SABSA CONCEPTUAL LAYER – FINAL PAPER

CSOL 520.FINAL PAPER. CHAD NELLEY

Abstract

A business forward look at implementing the Conceptual Layer of SABSA Security Architecture for IBFS

Chad Nelley

Nelley.chad@gmail.com; chad@nelleyconsulting.com

NELLEY CONSULTING, LLC
PROPOSAL FOR SERVICES

SABSA Security Architecture Model – Conceptual Layer Delivery

OVERVIEW & INTRODUCTION

Nelley Consulting, LLC is pleased to submit this proposal for services to support IBFS in achieving its goals for improving its security posture by providing direct consulting services to develop and deploy the Conceptual Architecture Layer of the SABSA Security Architecture model. We have partnered with dozens of small businesses throughout the North American market — businesses committed to improving their security posture through appropriate planning and understanding of Top Down security Architecture modeling. Nelley Consulting has selected the SABSA Model as a blue print for success as it is industry recognized and time tested as a premier model for building strong, effective and applicable security practices that are business requirements and attribute driven.

The Objective – Deliver the Conceptual Model Layer – The Security Strategy

Often referred to as the 2nd Layer of the SABSA Security Architecture Model, this layer deals specifically with aligning security posture to proper business drivers and business attributes that have been established at the most senior levels of the organization. By the time Nelley Consulting has completed this project on behalf of IBFS, the company will be well positioned to implement the logical and tactical security components that will make for a robust security posture. In this Phase we will outline and document the following as a final deliverable:

- Map Conceptual Elements to the Business Drivers
- Map Conceptual Elements to the Critical Success Factors of the Business
- Model to capture Critical Business Processes and Models such as: Impact of Time, Function, People and Location as they relate to the Organization's Security Strategy.

Deliverables

As part of this proposal and outline, Nelley Consulting intends to deliver the following assets to the Client:

- The SABSA Business Attribute Profile
- The SABSA Business Risk Model & Statement of Control Objectives
- Assessment of Current Status of Security Posture
- Major Security Strategies and Concepts mapped to Control Objectives
- A series of Break-out Documents that describe major security strategies as they relate to the business
- The Security Entity Model and trust framework
- The Security Domain Model
- A compilation of items, lifecycles and deadlines for lower level layers of the SABSA Model

Once compiled and complete as part of this project, this library of information will serve as the “Security Strategy” for the organization and will be utilized to develop the further layers of the model.

OUR PROPOSAL

IBFS has a well-deserved reputation for quality financial products and vehicles for consumer and B2B clients as well. However, faced with constant security attack threats and black hat operative activities on the rise in targeting financial institutions IBFS faces the possibility of decreasing sales revenues and significant brand tarnishment in the event of a breach.

We have developed solutions to help businesses stay on par with Black Hat security trends and propose that IBFS implement a comprehensive SABSA approach to security.

Pre-requisites

In order for Nelley Consulting to be effective in the delivery of the Conceptual Model assets outlined in the Deliverables section of this proposal, it is critical that IBFS Executive Team has convened and developed a comprehensive Contextual Layer outlay. It is critical that this document be delivered to Nelley Consulting 2 weeks prior to work commencement such that the team at Nelley Consulting can review and model the Conceptual Layer to the following critical Business Driver Elements:

- The Business (What)
- The Business Risk Model (Why)
- The Business Process Model (How)
- The People (Who)
- The Location(s) (Where)
- The Business Time Dependencies

SABSA Model Overview

Our execution strategy incorporates proven methodologies, extremely qualified and seasoned personnel, and a highly responsive approach to managing deliverables. Following is a description of the overall SABSA Model for context and understanding.

SABSA is a methodology for delivering security infrastructure solutions that support the critical facets of the Enterprise. Further, SABSA is a model for developing a risk-driven information security architecture for the organization. SABSA uses a layered, top down model hierarchy that begins with an examination of the business security posture from the primary business drivers first and foremost. There are 6 layers to the SABSA model and this brief paper will serve to identify and detail in brief those 6 layers and how they are activated in the business. SABSA is widely accepted today as the most mature and comprehensive security architecture and a firm understanding of it’s underpinnings is critical for anyone who is developing enterprise level security standards for an organization.

As stated above, the SABSA model consists of 6 layers – Identified and categorized in the table below:

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

In order to bring context to the model, SABSA uses the same 6 questions across each of the 6 layers. Those questions are:

1. What are you trying to do at this layer?
2. Why are you doing it?
3. How are you doing it?
4. Who is involved?
5. Where are you doing it?
6. When are you doing it?

