CSOL520 Final Project: Conceptual Security Architecture

John C. McGovern

University of San Diego

Table of Contents

Introduction 3

Methodology 3

Conceptual Security Architecture Deliverables 4

Extended Business Risk Model with Control Objectives 6

Business Attributes Profile 8

Assessment of Current Security Status of the Enterprise 10

Security Strategies and Architectural Layering 11

Sample Security Strategy and Architecture Layering Document 13

Discussion 14

Conclusion 15

References 16

Appendix 17

Introduction

Intergalactic Banking and Financial Services Inc. (IBFS) has contracted with The Consulting Group (TCG) to provide architectural discovery, development, and review for a new proposed IBFS security architecture. TCG is pleased to report initial findings after an extensive review of external and internal documentation, interviews with key stakeholders, and a survey of both employees and external constituencies associated with IBFS. This report includes a variety of findings in the form of key deliverables. Based on refinement and acceptance of this report, TCG would propose to leverage its expertise in developing more in-depth and specific guidance facilitating the full development and implementation of the enterprise security architecture.

Methodology

The Consulting Group, in coordination with Intergalactic Baking and Financial Services, has chosen to use the Sherwood Applied Business Security Architecture or SABSA methodology. The SABSA institute on their website describes the methodology as follows

> SABSA is a proven methodology for developing business-driven, risk, and opportunity focused Security Architectures at both enterprise and solutions level that traceably support business objectives.
>
> It is also widely used for Information Assurance Architectures, Risk Management Frameworks and to align and seamlessly integrate security and risk management into IT Architecture methods and frameworks (The SABSA Institute, 2018).

This report focuses specifically on the Conceptual Architecture, also described as the "Architect's View" in the SABSA model. The Conceptual Architecture is focused on the highest-level architectural details after the business drivers and requirements are identified in the layer above (the Contextual Layer). The Conceptual Layer identifies Business Attributes and maps them to

Business, Drivers, Risks, and Control Objectives. The output and deliverables associated with the Conceptual Architecture are critical for future use by the Designers, Builders, and Technicians in lower-level layers of the architecture where data flow, security policies, and technical specifics are decided amongst other items.

Conceptual Security Architecture Deliverables

As part of the current engagement, The Consulting Group is providing a subset of Conceptual Layer deliverables described in Table 1 to Intergalactic Baking and Financial Services. The broader catalog of deliverables is enumerated in the 36-Cell SABSA Matrix, as provided in Appendix Table A-1.

Table 1

Conceptual Layer Deliverables with Description

Deliverable Name	Description
Extended Business Risk Model (BRM) with Control Objectives	This document maps business drivers in risks discovered at the Contextual Layer to Business Attributes for use in the 2nd Business Attributes Profile document. It also associates Control Objectives, which provide high-level insight into how success towards a particular business driver and risk will be measured.
Business Attributes Profile	This document collects all business attributes enumerated in the BRM and described their classification, definition, and measurement mechanisms.
Assessment of Current Security Status of the Enterprise	This document provides a view into the current state of the enterprise security architecture and identified both positive attributes and gaps that merit further discussion and potential action in the future.
Security Strategy and Architectural Layering Document	This document describes at the highest level the security strategy to be employed by the organization. It outlines architectural tiers and guides towards controls implemented to regulate information flow between tiers.

Sample Architectural Layering Document	This document provides a concrete example of how the Security Strategy can be applied to a particular high-level security service implemented within the organization.
Security Entity Model	This document classifies the security entities within the organization. Security entities can be defined as any user, organizational group, or automation that accesses or takes action on data.

