

Business-Driven Security Architecture — Requirements Analysis

A SABSA Business-Attribute Profiling Work Sample

Author: Allison Manning **Methodology:** SABSA (Sherwood Applied Business Security Architecture) — Contextual & Conceptual layers **Client:** Victory Dream Team Realty (fictional case study)

About this document. This is a work sample demonstrating the SABSA approach to security architecture: deriving security requirements from business drivers rather than starting from technology. It develops the contextual layer (business drivers, business-attribute profile, asset assessment) for a fictional small real-estate firm, showing the traceability from *what the business cares about* to *what security must deliver* — the core competency behind business-aligned security architecture and second-line risk roles.

Introduction

Businesses of every size must give appropriate attention to the cybersecurity threats prevalent in their industry. Data is lucrative whether the target is a multi-billion-dollar enterprise or a family-owned business. A3C Consulting's multidisciplinary team brings knowledge across network security, incident response, and ethical hacking, applying current tools and methodologies to assess, mitigate, and prevent cyber threats and to develop defense strategies aligned to each client's business.

The following analysis develops the business-requirements foundation for securing a small to medium-sized real-estate firm — establishing the drivers, attributes, and assets that any subsequent control selection must serve.

Project Overview — Securing Victory Dream Team's Network

Victory Dream Team (VDT), a real estate company specializing in the Arizona and California markets, engaged A3C Consulting to secure its network. VDT is committed to quality homes and customer service, delivered by a team of ten professionals guiding clients through buying and selling. Network security is integral to those operations.

VDT's Organizational Structure

Understanding VDT's structure enables more nuanced, effective planning. At the helm is the Team Leader and Principal Broker, who sets strategic direction. The team comprises four Realtors reporting to the Team Leader; an Operations Manager and a Marketing Director; a digital-platform specialist who extends the reach of property listings; an administrative assistant managing key operational tasks; and a Transaction Coordinator who shepherds each transaction to closing.

Operating Environment and Infrastructure

VDT operates from a 2,400 sq. ft. office comprising a lobby, an open-concept realtor space for collaboration, four offices for strategic and operational management, a conference room, and a break room. The network includes laptops, desktops, mobile phones, tablets, and VoIP phones, connected through a commercial ISP router, firewall, switch, and wireless access points.

Software Utilized by VDT

VDT's realtors use industry-specific software including a regional MLS, Broker Mint, SkySlope, Follow Up Boss, YLOPO, DocuSign, and kvCORE. Several provide API integration enabling connection between applications and mobile solutions. Notably, initial research found no dedicated security software in use in the office or on agents' devices — a material gap the architecture must address.

Section 2 — Business Requirements

Business Drivers

ID	Business Driver
BD1	Protect reputation
BD2	Protect transmitted data
BD3	Protect stored data
BD4	Generate revenue
BD5	Protect brand
BD6	Maintain market lead in tiny-home market
BD7	Maintain customer loyalty
BD8	Provide value-added services to stakeholders/customers
BD9	Maintain a digital business platform
BD10	Generate leads
BD11	Ensure compliance is met
BD12	Maintain positive relationship with employees
BD13	Maintain availability of systems
BD14	Protect the trust that exists with stakeholders and partners
BD15	Maintain accuracy of information
BD16	Protect against fraud
BD17	Have ability to detect fraud
BD18	Maintain privacy of data
BD19	Provide accurate transactions and transaction history
BD20	Provide secure transactions
BD21	Provide quick transactions
BD22	Ensure only authorized users can access systems and data
BD23	Maintain personal device security
BD24	Ensure security solutions do not hinder operations
BD25	Ensure ease of use of security solutions

Business Attributes Profile

The SABSA business-attribute profile translates the drivers above into the qualities the security architecture must exhibit, grouped by stakeholder dimension.