Once applied, this overlay against the 6 Architecture's combined with the 6 questions, results in a matrix model of 36 individual components. The table below illustrates this matrix as it is applied:

The SABSA matrix

SABSA	Assets (WHAT)	Motivation (WHY)	Process (HOW)	People (WHO)	Location (WHERE)	Time (WHEN)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetime and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites and Platforms	Security Operations Schedule

So, how does it work? How do these elements all link together? In practice, 5 of the six layers are stand alone and need to be developed and fleshed out as such, while the sixth layer known as the Operational Security Architecture layer is the one that spans all of the layers and is implemented for day-to-day management and maintenance of the model. In referencing the table above, you'll see that the operational layer implements the 5 W's/1 H in the context of day-to-day tactical application. In looking at

the other 5 layers of the model, you'll also notice that the Contextual layer deals with high level strategic elements of the business to include organizational model, relationships, geography, BPM and overall business risk modeling. At the Conceptual layer, you'll notice that this is the layer at which application elements begin to come into play: Business Attributes Profile, Control Objectives, Security Strategies, Trust frameworks, Security Domain modeling and specific security related deadlines. As we move through the remaining 3 layers of the architecture (Logical, Physical & Component), referencing the table above, you'll notice that each layer becomes progressively more tactical in its application until finally we reach the day-to-day implements of the model at the Operational level. The Operational level, as stated above, is the level at which the rubber meets the road and all of the layers are subsequently validated through regular operations.

The IBFS Interview Takeaways

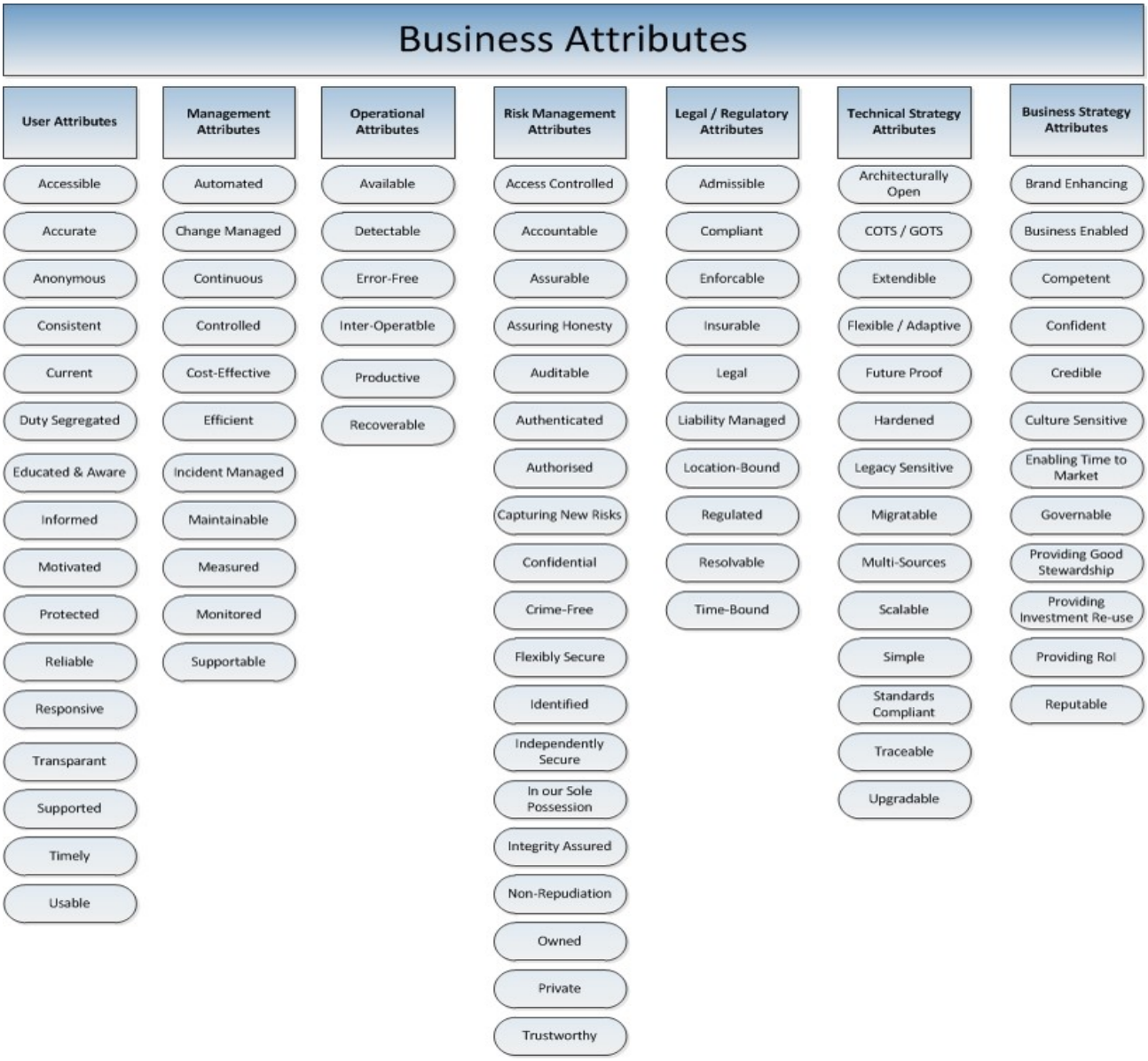
IBFS' Business Strategy is firmly rooted in the maintenance of its leadership position in the marketplace. According to CEO David Smith, a current reorganization process is underway and as part of this process IBFS is reengineering a number of it's processes. This document will serve to aid in the process of engineering an appropriate security posture which will fortify the mission to maintain market leadership positioning. Further, IBFS' footprint is global and their ability to scale security operations on a global scale to protect the brand is of paramount concern. Additionally, solutions must remain flexible, easy to use and promote the ability to give customers control in the customer lifecycle as explained by Rosemary Brown who heads up the eBusiness component of the business. Security strategy and solutions must take this into significant consideration if IBFS is to maintain its leadership position.