Table 2

Extended Business Risk Model with Control Objectives

1	2	3	4	5	6	7	8	9	10	11	12	13
ID	**Business Driver**	**Business Attributes**	**Business Requirements**	**High-Level Threat**	**Business Impact**	**Impact Value**	**Potential High-Level Vulnerability**	**Green Field Vuln Value**	**Green Field Risk Cat**	**High-Level Control Objectives**	**Target Vuln Value**	**Mitigated Risk Cat**
BD001	Customer experience impacts competitive advantage or disadvantage.	Usable	Security features of any customer-facing business system must not create difficulties in use.	Customer becomes frustrated by difficult login processes and other security features.	Many customer go somewhere else where the experience is easier.	H	Multiple logins and authentications, each required a new password	H	A (Red)	Establish consistent easy-to-use authentication login procedures	L	C (Green)
BD002	Business in the future will be customer-driven.	Trustworthy Private Confidential	Customer who provide private information must be confident that it will be protected form disclosure	Customer details disclosed to unauthorized parties, and this becomes generally known	Wide loss of customer confidence Censure or prosecution by the regulators Eventual loss of operating license	H	Inadequate control over privacy of information	H	A (Red)	Establish strong physical security surrounding all customer data in transit, during processing and in storage Establish strong logical security surrounding all customer data, in transit, during processing and in storage	L	C (Green)
BD003	Data protection legislation.	Compliant Private Confidential	Must comply with data protection legislation	Customer details disclosed to unauthorized parties, and this becomes generally known	Wide loss of customer confidence Prosecution by the regulators	H	Inadequate control over privacy of information	H	A (Red)	Establish strong physical security surrounding all customer data in transit, during processing and in storage Establish strong logical security surrounding all customer data, in transit, during processing and in storage	L	C (Green)
BD004	Customer trust relationship.	Trustworthy Confident	Information systems must be based on the protection of trust for the customer.	Business is built on a high degree of customer trust in IBFS handling the customer's financial and insurance data.	Loss of customer trust. Impact to net new account and ultimately revenue.	H	Any vulnerability and subsequent breach could lead to a loss of trust.	H	A (Red)	Establish strong logical and physical security practice for each customer facing and internal application that handles customer data.	L	C (Green)

BD005	Rapidly changing financial services market.	Flexible Extendible	Product offerings are changing rapidly in the market and IBFS must keep up and innovate.	Business must adopt new systems and products rapidly to stay relevant, potentially moving faster than security review allows for.	Loss of customer satisfaction. Customer attrition due to lack of competitive offerings.	H	New systems rapid development leads to errors. Loss of data.	H	A (Red)	Structured security review process for each new application that handles customer data.	L	C (Green)
BD006	Geo-distributed 24/7 business.	Scalable Responsive Available	Customers, offerings, and locations are provided in many countries. Business is operational 365/24/7.	Must maintain security across a wide array of geographies, real property, and business units.	Loss of revenue in various geographies and market segments. Inability to serve customers in specific geographies.	H	Loss of customer data due to varying local security posture. Regulatory compliance failure.	H	A (Red)	Creation and implementation of standard security architecture across geographies. Ongoing logical and physical monitoring.	L	C (Green)
BD007	ICT infrastructure flexibility.	Flexible Flexibly Secure Future Proof	Ability to adapt business ICT systems to a rapidly changing business environment.	ICT systems must support rapidly changing business while still providing security in service of customer BD001.	Inability to deliver highly reliable, available, and relevant services to customers.	H	Security vulnerability exposure due to quick iteration and rapid release cycles.	H	A (Red)	Continuous security monitoring practice. Ongoing vulnerability scanning. Application security audits	L	C (Green)
BD008	Ease of use of business systems.	Simple Usable	Joint venture partners and 3rd parties evaluate partnership based on systems ease of use.	Ease of use is in some cases counter to the overall security of the solution or 3rd party exposed system.	Loss of joint venture interest. Loss of partner revenue and mindshare due to attrition.	H	Insufficient authentication and attribution controls lead to data exposure or loss.	H	A (Red)	Modern single sign-on system with extensive real-time monitoring. Secure development practices.	L	C (Green)
BD009	Systems modernization and data warehouse.	Legacy sensitive Extendible Productive	Centralize data "source of truth" allowing application to current, real-time datastore organization wide.	Data centralization creates a single large target, subject to high risk of attack due to centralization of data.	Inability to view most accurate data in a real time fashioned. Siloed views of information negatively impacts business decision making.	H	Data warehouse or middleware integration leads to data exposure or loss.	H	A (Red)	Data record access audit. Ongoing vulnerability scanning.	L	C (Green)

(Sherwood et al., 2019)

