Assignment 1.1: CSOL Capstone Scenario Experience

Joshua A. Wortz

University of San Diego

CSOL-599

Dr Moore

06/29/2026

Assignment 1.1: CSOL Capstone Scenario Experience

Part 1. Overview and Security Policies

Scenario Overview:

Acuity Health (Bene Gesserit Urgent Care Model) *From the perspective of the CEO/COO to the new CISO:*

Welcome to the team. As our new Chief Information Security Officer, your primary mandate is to secure our rapidly expanding network of urgent care clinics. Our strategic business objective is to provide seamless, highly available patient care across multiple geographic locations while supporting modern healthcare demands, including telemedicine, online patient check-ins, and digital prescription transmissions. This business-driven architectural approach is critical to ensuring that our technology foundation enables our clinical performance (Sherwood, Clark, & Lynas, 2009).

However, we are operating under significant constraints. Foremost, our IT and Security departments are disproportionately small compared to our rapid multi-site growth. Second, we operate in a highly regulated environment that requires strict adherence to HIPAA and PCI DSS standards (U.S. Department of Health and Human Services [HHS], 2022). Because we cannot afford to deploy and manage heavy on-premise infrastructure at every new clinic, our future architecture must be highly scalable. It will rely heavily on cloud-hosted services and a Zero Trust Architecture (ZTA) paradigm, shifting our defenses away from a static, network-based perimeter toward a focus on users, assets, and resources (Rose, Borchert, Mitchell, & Connelly, 2020). We need you to design a high-level security architecture and policy framework that protects our centralized Electronic Medical Records (EMR), secures our integrations with

external pharmacies, and ensures high availability without overwhelming our small operational staff.

Overarching Business Operational Risk Management Policy

- **Purpose:** To systematically identify, evaluate, and mitigate risks that threaten the operational continuity, strategic objectives, and regulatory standing of the medical center.
- **Scope:** This policy applies to all enterprise operations, third-party vendor integrations (such as pharmacy and payment processors), clinical workflows, and cloud service deployments.
- **Definitions:**
    - **Operational Risk:** The prospect of loss resulting from inadequate or failed internal processes, people, and systems, or from external events.
    - **Supply Chain Risk:** The risk introduced by external vendors interacting with the trusted internal domain (NIST, 2018).
- **Responsibilities**: Executive leadership is responsible for final risk acceptance. The CISO is responsible for designing the risk assessment framework. All department heads are responsible for identifying risks within their respective clinical or operational units.
- **Compliance:** Risk management practices must comply with the NIST Cybersecurity Framework version 1.1 and HIPAA Security Rule requirements for annual risk assessments (NIST, 2018; HHS, 2022).

- **Monitoring:** The security team will continuously monitor operational risks using a centralized Security Information and Event Management (SIEM) system to detect anomalies and track threat vectors.
- **Review:** This policy and all associated risk registers will be reviewed and updated annually by the CISO and the executive board, or immediately following a significant security incident.

Information Security Policy

- **Purpose:** To protect the Confidentiality, Integrity, and Availability (CIA) of patient Electronic Medical Records (EMR), financial data, and intellectual property against internal and external cyber threats.
- **Scope:** This policy applies to all employees, contractors, endpoints, networks, and cloud environments interacting with the medical center's data. Specifically, it governs high-risk entry points vulnerable to session hijacking on clinical tablets, unauthorized lateral movement from public clinic Wi-Fi zones into internal subnets, and data exfiltration risks occurring via external pharmacy or insurance API connections.
- **Definitions:**
    - **Zero Trust Architecture (ZTA):** An enterprise cybersecurity architecture designed to prevent data breaches and limit internal lateral movement by assuming no implicit trust is granted based on network location (Rose et al., 2020).
    - **PHI:** Protected Health Information.