Financial concerns and ability to scale models across acquisitions and joint ventures are of paramount concern to Mr. Meyer who heads the Finance function of the IBFS organization. This Strategic approach must provide value and show ROI in order to convince a skeptical Meyer that security is a significant value add and business continuity pillar. Usability of core business systems as well as flexibility of those systems have been identified as significant concerns by both the SVP of Marketing and the CIO – stovepipe scenarios and integration complexities present challenges for the business and security posture and the security strategy must keep this in mind as it is developed to support the business. And finally, because IBFS operates in the Financial Sector, there are significant compliance requirements to various industry standards bodies.

All of the deliverables outlined in the "Deliverables" section, will contain very specific strategy and tactical recommendations to address each of these primary areas of concern.

Our Focus for this Proposal – The Conceptual Layer (Security Strategy)

First things first – In order to properly develop the Conceptual Layer of the model we will need to first develop the Business Attribute framework. At the header level of the business attribute framework are the following core areas: User Attributes; Management Attributes; Operational Attributes; Risk Management Attributes; Legal & Regulatory Attributes; Technical Strategy Attributes and finally Business Strategy Attributes. Each of these header categories has a number of sub items to be considered. In the below diagram provided you will find the expanded Business Attribute Framework:



Once we have been able to map all of these business attributes back to the Business Drivers and top level output obtained from the Contextual Layer report received as part of the prerequisites, we will be able to effectively create the Security Strategy Roadmap and begin to develop mapping structures for the subsequent Logical, Physical, Component and Operational layers of the SABSA model.

Once this has been fully developed and mapped we will take a specific look at the layering model of the organization – specifically a multi-layered security and multi-tiered incident handling approaches. From the highest levels working downstream in a multi layered model we will look at, address and document the following as outputs for your organization:

Multi-Layered Security Framework:

- Tier 1 Top Level – Policy, Organization & Responsibilities

- Tier 2 – Procedures & Practices; Security Management; Training & Awareness; Personnel Security; Document Security; Security Audit and Business Continuity Planning
- Tier 3 – Physical Security
- Tier 4 – Hardware Security
- Tier 5 – System Software Security
- Tier 6 – Application Software Security
- Tier 7 – Cryptography & Encryption Security
- Tier 8 – Information Assets

As part of the Security Infrastructure Layered Architecture deliverable, Nelley Consulting will deliver the following roadmaps for provisioning of Security Services across the organizations:

- A set of common security services delivered to applications through a common API model
- Recommendations on Security Middleware to integrate and deliver security services across distributed applications
- Security Services Recommendations for Systems/Platforms
- Security Services Recommendations for services embedded in the Network

Specific Outputs will be delivered as real world diagrams and Visio outputs that IBFS Security Operatives can use as a toolset for success. These assets will become part of the IBFS Best Practices and Procedural binders that will accompany the final delivery package should IBFS select Nelley Consulting to perform the work outlined in this engagement proposal.