Table 3

Business Attribute Profile

Business Attribute	Attribute Classification	Attribute Explanation	Business Driver	Owner (Accountability Structure)	Recommended Measurement Category	Recommended Measurement Approach
Available	Operational Attribute	The information and services provided by the system should be available according to the requirements specified in the SLA.	BD006	Chief Information Office	Uptime	As specified in the SLA.
Compliant	Legal & Regulatory Attribute	The system should comply with all applicable regulations, laws, contracts, policies, and mandatory standards, both internal and external.	BD003	Chief Legal Officer Chief Compliance Officer	Audit Findings	Independent audit and review against Security Architecture Capacity Maturity Model by computer forensics expert.
Confident	Business Strategy Attribute	The system should behave in such a way as to safeguard confidence placed in the organization by customers, suppliers, shareholders, regulators, financiers, the marketplace, and the general public.	BD004	Chief Information Security Officer	Survey Results	Independent audit, or focus groups, or satisfaction surveys.
Confidential	Risk Management Attributes	The confidentiality of (corporate) information should be protected in accordance with security policy. Unauthorized disclosure should be prevented.	BD002 BD003	Chief Information Security Officer	Internal Reporting	Reporting of all disclosure incident, including number of incidents per period, severity and type of disclosure.
Extendible	Technical Strategy Attribute	The system should be capable of being extended to incorporate new functional modules as required by the business.	BD005 BD009	Chief Information Office	Audit Findings	Independent audit and review against Security Architecture Capability Maturity Model of technical architecture (conceptual, logical, physical).
Flexible	Technical Strategy Attribute	The system should be flexible and adaptable to meet new business requirements as they emerge.	BD005 BD007	Chief Information Office Chief Product Officer	Audit Findings	Independent audit and review against Security Architecture Capability Maturity Model of technical architecture (conceptual, logical, physical).
Flexibly Secure	Risk Management Attributes	Security can be provided at various levels, according to business need. The system should provide the means to secure information according to these needs, and may need to offer different levels of security for different types of information (according to security classification).	BD007	Chief Information Security Officer	Audit Findings	Independent audit and review against Security Architecture Capability Maturity Model.
Future-proof	Technical Strategy Attribute	The system architecture should be designed as much as possible to accommodate future changes in both business requirements an technical solutions.	BD007	Chief Information Office Chief Product Officer	Audit Findings	Independent audit and review against Security Architecture Capability Maturity Model of technical architecture (conceptual, logical, physical).

Legacy-sensitive	Technical Strategy Attribute	A new system should be able to work with any legacy systems or databases with which it needs to inter-operate or integrate.	BD009	Chief Information Officer	Audit Findings	Independent audit and review against Security Architecture Capability Maturity Model of technical architecture (conceptual, logical, physical).
Private	Risk Management Attribute	The privacy of (personal) information should be protected in accordance with relevant privacy or data protection legislation, and so as to meet the reasonable expectation of citizens for privacy. Unauthorized disclosure should be prevented.	BD002 BD003	Chief Information Officer Chief Privacy Officer	Internal Reporting	Reporting of all disclosure incident, including number of incidents per period, severity and type of disclosure.
Productive	Operational Attribute	The system and its services should operate so as to sustain and enhance productivity of the user with regard to the business processes in which they are engaged.	BD009	Chief Operations Officer	Performance Metrics	User output targets related to specific business activities.
Responsive	User Attribute	The users obtain a response within a satisfactory period of time that meets their expectations.	BD006	Chief Product Officer Chief Information Officer	Performance Metrics	Response time.
Scalable	Technical Strategy Attribute	The system should be scalable to the size of the user community, data storage requirements, processing throughput and so on, that might emerge over the lifetime of the system.	BD006	Chief Information Officer	Audit Findings	Independent audit and review against Security Architecture Capability Maturity Model of technical architecture (conceptual, logical, physical).
Simple	Technical Strategy Attribute	The system should be as simple as possible, since complexity only adds further risk.	BD008	Chief Product Officer	Audit Findings	Independent audit and review against Security Architecture Capability Maturity Model of technical architecture (conceptual, logical, physical).
Trustworthy	Risk Management Attribute	The system should be able to be trusted to behave in the ways specified in its functional specification and should protect against a wide range of potential abuses.	BD002 BD004	Chief Information Officer Chief Information Security Officer	Survey Results	Focus groups or satisfaction surveys research around the question "Do you trust the service?"
Usable	User Attribute	The system should provide easy-to-user interfaces that can be navigated intuitively by a user of average intelligence and training level (for the given system). The user's experience of these interactions should be at best interesting and at worst neutral.	BD001 BD008	Chief Product Officer	Performance Metrics	Number of clicks or keystrokes required. Conformance with industry standards - e.g. color palettes. Feedback from focus groups.

Assessment of Current Security Status of the Enterprise

As part of the engagement, The Consulting Group has performed an initial assessment of security strengths and weaknesses regarding the Intergalactic Banking and Financial Services environment mapped to the Extended Business Risk Model and Control Objectives Drivers. This assessment was based on interviews with various stakeholders in a variety of business units. Qualitative results were scored and averaged based on a scale of Negative to Positive with five total gradations.

