Group Assignment 4.1: Creating the Logical Architecture

Jacob Harrison

Joshua A. Wortz

Stephanie Wright

University of San Diego

CSOL-520

Melanie Thomas, M.S.

03/24/2025

Creating the Logical Architecture

Bene Gesserit Urgent Care (BGUC) is a growing healthcare network with multiple locations connected to a centralized data management system. This system allows seamless sharing of patient data, prescriptions, insurance details, and payments across its offices. To implement an effective security architecture using the SABSA framework, it's important to assess the organization's current security environment and identify future needs.

Existing Security Infrastructure and Components

BGUC currently relies on various critical systems, including network security with firewalls, VPNs, and secure routers; a centralized Electronic Medical Records (EMR) system for patient data management; e-prescriptions linked to pharmacies; secure online payment services for insurance and billing; and patient-facing services like online check-ins and payment portals. Core security controls are in place, such as role-based access controls (RBAC), multi-factor authentication (MFA), data encryption, endpoint protection, SIEM monitoring, and an incident response plan. BGUC also adheres to HIPAA, PCI-DSS, and other regulations, supported by a dedicated IT and security team, a compliance officer, and third-party vendors.

Raw Materials Needed for Security Planning

For effective security planning, essential materials include business and regulatory requirements (such as HIPAA and PCI-DSS), an inventory of assets and systems, risk assessments, and past incident reports. Comprehensive documentation is needed for the security plan, including asset inventory, network and data flow diagrams, compliance documentation, and incident response plans.

Architectural Tools for Documenting the Security Design and Existing Resources

Several tools are available for documenting the security design, including Microsoft Visio for network diagrams, Lucidchart for collaborative work, threat modeling tools like OWASP Threat Dragon, and enterprise tools like ArchiMate for complex architecture documentation. BGUC's existing resources, such as the EMR system, network security tools, HIPAA-aligned policies, vendor agreements, and IT/security teams, can be leveraged in the planning process.

Resources Available for Security Design

In the security design phase, BGUC can rely on internal IT and security teams, vendor support, compliance guidance, project management resources, and existing training programs. By aligning security services with BGUC's operational needs and using the SABSA framework, the organization can create a scalable, secure environment to protect sensitive healthcare data as its network of urgent care centers grows.

For further guidance, resources like The SABSA Institute and *Enterprise Security Architecture: A Business-Driven Approach* by Sherwood, Clark, and Lynas provide in-depth knowledge of the SABSA methodology, helping to align security services with business goals and risk management strategies in the healthcare sector.

Given BGUC's handling of sensitive patient data and electronic prescriptions, regulatory compliance is crucial. Resources such as the U.S. Department of Health & Human Services (HHS) HIPAA Security Rule and NIST Special Publication 800-66 Revision 1 provide essential frameworks for implementing necessary safeguards. The NIST Cybersecurity Framework (CSF)

is recommended for developing robust healthcare security programs, while NIST SP 800-53 Revision 5 offers technical controls suitable for securing federal or healthcare systems. The Center for Internet Security (CIS) Controls Version 8 provides practical guidance to enhance security posture.

For architecture and documentation, tools like Microsoft Visio, Lucidchart, and Draw.io are commonly used to visualize system and security designs, with Lucidchart offering healthcare-specific templates. Threat modeling tools such as Microsoft's Threat Modeling Tool and OWASP Threat Dragon assist in identifying and mitigating security risks in systems handling electronic health records, insurance data, and prescriptions.

Industry reports like the Verizon Data Breach Investigations Report (DBIR) and the HIMSS Cybersecurity Survey provide valuable insights into healthcare-specific risks and controls. Academic databases like Google Scholar, ACM Digital Library, and IEEE Xplore offer peer-reviewed articles on cybersecurity architecture, SABSA, and healthcare data security. Utilizing these resources will enable BGUC to develop a comprehensive security architecture that meets business needs and regulatory compliance.

