Information Security Journal: A Global Perspective, 21:47–54, 2012
Copyright © Taylor & Francis Group, LLC
ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393555.2011.629341

Taylor & Francis
Taylor & Francis Group

Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®

Jason S. Burkett
Veris Group, Vienna, Virginia, USA

ABSTRACT Information security is an imperative factor in organizational success, driven by the need to protect information assets. The continuous evolution of external and internal threats and the associated need to protect and secure information from exploitation of vulnerabilities has become a struggle for many organizations in both the public and private sectors. This struggle is the direct result of the narrow focus on operational security. Just as the lines between business and information technology have disappeared, so have the lines between business and information security. Some organizations simply "check the box" by performing the minimum actions required to pass or meet mandated compliance standards. Without practicing due diligence and by only meeting the minimum requirements, leads to the reactive response of exploited vulnerabilities in addition to the increase of after the fact incident investigations. Organizations need to take a proactive approach using established methodologies known to incorporate security into information technologies and systems. The Sherwood Applied Business Security Architecture (SABSA) is a solution oriented methodology for any business enterprise that seeks to enable its information infrastructure by applying security solutions within every layer of the organization. This article describes how SABSA can be integrated into organizations' existing architectures utilizing organizational business drivers.

KEYWORDS enterprise security, security architecture, enterprise architecture, cyber security, information security, enterprise security management practices

Address correspondence to
Jason S. Burkett, Senior Associate,
Veris Group, LLC, 3429A
W. Franklin Street, Richmond, VA
23221. E-mail: Jason.Burkett@gmail.com

INTRODUCTION

SABSA® focuses on the use of "best practices" for any organization that needs to develop information security solutions and traceable business enterprise initiatives. SABSA provides integrated frameworks, models, methods, and processes that are risk-focused and address both threats and opportunities. The SABSA methodology uses a "business-driven approach" consisting of a "six-layer model covering all four parts of the IT lifecycle: Strategy, Design, Implementation, and Management & Operations." Information security solutions are derived from all views and layers of enterprise architecture in order to produce requirements driven by the business, not because of the latest buzz words (Sherwood, Clark, & Lynas, 2005).

Information security professionals have been viewed as inhibiting operations because they identify problems in the protection of information assets after an information technology solution has been designed, implemented, and put into operation. These problems exist because security considerations were not incorporated into a technology solution during the initiation phase and aligned with all layers of the organization throughout implementation. Typical information security assessments include recommended mitigation actions, but they are seldom remediated as recommended. Reasons usually include the lack of funding, lack of resources, or statements such as "the priority of mission operations will suffer" if the recommended security actions are implemented. In most cases, it is not until after organizations have become "intrusion victims" of an "Advanced Persistent Threat" (APT) that remediation efforts are taken seriously (Stamos, Grattafiori, Daniels, Youn, & Orvis, 2011). These are all symptoms of the root problem, incorporating security into the enterprise at all levels. Each level or layer of an organization has its own business priorities and objectives to support the mission. The need to implement an enterprise security solution is commonly overlooked or not even recognized. Another reason for not implementing security is that information security can be addressed later in the development of the technology or system, during the operations phase where operational security is applied. However, operational security focuses on security at the operational layer of an organization and does not take into account a strategic point of view. SABSA is used to address these issues by taking the strategic view into consideration.

SABSA brings information security professionals the arsenal they need to become business security solution providers instead of the business operations inhibitors they have been portrayed to be. Reporting on information security only gives organizations an idea of what risks exist; it does not show organizations how to become more secure by mitigating risk. The same holds true for applying security only through operations; tactical information security only meets the immediate need rather than establishing strategic, long-term solutions to an organization's information protection ailments. SABSA gives organizations a roadmap to protecting company assets through the SABSA Development Process, developing security solutions as viewed by all six layers of an organization. The SABSA Development Process diagram is shown in Figure 1 (Sherwood, Clark, & Lynas, 2005).