- **Responsibilities:** The IT and Security departments are responsible for implementing technical controls. All staff members are responsible for adhering to data handling guidelines and completing security awareness training.
- **Compliance:** The organization will enforce mandatory Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and encryption for data at rest and in transit to maintain compliance with HIPAA and PCI DSS (HHS, 2022).
- **Monitoring:** Compliance with this policy is monitored through continuous automated entitlement checks, Intrusion Detection Systems (IDS), and audit trails tracking user access to the EMR.
- **Review:** The Information Security Policy will be reviewed biannually by the CISO to ensure alignment with emerging cyber threats and new clinical technologies.

Physical Security Policy

- **Purpose:** To safeguard the medical center's physical assets, clinical facilities, personnel, and localized hardware from unauthorized physical access, theft, or environmental damage.
- **Scope:** Encompasses all clinic locations, administrative offices, server closets, and remote/mobile hardware used by medical staff.
- **Definitions:**
    - **Restricted Zone:** Areas housing sensitive IT infrastructure or physical patient records.

    - **Environmental Controls:** Systems monitor temperature, power, and humidity.
- **Responsibilities:** Facility managers are responsible for on-site physical security mechanisms. The IT department is responsible for securing remote mobile devices. All staff must challenge unbadged individuals in restricted zones.
- **Compliance:** Facilities must comply with physical access control standards and ensure physical separation between public patient Wi-Fi areas and clinical network access points.
- **Monitoring:** Physical security will be monitored via closed-circuit video surveillance, electronic badge access logs, and automated environmental sensors that alert the IT team to power or climate anomalies.
- **Review:** Facility physical security postures and corresponding policies will be reviewed annually, during the acquisition and onboarding of any new clinic locations.

Business Continuity Policy

- **Purpose:** To ensure the uninterrupted delivery of critical patient care and the rapid recovery of IT systems in the event of a disaster, cyberattack (e.g., ransomware), or system failure.
- **Scope:** Applies to all critical infrastructure, including the centralized EMR, telemedicine platforms, communication systems, and automated data backups.
- **Definitions:**

    - **Recovery Time Objective (RTO):** The length of time allowed for the restoration of business processes and the achievement of a stated level of service following a disruption (University of California, 2021).
    - **Maximum Tolerable Downtime (MTD):** The amount of time a mission/business process can be disrupted without causing significant harm to the mission (University of California, 2021).
- **Responsibilities:** The Unit IT Recovery Lead and CISO are responsible for coordinating recovery efforts. Clinical directors must ensure that staff are trained in manual downtime procedures when systems are temporarily unavailable (University of California, 2021).
- **Compliance:** Recovery plans must comply with enterprise IT Recovery policy standards to protect backups and ensure they are isolated from modern cyber risks such as ransomware.
- **Monitoring:** The IT team will monitor the integrity of encrypted cloud backups daily. Disaster recovery and incident response timelines will be tracked and tested via scheduled tabletop exercises.
- **Review:** This policy and the associated disaster recovery plans will be reviewed annually and updated whenever major architectural changes are made to the cloud infrastructure or EMR system.

Part 2: Security Requirements and Architecture Design

Security and Functionality Requirements

To secure Acuity Health's rapidly growing network of urgent care clinics while accommodating a small IT department, the security architecture must be driven by a highly

automated, scalable cloud infrastructure. The following security requirements establish the foundation for this design and are directly traceable to the organization's business drivers, governing policies, and operational environment.

1. Traceability to Business Drivers

Acuity Health's primary business drivers include rapid multi-site expansion, extended operational hours, integrated electronic prescribing, and a mandate to manage these complex workflows with a severely limited internal IT staff. To support these drivers without introducing crippling administrative overhead, the security architecture purposefully utilizes cloud-hosted enterprise security services via Microsoft Azure rather than localized on-premise hardware. Furthermore, interoperability requires secure Application Programming Interfaces (APIs) that use healthcare data standards (HL7/FHIR) to seamlessly transmit e-prescriptions to external pharmacies and clinical data to primary care providers without compromising data integrity. Due to the 24/7 nature of urgent care operations, high availability is achieved through redundant cloud-based storage arrays and automated failover capabilities to preserve continuous access to the Electronic Medical Records (EMR).

