp 34) of the SABSA Blue Book.

[1] See TOGAF 8.1.1, Part IV: Resource Base, Chapter 39: ADM and the Zachman Framework.

SABSA Matrix

At each of the horizontal layers of abstraction of the architecture model a series of vertical cuts through each of these horizontal layers is made, answering the questions: what, why, how, who, where, and when. This is called the SABSA Matrix. In fact, this is the SABSA content framework. For service management, a separate matrix is exists.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	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
CONCEPTUAL ARCHITECTURE	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
LOGICAL ARCHITECTURE	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
PHYSICAL ARCHITECTURE	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
COMPONENT ARCHITECTURE	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
SERVICE MANAGEMENT ARCHITECTURE	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

Figure 4: The SABSA Matrix

SABSA Lifecycle

In the SABSA Lifecycle, the development of the contextual and conceptual layers is grouped into an activity called Strategy & 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 & Measure. The significance of the Manage & Measure activity is that once the system is operational, it is essential to measure actual performance against targets, to manage any deviations observed, and to feed back operational experience into the iterative architectural development process. See Chapter 7 (pp 113) of the SABSA Blue Book.

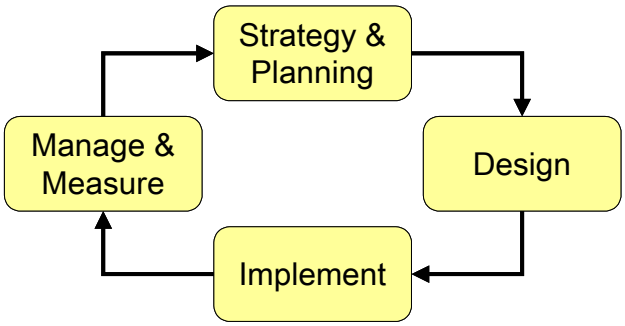

Figure 5: The SABSA Lifecycle

SABSA Business Attribute Profile

The SABSA Business Attribute 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. See Chapter 6 (pp 88) of the SABSA Blue Book.

Business Attribute Profiling can also be used in the TOGAF ADM context. The alignment of the services through the business attributes as described in the SABSA example shown in Figure 6 can be carried out using pure TOGAF artifacts. See Figure 10.

Each SABSA Business Attribute in the example taxonomy shown in Figure 6 is an abstraction of a real business requirement previously encountered in several organizations; most of them encountered many times over. This example taxonomy has emerged from many years of consulting work, and provides generic definitions for each element of the taxonomy. Therefore, it is more than just an example, but also a baseline framework that can assist security architects in taking a comprehensive approach to security requirements definition. The taxonomy serves as a starting point for the development of customized, situation-specific profiles, thus avoiding the "blank sheet of paper" syndrome that can often be such a deterrent in getting started.

Each SABSA Business Attribute in the example taxonomy has a detailed generic definition and some suggested guidelines for applying metrics to that attribute, not included in this overview. A Business Attribute Profile is built by the architects using the taxonomy as a guideline to select the relevant attributes for the business case in hand, redefining each selected attribute in terms of the business case, developing a measurement approach, specific metrics and performance targets, again related to the business case, and adding new attributes and new definitions as required to fulfil the business requirements in the specific case in hand. Thus, although the method is well-defined, the Business Attribute taxonomy can be extended as much as is appropriate and each Business Attribute Profile is highly customized according to the business case being considered by the architecture team.

Business Attribute Profiling is a very powerful tool that allows any unique set of business requirements to be translated, standardized, and normalized into a SABSA format. Each profile selects only those SABSA business attributes that apply to the specific business of the organization (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 Attribute Profile is an important conceptualization of the real business, and forms a core part of the conceptual security architecture. It also serves as a set of "proxy assets" against which a risk assessment can be carried out. Each individual attribute is considered as an "atomic" component of a much more complex "molecular" business capability, which is the primary business asset at risk. (See Operational Risk and its Relevance to Enterprise Architecture below for a more detailed discussion on operational risk management.)

It also allows the selection of metrics that are used to set performance targets as an integral part of the SABSA Business Attribute Profile that can later be measured (e.g., "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. This enables the creation of a real-time operational risk dashboard or scorecard that monitors performance of operational capabilities against the predetermined performance targets, and provides early warnings of up-coming risk events that may require management intervention.

Thus the Manage & Measure activity in the SABSA Lifecycle is based upon the SABSA Business Attribute Profile that was set out during the Strategy & Planning activity, and which has been customized specifically to conceptualize the business of this unique organization.

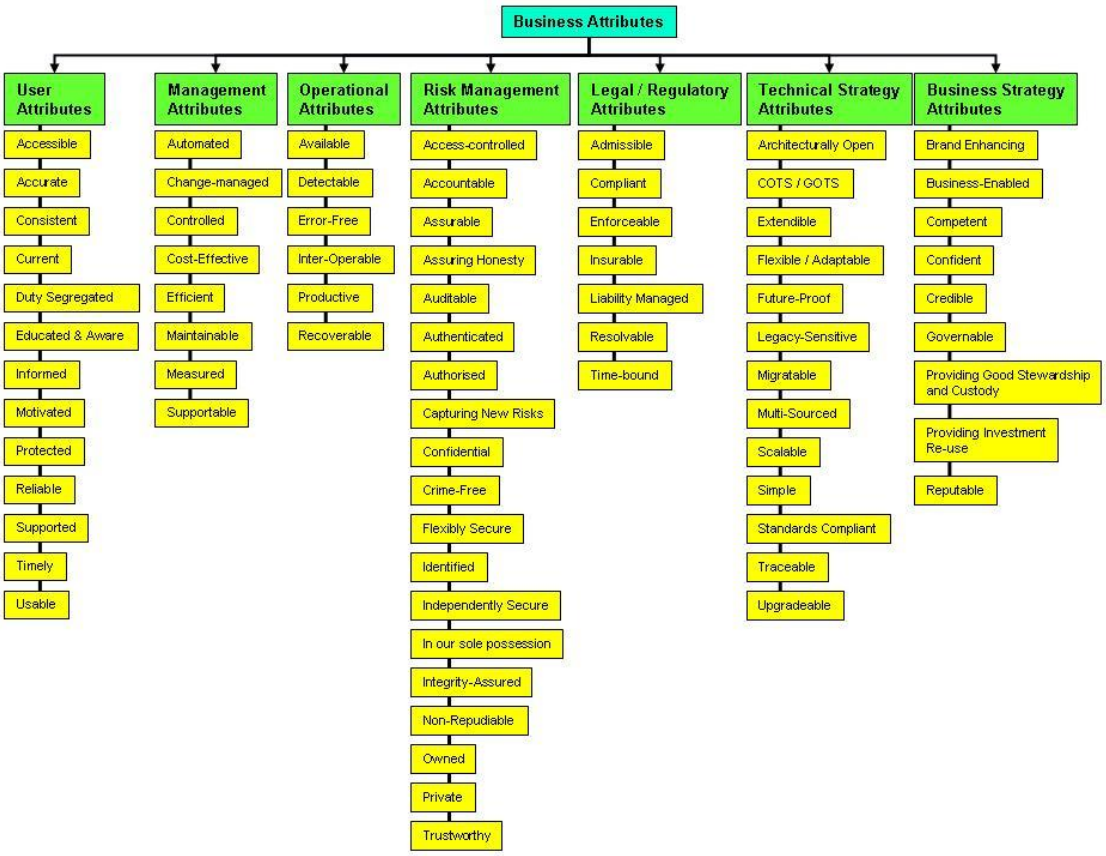

Figure 6: SABSA Business Attribute Taxonomy

What is the TOGAF-SABSA integration approach?

Principles

SABSA and TOGAF are culturally and philosophically very similar, both being business-focused and both having a vision of architecture as an enterprise-wide blueprint. They have different roots and different histories, however, and therefore the actual frameworks are not identical. Each time a particular link is made, it is possible to dispute it when viewing it from a different angle. Mappings that seem obvious for one person make no sense to the other. No trivial, single mapping exists between TOGAF and SABSA that seems logical to all. Making the integration work requires a degree of "can do" attitude and some rules-of-thumb which avoid lengthy detailed discussions without a logical resolution.

In order to achieve a meaningful result in this context, the following rules are applied:

- When an artifact seems to appear at different levels of the architecture, the highest level of abstraction is used for the mapping. This way, the integration keeps its main focus on the enterprise level. And the enterprise level is exactly where SABSA offers added value.
- When two different mappings are both defendable, the most obvious one is used. This is because the majority of the architects' community is likely to accept the most obvious mapping, which makes it more practical.
- The scope of the integration is limited to the elements and concepts that are most important and useful.

The cornerstones of the TOGAF-SABSA integration

The TOGAF-SABSA integration is based on three cornerstones:

1. Risk management is the driver for the selection of security measures – the SABSA approach to operational risk management is business-driven instead of threat-driven. The business-driven approach also considers the risk context in achieving a positive outcome, whereas the threat-driven approach only looks to minimize or eliminate the possibility of a loss event; this is further elaborated in Figure 7. This complementary positive view on risk is an essential basis for the TOGAF-SABSA integration.
2. Requirements management plays a central role in successful architecture development – TOGAF follows a requirements-driven approach and SABSA Business Attribute Profiling provides a powerful technique to capture architectural requirements.
3. The TOGAF Architecture Development Method (ADM) is a popular architecture delivery process – this paper shows which security architecture artifacts are relevant to each phase of the ADM, so that the security architecture becomes an integrated part of the enterprise architecture. This way, SABSA is expressed in TOGAF words, providing a common language between TOGAF and SABSA to facilitate better information exchange between practitioners.

Needless to say, to make the integration of security architecture into enterprise architecture work well, the security architect must be a member of the enterprise architecture team.

Operational Risk and its Relevance to Enterprise Architecture

The approach to risk in SABSA

The IT security and information security industry has evolved over its lifetime a view of operational risk that is concerned only with threats, vulnerabilities, and loss events (negative impacts). The emergence of operational risk management in the banking industry during the 1990s was driven almost entirely from within the IT/information security centers of expertise in banks, and hence this culture of focusing only on threats and losses has now been incorporated into general banking regulations, such as in the definition of operational risk in the Basel Accord.[2] This negative approach to risk management has also found its way into the ISO/IEC 27005:2011 standard [4] on information security risk management, again because of its cultural roots.

However, this entirely negative view of risk is not reflected in the international standards that have evolved from other cultural roots, mainly the development of thinking on corporate governance. In these standards "risk" is seen simply as "uncertainty of outcomes" and "risk management" is presented as striking a balance between positive and negative outcomes resulting from the realization of either opportunities or threats. It is this balanced view of risk that is embedded in SABSA, including the enabling of benefits arising from opportunities as well as the control of the effects of threats.

The three most important risk management standards of major international standing are:

- ISO 31000:2009: Risk Management – Principles and Guidelines

"*ISO 31000:2009 sets out principles, a framework, and a process for the management of risk that are applicable to any type of organization in the public or private sector. It does not mandate a "one size fits all" approach, but rather emphasizes the fact that the management of risk must be tailored to the specific needs and structure of the particular organization.*[3] *It has a related standard ISO/IEC 31010:2009 [5] that describes examples of qualitative risk assessment methods.*"

- M_o_R: Management of Risk (2007), Office of Government Commerce (OGC), UK

"*The M_o_R guide is intended to help organizations put in place an effective framework for taking informed decisions about the risks that affect their performance objectives across all organizational activities, whether these be strategic, program, project, or operational.*"[4]

- Enterprise Risk Management – Integrated Framework (2004), Committee of Sponsoring Organizations (COSO)

"*The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity,*

[2] The Basel Accords refer to the banking supervision accords, which are recommendations on banking laws and regulations.
[3] Source: www.iso.org/iso/iso_catalog/management_standards/specific_applications/specific-applications_risk.htm.
[4] Source: www.mor-officialsite.com/AboutM_o_R/WhatIsM_o_R.asp.

with the potential to erode or enhance value. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value."[5]

In addition, in January 2009 The Open Group Security Forum published its Risk Taxonomy standard [6], which defines a new approach to producing risk assessments based on a technique called Factor Analysis of Information Risk (FAIR). This standard is gaining recognition for producing more quantitative – and therefore more repeatable – results from risk assessments, including for use to complement risk assessments using ISO/IEC 27005:2011.

Definition of Risk

All of the above standards agree closely on the definition of risk. A clear example is the following definition from M_o_R:

"*Risk is an uncertain event or set of events which, should it occur, will have an effect on the achievement of objectives. A risk consists of a combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives.*"

With this definition, "threat" is used to describe an uncertain event that could have a negative impact on objectives or benefits; and "opportunity" is used to describe an uncertain event that could have a favorable impact on objectives or benefits.