SABSA is easily integrated with existing enterprise architectures because it is holistic, accounting for all organizational business units. The major enterprise architectures in use today are listed below (Sessions, 2007):

- The Zachman Framework (Zachman, 2008)
- The Open Group Architectural Framework (TOGAF®) (The Open Group, 2008)
- The Federal Enterprise Architecture (FEA) Security and Privacy Profile (Federal CIO Council, 2010)
- The Gartner Enterprise Architecture Framework (GEAF) (Gartner, 2006)

In Robert Sessions' white paper "Comparison of the Top Four Enterprise Architecture Methodologies," he describes Zachman to be a "taxonomy," TOGAF to be a "process," FEA to be a "methodology," and Gartner's to be a "practice" (Sessions, 2007).

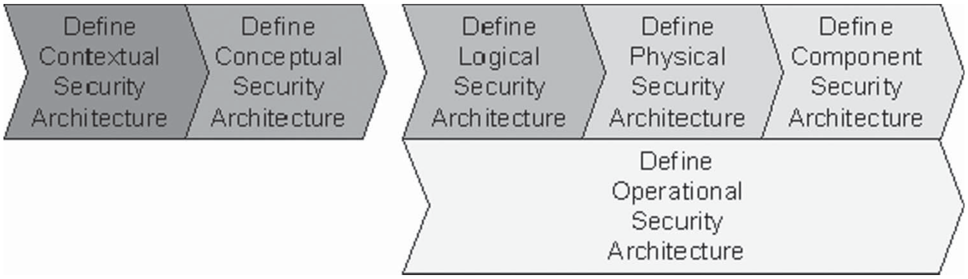

Define Contextual Security Architecture
Define Conceptual Security Architecture
Define Logical Security Architecture
Define Physical Security Architecture
Define Component Security Architecture
Define Operational Security Architecture

FIGURE 1 SABSA® Development Process.

Similar to how a building architect designs security into a building, SABSA assimilates information security elements throughout the layers of an organization and aligns it with the current enterprise architecture, be it any of the four listed above.

SABSA enables business growth by strengthening the ability of an organization to produce more information products and services in a secure fashion. All layers of the organization have signed off on information security attributes and requirements, enabling strategic organizational objectives to be achieved while protecting operations. As more organizations realize the best way to protect the business is by establishing an information security strategy at each layer of the organization, SABSA becomes the solution of choice.

INTEGRATING SABSA

Many white papers, articles, and books have been written on information security and enterprise architecture, but these topics are typically separated, and there are few that combine the two. It is hard to believe that one of the most important aspects of enterprise architecture (information security) could be left out of defined methodologies and frameworks. Enterprise architectures that fail to include security leave gaps in the protection of information assets. These gaps can be closed at the enterprise level by implementing a strong Enterprise Security Architecture derived from the business and its stakeholders.

The SABSA Methodology

SABSA was originally developed in 1995 as an "idea" by John Sherwood. In 1996, he published "SABSA: A Method for Developing the Enterprise Security Architecture and Strategy" This white paper details the SABSA methodology and framework.

The SABSA methodology includes six layers, each representing the view of a different stakeholder in the enterprise. Shon Harris, author of the *Certified Information System Security Professional (CISSP) All-in-One Exam Guide*, mentions in a recent article that SABSA also establishes a "time-tested" framework for building secure information systems that account for the security needs of each layer. She also indicates that SABSA is similar to "software development" as when someone "uncovers a business need to develop a specific software product" and applies more granularity as the software goes through each layer of development (Harris, 2011). The six layers of SABSA are mapped to six stakeholder views, and the six interrogatives defined for each layer of an enterprise security architecture. This mapping is shown in Figure 2 in the SABSA Matrix (Sherwood, Clark, & Lynas, 2005).