2. Traceability to Security Policies

The technical controls embedded within the architecture are explicitly mapped to enforce the four high-level security policies established by Acuity Health. To uphold the Information Security Policy, the network mandates a strict Zero Trust Architecture (ZTA) that logically separates the Control Plane from the Data Plane, forcing all users and endpoints to undergo rigorous identity verification through Azure AD before accessing the core EMR layer. Data confidentiality is maintained using AES-256 encryption at rest and TLS 1.3 in transit to satisfy

both HIPAA and PCI DSS constraints. To support the Business Continuity Policy, the system integrates automated, encrypted cloud backups that are logically isolated from primary subnets to safeguard against ransomware propagation. Finally, because physical access cannot ensure total device security across disparate clinical environments, the Physical Security and Risk Management policies serve as technical enforcers via Microsoft Intune Mobile Device Management (MDM) for remote wiping and Microsoft Sentinel for real-time security log ingestion.

3. Traceability to the Organizational Environment

Following the SABSA framework, the architecture directly accounts for the unique operational realities of the organization's people, processes, and technology. Regarding people, clinical and administrative staff are subject to strict Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) to restrict exposure of Protected Health Information (PHI). Conversely, patients are isolated inside a secure, web-facing Demilitarized Zone (DMZ) via a dedicated Patient Portal, while third-party pharmacies remain bounded by explicit API gateways. Internal engineering processes are optimized through automated vulnerability scanning, centralized patch distribution, and predefined incident response playbooks to offset the constraints of a small team. Technologically, because local facility networks must be treated as untrusted, the architecture mandates Endpoint Detection and Response (EDR) agents on all workstations, alongside Next-Generation Firewalls (NGFWs), to segment public patient Wi-Fi from clinical production environments.