Business Information Model:

System/Function	Purpose/Functionality	Connection/Integration

(EMR)	Secure management of patient medical records	Linked to patient portal, billing systems, and pharmacy database
E-Prescription System	Secures prescription transfer to pharmacies	Intertwines EMR and Pharmacies via API
Insurance & Billing System	Manage insurance claims, patient billing, and secure online transactions	Connected with EMR for patient data and payment systems
Patient Facing Portal	Allows online check-ins, reservation scheduling, virtual waiting rooms, payment access	Integrated into EMR and billing processes with desktop and mobile access
Security Information & Event Management (SIEM)	Oversees system logs, identifies anomalies, and triggers intrusion alerts	Merges data logs from EMR, billing, client portal, workstations, and network devices
Network & Endpoint Security	Secures network traffic and devices using firewalls, VPNs, antivirus, and EDR	Secures information flow between all processes, locations, and external third-party vendors
Vendor Systems	Facilitates collaboration between pharmacies, payment processors, and insurers for prescription and payments	Establishes connections through secure APIs, VPNs, and mandates vendor compliance agreements.

Security Policy Statement:

Bene Gesserit Urgent Care (BGUC) is dedicated to securing sensitive patient information through a comprehensive security policy. This policy mandates that all BGUC systems and devices, including workstations, mobile devices, and remote access points, adhere to strict access control protocols such as role-based access controls (RBAC), multi-factor authentication (MFA), and encryption. To prevent data exfiltration, Data Loss Prevention (DLP) tools will be implemented alongside Endpoint Detection and Response tools to protect against malware and cyber threats. BGUC's supply chain vendors must comply with security requirements through service level agreements and annual assessments. The security policy also includes regular patch management, vulnerability scans, and firewall rule analysis to mitigate risk exposure. In the

event of a security breach, BGUC has an incident response plan in place to ensure proper reporting and response. All employees and vendors are required to undergo regular security awareness training, promoting a positive cyber culture and safeguarding patient data.

Proposed Security Services:

BGUC plans to implement a multi-layered security approach based on the SABSA framework, as well as HIPAA and NIST standards. Core services will include Single Sign-On (SSO) and Multi-Factor Authentication (MFA), both compliant with HIPAA Security Rule requirements for access control. To strengthen network security against insider threats, BGUC will adopt a Zero Trust architecture, incorporating micro-segmentation and least privilege-access protocols. This approach helps mitigate cybersecurity risks like ransomware, phishing, and business email compromise.

Additional protections will include Endpoint Detection and Response (EDR) and Data Loss Prevention (DLP) tools to prevent malware and unauthorized data breaches. BGUC will also implement a Security Information and Event Management (SIEM) tool for centralized monitoring and incident response. A role-based entity schema will categorize users (e.g., admin staff, healthcare staff, finance staff, third-party contractors, and patients) to ensure customized privilege access aligned with business objectives and compliance standards.

Security Domain Definitions and Associations

Security Domain	Purpose	Controls & Policies

Trusted Internal Domain	Facilitates critical systems: EMR, billing, insurance processes	RBAC, MFA, Encryption, HIPPA compliance
Demilitarized Zone (DMZ)	Features public interface services: patient portals, transaction gateways	Firewalls, IDS, regulated third party access
External Vendor Domain	Supply chain vendors (pharmacy systems, payment platforms, and insurance integrations) included	API controls, contractor audits, supply chain reviews
Secure Cloud Services Domain	Manages backups, telemedicine, and future cloud solutions	Recurring SIEM monitoring, Data encryption (at rest & in-transit)
Network Perimeter	Parameter between internal systems and external networks	Firewalls, VPNS, IDS/IPS, Zero Trust rules to regulate unauthorized access

Security Processing Cycle:

BGUC adheres to a systematic and structured security processing cycle to ensure operational security and compliance with regulatory requirements. Password renewal policies will be enforced which require users to change their passwords every 90 days to mitigate password attacks. Additionally, firewall rules will be regularly reviewed to keep pace with evolving cyber threat trends. Operating system and critical patches will be updated within 15 days, followed by regular vulnerability scans to maintain robust security measures. BGUC will conduct quarterly incident response simulations to ensure resilience. This will confirm employee compliance with regulations and provide training opportunities. Our SIEM logs will undergo regular reviews and updates. These processing cycles comply with best practices as recommended by the NIST Cybersecurity Framework (NIST, 2018).

References

Cybersecurity Framework | NIST. (2025, March 14).NIST. https://www.nist.gov/cyberframework

Rights, O. F. C. (2022, October 20). *The security rule*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/security/index.html

Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise Security Architecture: a Business-Driven Approach*

The SABSA Institute. (2025, March 5). *The SABSA Institute*. https://sabsa.org/

Verizon Business. (n.d.). Verizon Business. https://www.verizon.com/business/resources/reports/dbir/