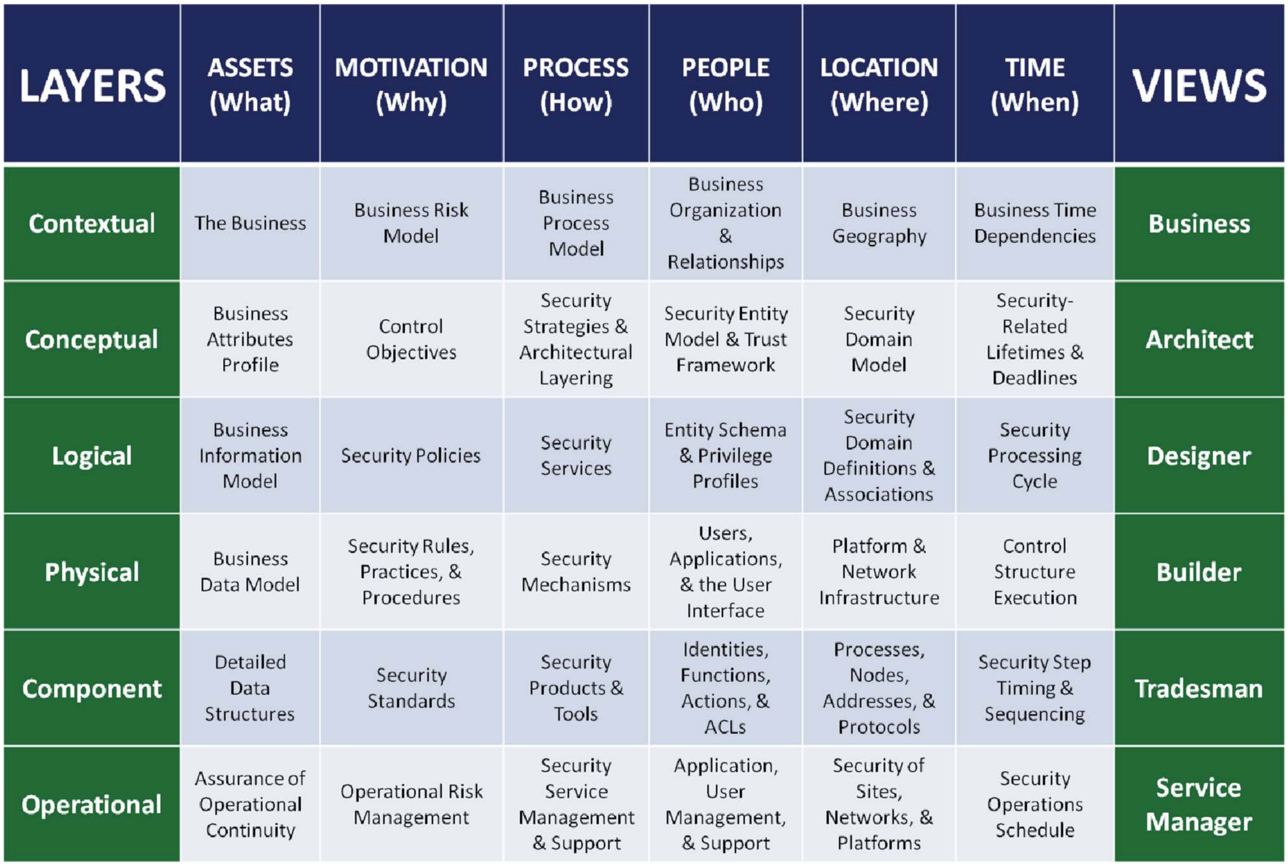
SABSA takes a holistic approach in identifying security solutions for business problems that executives face, not the "technically led approach" that solves only the tactical operational issues. Within the past few years, business and technology have become one and the same as organizations have not been able to stay competitive without incorporating technologies that give them an edge. For many years, the security of business and technology has focused on the confidentiality, integrity, and availability of information. However, by focusing on only three attributes, security gaps have existed throughout organizations and their systems. There are other attributes that an organization needs to include in order to mitigate risks unique to its enterprise.

SABSA uses a business attribute taxonomy to capture these attributes and to show measurable organizational value (MOV) based on these unique needs. Using the profiling technique, security solutions can be measured against predetermined targets. A large multinational banking group (unnamed to prevent unnecessary threats) has used SABSA successfully to ensure strategic development of a single application for high-value Internet transactions. Challenges that were overcome using targeted metrics consisted of availability, inter-operability with legacy systems, and real-time transactions (www.SABSA.org).

SABSA and the Zachman Framework

The SABSA model closely follows the Zachman Framework in that both attempt to answer the "primitive interrogatives" of who, what, when, where, why, and how for each layer of an organization. Both SABSA and the Zachman Framework were developed independent of each other. SABSA does not replace the Zachman Framework but instead enhances it by including security. SABSA helps align security to business strategy by filling the security gaps in enterprise architecture and service management. The Zachman Framework is shown in Figure 3 (Zachman, 2011).

As indicated in the Zachman Framework, there is no mention of security in any of the quadrants.