Definition of Risk Management

Here again there is broad agreement between these international standards. As an example, ISO 31000:2009 defines risk management as:

"*The systematic application of management policies, procedures, and practices to the tasks of communicating, establishing the context, identifying, analyzing, evaluating, treating, monitoring, and reviewing risk.*"

Operational risk and enterprise architecture

Operational risk is concerned with the threats and opportunities arising in business operations, as opposed to strategic risk or specific financial investment risks such as credit risk or market risk.

Operational risk is relevant within the practice of enterprise architecture because business operations are effected through the processes and systems (people plus technology) that are created through architectural work. The output of architecture work is the creation of operational capability. In this context we take "operational capability" in its broadest sense, including, for example, the capability to make strategic plans, the capability to gather and analyze business intelligence, the capability to manage programs and projects, and many more similar capabilities, the output of which is of strategic benefit rather than merely operational. Nevertheless, these activities are in themselves all "operational" at the point of execution. As a specific example, the failure of a "due diligence" process can lead to the failure of a strategic corporate acquisition because a poor strategic decision is taken. The due diligence process itself is operational, and the failure of such a process is an operational risk, but in this case the outcome is a severe strategic (and probably reputational) negative impact. Thus the enterprise architect must be aware of and design for the business risks that will be faced during the operational lifecycle of these processes and systems. Arguably, the sole role of

[5] Source: www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf.

the enterprise architect is to create an operational environment in which operational risk can be optimized for maximum business benefit and minimum business loss.

Operational risk management and SABSA

SABSA is an architectural and operational framework for reaching out to opportunities and enabling positive outcomes to attain defined business targets, thus achieving operational excellence in processes, people, and technical systems and managing negative outcomes of loss events to within an enterprise's tolerance towards risk – namely their risk appetite.

SABSA defines operational risk as follows:

"*Operational risk is the set of risks that includes the opportunities to attain business benefits through operational excellence in processes, people, and technology, and the threats of loss originating from inadequate or failed internal processes, people, and technology or from external events, or systemic failures. In all cases, although the threats are restricted to the operational domain, negative impacts may include both strategic failure and reputation damage.*"

Assets at risk

The output of architecture work is the creation of operational capability. See Operational risk and enterprise architecture above. In SABSA thinking these operational capabilities are the primary assets at risk. Examples of such assets include:

- Production capability
- Service delivery capability
- Marketing capability
- Sales capability
- Financial management capability
- People management capability
- Capability to satisfy customers
- Capability to build and sustain brands and reputation

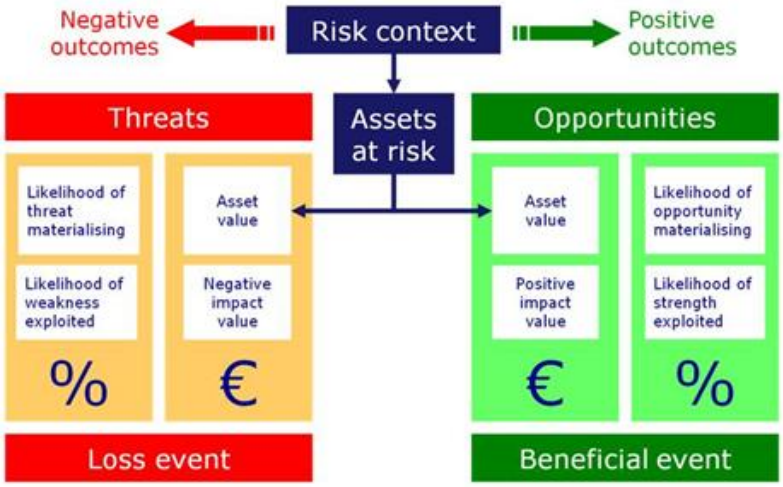

Figure 7: The SABSA Operational Risk Model

In traditional information and IT risk management frameworks (such as those mentioned earlier and exemplified by ISO/IEC 27005:2011) the assets at risk are usually classified as information assets (databases, files, documents, etc.) and IT assets (computer hardware, software, communications networks, etc.). These are regarded in SABSA as secondary assets, supporting the primary assets of business capability. SABSA risk assessment, risk measurement, and risk monitoring focuses on the primary assets, not these secondary assets.

In this respect SABSA is leading-edge thinking, challenging the traditional IT view of operational risk management, but aligning operational risk with true business risk. The business-to-IT alignment that has been so elusive in most IT methodologies is therefore achieved in SABSA by the application of this business risk view.

A Central Role for Requirements Management

Requirements management plays a central role in architecture work. This is recognized in both TOGAF and SABSA. The TOGAF method validates and updates business requirements in every stage of an architecture development project. However, TOGAF does not provide a concrete technique for describing or documenting requirements. In contrast, SABSA presents its unique Business Attribute Profiling technique as a means to effectively describe requirements. This section describes the use of Business Attribute Profiling with respect to security requirements management, along with the added value this technique offers for requirements management in general. Together, the TOGAF concept of validating architecture and validating and updating requirements based upon information uncovered during the development of the architecture and SABSA's Business Attribute Profiling improve requirements management, traceability, and architecture development.

Architecture in general should provide continuous alignment of capabilities with business goals and support achieving these goals in an effective and efficient manner, even when the environment or business goals change. This alignment is in many cases the major rationale for using methodologies such as TOGAF and SABSA and therefore both frameworks define a requirements management process to ensure this continuous alignment.

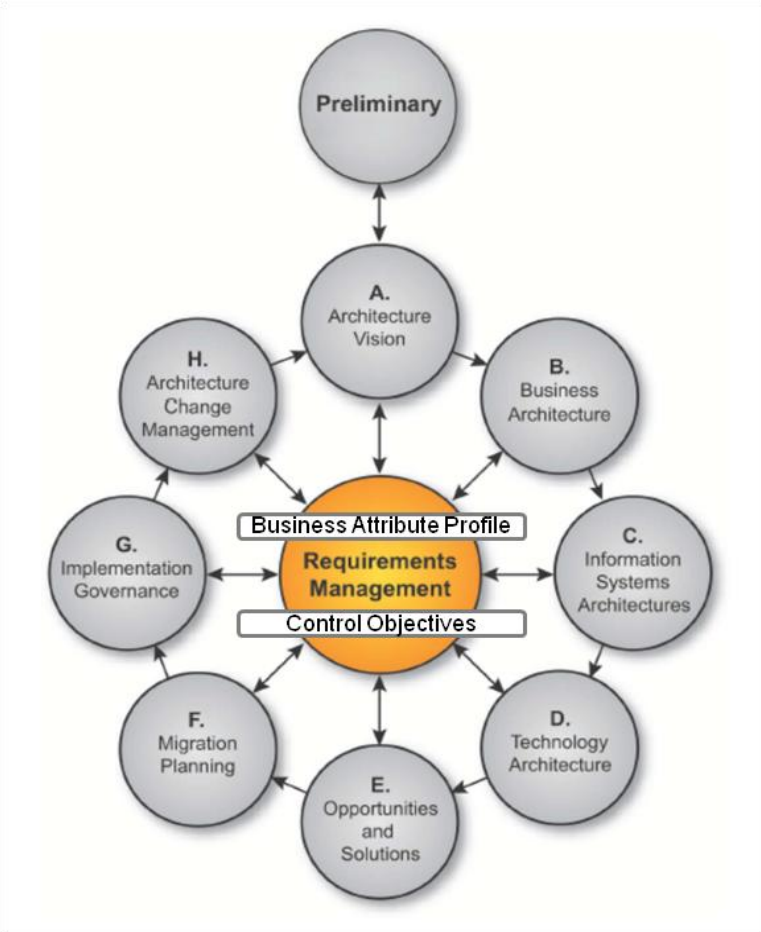

Figure 8: The Central Role of Requirements Management in TOGAF ADM

Introduction to requirements management

The purpose of requirements management in the context of this White Paper is to identify, store, maintain, and communicate business requirements through the different phases of architecture development by means of a controlled and repeatable process. Additionally, in the Manage & Measure phase of the SABSA Lifecycle, operational performance is monitored against target requirements. This is not explicitly addressed in the TOGAF ADM but lies within Phase H: Architecture Change Management, and the continual validation of requirements management. Operational performance is explicitly within the scope of the Information Security Management Maturity Model standard (O-ISM3) [7] of which there is further discussion later in this paper.

The ability to deal with changes in requirements is crucial. Architecture is an activity that by its very nature deals with uncertainty and change – the "grey area" between that to which the stakeholders aspire and what can be specified and engineered as a solution. Architecture requirements are therefore invariably subject to change. Moreover, architecture often deals with external drivers and constraints, many of which by their very nature are beyond the control of the enterprise (changing market conditions, new legislation, etc.), and which can result in changes in requirements in an unforeseen manner.

The TOGAF Requirements Impact Assessment supports handling these changes. It assesses the impact on the current architecture requirements and specification to identify changes that should be made and the implications of those changes.

The world of requirements management is rich with emerging recommendations and methodologies for requirements engineering. TOGAF does not mandate or recommend any specific process or tool; it simply states what an effective requirements management process should achieve (i.e., the "requirements for requirements management"). In contrast, SABSA does have its own requirements engineering technique in the form of Business Attribute Profiling, which is explained in the next paragraph.

Business Attribute Profiling

Business Attribute Profiling is at the heart of the SABSA framework. It is a requirements engineering technique that translates business goals and drivers into requirements using a risk-based approach. Some important advantages of this technique are:

- Executive communication in non-IT terms
- Grouping and structuring of requirements, which facilitates understanding and oversight by architects, analysts, and other stakeholders
- Traceability mapping between business drivers and requirements

Each business capability can be regarded as a complex "molecular" structure comprising many "atomic" parts. Business Attribute Profiling decomposes the complex molecule into its atomic parts. Each atomic part is a single business attribute. Examples of business attributes are:

- Confidential
- Available
- Accurate

- Authorized
- Supportable
- Flexible

Each business attribute is defined in terms that are meaningful to the business of the specific enterprise, the so-called taxonomy of business attributes. An example taxonomy of attributes is provided in the SABSA documentation, along with generic definitions (already discussed earlier in this paper). This taxonomy is for example purposes only, and the concept of a Business Attribute Profile is that new attributes can be defined to suit the specific business goals. Not every attribute in the example taxonomy may be applicable to a particular business. Every Business Attribute Profile is customized to represent the requirements of a specific business capability in a specific enterprise. This means that each business capability or set of capabilities will attract a specific Business Attribute Profile.

If a business decides that a given attribute is relevant to a capability (primary asset) then there must be a means by which it can be measured – answering the question: at what point do we have enough of this attribute to satisfy our needs? This is achieved by defining a measurement approach, a specific metric (or metrics), and a performance target for that attribute in terms of the specific metric(s).

Thus, Business Attribute Profiling is the conceptualization of the primary business assets and is used to represent the business requirements for a given business capability. It enables enterprise architects to consult business capability owners and to translate their business requirements into a standardized, normalized format that can be worked on by technology designers and process engineers to build the capability according to the real business needs. Because these requirements have been quantified, it is also possible to determine the effectiveness and efficiency of the capabilities, and to monitor actual performance of the processes and systems during the operational lifecycle.

This methodology is powerful and one which TOGAF may find useful to include so as to satisfy the requirements management process.

Requirements management in SABSA using Business Atributes Profiling

In an effective security architecture, each business driver should be fully supported by security services. In an efficient security architecture, each security service should be justified by a business driver and perform with minimal costs. Traceability from business driver to security service and *vice versa* is key. This is achieved by relating the different artifacts together, and defining the quality of each relationship.

According to ITIL,[6] a Service Catalog is:

"*A document produced by the IT department for the information of its customers and users. It provides a brief overview, in business terms, of all the business and infrastructure services offered by the IT provider and may include service charges. This information, together with more detailed technical knowledge, will be maintained for internal use.*"

In analogy to this definition, a "Security Services Catalog" is an overview in business terms of the provided set of security services. To illustrate the value of Business Attribute Profiling, this section demonstrates how to define a security services catalog that best serves the business needs.

[6] Information Technology Infrastructure Library (ITIL); refer to: www.itil-officialsite.com.