Table 4

Current Security Status Sentiment

Business Driver	High-Level Threat	Current Status	Notes
BD001	The customer becomes frustrated by complicated login processes and other security features.	Slightly Positive	Current customer sentiment is generally positive towards the majority of IBFS services.
BD002	Customer details disclosed to unauthorized parties, and this becomes generally known.	Positive	Currently, no known breaches. Current controls have proven effective in the legacy toolset.
BD003	Customer details disclosed to unauthorized parties, and this becomes generally known.	Neutral	Compliance with data protection legislation is an ongoing effort that is starting to get board-level visibility to the GRC committee.
BD004	Business is built on a high degree of customer trust in IBFS handling the customer's financial and insurance data.	Positive	Up to this point, customer trust has been protected. The business has currently avoided major breaches but is looking to continue strengthening its security posture while accelerating product innovation.
BD005	Business must adopt new systems and products rapidly to stay relevant, potentially moving faster than security review allows for.	Neutral	The cybersecurity or has so far been able to review new apps handling customer data. However, emergent technologies (cloud, containerization, etc.) and acceleration could threaten this capability in the future.

BD006	Must maintain security across a wide array of geographies, real property, and business units.	Negative	Currently, security standards and implementation vary based on geographic region. Work towards a central security architecture is beginning.
BD007	ICT systems must support rapidly changing business while still providing security in service of customer BD001.	Slightly Negative	Further architectural review and additional controls on internal ICT system supporting employees would help ensure secure access to customer data is enforced.
BD008	Ease of use is, in some cases, counter to the overall security of the solution or 3rd party exposed system.	Slightly Negative	Business must streamline security authentication for 3rd parties and trusted joint ventures while preserving ease of use. Current efforts and analysis in this regard are ongoing, but the adoption of a Single Sign-On Mechanism is delayed due to legacy system support.
BD009	Data centralization creates a single large target, subject to a high risk of attack due to centralization of data.	Slightly Positive	Data warehouse initiative is off to a promising start, and a "greenfield" project allows for security control in monitoring to be put in place early and validated.

Security Strategies and Architectural Layering

TCG recommends that Intergalactic Banking and Financial Services leverages a Zero Trust model for their primary security architecture. Zero Trust is a thoroughly modern take on cybersecurity architecture, and it has seen adoption by a large number of organizations and cybersecurity vendors as the architectural standard of choice. This is especially true in greenfield or cloud-native scenarios where traditional architectures are rendered less effective based on shifting application topology and cloud services (Pratt, 2018). Table 5 describes the differences between a perimeter architecture (also known as "castle and moat" or "eggshell") and a Zero Trust architecture.

Table 5

Perimeter-Based vs. Zero Trust Security Architecture Comparison

Item	Perimeter-Based	Zero Trust
Trust Model	Outside the network perimeter is untrusted, and insider the perimeter is a largely trusted network. Services can communicate freely.	All services and communications are considered untrusted. Specific exceptions are made so services can communicate using specific protocols.
Protocol Controls	Any protocol-level control is limited to TCP/UDP level port allowances.	Application introspection into each open port ensures not only port but protocol level enforcement (i.e., no SSH reverse tunneling running over DNS).
Entity Authentication	Security entities are represented and controlled as IP addresses, which may change based on network type or location.	Security entities are represented and controlled through a distinguished name ascribed to a particular entity at a point in time, which may change based on who is using the device.
Supports Modern Distributed Architectures	Limited support for the new distributed perimeter models and cloud-based architectures.	Supports multi-perimeter micro segmentation-based deployments using a mixture of on-prem, cloud, and SaaS.
Best For	Support of traditional or legacy applications for which full knowledge of application and entities is not available.	Greenfield applications and applications that don't have a defined perimeter. Areas where next-generation controls can be implemented.
Complexity	Lower complexity due to lowered visibility and control requirement. Communication by default.	Increased complexity due to micro-segmentation and additional controls.
Cost	Lower.	Higher.

To realize a Zero Trust approach to enterprise security architecture, each security entity must be authenticated to the network. That authentication data (based on a distinguished name or DN) should be used as a control for any access to a system or application. For example, access to the core Enterprise Resource Planning (ERP) system would require an IP address from a trusted network or Virtual Private Network (VPN) and confirmed entity authentication. An entity with the same address but failing authentication would not be allowed access to the resource. Furthermore, protocol level application inspection ensures that traffic sent to a system or application is actually of the intended protocol. Finally, if a system fails a security audit, it will not be allowed to access trusted resources, regardless of the entity privilege level (Pratt, 2018).