LAYERS	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)	VIEWS
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization & Relationships	Business Geography	Business Time Dependencies	Business
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies & Architectural Layering	Security Entity Model & Trust Framework	Security Domain Model	Security-Related Lifetimes & Deadlines	Architect
Logical	Business Information Model	Security Policies	Security Services	Entity Schema & Privilege Profiles	Security Domain Definitions & Associations	Security Processing Cycle	Designer
Physical	Business Data Model	Security Rules, Practices, & Procedures	Security Mechanisms	Users, Applications, & the User Interface	Platform & Network Infrastructure	Control Structure Execution	Builder
Component	Detailed Data Structures	Security Standards	Security Products & Tools	Identities, Functions, Actions, & ACLs	Processes, Nodes, Addresses, & Protocols	Security Step Timing & Sequencing	Tradesman
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management & Support	Application, User Management, & Support	Security of Sites, Networks, & Platforms	Security Operations Schedule	Service Manager

FIGURE 2 **The SABSA® Matrix for security architecture. (color figure available online.)**

SABSA can be easily integrated with the Zachman Framework because both are flexible and meet an organization's unique set of business requirements. When integrated, SABSA fills in the missing security gaps providing an organization with more complete enterprise architecture.

SABSA and The Open Group Architecture Framework (TOGAF)

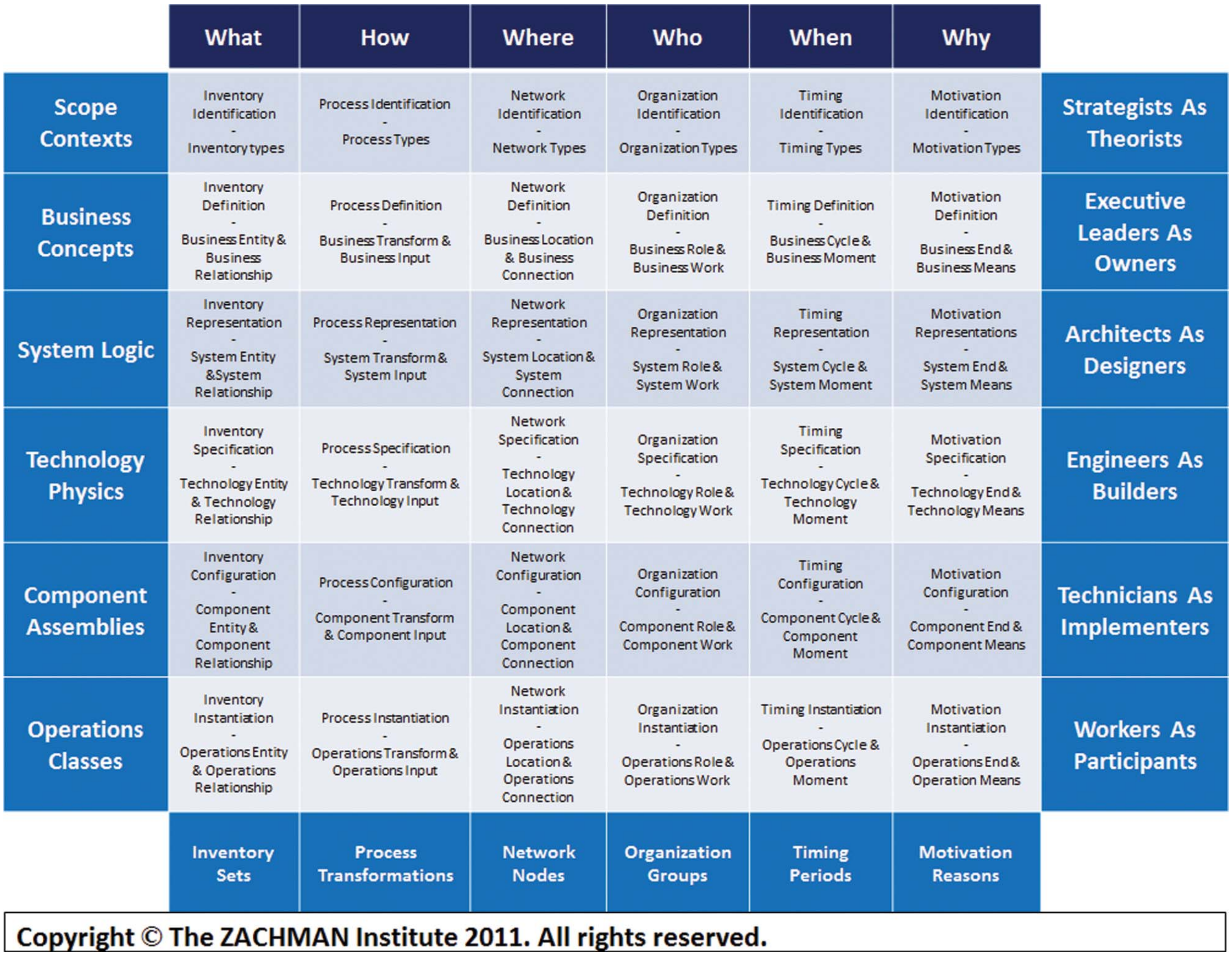
TOGAF[1] is owned by the Open Group and is a tool or process used to develop different information technology (IT) architectures. TOGAF's architecture development model is shown in Figure 4 (The Open Group, 2008).