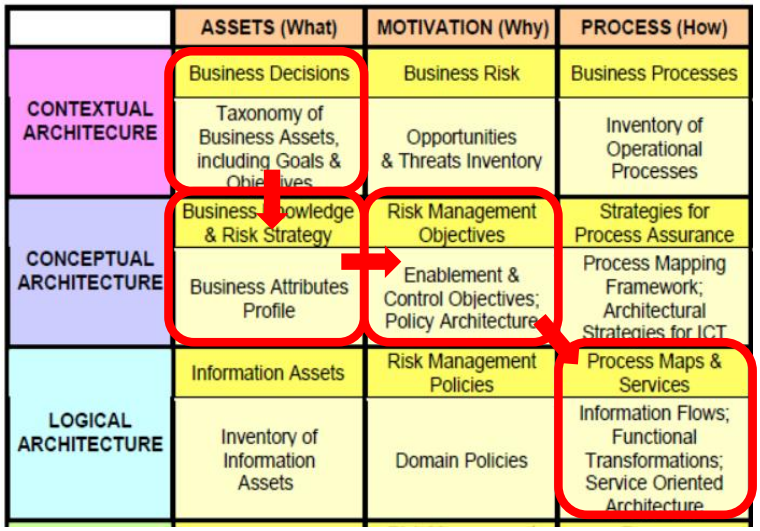

Figure 9: Alignment in the SABSA Matrix between Business Drivers and Services through Business Attribute Profiling

Figure 9 shows the key role that the Business Attribute Profile plays. It organizes and adds business context to the control objectives (*a.k.a.* security requirements), indirectly defining the relationship with the security services. It also is directly linked to the business drivers in the Contextual Layer. Readers should realize that the arrows reflect a bundle of all the actual relationships between the entities present in both boxes.

The following SABSA artifacts are linked together to provide the traceability from business needs to security services:

- Business Decisions: Business Drivers, Taxonomy of Business Assets, including Goals & Objectives.
- Business Attribute Profile: Expressing the assets that need protection.
- Risk Management Objectives: Enablement and Control Objectives, a set of specific security requirements. These control objectives can be selected from a relevant control framework, such as ISO/IEC 27001:2005 [8] or COBIT [9], as long as they are justified by the Business Attribute Profile. However, SABSA encourages a broader view by mentioning "enablement objectives" as well, which specifically relate to enabling an opportunity.
- Process Maps and Services: The Security Services Catalog, an overview of the security services that are defined to meet the security requirements.

Requirements management in the TOGAF ADM using Business Attribute Profiling

Business Attribute Profiling can also be used in the TOGAF ADM context. The alignment of the services through the business attributes as described in the SABSA example above can be carried out using pure TOGAF artifacts. See Figure 10.

This is how it works:

- **Business-related Artifacts**: Normally, the business principles, business goals, and strategic drivers of the

organization are already defined elsewhere in the enterprise. If so, the activity in Phase A: Architecture Vision involves ensuring that existing definitions are current and clarifying any areas of ambiguity. If not, it involves defining these essential items for the first time. Business scenarios can be used to discover and document business requirements. See TOGAF 9 for more detail.

In TOGAF, the key interests that are crucially important to architecture stakeholders are called concerns. Concerns are captured in Phase A and may pertain to any aspect of the system's functioning, development, or operation, including considerations such as performance, reliability, security, distribution, and scalability. Addressing these concerns determines stakeholder buy-in and the acceptability of the architecture and resulting systems.

- **Business Attribute Profiling**: This describes the level of protection required for each business capability (see Business Attribute Profiling earlier in this paper).
- **Requirements Catalog**: This stores the architecture requirements of which security requirements form an integral part.

  The Business Attribute Profile can form the basis for all quality requirements (including security requirements) and therefore has significant potential to fully transform the current TOGAF requirements management approach.
- **Business and Information System Service Catalogs**: TOGAF defines a business service catalog (in Phase B: Business Architecture) and an information system service catalog (Phase C: Information Systems Architecture). The creation of the information system services in addition to the core concept of business services is intended to allow more sophisticated modeling of the service portfolio.
- The **Security Service Catalog**: As defined by the SABSA Logical Layer, this will form an integral part of the TOGAF Information System Service Catalogs.

As described above, SABSA Business Attribute Profiling can be used within a TOGAF-based architecture, using only TOGAF artifacts. When doing so, the scope of the Business Attribute Profile can easily be expanded to address all relevant business requirements and not just the security attributes. This approach, in which Business Attribute Profiling is applied to the entire ADM requirements management process, provides a significantly more robust method than is currently specified within the TOGAF standard, and ensures that the TOGAF goal of business alignment can realistically be achieved.

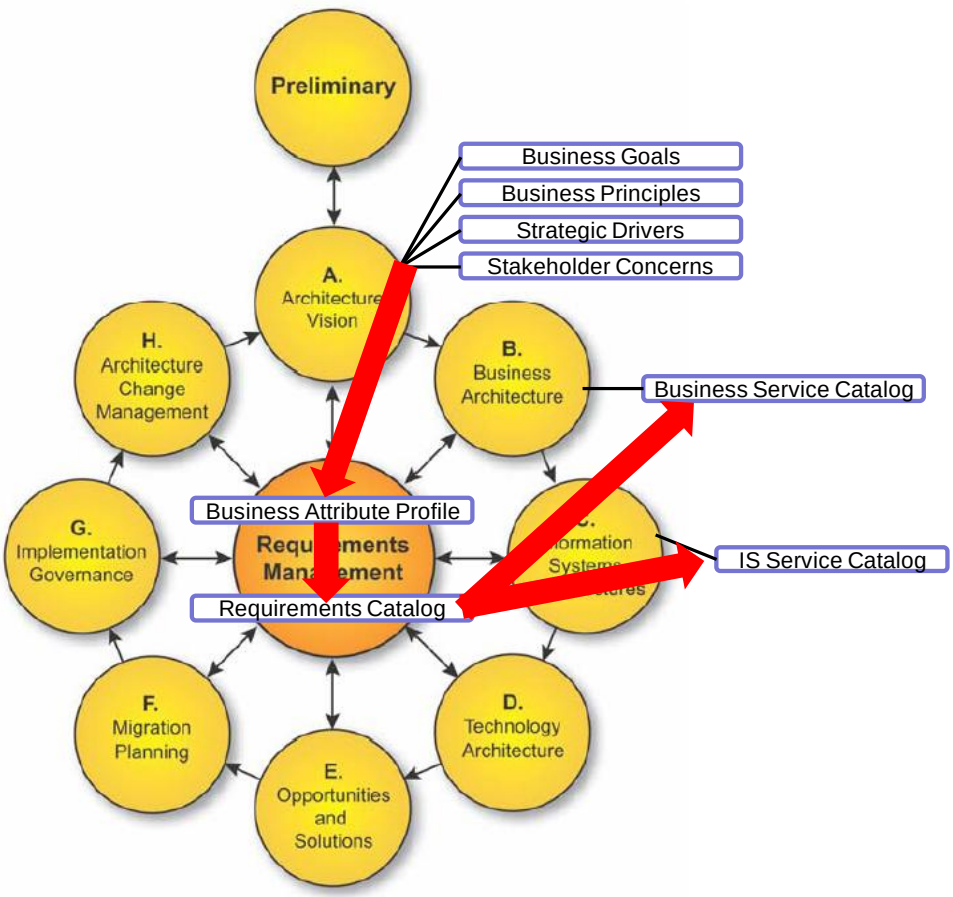

Figure 10: Requirements Management in TOGAF using SABSA Business Attribute Profiling

Requirements management in the TOGAF Content Metamodel using business attributes

The main purpose of the TOGAF Content Metamodel is the documentation of relationships between entities. When using the new Business Attribute Profile entity, this metamodel will need to be augmented to ensure it is complete. The rough position of the Business Attribute Profile and the relationships within the metamodel are given in Figure 11.

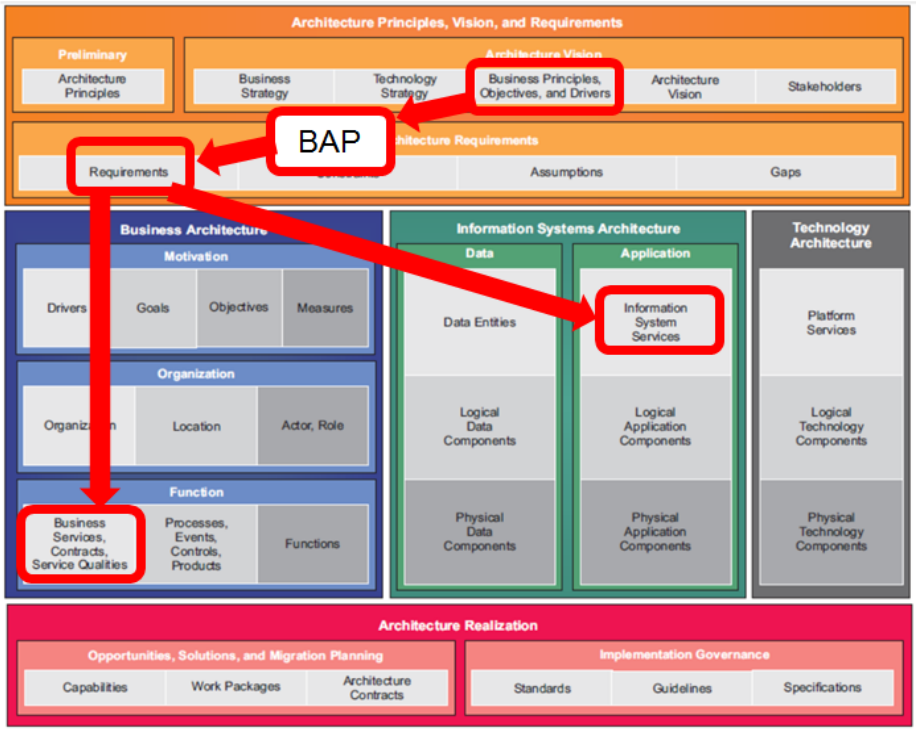

Figure 11: The Business Attribute Profile Mapped onto the TOGAF Content Metamodel

The most suitable location in the current metamodel for the Business Attribute Profile is in the Motivation Extension, at the location of the object "Goal". Goal has exactly the right relationships, namely with Driver (compare with SABSA business driver) and "Objective" (compare with SABSA control objective).

The object Goal has the following object attributes which also apply to the Business Attribute Profile:

- ID (Unique Object Identifier)
- Name (brief name of the object)
- Description (textual description of the object)
- Category (user-definable categorization taxonomy)
- Source (location where the information was collected)
- Owner (owner of the architecture object)

The object attributes that should be added for the Business Attribute Profile are:

- Measurement approach (for example, measure capacity usage)
- Specific metric(s) (for example, number of gigabytes of storage available)
- Performance target (for example, at least 20% available at least 95% of the time)

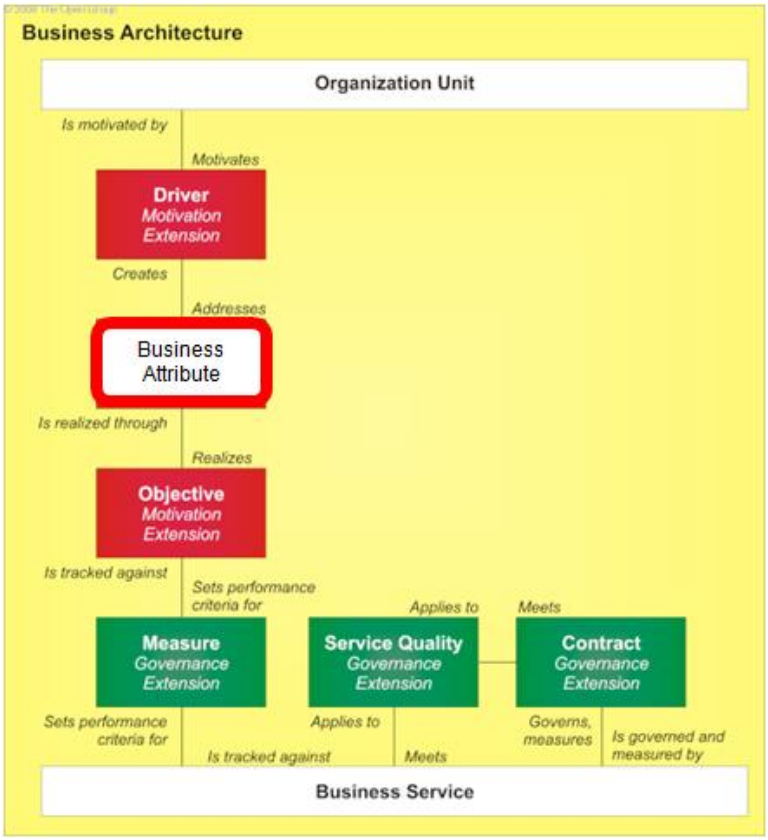

Figure 12: The Business Attribute Profile Position in the TOGAF Content Metamodel Motivation Extension

Creating an Enterprise Architecture with Integrated Security

The ultimate goal is that the security architecture is fully integrated in the enterprise architecture. The TOGAF Architecture Development Method (ADM) is the heart of TOGAF and is therefore the designated place to integrate the security architecture. The following sections describe the way SABSA can be integrated into the ADM. Both SABSA and TOGAF are business-driven; therefore, it is only natural to use this business-driven aspect as the binding element between the two.