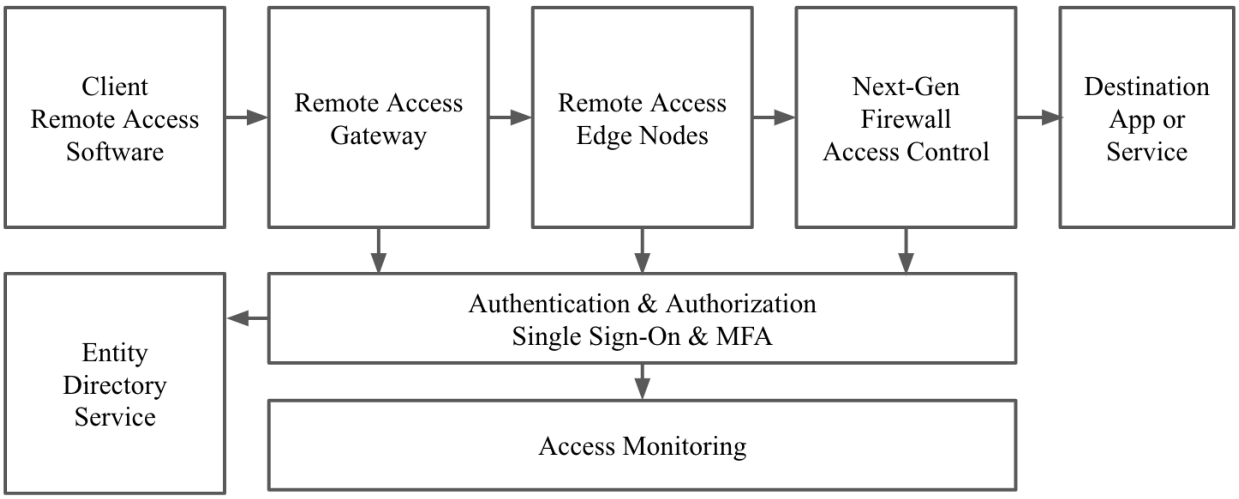
All access to secured applications and systems should be monitored. Anomalous access or failed access should raise an alert in the monitoring system.

Sample Security Strategy and Architecture Layering Document

Each subsegment of the security architecture should be described by a Security Strategy and Architectural layering breakout document. These documents exist to further describe the components of the security architecture in more detail for later use in the logical and physical security deliverables. Figure 1 provides an example illustrating the remote access components of the enterprise security architecture.

Figure 1

Remote Access Architectural Layering Document



In this Figure, the client system uses remote access (VPN) software to connect to a secure remote access gateway. The gateway's function is to first authenticate the connection to a particular security entity (using distinguished name or e-mail, password, and multi-factor (MFA) token) and then pass on the connection to the closest available edge node. The edge node and next-gen firewall can use authentication information to enforce access levels and only provide access to resources over the network as needed based on the entity's aggregate permission level. Finally, traffic is passed to the destination application or service as required. Connection, authentication, authorization, and ultimately access information is logged to a monitoring database for auditing purposes. These mechanisms ensure that the security entity only receives the appropriate level of access, and all access is audited.

Discussion

Significant progress has been made in support of an updated Enterprise Security Architecture for IBFS. There is more to be done to deliver on the next, more tactical layers of the enterprise security architecture. TCG recommends that work begins on first the Logical

architecture, and after that, the Physical architecture layer mapped to the SABSA model. Logical Layer deliverables would include Security Policy Architecture, Security Policies, Security Services, Entity Schema, and Security Domain assessment and documentation. Physical Layer deliverables would include Business Data Model, Security Rules, Practices, & Procedures, Security Mechanisms, and Platforms & Network Infrastructure documentation. These deliverables would be provided with the ultimate goal of building IBFS and comprehensive well-architected cybersecurity architecture that aligns with business needs, secures the flow of information throughout the organization, and ultimately provides practitioners with tactical guidance to carry out their responsibilities.

Conclusion

The Consulting Group is deeply appreciative of the opportunity to work with the Intergalactic Banking and Financial Services organizations and teams within. The work product provided in this report lays the foundation for a sound Enterprise Security Architecture that is rooted in an understanding of the complex structure and workings of IBFS as a global leader in the Financial Services industry and takes into account the unique challenges and objectives of the organization. We look forward to further defining each layer of the architecture through continued partnership and work with key stakeholders to deliver the various component pieces to the organization.

References

Pratt, M. K. (2018, January 16). *What is Zero Trust? A model for more effective security*. CSO Online. https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

Sherwood, J., Clark, A., & Lynas, D. (2019). Enterprise Security Architecture: A Business-Driven Approach. Routledge.

The SABSA Institute. (2018, October 29). *SABSA Executive Summary*. https://sabsa.org/sabsa-executive-summary/

Appendix

Table A-1

36-Cell SABSA Matrix

	Assets (What)	**Motivation (Why)**	**Process (How)**	**People (Who)**	**Location (Where)**	**Time (When)**
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization 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