SABSA complements TOGAF because it incorporates security into the process for creating IT architecture solutions. TOGAF categorizes architecture into four areas (business, application, data, and technical) but does not include security in any of these categories. SABSA supports all categories and takes this architecture a step further by incorporating the business need of security architecture and security service management into all layers of the organization. A SABSA and TOGAF integration model would resemble Figure 5.

SABSA and The Federal Enterprise Architecture Security & Privacy Profile (FEA SPP)

The FEA SPP, version 3, is "a scalable, repeatable, and risk-based methodology and framework for addressing information security and information privacy requirements in the context of an agency's architecture at the enterprise, segment, and solution levels." It provides guidance on the mandates for federal government departments and agencies to protect information and information systems by implementing "security and privacy protections."

The FEA SPP Framework shown in Figure 6 provides a roadmap on how departments or agencies can integrate the NIST Risk Management Framework into the FEA to develop an "Enterprise Level Common Control" solution (The Federal CIO Council, 2010).



	What	How	Where	Who	When	Why	
Scope Contexts	Inventory Identification - Inventory types	Process Identification - Process Types	Network Identification - Network Types	Organization Identification - Organization Types	Timing Identification - Timing Types	Motivation Identification - Motivation Types	Strategists As Theorists
Business Concepts	Inventory Definition - Business Entity & Business Relationship	Process Definition - Business Transform & Business Input	Network Definition - Business Location & Business Connection	Organization Definition - Business Role & Business Work	Timing Definition - Business Cycle & Business Moment	Motivation Definition - Business End & Business Means	Executive Leaders As Owners
System Logic	Inventory Representation - System Entity &System Relationship	Process Representation - System Transform & System Input	Network Representation - System Location & System Connection	Organization Representation - System Role & System Work	Timing Representation - System Cycle & System Moment	Motivation Representations - System End & System Means	Architects As Designers
Technology Physics	Inventory Specification - Technology Entity & Technology Relationship	Process Specification - Technology Transform & Technology Input	Network Specification - Technology Location & Technology Connection	Organization Specification - Technology Role & Technology Work	Timing Specification - Technology Cycle & Technology Moment	Motivation Specification - Technology End & Technology Means	Engineers As Builders
Component Assemblies	Inventory Configuration - Component Entity & Component Relationship	Process Configuration - Component Transform & Component Input	Network Configuration - Component Location & Component Connection	Organization Configuration - Component Role & Component Work	Timing Configuration - Component Cycle & Component Moment	Motivation Configuration - Component End & Component Means	Technicians As Implementers
Operations Classes	Inventory Instantiation - Operations Entity & Operations Relationship	Process Instantiation - Operations Transform & Operations Input	Network Instantiation - Operations Location & Operations Connection	Organization Instantiation - Operations Role & Operations Work	Timing Instantiation - Operations Cycle & Operations Moment	Motivation Instantiation - Operations End & Operation Means	Workers As Participants
	Inventory Sets	Process Transformations	Network Nodes	Organization Groups	Timing Periods	Motivation Reasons	

FIGURE 3 The Zachman Enterprise Framework. (color figure available online.)