It should be noted here that as mentioned in the Executive Summary to this White Paper, in December 2005 The Open Group Security Forum submitted a White Paper (W055: Guide to Security Architecture in TOGAF) to the Architecture Forum expressing similar intent regarding integrating security and risk management into TOGAF. This was included in TOGAF 9 but not in the integrated manner that the Security Forum had intended. The Security Forum is revising W055 to submit as complementary to this TOGAF and SABSA Integration White Paper.

SABSA Lifecycle and TOGAF ADM

Just as the ADM is the core process model of TOGAF, so is the SABSA Lifecycle the core process model of SABSA. Mapping one to the other, it becomes obvious that both models have partly overlapping and partly differing phases. TOGAF is all about managing the change and migration of an enterprise architecture from one state to another. SABSA is about creating a new state for the security architecture as well as maintaining that new state during business operations. The latter is the link to the operational and exploitation phase of the security architecture, and in this regard this SABSA phase aligns with O-ISM3. In comparison, this operation is included in Phase H: Architecture Change Management and the continuous requirements management process in TOGAF – as a continual monitoring and change management activity to ensure that the architecture responds to the needs of the enterprise and maximizes the value of the architecture to the business.

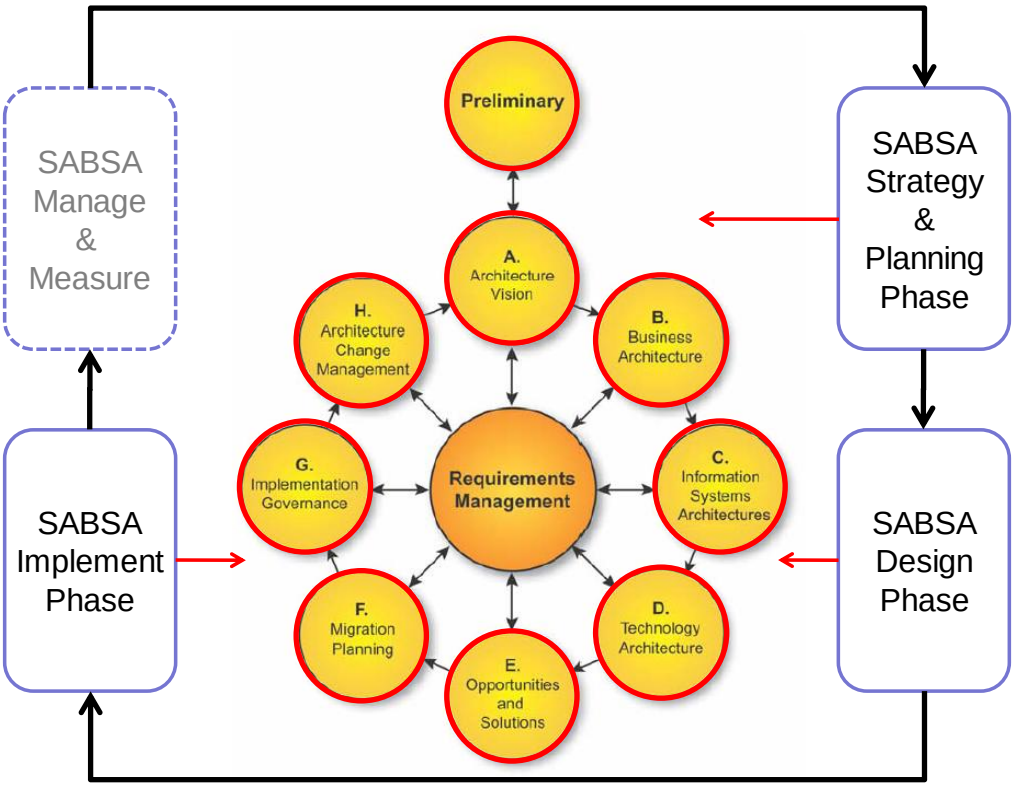

Figure 13: SABSA Lifecycle Phases Mapped to the TOGAF ADM

This helicopter view of both process models identifies possible overlapping areas.

Architecture scope and abstraction layers

When trying to map a SABSA security artifact to a particular ADM phase, differences in abstraction level definitions lead to discussion. For example, an access control policy is usually produced at the Information Systems Architectures phase (Phase C) of a solution architecture, but in an enterprise architecture, this is too much detail and left to the Implementation Governance phase (Phase G). How do we cope with this?

Formally, the TOGAF ADM should only be applied at the enterprise level. TOGAF defines the Strategy – Segment – Capability concept to narrow down the scope of the enterprise. The framework is not equipped for solution architectures. The phase that comes closest to a solution architecture is Phase E: Opportunities & Solutions of a capability architecture, but this produces a roadmap rather than an implementation design or plan. The actual design of specific technical solutions is out of scope for TOGAF.

In practical applications, however, TOGAF often mixes enterprise and solution architectures. The TOGAF ADM may be applied at different enterprise layers but also at the solution level. In fact, in TOGAF 9 a capability can be at enterprise level as well as solution level, depending on the scope of the project. This sometimes leads to ambiguities in the scoping of a TOGAF-based enterprise architecture design.

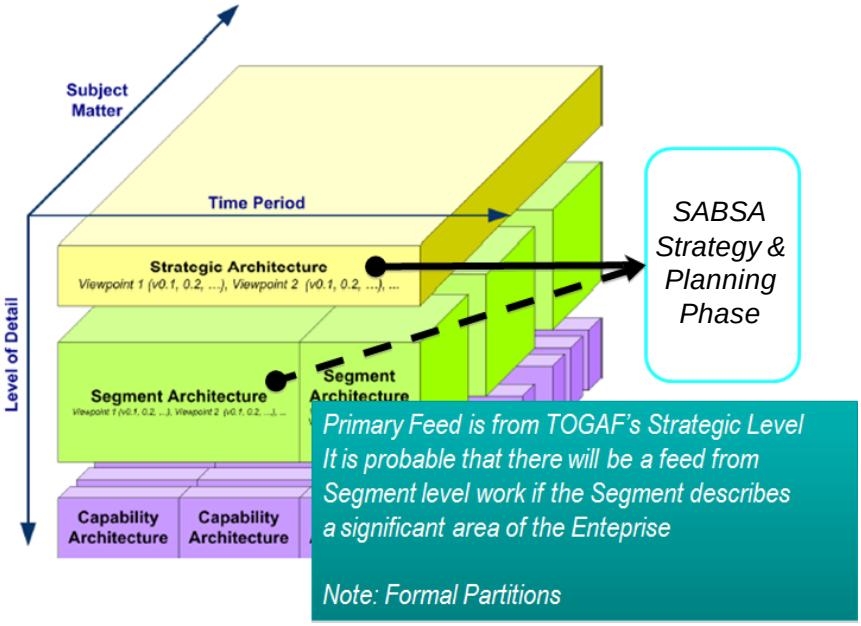

Figure 14: Mapping TOGAF and SABSA Abstraction Layers

SABSA scopes architectures using the Domain Modeling technique and this covers all SABSA phases in the SABSA Lifecycle. As the SABSA phases extend beyond the core phases of the TOGAF ADM, the scoping provided by the SABSA Domain Model extends beyond these core phases of TOGAF, both in terms of solution design and system and process management during the operational lifecycle. The relationship between these two scoping approaches is shown in Figure 15.

What this diagram means is that SABSA Domain Modeling is so generic and versatile that it can be applied to the enterprise in almost any relevant conceptual dimension. For example, taking the organizational dimension, the SABSA super-domain/sub-domain hierarchy would run something like: extended enterprise/enterprise/business unit/line of business/department/team. Another possible domain dimension could be functional roles within the enterprise organizational structure, and for those organizations that deploy "matrix management" (functions *versus* business processes) the domain modeling technique works extremely well. Yet another domain hierarchy can be based on views of the enterprise from a strategic/tactical/operational lifecycle dimension. Domain modeling is so flexible as to not require the formal definitions that TOGAF uses for various scopes. SABSA allows the architect to define scopes entirely based on business need with no predetermined framework to constrain the model. Another advantage to this flexibility is the inheritance of Business Attribute Profiles down through a domain hierarchy, but a description of this concept is well beyond the scope of this White Paper.

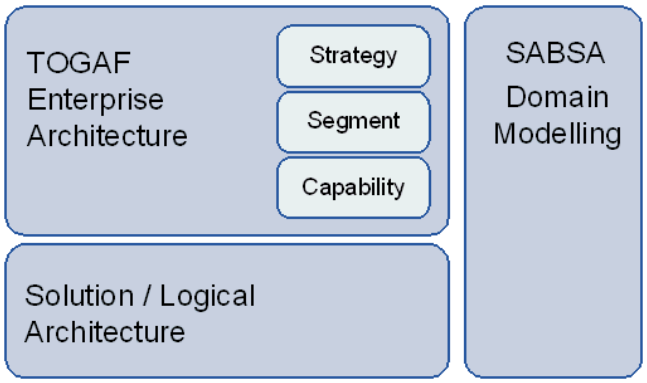

Figure 15: Mapping of TOGAF to SABSA Strategy & Planning Phase

For this TOGAF-SABSA integration White Paper, if an artifact could in theory be mapped against different levels of architectures, the enterprise level is always chosen above the solution level. Where applicable, these scoping and levelling consequences are mentioned for each security artifact.

Artifacts that make up an enterprise security architecture

The ADM contains the concept of artifacts that are consumed or produced by each phase. To match this, SABSA is also split up into artifacts and divided over the TOGAF phases. This way, SABSA is expressed in TOGAF words which will ensure correct embedding of the relevant SABSA components at the appropriate ADM phases.

This means that for the proper integration of TOGAF and SABSA, a subset of SABSA concepts and artifacts will be used. Only SABSA artifacts are selected that are:

- Security-specific (not general architecture)
- Architecture-related (not specific security measures)
- Well defined in the SABSA Blue Book or in later publications that are widely and easily available (clear reference for guidance)
- Relevant to the ADM phases (on enterprise level)

A complete overview of all selected SABSA artifacts is given in Figure 16.

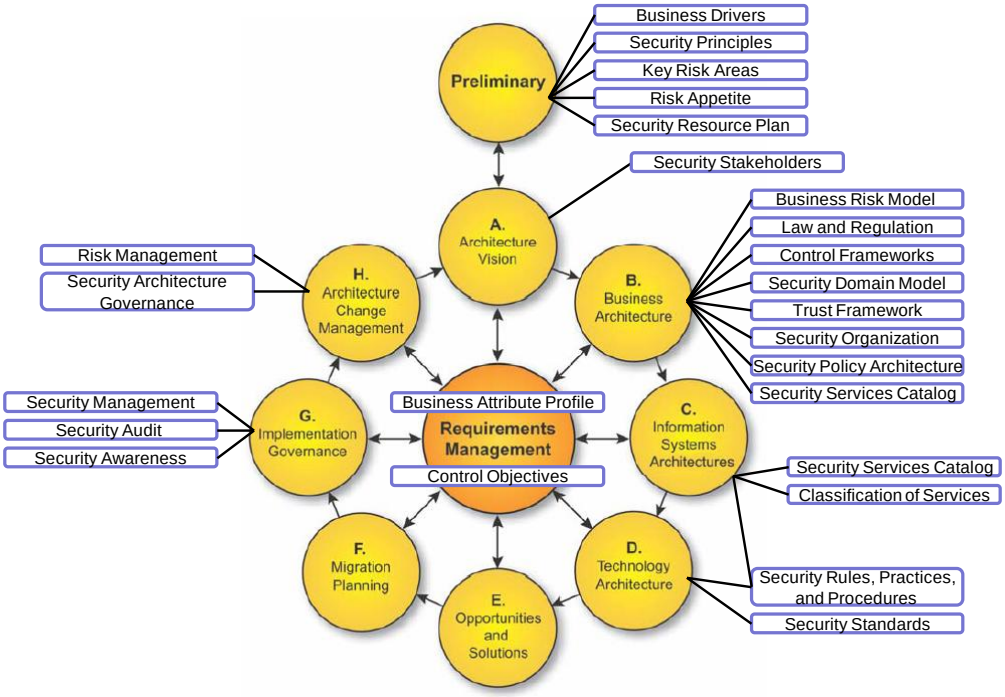

Figure 16: Overview of Security-Related Artifacts in the TOGAF ADM

These security artifacts are explained in more detail in the following sections for each TOGAF phase.

ADM security artifacts by phase

Preliminary Phase

The Preliminary Phase establishes the security context required to guide the security architecture design.