Dimension	Attributes
User	Accessible, Accurate, Consistent, Educated & aware, Informed, Motivated, Protected, Reliable, Supported, Timely, Usable
Management	Automated, Change-managed, Controlled, Efficient, Maintainable, Measured, Supportable
Operational	Available, Continuous, Detectable, Error-free, Inter-operable, Productive, Recoverable
Risk Management	Access-controlled, Accountable, Assurable, Assuring honesty, Auditable, Authenticated, Authorized, Capturing new risks, Confidentiality, Crime-free, Flexibly secure, Identified, Independently secure, Integrity-assured, Non-repudiable, Owned, Private, Trustworthy
Legal & Regulatory	Compliant, Insurable, Liability-managed, Resolvable, Time-bound
Technical Strategy	Architecturally open, COTS-compliant, Extendable, Flexible & adaptable, Future-proof, Legacy-sensitive, Migratable, Multi-sourced, Scalable, Simple, Standards-compliant, Traceable, Upgradeable
Business Strategy	Brand-enhancing, Business-enabled, Competent, Confident, Credible, Culture-sensitive, Enabling time-to-market, Governable, Good stewardship/custody, Investment re-use, Return on investment, Reputable

Business Organization & Relationships

#	Concept	Description	Interactions	Quality Measure
1	Customer Empowerment	Customers make informed decisions using accessible, timely, accurate digital tools (listings, virtual tours, comps).	Information Systems, Customer Service, Technical Systems	Accuracy of property information; smoothness of digital interactions
2	Customer Service	Reliable, consistent service builds trust, loyalty, and referrals.	Customer Empowerment, Trust, Technical Systems	Responsiveness; market and procedural knowledge
3	Information Security	Compliant safeguards ensuring reliability and accessibility of platforms while protecting client information.	Customer Service, Information Systems	Data protection; system availability; transaction trust
4	Trust	Built through controlled, consistent, protected, traceable dealings, often via third-party verification.	Customer Service, Third-Party Verification, Technical Systems	Consistency and transparency; honesty in representation
5	Third-Party Verification	Protected, compliant entities (inspectors, lenders) that authenticate information and enhance trust.	Trust, Technical Systems	Reliability and trustworthiness of third parties
6	Technical Systems	Infrastructure (websites, CRM, security, comms) supporting operations; must be flexible, adaptable, brand-enhancing.	Customer Empowerment, Information Systems, Information Security, Customer Service, Trust	Reliability; usability; security of infrastructure
7	Information Systems	Usable, compliant, accurate platforms providing property information and enabling communication.	Customer Empowerment, Technical Systems, Information Security	Usability; data accuracy

An Organizational Process Model diagram accompanies this section in the source document (not reproduced here).

Asset Assessment

Assets classified as physical or digital, with owner, users, location, and importance.

Asset	Owner	Users	Location	Importance
Employees	CEO	Potential clients	Remote & in-office	Daily client interface; primary driver of reputation and growth
Office space	Operations Manager	Employees, clients	Office	Professional environment; enables collaboration
Technology endpoints	Operations Manager	Employees	Office & remote	Anywhere-access; efficiency; data availability
Business licensing	CEO	Employees, stakeholders	Office (paper) / Cloud	Legal authority to operate
Company website	Marketing Director	Employees, clients	Server / hosted	Online presence; lead generation; testimonials
Reputation	CEO	Stakeholders	Conceptual	Trust and credibility; talent recruitment
Branding	CEO	Employees, clients, stakeholders	Conceptual	Market presence; trust and credibility
Digital marketing software	Listing Agent	Employees, stakeholders	Cloud	Marketing automation; targeted campaigns
Document management software	Operations Manager	Employees, clients	Cloud	Central document repository; workflow automation; backups
CRM software	Operations Manager	Employees	Cloud	Centralized customer data; relationship management; performance tracking
Real estate platform	CEO	Employees, clients	Cloud	Property repository; lead generation
Market trend reports	CEO	Employees, stakeholders	Office / Cloud	Decision support; competitiveness

Success Factor Statement

Security is paramount in real estate: the organization handles sensitive data and carries a brand and reputation to protect. From the drivers, attributes, assets, organizational structure, and process model above, A3C developed a well-rounded plan to protect the business and ensure continuity as threats evolve — prioritizing transparent security and business continuity so VDT can focus on growth and on establishing a foothold in the tiny-home market. Robust security supports stakeholder confidence and compliance, positioning VDT as an industry leader while enabling exceptional service and stronger lead generation.

Business Needs: transparent security · data security · business continuity · loss/fraud prevention · brand and reputation protection · asset-risk management

Business Goals: grow the business · gain a tiny-home market foothold · increase brand awareness · deliver exceptional customer service · improve lead generation and customer relations · become tiny-home market leader · meet compliance · garner stakeholder confidence · give agents tools to succeed

Success Factors: increased customer base · brand recognition (tiny-home leader) · quick transactions · easy-to-use technology — *security drives the business needs and goals.*