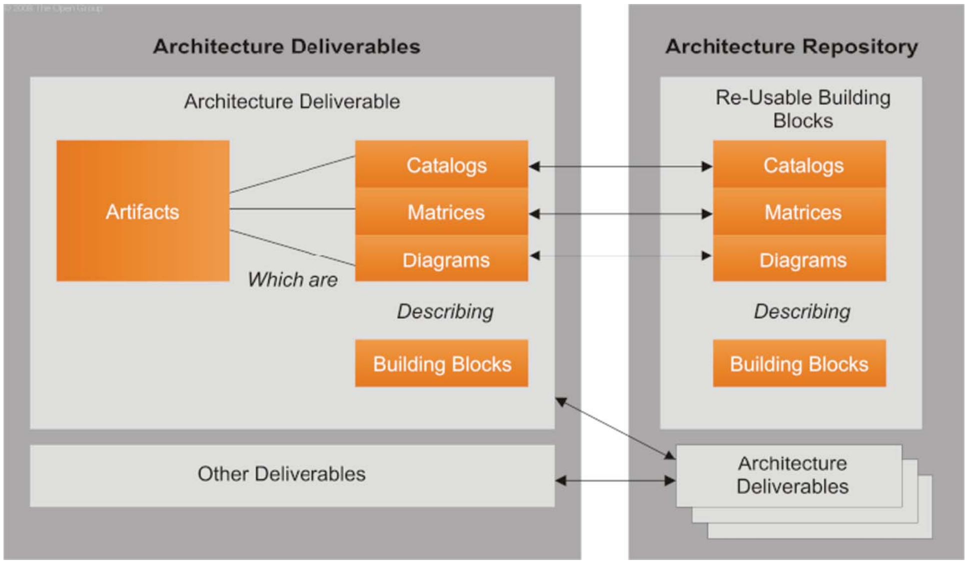


FIGURE 4 TOGAF Architecture development model. (color figure available online.)

Figure 6 depicts SABSA attributes included in the framework to illustrate how SABSA incorporates additional controls that might have been overlooked when using FEA SPP. The diagram in Figure 6 also includes the SABSA methodology as part of enterprise architecture guidance and information security

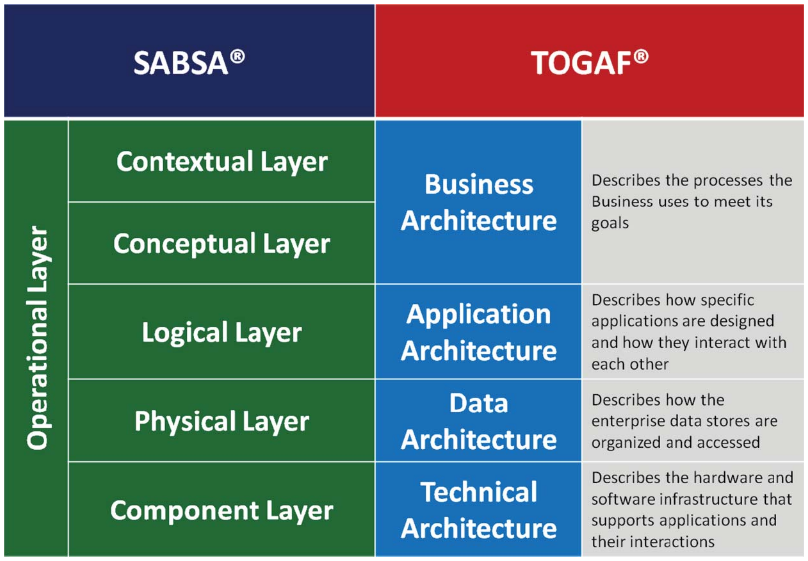

SABSA®
TOGAF®
Operational Layer
Contextual Layer
Conceptual Layer
Logical Layer
Physical Layer
Component Layer
Business Architecture
Describes the processes the Business uses to meet its goals
Application Architecture
Describes how specific applications are designed and how they interact with each other
Data Architecture
Describes how the enterprise data stores are organized and accessed
Technical Architecture
Describes the hardware and software infrastructure that supports applications and their interactions

FIGURE 5 SABSA and TOGAF integration model. (color figure available online.)