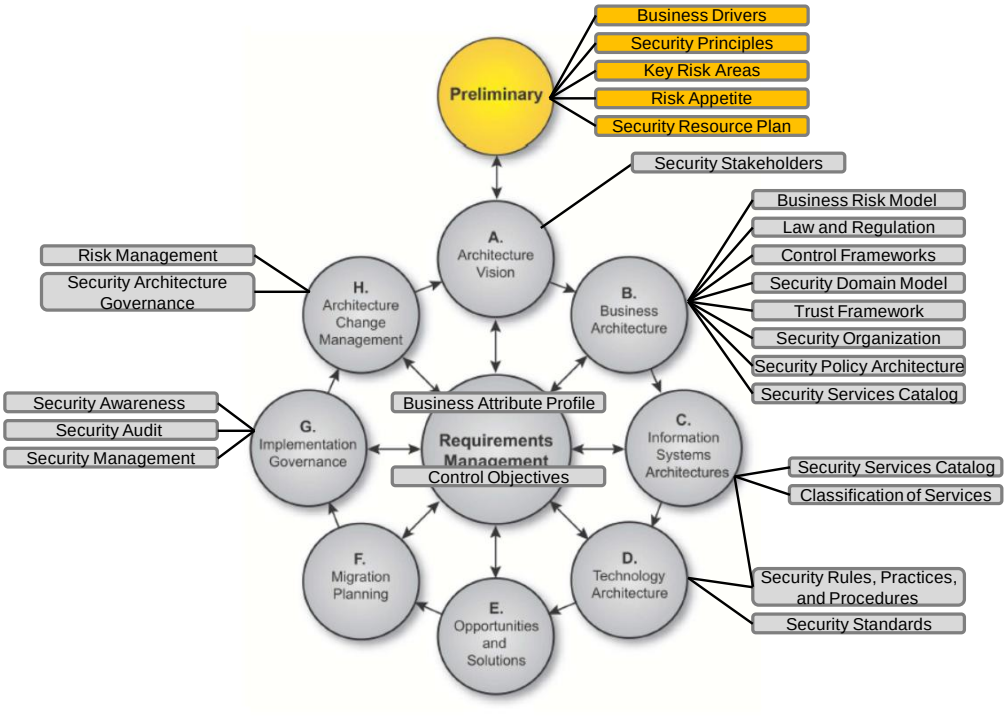

Figure 17: Security Artifacts in the Preliminary Phase

To build the security context, the following security artifacts need to be determined during this phase. These artifacts can be integrated into existing architecture documentation, but it is important that they be properly identified and that they convey the necessary information to make quality decisions:

- **Business Drivers for Security** – the subset of TOGAF business drivers impacting security, presented as an integral part of the overall architecture business drivers artifact or deliverable.
- **Security Principles** – the subset of Business Principles addressing security architecture. This is presented as an integral part of the overall Architecture Principles artifact or deliverable. Security principles like other architecture principles will provide valuable guidance to making business decisions to comply with the enterprise's risk appetite.
- **Key Risk Areas** – the list of the key risk areas within the architecture scope. The key risk areas should be related to the business opportunities which the security architecture enables using the risk appetite artifact which informs the balance of risk *versus* opportunity. The key risk area should be included in the overall architecture risk management deliverable produced during the Preliminary Phase.
- **Risk Appetite** – describes the enterprise's attitude towards risk and provides decision-making guidance to the organization to balance the amount of risk taken to achieve an expected outcome. The risk appetite

could be expressed as, for example, a boundary on a risk/business impact and likelihood grid, profit, and loss measures or qualitative measures (zero tolerance for loss of life or regulatory compliance breaches). Risk appetite can also be represented by suitably worded security principles or produced as a stand-alone deliverable if a key stakeholder exists who needs to specifically approve it. It defines the level of risk (damage) that the organization is willing to accept and what their strategy is in defining this level. For risks above this acceptable level, it defines the strategy used for mitigation (transference, avoidance).

- **Security Resource Plan** – based on the content of the artifacts and the characteristics of the planned architecture project, it must be decided during the Preliminary Phase which security resources are required to deliver the security elements. Finding answers to the following questions through sufficient stakeholder analysis in the Preliminary Phase can help determine the security-related effort required:
    - Do key and influential security or risk-related stakeholders exist who require specific security views?
    - Does the architecture address high-risk areas or is the risk appetite low which warrants security subject matter expertise?
    - Can security support be requested on an as-needed basis from an existing security team or are dedicated security architecture resources required as part of the overall architecture team?
    - How many security resources would be needed?

During the Preliminary Phase it is decided which security artifacts are really needed in the enterprise architecture and which will be created by whom. It might not be necessary to deliver all security artifacts in order to address security properly. The reverse applies too: delivering all artifacts does not guarantee that security is taken care of properly – more artifacts may be required.

For enterprise-level architectures, the artifacts need to be created based on discussions with key stakeholders; preliminary assessments carried out by the architecture team; and assessing relevant statutes, applicable jurisdictions, legislation, and regulations.

For solution-level architectures, existing sources might be available. For instance, an enterprise-level security policy or risk assessment describes the security principles, risk appetite, and key risk areas for a particular solution context.

Phase A: Architecture Vision

In general, Phase A: Architecture Vision describes enough of the TOGAF ADM Phases B, C, and D to ensure that key stakeholders can agree to the end-state which represents a solution to a defined problem.

In Phase A sufficient security-specific architecture design is carried out to:

- Satisfy the security stakeholders that the end-state does not represent any unknown or unacceptable risk and aligns with corporate policies, standards, and principles
- Satisfy business stakeholders – in particular those who control the budget – that the security architecture is instrumental in enabling and supporting the overall architecture required to deliver the business opportunities and benefits identified

In Phase A, it is essential to identify the complete list of all (including security-related) stakeholders and to determine their requirements for approval of the architecture engagement. This might simply involve the validation of the stakeholder analysis carried out in the Preliminary Phase or require a more involved activity to identify the stakeholders with informal power to influence approval.

The stakeholder requirements for approval are gathered to determine the security blueprint needed to address the various concerns the stakeholders may have. The security blueprint is defined at a high level giving sufficient assurance to the stakeholders that the final artifacts and deliverables will address their concerns appropriately. The subsequent three TOGAF phases complete the blueprint and add the required detail.

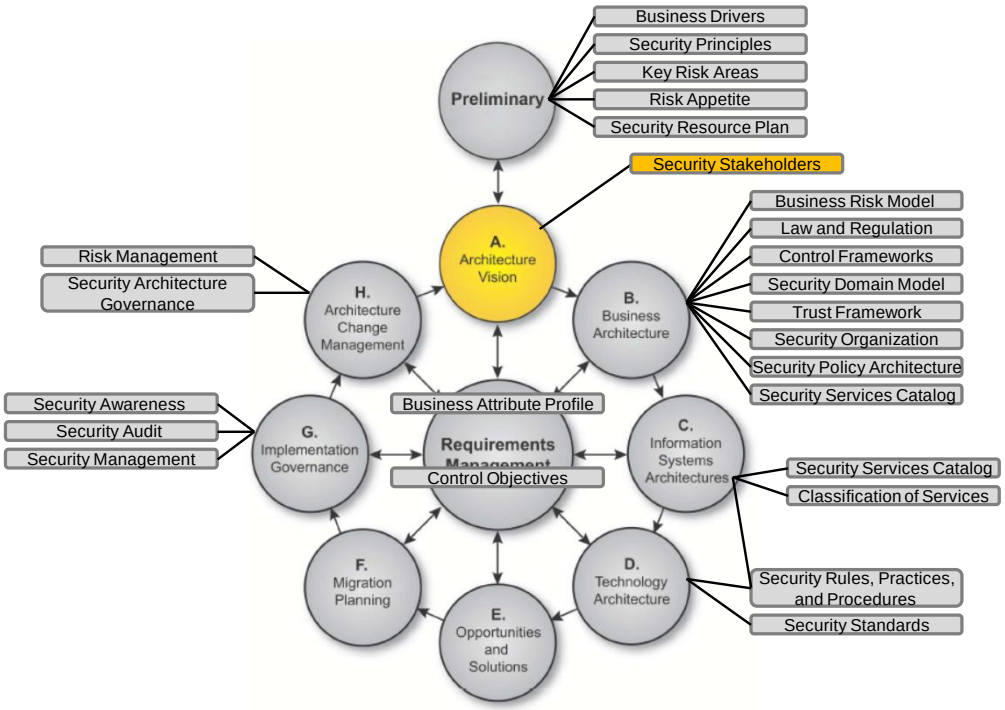

Figure 18: Security Artifacts in Phase A: Architecture Vision

In some cases stakeholders may insist on a business case which describes the benefits of the security architecture, such as reduced risk and enablement of the overall architecture. The Business Attribute Profile[7] can be useful as a basis for the business case. As a specific Business Attribute Profile may not yet be available, the SABSA-provided Business Attribute Profile can be used as a starting point. If this does not fit the business case, a scenario-based approach may be used to obtain stakeholder approval.

The views and business cases must build on the outputs from the Preliminary Phase such as security principles, drivers, key risk, and risk appetite/strategy and should be an integral part of the overall Architecture Vision deliverables.

It is important to keep the evidence of stakeholder and budget approval at hand to justify continued security architecture development in case of changes to the overall environment or architecture engagement. This output could also be used to communicate the impact changes to the stakeholders and budget when business or external drivers change.

[7] See Chapter 6 (pp 87-97) of the SABSA Blue Book

Phase B: Business Architecture

The security elements of Phase B: Business Architecture comprise business-level trust, risk, and controls, independent from specific IT or other systems within the specific scope of the architecture engagement.

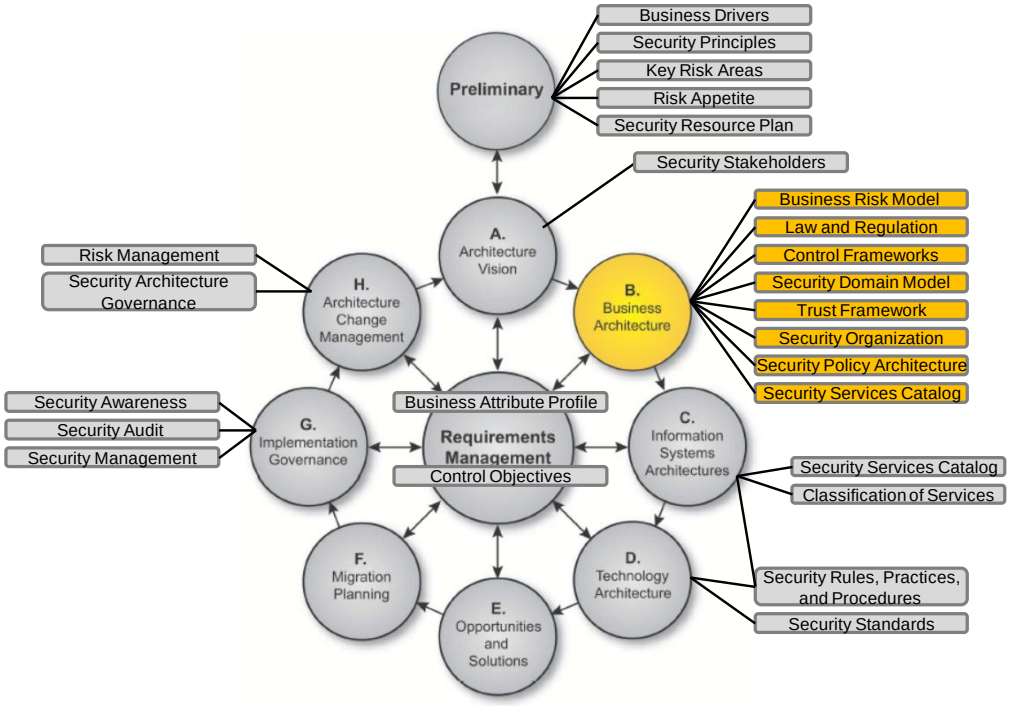

Figure 19: Security Artifacts in Phase B: Business Architecture

The security-related Business Architecture artifacts are:

- **Business Risk Model**[8] – the business risk model determines the cost (both qualitative and quantitative) of asset loss/impact in failure cases. It is the result of a risk assessment, based on identified threats, likelihood of materializing, and impact of an incident. Business impact should be aligned with the definitions in the Business Attribute Profile which act as pseudo-assets. Security classification should be carried out at this stage based on the risks identified. The business risk model is a detailing of the risk strategy of an organization. All information in the enterprise should have an owner and be classified against a business-approved classification scheme. The classification of the information determines the maximum risk the business is willing to accept, and the owner of the information decides what mitigation is enough for his/her information. These two aspects determine the context for the business risk model.

[8] See Chapter 9 (pp 189-209) of the SABSA Blue Book.