Further, as part of this set of deliverables, Nelley Consulting will also look to establish and frame out Explicit and Implicit Security Services at the Security Services in the Application Layer along with Data Management and Information Transfer Security Services. So what does this mean? In the framework above, these services relate specifically to Tiers 5-7.

Explicit Security Services refer specifically to security services called specifically by any/all applications through the API.

Implicit Security Services refer specifically to those services provided by the middleware transparently through the application.

Data Management Security Services refer specifically to those services related to controlled access to data. Specifically we will document and outline strategies for:

- Metadata Management
- Relational Database Management
- Object Oriented Database Management
- Management Systems
- Database Access
- Data Warehousing
- Data Mining
- Transaction Process Monitoring

Data management Sub System Structures will also be included as part of the DMSS deliverable. These include but are not limited to the following recommendations on:

- Access Controls at the application & object levels
- Authorization Models based on Business Needs as defined in the Contextual Layer
- Data Availability Protection and Back-up/DR techniques
- Data Integrity Protection Implements

Information Transfer Security Services refer specifically to those services related to information transfer over your network – More specifically rules for data transfer at the subnet, network and transport layers. Specifically we will document and outline strategies for:

- LAN's (Local Area Networks)
- Campus Area Networks
- WAN's (Wide Area Networks)
- The Internet
- Intranets, Extranets and the Cloud
- VPN's

Subsequently, as part of this set of deliverables, Nelley Consulting will also provide specific strategic guidance and outputs for:

- Network Security Policy
- Domain Segregation Strategy
- Network Redundancy & Resilience
- Entity Authentication & Authorization
- Boundary Access and Connectivity Control
- Network Management Security & Resource Integrity Protection
- IDS/IPS & Network Monitoring Strategy
- Incident Response and Handling Strategy
- Network Vulnerability Handling & Research

With regard to Tier 8 – Information Assets, Nelley Consulting will also prepare a complete dossier of strategic outputs for the information processing layer which encompasses comprehensive strategies for handling devices, peripherals and operating systems that will be in use in the environment. Some examples of these include: Laptops, Printers, Peripherals, Other End Points (Mobile devices, dumb terminals, etc.). The list of items to be covered in this component of the deliverable is extensive and comprehensive. In the interest of saving time and brevity in the conveyance of this document, we will be happy to provide a comprehensive list of these items upon client request.

Finally, in regards to closing the loop on Information Security Services as part of the Strategic Security Plan Model, Nelley Consulting will also prepare specific strategies for the Authentication, Authorization and Audit outputs to ensure there are mechanisms in place to provide ongoing "check-downs" throughout the environment. These will translate into specific activities and procedures that will be outlined in the lower levels of the Architecture model.

As we move across the Conceptual Layer Model, next we will look at the Security Service Management Strategy. This can be broken down into two core areas:

1. The Management of Security Services
2. The Security of Service Management

The Management of Security Services speaks specifically to items related to provisioning security parameters for users, for applications, for embedded systems and equipment while also establishing routine security operations to maintain corporate systems to policy standards. Further, it establishes the security monitoring and intrusion detection criteria and breach recovery operations plans and procedures. These documents and procedural guidelines will also be developed as part of the Conceptual Layer set of deliverables.

The Security of Service Management components entail specific protocols for authorization of operator entities that will perform any of the service management functions. As part of this deliverable we will also outline the segregation of duties to protect the corporate environment from malicious activities of any single operator. We will achieve this through proper role definitions and deliver this schema as part of the deliverables package upon completion of the project scope.