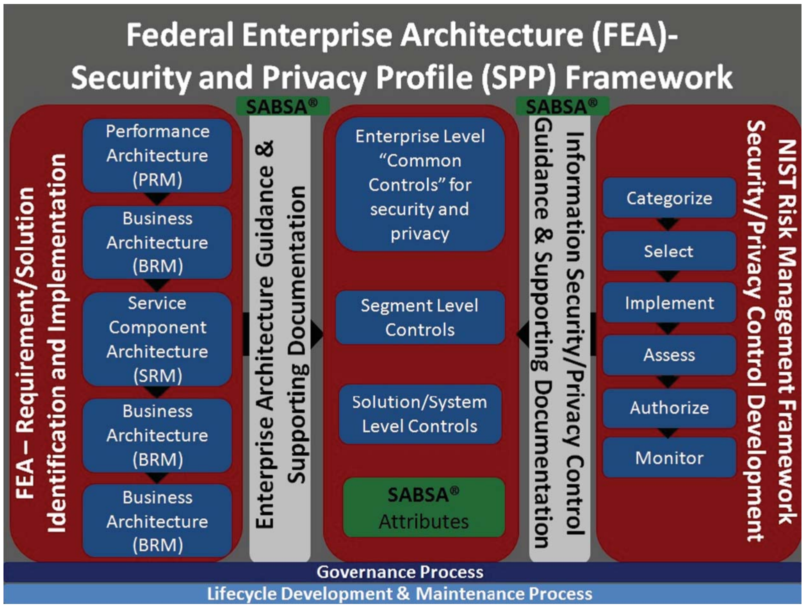

Federal Enterprise Architecture (FEA)-
Security and Privacy Profile (SPP) Framework
FEA – Requirement/Solution Identification and Implementation
Performance Architecture (PRM)
Business Architecture (BRM)
Service Component Architecture (SRM)
Business Architecture (BRM)
Business Architecture (BRM)
SABSA®
Enterprise Architecture Guidance & Supporting Documentation
Enterprise Level "Common Controls" for security and privacy
Segment Level Controls
Solution/System Level Controls
SABSA® Attributes
SABSA®
Information Security/Privacy Control Guidance & Supporting Documentation
Categorize
Select
Implement
Assess
Authorize
Monitor
NIST Risk Management Framework Security/Privacy Control Development
Governance Process
Lifecycle Development & Maintenance Process

FIGURE 6 FEA SPP Framework. (color figure available online.)

guidance because it would be considered supporting documentation.

By itself, the FEA SPP methodology consists of a compliance element that is not necessarily flexible enough for all departments or agencies to meet. Incorporating SABSA into the FEA SPP takes into account unique agency missions that require additional security attributes. Unique agency missions have trouble meeting compliance requirements because of the lack of flexibility in federal directives and requirements (The Federal CIO Council, 2010).

SABSA and the Gartner Model

The Gartner model is often called a practice as it rests on the interpretation, experience, and shared knowledge of enterprise service providers. Unfortunately, Gartner did not grant permission to publish their model in this paper because they indicated an updated model is forthcoming. The original model was published in the 2006 Gartner white paper "Incorporating Security into the Enterprise Architecture Process." Since its publication, security architecture has become a focus of enterprise operations, applying the concept of a service-oriented architecture. The model illustrates how "current-state architecture," or "as-is" architecture, can be transformed into "future-state architecture," or the "to-be" architecture (Gartner, 2006). The Gartner practice focuses on services that an enterprise can provide and "closing the gap" between the "current-state" and the "future-state." It answers the questions of how, why, and for what as identified in SABSA and Zachman but does not necessarily include the who, where, and when. The architecture effort itself is influenced by business strategy and environmental trends. The integration of the SABSA would complement the Gartner practice by closing any gaps in security that do not address the enterprise stakeholders (the who), the enterprise locations (the where), and the timing (the when). SABSA also supports the alignment of security with strategic objectives identified in the to-be architecture.

SABSA Benefits and Challenges

All methodologies and frameworks are met with challenges despite the benefits that are offered to an industry. An example is the Project Management Methodology and Project Management Institute (PMI). Founded in 1969, the PMI consisted of a small group of project managers practicing what was thought of at the time to be questionable unproven methods, but now is considered a valuable repository called the Project Management Body of Knowledge (PMBOK). It was not until 1984, 15 years later, that the first Project Management Professional (PMP) certification exam was held. The first certified group numbered 43 PMPs. There are now 180,000 PMPs in 175 countries (Owens, 2011).