- **Applicable Law and Regulation** – determines the specific laws and regulations that apply within the scope of the enterprise architecture engagement.
- **Control Frameworks** – determine the suitable set of control frameworks that would best satisfy the requirements and address the risks related to the engagement scope and context.
- **Security Domain Model**[9] – a security domain represents a set of assets in the engagement scope which could be described by a similar set of business attributes (i.e., a security domain has a set of very similar business attributes for all entities in that domain). The security domain model describes the interactions between the various domains, parties, and actors and must be aligned with the Business Architecture model. This includes defining all people, processes, and system actors known at this stage, including third parties and external actors. The security domain model helps in defining responsibility areas, where responsibility is exchanged with external parties and distinguishes between areas of different security levels and can inform the engagement scope, as shown Figure 15.
- **Trust Framework**[10] – the trust framework describes trust relationships between various entities in the security domain model and on what basis this trust exists. Trust relationships can be unidirectional, bidirectional, or non-existent. The onus for assessing trust is the responsibility of those choosing to enter into the contracts and their legal counsel. It is important to note that technology (e.g., digital certificates, SAML, etc.) cannot create trust, but can only convey in the electronic world the trust that already exists in the real world through business relationships, legal agreements, and security policy consistencies.
- **Security Organization** – the corporate organization of risk management and information security which assigns ownership of security risks and defines the security management responsibilities and processes. Security management processes include risk assessment, the definition of control objectives, the definition and proper implementation of security measures, reporting about security status (measures defined, in place, and working) and the handling of security incidents.
- **Security Policy Architecture**[11] – the security policy architecture addresses the alignment of operational risk management in general with the various security aspects such as physical security, information security, and business continuity. Within the scope of the architecture engagement, decide which existing policy elements can be re-used or have to be developed new. The hierarchy should map the policy development to the various stages in the ADM.
- **Security Services Catalog** – a list of security-related business services, defined as part of the Business Services Catalog.

[9] See Chapter 9 (pp 266-272) of the SABSA Blue Book.
[10] See Chapter 10 (pp 254-265) of the SABSA Blue Book.
[11] See Chapter 11 (pp 293-294) of the SABSA Blue Book.

Phase C: Information Systems Architecture

The security elements of Phase C: Information Systems Architectures comprise information system-related security services and their security classification.

The artifacts described in more detail are:

- **Security Services Catalog** – a list of services which provide security-specific functionality as part of the overall information system architecture. It is mapped to the principles, drivers, risks, and threats determined in earlier phases to provide traceability and justification. The Security Services Catalog must be produced both for the existing and target situation if a gap analysis has to be carried out. The Security Services Catalog can be produced based on the reference list given in the SABSA Blue Book.[12] This list is part of the SABSA Logical Layer and needs to be amended to fit the scope and abstraction level of the TOGAF architecture project. For instance, a security policy service might be needed as a security measure for enterprise-level TOGAF architectures, but is likely to be available as input for solution or logical service architectures. When integrating TOGAF and SABSA, the security services become part of the TOGAF Information System Services Catalog.

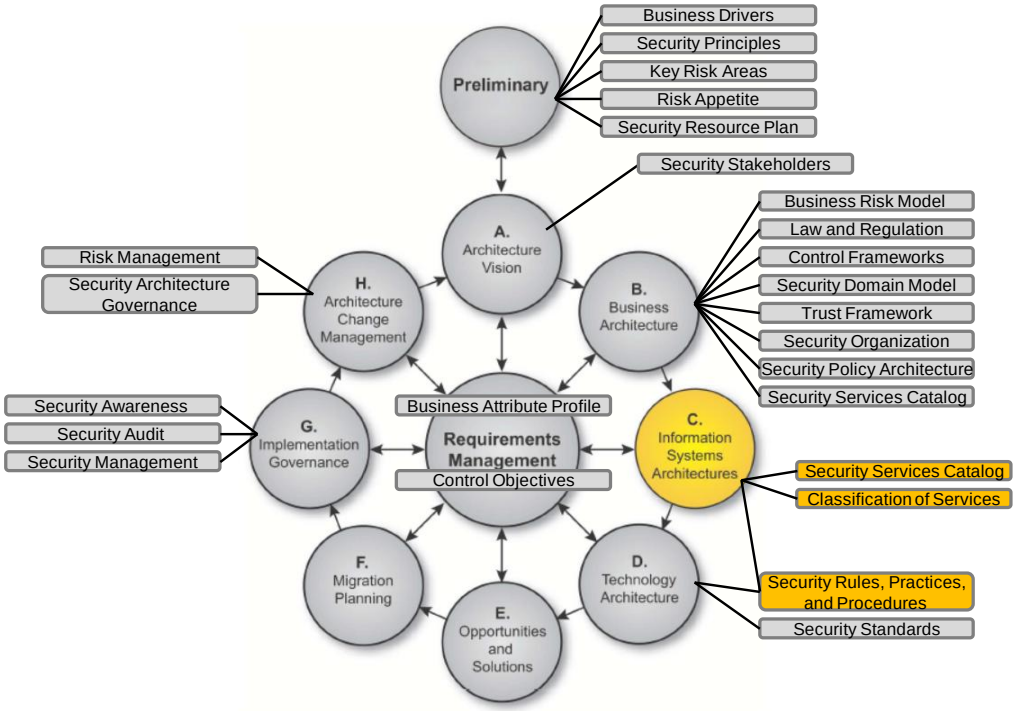

Figure 20: Security Artifacts in Phase C: Information Systems Architectures

[12] See Chapter 11 (pp 294-319) of the SABSA Blue Book.

- **Classification of Services** – the assignment of a security classification to the list of services in the Information System Services catalog according to the enterprise classification scheme. In most cases this scheme is defined and described in the corporate information security policy and is based on the information processed or stored by the service.
- **Security Rules, Practices, and Procedures** – are relevant artifacts for solution-level architectures. They are mentioned here because at the solution architecture level guidelines and designs for rules, practices, and procedures are expected to be produced in Phase C and D.

Phase D: Technology Architecture

The security elements of Phase D: Technology Architecture comprise security rules, practices and procedures, and security standards:

- **Security Rules, Practices, and Procedures** – artifacts mainly relevant for solution-level architectures, mentioned here because at solution architecture level guidelines and designs for rules, practices, and procedures are expected to be produced in Phase C and D.
- **Security Standards** – guide or mandate the use of technical, assurance, or other relevant security standards. The artifact is expected to comprise publicly available standards such as Common Criteria, TLS, and SAML.

In most cases the development of specific technology security architecture artifacts is not necessary as long as it incorporates the relevant security controls and mechanisms defined in earlier phases. The security architect must ensure that the required controls are included in the Technology Architecture and verify whether the controls are used in an effective and efficient way. This includes the technology for the provision and regulation of system resources, such as electric power, processing capacity, network bandwidth, and memory.

A security stakeholder may request the creation of a specific Technology Architecture security view or deliverable which describes all security-related technology components and how they inter-relate. This deliverable or view should describe which business risks are mitigated using technology and how.

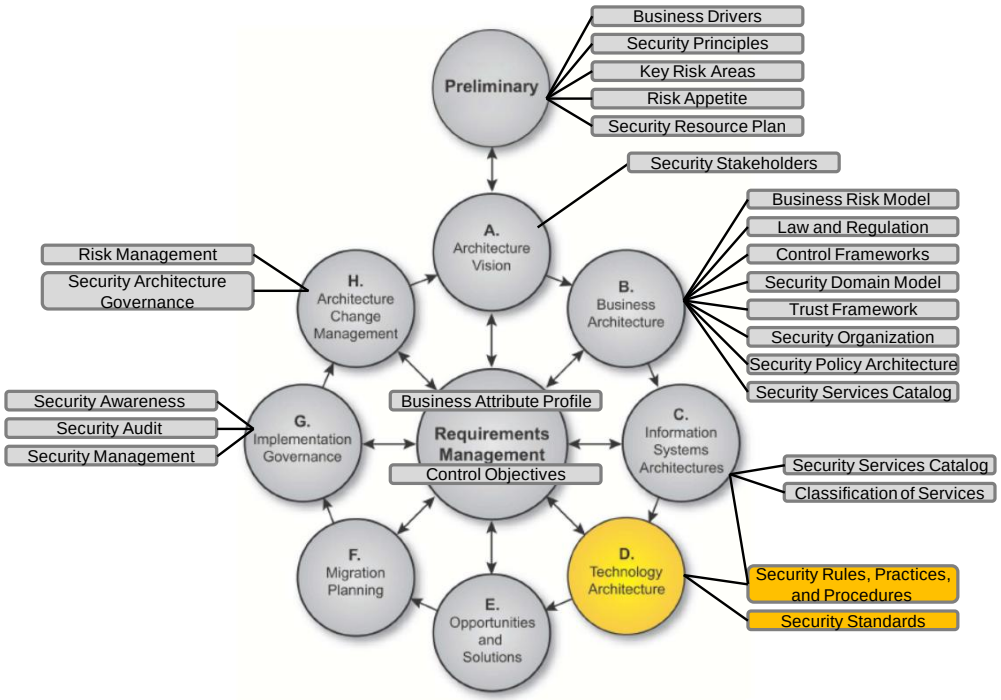

Figure 21: Security Artifacts in Phase D: Technology Architecture

Phase E: Opportunities and Solutions

No specific security-related architecture artifacts are produced in this phase. However, in defining the roadmap and deciding which architecture elements must be implemented first, it is imperative that the security risks are evaluated and that risk owners are consulted when defining the place on the roadmap for high priority mitigations. This phase could also be used to verify the process and results, feeding back to the business goals and drivers.

The efficacy of existing security services and controls earmarked for re-use must be verified to ensure that the end-state contains security measures which work and integrate well. If existing services and controls are not satisfactory, decide whether to include remediation in the migration plan or re-iterate Phases B through D to include new services and components.

Phase F: Migration Planning

No specific security architecture aspects apply to this phase; however, as part of the overall planning care must be taken to ensure that, for each stage on the roadmap, appropriate risks and associated controls are identified.

For instance, a pilot project which processes personal data must be fully compliant with the data protection act and requires an effective security infrastructure even though it only processes a small amount of data and supports only a few users.

Program and project managers should note that management of program and project risks can also be facilitated through the development of a Business Attribute Profile that focuses on the planning and execution of program or project tasks, leading to the provision of a real-time project risk dashboard. After all, program and project risks are simply special categories of operational risk.

Phase G: Implementation Governance

Security architecture implementation governance provides assurance that the detailed design and implemented processes and systems adhere to the overall security architecture. This ensures that no unacceptable risk is created by deviations from Architecture Principles and implementation guidelines.

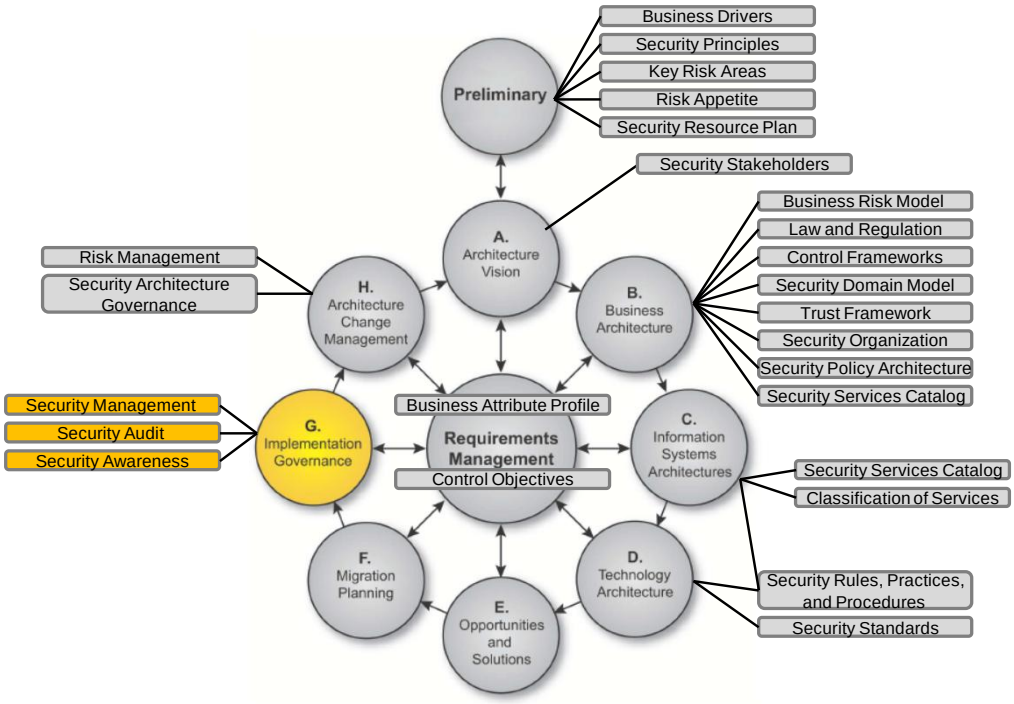

Figure 22: Security Artifacts in Phase G: Implementation Governance

The following artifacts are relevant in this phase:

- **Security Management** – definition of the detailed security roles and responsibilities, implementation of security governance, definition of security key performance and risk indicators, etc.
- **Security Audit** – reports which include security reviews of implemented processes, technical designs, and developed code against policies and requirements, and security testing comprising functional security testing and penetration testing.