Additional Strategies that will be developed as part of the Conceptual Layer Package Delivery are as follows:

- System Assurance Strategy
- Directory Services Strategy (Management & Objects)
- PKI Strategy
- Security Entity Model & Trust Framework
- Registration Process Outline
- Domain Strategies (Logical, Physical & Multi Domain Environment Management)

Finally – As we look to button up any all remaining conceptual items for delivery as part of this SOW, we will review and deliver a template that outlines a lifecycle management strategy for the following elements:

- Registration Lifetimes
- Certification Lifetimes
- Crypto Key Lifetimes
- Policy Lifetimes
- Token Lifetimes
- Password Lifetimes
- TTL for Messages
- Stored Data Lifetime Standards
- Data Secrecy Lifetimes
- User Session Lifetimes
- System Session Lifetimes
- Response Timeout Lifetimes
- Inactivity Rules
- Time Stamping Rules
- Trusted Time Parameters
- DR and Business Continuity timing Parameters

Supplied Material & Physical Deliverables of the Engagement

The following materials are to be supplied by IBFS for this project. For Nelley Consulting, LLC to meet project milestones, this material must be supplied on schedule. The due dates included in the following table represent our best guess based on current proposed project dates:

Deliverables to be supplied by IBFS	Due Date*
Business Attributes Model Architecture Diagram modeled for IBFS	PA + 2 weeks**
Comprehensive Multi-Layered Security Framework Document	PA + 4 weeks**
Roadmap Documents that outline a comprehensive Security Services Model & Strategy for DMI (Explicit, Implicit, Data Mgmt, Info Transfer)	PA + 5 weeks**
Specific Categorical Strategies (SA, DS, PKI, Domain)	PA + 6 weeks**
Provide a Document that outlines the Security Entity Model & Trust Framework as well as the Registration Process Outline	PA + 6 weeks**
Comprehensive Lifecycle Planning Document & Framework	PA + 7 weeks**
Security Metrics Framework Strategy for ROI – Mapped to Business Drivers	PA + 10 weeks**

**We cannot be responsible for cost overruns caused by client's failure to deliver materials by agreed-upon due dates.*

***PA = Date of Performance Agreement signature*

EXPECTED RESULTS

We expect our proposed solution to IBFS's requirements to provide the following ROI and benefit results:

Financial Benefits

- Reduced Overheads on Insurance Premiums related to Information Security Risk
- Penalty and fine avoidance in relation to security compliance standards for Financial Industry
- Reduced risk of Brand Tarnishment post implementation based on increased and elevated security posture
- Future Asset Loss Prevention – Elevated security strategy and posture should reduce risk profile post implementation

Functional Benefits

- Formalized and Documented set of Strategic Plans to map to lower layers of the SABSA Architecture Model
- Roadmaps for daily operatives to map strategic intention to tactical and day-to-day activities
- Documented Policies and Procedures that tie directly to business drivers established at Board and Executive Level

CONCLUSION

In conclusion, throughout this proposal document, we have attempted to outline a plan to deliver the Conceptual Layer outputs that will be critical for IBFS and its subsidiaries to enable build out of a robust security framework based on the SABSA Architecture model. If you accept this performance agreement and the deliverables set forth here-in, by the end of this phase of your engagement you will be prepared to move into the Design and Logical layers of the SABSA model and begin to identify physical, system and operational solutions that will shore up your overall security posture.

The Conceptual Security Layer that will be delivered here will serve as the “Big Picture” security strategy for your organization. It will effectively set the stage for all of your ongoing security operations and will provide a set of documents, policies and procedures that your Infosec staff and non Infosec staff can reference as the Security “Bible” of sorts. Everything about and within your business is an asset and you must find the most effective ways of protecting those assets.

If you select Nelley Consulting to perform this body of work, the Assets identified in the Business Attribute Profile will be used to deliver and drive a risk assessment methodology that will reflect a prioritized view of the risk landscape. The risk assessment outcomes from these deliverables will properly enable IBFS to develop an appropriate set of control objectives to mitigate risk. The layering techniques outlined here-in will help to solidify the Enterprise security posture and position IBFS for business continuity success. Here-in we have attempted to provide an overarching security service layered approach that maps to the overall SABSA Layer 2 Architecture assertion.

Finally, in tying back to specific commentary made in the series of interviews that were conducted by security analysts in support of the security reorganization for IBFS this package deliverable will help to ensure IBFS maintains a strong, secure global footprint as well as a strong leadership position in the markets they serve. Further, our recommendations will take into account the need for ease of use and interaction of IBFS’ global customer base, will live up to the highest security compliance standards and will set a course for securing data and information as it travels between independent systems within the network environment as well as those systems and platforms that are distributed beyond the firewall.

Only one question remains. When can we sign a performance agreement and get underway to ensuring a robust security posture for IBFS?

REFERENCES

Sherwood, Clark & Lynas; ***Enterprise Security Arhitecture – A Business Driven Approach***, Copyright CMP Media 2005

Andywood.info

Sabsa.org