Table 1

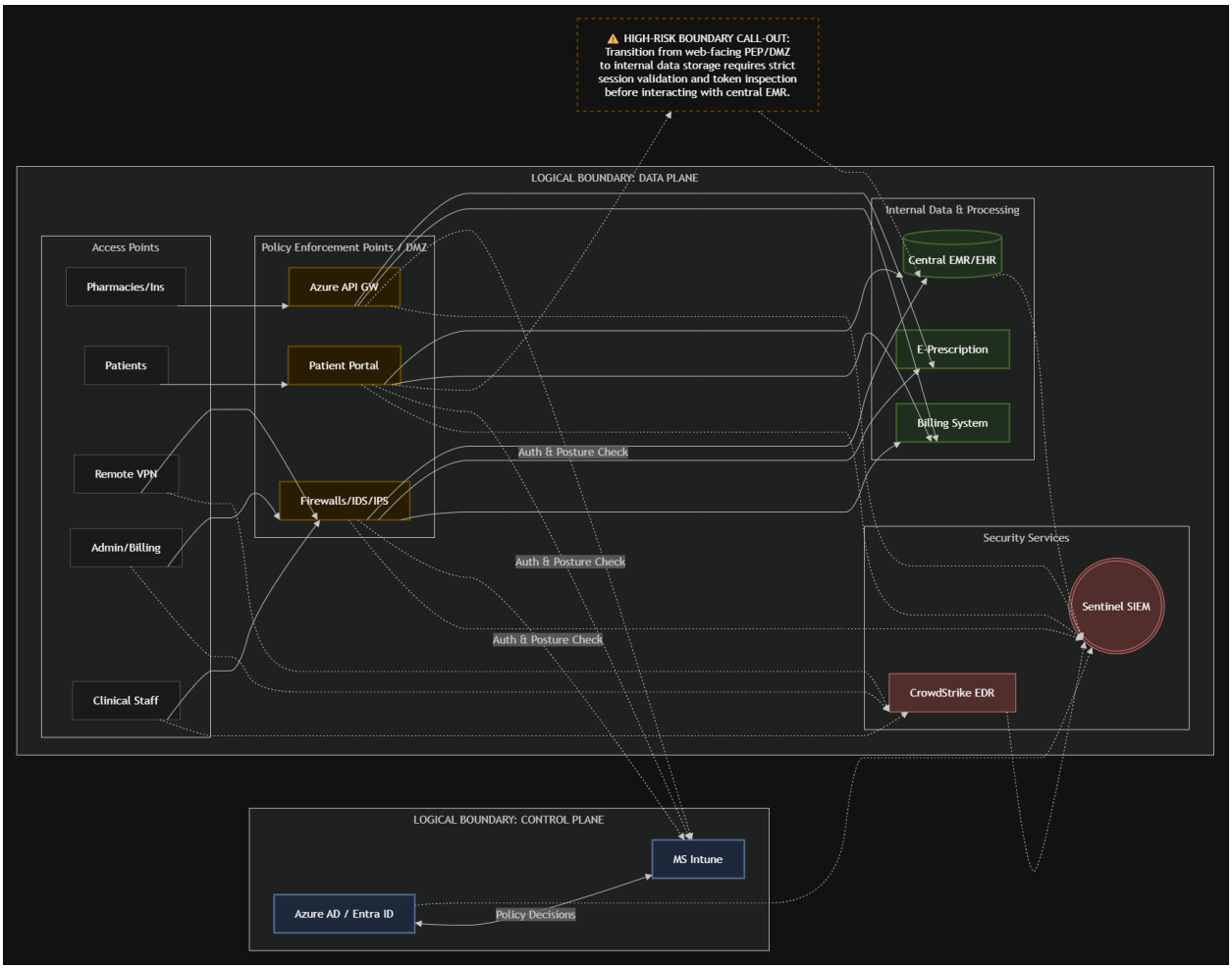
Architectural Traceability Matrix

Requirement ID	Business Driver / Policy Alignment	Functional Security Requirement	Diagram Enforcement Point
REQ-01	**Driver:** Small IT Staff / Rapid Multi-site Growth **Policy:** Information Security Policy	Shift perimeter security from hardware-defined layers to identity-defined boundaries via Zero Trust.	**Control Plane:** Azure AD / Entra ID + MS Intune
REQ-02	**Driver:** Online Patient Check-ins & Payments **Policy:** Operational Risk Management	Isolate web-facing ingress traffic from the core internal data processing network.	**PEP / DMZ:** Azure API Gateway & Patient Portal
REQ-03	**Driver:** E-Prescriptions & External Pharmacies **Policy:** Operational Risk Management	Strict token validation, session checks, and boundary inspection for third-party traffic.	**High-Risk Boundary Call-Out** (PEP to Central EMR/EHR)
REQ-04	**Driver:** Extended Operating Hours **Policy:** Business Continuity Policy	Provide immutable, cloud-native backup orchestration and centralized ingestion of audit logs.	**Security Services:** Sentinel SIEM & Automated Cloud Backups

Note. This traceability matrix maps Acuity Health's core operational business constraints and high-level security policies directly to technical enforcement mechanisms. All architectural enforcement points correspond with the logical components detailed in the Zero Trust Architecture network layout in Figure 1.

Figure 1

High-Level Architecture diagram



Note. This diagram illustrates the zero trust architecture (ZTA) data and control plane relationships, mapped according to the National Institute of Standards and Technology (NIST) Special Publication 800-207 framework. The control plane handles centralized identity evaluation and policy deployment via Azure Active Directory/Entra ID and Microsoft Intune. The data plane segregates clinical and administrative workflows via dedicated policy enforcement points before access to backend healthcare databases and electronic medical record (EMR) systems. Security logging and endpoint protection are managed through centralized detection platforms.

Part 3: Security Services

Enterprise Security Services

To realize the Zero Trust Architecture (ZTA) and secure Acuity Health's cloud-hosted infrastructure, a defense-in-depth approach is required. The following enterprise security services are categorized according to the SABSA Multi-Tiered Security Architecture model (Sherwood, Clark, & Lynas, 2005) and outline the mechanisms protecting the organization.