  Implement an auditing process or add to an existing internal control process to guarantee long-term effectiveness. While planning and specification is necessary for all aspects of a successful enterprise, they are insufficient in the absence of testing and audit to ensure adherence to that planning and specification in both deployment and operation. Among the methods to be exercised are:

  - Review of system configurations with security impact to ensure configuration changes have not compromised security design
  - Audit of the design, deployment, and operations against business objectives, security policies, and control objectives

  - Functional and non-functional testing, including security, performance, and maintainability testing

- **Security-Awareness** – implement necessary training to ensure correct deployment, configuration, and operations of security-relevant subsystems and components; ensure awareness training of all users and non-privileged operators of the system and/or its components.

Training is not necessary simply to preclude vulnerabilities introduced through operations and configuration error, though this is critical to correct ongoing secure performance. In many jurisdictions, proper training must be performed and documented to demonstrate due diligence and substantiate corrective actions or sanctions in cases where exploits or error compromise business objectives or to absolve contributory responsibility for events that bring about harm or injury.

Phase H: Architecture Change Management

Phase H does not produce tangible security outputs but defines two processes essential for continued alignment between the business requirements and the architecture: risk management and security architecture governance. Even though they are not formal artifacts, they are added here to emphasize their importance.

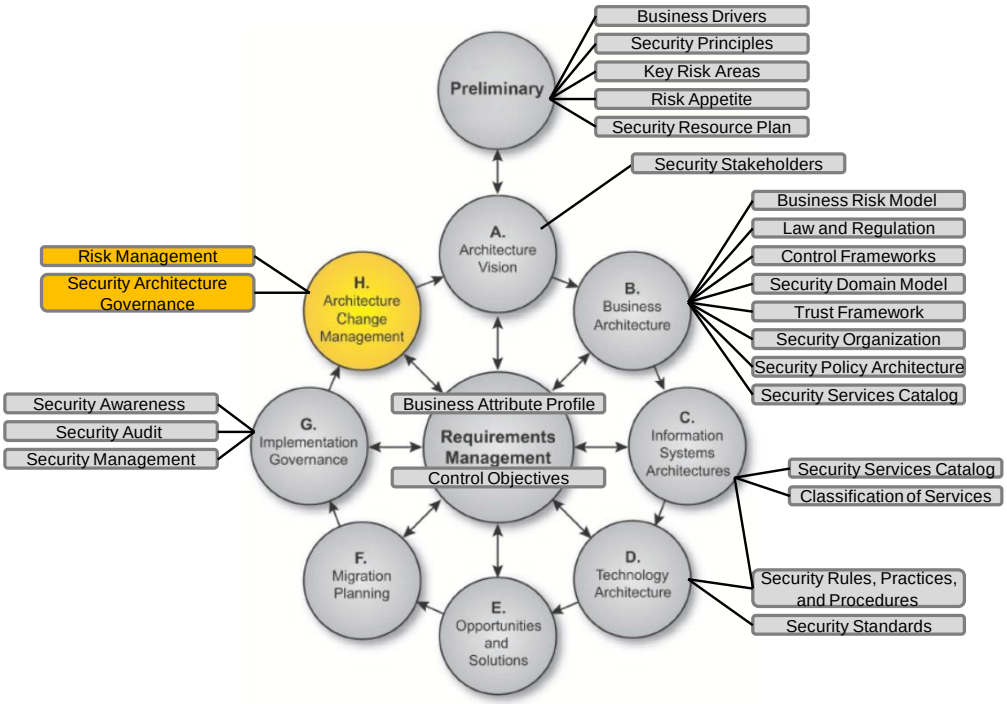

Figure 23: Security Artifacts in Phase H: Architecture Change Management

- **Risk Management** – the process in which the existing architecture is continuously evaluated regarding changes to business opportunity and security threat. If based on the results of this process, the current architecture is deemed unsuitable to mitigate changed or new risks or constrains the business too much in exploiting new opportunities, a decision on architecture change must be made.
- **Security Architecture Governance** – the process in which decisions are made on changes to the existing architecture, either by minor changes in the current iteration or by means of a completely new iteration.

Change is driven by new requirements or changes in the environment. Changes in security requirements can, for instance, be caused by changes in the threat environment, changed compliance requirements, or changes due to discovered vulnerabilities in the existing processes and solutions. Changes required due to security-related causes are often more disruptive than a simplification or incremental change.

Due care must be taken in deciding whether a security change triggers a new iteration though the TOGAF ADM cycle; for instance, when enterprise risk appetite changes; a seemingly small security requirement change can easily trigger a new architecture development cycle.

An example of where changes can be applied within the existing architecture is when security standards or requirements change. This is usually less disruptive since the trade-off for their adoption is based on the value

of the change – that is, evaluation of the risk – the trade-off between the opportunity for business improvement, the perceived threat to the business in security terms, and the threat posed by the change itself, which would perhaps be very disruptive and expensive. This is an excellent example of where the SABSA concept of balancing risks can be applied to decision-making.

It is therefore essential that the architecture change board or any other governance structure that is responsible for applying appropriate architecture change management comprises suitable security skilled individuals.

Appendix A: Glossary

The following definitions are relevant for the SABSA and TOGAF integration:

Business directives

Used in Section 6.2.2 and Chapter 6 – not a core term in TOGAF in explanatory text. TOGAF assumes the reader knows what a "business directive" is.

TOGAF standard dictionary definition of directive: "an official or authoritative instruction".

Business drivers

Business drivers for security – the subset of TOGAF business drivers impacting security architecture:

- Used throughout in the text. In text TOGAF assumes reader knows what a "business driver" is.
- TOGAF standard dictionary definition of driver: "(of a fact or feeling) compel (someone) to act in a particular way, especially one that is considered undesirable or inappropriate; [trans.] bring (someone) forcibly into a specified negative state; [trans.] force (someone) to work to an excessive extent".
- "Drive" defined specifically in the metamodel: "an external or internal condition that motivates the organization to define its goals. An example of an external driver for change in regulation or compliance rules which, for example, require changes to the way an organization operates; i.e., Sarbanes-Oxley in the US.

Business goals versus (SABSA) business drivers

Used throughout TOGAF. In text TOGAF assumes reader knows what a "business goal" is.

TOGAF 9 Section 26.9 provides guidance on defining goals.

TOGAF standard dictionary definition of goal: "the object of a person's ambition or effort; an aim or desired result; the destination of a journey".

In metamodel motivation entity. Goal is: "a high-level statement of intent or direction for an organization. Typically used to measure success of an organization".

Business imperatives

Not used in TOGAF 9.

Government and legal obligations that an agency must fulfil that may not be explicit in their business strategy documents; for example, payroll, financial reporting obligations, ministerial briefs.

Business principles

Used in two forms in TOGAF. One is the Architecture Principles that address the Business Architecture domain. The second is overall Business Principles that do not necessarily have an architectural context.

Architecture Principles are defined as: "a qualitative statement of intent that should be met by the architecture. Has at least a supporting rationale and a measure of importance". Business Principles would be read as: "a qualitative statement of intent that should be met by the Business Architecture".

Business strategies

Not a core term in TOGAF.

Used to provide context throughout. Defined in context in Phase B as: "business strategy typically defines what to achieve – the goals and drivers, and metrics for success – but not how to get there".

TOGAF standard dictionary definition of strategy is: "a plan of action or policy designed to achieve a major or overall aim".

Concerns versus (SABSA) business principles

In TOGAF associated with requirements. Used in description of what an architecture is.

Defined as: "the key interests that are crucially important to the stakeholders in the system, and determine the acceptability of the system. Concerns may pertain to any aspect of the system's functioning, development, or operation, including considerations such as performance, reliability, security, distribution, and evolvability".

Enterprise architecture

In this White Paper, "enterprise architecture" is used as an inclusive term to refer to all flavors of architectural views – operational, system, security, etc.

Key risk areas

The list of the key risk areas within the enterprise. Balanced with opportunities enabled by security, linked with risk appetite which informs the balance of risk *versus* opportunity.

Requirements versus (SABSA) business drivers

In TOGAF core term. Defined as: "a statement of need that must be met by a particular architecture or work package".

Work package is used primarily in Phase E and a core term: "a set of actions identified to achieve one or more objectives of the business. A work package can be part of a project, a complete project, or a program".

Risk appetite

Describes the enterprise's attitude towards risk and provides decision-making guidance to the organization to balance the amount of risk taken to achieve an expected outcome. The risk appetite could be expressed as, for example, a boundary on a risk/business impact and likelihood grid, profit, and loss measures or qualitative measures (zero tolerance for loss of life or regulatory compliance breaches). It could also be reflected in security principles.

Security principles

"The subset of business principles addressing security architecture".

TOGAF does not define specific "security principles". This issue is, however, included in the Security Forum forthcoming revision to W055 which will be submitted as complementary to this TOGAF and SABSA Integration White Paper.

See Business principles.

Appendix B: TOGAF Benefits for SABSA Practitioners

Some TOGAF concepts are very useful to SABSA practitioners. This section outlines a few good TOGAF ideas that are not present in SABSA, and specifies where in SABSA they can be used.

Preliminary Phase

The Preliminary Phase is about defining "where, what, why, who, and how we do architecture" in the enterprise concerned. The main aspects are:

- Defining the enterprise
- Identifying key drivers and elements in the organizational context
- Defining the requirements for architecture work
- Defining the Architecture Principles that will inform any architecture work
- Defining the framework to be used
- Defining the relationships between management frameworks
- Evaluating the enterprise architecture maturity

Translated to SABSA, it means that before using SABSA, first decide which specific parts to use and in what format the enterprise security architecture will be delivered. This phase determines what will be delivered and which methods or concepts will be used for that. Only if this is clear, it is possible to cooperate and deliver a security architecture.

This phase also includes the definition of abstraction layers that the enterprise security architecture is to contain. It may only be used at enterprise level, or perhaps used to work out some logical services in separate security views of the architecture.

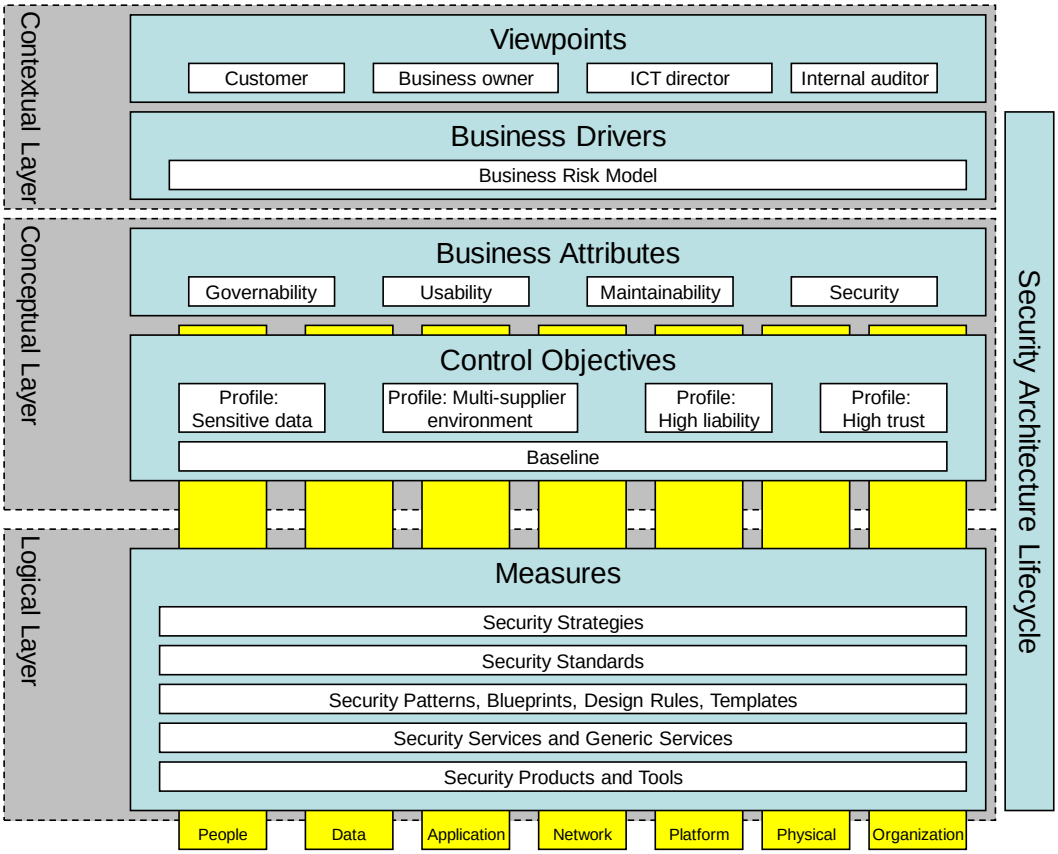

Figure 24: Example of an Enterprise Security Architecture Format (in this case only three architectural layers are used)

Architecture Development Method (ADM)

The TOGAF Architecture Development Method (ADM) cycle is a process model that can be used as a delivery model for an enterprise security architecture. It can be helpful for guidance in specific phases of the SABSA Lifecycle.