SABSA does not replace existing organizational processes or frameworks. The biggest benefit to using it is to align and enhance that which works in an organization, building on existing strengths without introducing weaknesses or risks. Figure 7 illustrates some of the benefits and challenges that are introduced when integrating SABSA in an organization.

CONCLUSION

SABSA is an enabler of business, providing features and advantages that lead to many benefits for every layer of an organization, regardless of the existing enterprise architecture. Organizations can realize tremendous gains by implementing a security architecture based on the SABSA methodology. SABSA meets the unique needs of any business mission, and it is flexible enough to integrate with any existing architecture. It helps organizations manage complexity by providing architectural governance, ensuring two-way traceability on key decisions, measuring the true organizational value added, and by being risk driven as well as business driven. Organizations that realize business and security are now inseparable, just as business and technology, will also understand the need to incorporate information security at every layer of the enterprise for every technology solution and not wait until the solution is already operational. This is the time to be proactive instead of reactive.

BENEFITS	CHALLENGES
Simplicity & Clarity of Framework	Differing Terminologies
Risk-Based & Cost/Benefit Proven	Historical Attempts of Methodologies
Measurable Organizational Value	Non-Existent Repeatable Processes
Roadmap Definition	Continuous Reactive Actions (Firemen)
Lower Cost of Ownership	Obtaining Buy-In from Stakeholders
Easily Aligns and Enhances Existing Frameworks	Resistance to Change
Inter-Operability	Legacy Systems
Enables Business through Security	Perception of Security as "Inhibitor"
Governance	Complex Business Procedures
Compliance	Fear of Audit

FIGURE 7 **Benefits and challenges of SABSA.**

NOTE

1. TOGAF® is a registered trademark of The Open Group in the United States and other countries.

REFERENCES

Gartner. (2006). Incorporating security into the enterprise architecture process. Toronto, Canada: Gartner. Retrieved from http://www.gartner.com/DisplayDocument?ref=g_search&id=488575

Harris, S. (2011). Developing an information security program using SABSA, ISO 17799. Retrieved from http://searchsecurity.techtarget.com/tip/Developing-an-information-security-program-using-SABSA-ISO-17799

Owens, J (2011). PMBOK® history and overview. Available from http://jimowenspmp.com/dotnetnuke_4/PMBOK/tabid/158/Default.aspx

Sessions, R. (2007, May). A comparison of the top four enterprise-architecture methodologies. Retrieved from http://www.objectwatch.com/whitepapers/4EAComparison.pdf

Sherwood, J., Clark, A., and Lynas, D. (2005). Enterprise security architecture: A business-driven approach. San Francisco, CA: CMPBooks. Available from http://www.sabsa.org

Stamos, A., Grattafiori, A., Daniels, T., Youn, P., and Orvis, B.J. (2011). *Macs in the age of the APT*. Retrieved from http://www.blackhat.com/html/bh-us-11/bh-us-11-briefings.html

The Open Group. (2008). TOGAF version 9 – a manual. Zaltbommel, Netherlands: Van Haren Publishing. Retrieved from https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?catalogno=g091

The Federal Chief Information Officers Council. (2010). Federal enterprise architecture security and privacy profile, version 3. Retrieved from http://www.cio.gov/documents_details.cfm/uid/480F4A03-BDBE-6B59-FF19F5759D020C31/structure/Information%20Technology/category/IT%20Security-Privacy

Zachman, J.A. (2008). The Zachman framework for enterprise architecture: Primer for enterprise engineering and manufacturing. John A. Zachman. Retrieved from http://www.zachmanframeworkassociates.com/

BIOGRAPHY

Jason S. Burkett is a Senior Security Associate at Veris Group. He has led and managed initiatives for federal agency security programs and supported the development of security enterprise architecture solutions that enable organizations to meet mission objectives. He holds a Masters degree in Information Systems Technology from The George Washington University, is a Certified SABSA® Practitioner in architecture design (SCPA), a Certified Information Systems Security Professional (CISSP), and a Project Management Professional (PMP).