1. Azure Active Directory (Entra ID) & Identity Management

- **Description:** This service acts as the core Policy Engine for the organization, handling unified credential management, Single Sign-On (SSO), and Role-Based Access Control (RBAC). It strictly authenticates internal staff and external vendors before granting them access to the Electronic Medical Record (EMR) system or billing databases (Harrison, Wortz, & Wright, 2025).
- **Category:** Prevention Services (specifically addressing access control and authentication).
- **Status:** Currently employed.

2. Microsoft Intune (Mobile Device Management)

- **Description:** Intune functions as the Policy Administrator, enforcing device-level compliance across clinical tablets and remote workstations. It ensures data confidentiality by enforcing BitLocker encryption on all endpoints and can isolate or remotely wipe devices if they are compromised or stolen (Rose, Borchert, Mitchell, & Connelly, 2020).
- **Category:** Containment Services (specifically addressing software integrity and stored data confidentiality).

- **Status:** Currently employed.

3. CrowdStrike Falcon (Endpoint Detection and Response)

- **Description:** An advanced endpoint protection agent deployed across all endpoints and servers. It actively monitors for malware signatures, conducts behavioral analytics to detect abnormal lateral movement, and intercepts active intrusions before payloads can execute (Harrison, Wortz, & Wright, 2025).
- **Category:** Detection and Notification Services (specifically addressing intrusion detection and security alarm management).
- **Status:** Currently employed.

4. Microsoft Sentinel (SIEM)

- **Description:** A cloud-native Security Information and Event Management (SIEM) platform that ingests, aggregates, and correlates audit trails and network traffic logs from the firewalls, EMR, API gateways, and CrowdStrike agents to provide centralized security operations management (NIST, 2012).
- **Category:** Event Collection and Event Tracking Services (specifically addressing audit trails and security monitoring).
- **Status:** Currently employed.

5. Azure Automated Cloud Backups

- **Description:** A highly redundant data replication service that maintains encrypted, off-site, and immutable copies of the centralized EMR, financial records, and critical system configurations. It ensures that the organization can meet its Recovery Time Objectives (RTOs) following a system failure or ransomware attack (University of California, 2021).

- **Category:** Recovery and Restoration Services (specifically addressing disaster recovery and data replication).
- **Status:** Currently employed.

6. Qualys Cloud Platform (Vulnerability Management)

- **Description:** An automated scanning platform used to evaluate the architecture's security posture continuously. It conducts daily vulnerability scans, patch compliance tracking, and periodic automated security audits to ensure ongoing adherence to HIPAA and PCI DSS standards (Harrison, Wortz, & Wright, 2025).
- **Category:** Assurance Services (specifically addressing security audits and measurement metrics).
- **Status:** Planned for a future project (currently deferred due to the small size of the IT team, but prioritized for the next fiscal year's cyber budget expansion). Immediate Mitigating Control: To mitigate the risk of zero-day exploits on cloud-hosted infrastructure in the interim, the IT team will immediately enable native, low-overhead features within Azure Defender for Cloud. This provides automated, agentless baseline vulnerability assessments and asset tracking without requiring dedicated administrative management resources until the full Qualys deployment is realized.

References

Canavan, S. (2003). *An Information Security Policy Development Guide For Large Companies.* SANS GIAC Certifications.

Harrison, J., Wortz, J. A., & Wright, S. (2025). *Bene Gesserit Urgent Care (Bguc) Enterprise Security Architecture Deliverables.* University of San Diego, CSOL-520.

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide (Nist Special Publication 800-61 Rev. 2).* U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r2

National Institute of Standards and Technology. (2018). *Framework For Improving Critical Infrastructure Cybersecurity, Version 1.1.* U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise security architecture: A business-driven approach.* CRC Press.

Sherwood, J., Clark, A., & Lynas, D. (2009). *Enterprise security architecture: A business-driven approach* [White Paper]. The SABSA Institute.

U.S. Department of Health and Human Services. (2022). *Health information privacy: Summary of the HIPAA security rule.* https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

University of California. (2021). *IS-12: IT recovery.* UCLA DMS.