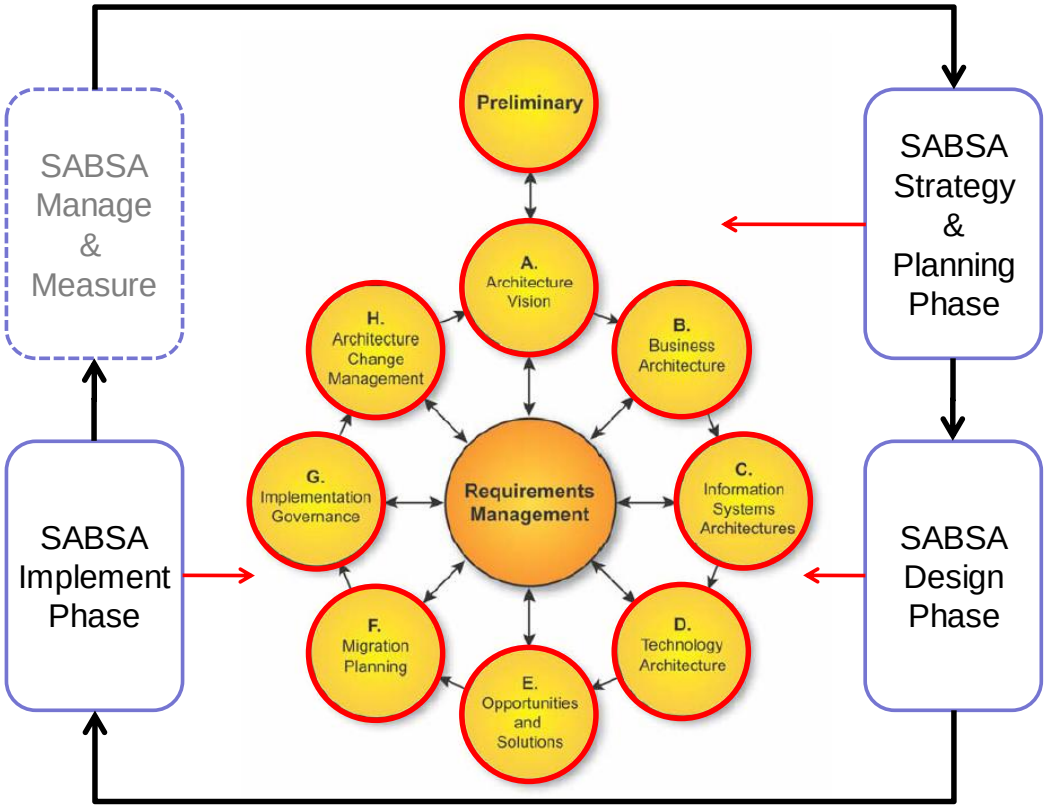

Figure 25: Mapping of SABSA Lifecycle and the TOGAF ADM

Relationship with O-ISM3

However, as indicated by the ghosted SABSA Manage & Measure phase in Figure 25, this phase of SABSA is out of scope for the TOGAF ADM. The relationship of this phase of SABSA is with another Open Group standard, the Information Security Management Maturity Model (O-ISM3). The following short quotation from the introductory chapter of O-ISM3 will demonstrate the philosophical alignment between SABSA and O-ISM3:

"*O-ISM3 defines information security management maturity in terms of the operation of an appropriate complementary set of O-ISM3 information security processes. It defines capability in terms of the metrics and management practices used, and it requires the linking of security objectives and targets to business objectives. Market-driven maturity levels help organizations choose the scale of ISMs most appropriate to their needs. The maturity spectrum facilitates the trade-off of cost, risk, and usability and enables incremental improvement, benchmarking, and long-term targets.*"

Readers should note that at the present time there has been no attempt to align SABSA and O-ISM3 in any detail, and such alignment is well beyond the scope of the current TOGAF and SABSA integration project.

Nested architectures

Each architecture typically does not exist in isolation and must therefore sit within a governance hierarchy. Broad and summary architectures set the direction for narrow and detailed architectures.

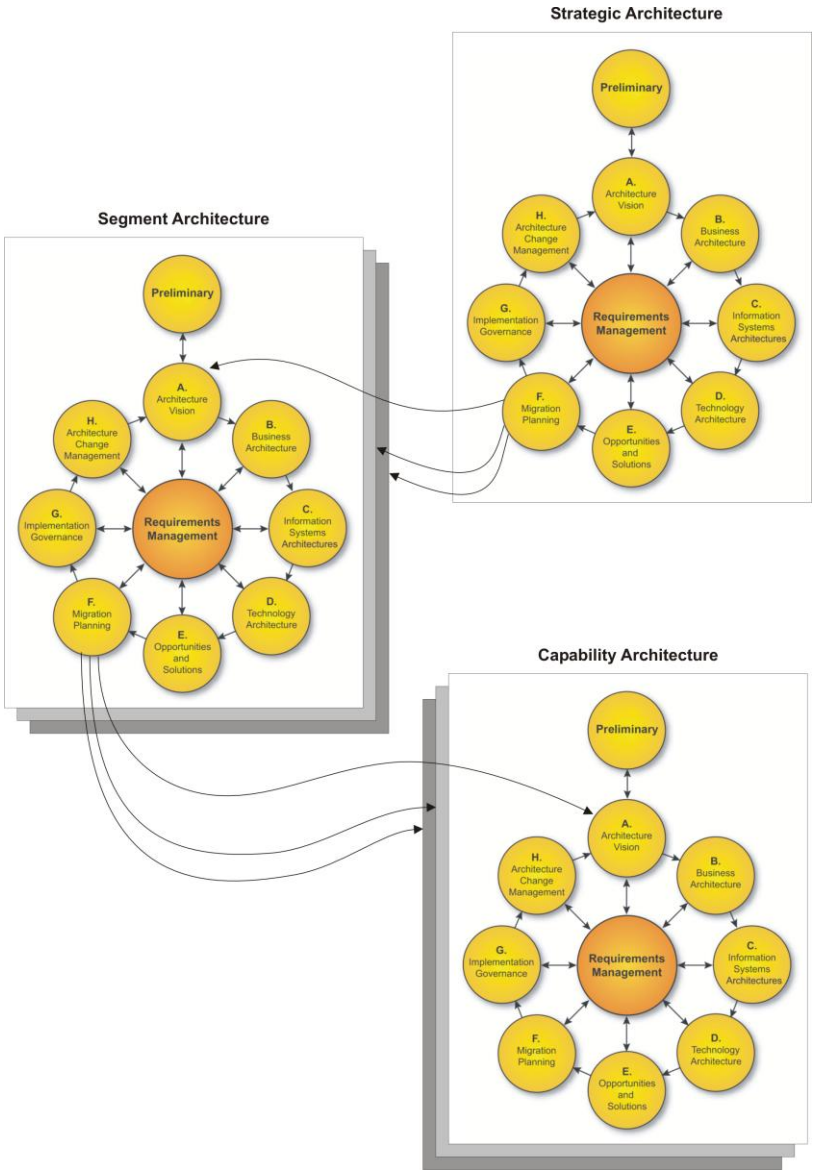

Figure 26: TOGAF Nested Architectures

TOGAF contains a number of techniques that can be employed to use the ADM as a process that supports such hierarchies of architectures. In cases where larger-scale architectures need to be developed, the ADM uses Phase F: Migration Planning of one ADM cycle to initiate new projects, which will also develop architectures.

- **Capability Architecture**: A highly detailed description of the architectural approach to realize a particular solution or solution aspect.

- **Segment Architecture**: A detailed, formal description of areas within an enterprise, used at the program or portfolio level to organize and align change activity.
- **Strategic Architecture**: A summary formal description of the enterprise, providing an organizing framework for operational and change activity, and an executive-level, long-term view for direction setting.

This concept of nested architectures can also be applied to SABSA. For example, to create security architectures at three architecture levels: Enterprise, Domain, and Solution. At each level, the SABSA layers can be matched.

Baseline and Target Architecture

TOGAF is about the transition from Baseline to Target Architecture. One of the activities in TOGAF is, for example, the impact assessment of the target requirements *versus* the baseline requirements.

SABSA risk management recognizes a green-field, current state, and desired state, but definition of the security architecture is aimed at desired state. The Baseline and Target Architecture concept of the TOGAF ADM can be used to facilitate a migration from existing to desired security architecture.

Views and stakeholder management

Views are a powerful concept to represent the interests of a group of stakeholders. SABSA practitioners can use views to improve communication to specific stakeholder groups, and to guarantee stakeholder buy-in for security-specific issues.

SABSA also contains the views concept. These are tied to the architectural layers in the SABSA Matrix. For example, the contextual layer is the Business View. The TOGAF views differ from the SABSA views. SABSA views correspond with layers of people creating the security architecture, not with stakeholders that you communicate with. On each SABSA layer, multiple TOGAF views could be created to express the interest of a stakeholder group. So within the Business View, one can distinguish different views for Business Owner, Auditor, IT Director, etc.

The TOGAF views concept can also be used to tie business drivers to specific stakeholders.

TOGAF emphasizes the importance of stakeholder management. It gives guidance on how to do this. Interested stakeholders are easy to find, but also look for the powerful uninterested stakeholder.

References

[1] TOGAF 9, an Open Group Standard; available at: www.opengroup.org/togaf.

[2] SABSA Blue Book: Enterprise Security Architecture: A Business-Driven Approach (John Sherwood, Andy Clark, & David Lynas, 2005); refer to: www.sabsa-library.org/index.php?language=en.

[3] SABSA White Paper; available at: www.sabsa.org/whitepaperrequest.aspx?pub=Enterprise+Security+Architecture.

[4] ISO/IEC 27005:2011: Information Technology – Security Techniques – Information Security Risk Management.

[5] ISO/IEC 31010:2009: Risk Management – Risk Assessment Techniques.

[6] Risk Taxonomy, Technical Standard (C081), January 2009, published by The Open Group; refer to: www.opengroup.org/bookstore/catalog/c081.htm.

[7] Open Information Security Management Maturity Model (O-ISM3), Technical Standard (C102), February 2011, published by The Open Group; refer to: www.opengroup.org/bookstore/catalog/c102.htm.

[8] ISO/IEC 27001:2005: Information Technology – Security Techniques – Information Security Management Systems – Requirements.

[9] Control OBjectives for Information and related Technology (COBIT), Version 4.0, IT Governance Institute, 2005.

About The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. With more than 375 member organizations, The Open Group has a diverse membership that spans all sectors of the IT community – customers, systems and solutions suppliers, tool vendors, integrators, and consultants, as well as academics and researchers – to:

- Capture, understand, and address current and emerging requirements, and establish policies and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

Further information on The Open Group is available at www.opengroup.org.

About the SABSA Institute

The SABSA Institute is the professional member and certification body for Enterprise Security Architects of all specialisms and at all career levels. It governs the ongoing development and management of SABSA intellectual property and the associated certification and education programs worldwide.

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

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

About the SABSA-TOGAF Integration Working Group

This TOGAF-SABSA Integration project started in May 2010 as a joint initiative of both the Architecture Forum and the Security Forum of The Open Group, and the SABSA Institute.

Three face-to-face meetings were held in Rome, Amsterdam, and London. The remaining communications were conducted using webinars and phone conferences.

Contributors to the project

Lead developers:

- Pascal de Koning, KPN Corporate Market: Project Leader
- John Sluiter, PricewaterhouseCoopers (PwC): Lead Author
- John Sherwood, Founder, SABSA Institute: Lead SABSA Contributor
- Dave Hornford, Connexiam: Chair of The Open Group Architecture Forum
- Jeroen van Esch, Ideas to Interconnect (i-to-i)
- Arthur Donkers, 1Secure
- Jim Hietala, VP Security, The Open Group
- Rick Holod, Seccuris
- François Jan, Arismore
- Ian Dobson, Director, Security Forum, The Open Group

Lead contributors/reviewers (alphabetical order):

- Chris Armstrong, Armstrong Process Group
- Iver Band, Standard Insurance Company
- Ian Cole, Architecting the Enterprise
- Ajit Gaddam, Progressive Insurance
- Vladimir Jirasek, Nokia
- Christian Mark, IBM
- Jan de Meyer, Ascure
- Kris Boulez, Ascure
- Tamim Rahman, QRS
- Robert Weisman, Build the Vision