Conduct an Application Security Review

Security Assessment Template

Executive Summary

The Customer Information Management System (CIMS) is a critical application managing sensitive customer data, billing information, and usage analytics across three user groups: customers, relationship managers, and data scientists. Our security assessment has identified several high-risk vulnerabilities including unencrypted credit card storage, SQL injection risks, and exposed database access, all of which violate PCI/DSS and SOX compliance requirements. Key recommendations focus on implementing data encryption, secure access controls, audit logging, and network security measures to protect customer data and achieve regulatory compliance.

Risk 1: *Unencrypted Credit Card Storage with Public Database Exposure*

Risk Rating: *Critical*

Related Security Frameworks (if any): *PCI DSS 3.2.1 (Requirements 3.4, 3.6, 4.1), SOX (Section 404)*

Explanation of Risk
The PostgreSQL database is currently storing credit card information in an unencrypted format while being accessible via a public IP address. *This configuration creates an extremely high-risk scenario as it violates core PCI DSS requirements.*

Recommendations **(Include at least two. Or, if only giving one, explain why that is the only feasible solution.)**	**How does the recommendation mitigate the risk?**
Migrate to a Third-Party Payment Processor	Eliminates need to store credit card data in our database Transfers PCI compliance burden to specialized provider Provides tokenization for recurring billing Significantly reduces scope of PCI DSS requirements

The implementation timeline is estimated at 12-16 weeks for integration, testing, and secure data migration.	The solution incurs ongoing transaction fees and initial integration costs, these are minimal compared to the potential costs of a data breach or PCI compliance violations. The technical complexity is manageable with existing development resources but requires detailed attention to secure API integration and careful handling of sensitive data during migration.
Enhanced Access Controls and Monitoring	Provides accountability for all data access Limits exposure of sensitive data Enables quick detection of potential breaches Supports compliance reporting requirements
Can be executed within 6-8 weeks	*The primary resource investment will be in configuring audit logging, establishing monitoring procedures, and training staff on new security protocols. Long-term maintenance costs are predictable and align with standard security operations budgets.The primary resource investment will be in configuring audit logging, establishing monitoring procedures, and training staff on new security protocols. Long-term maintenance costs are predictable and align with standard security operations budgets.*

Risk 2: *SQL Injection Vulnerability Through Direct Query Passing*

Risk Rating: *Critical*

Related Security Frameworks (if any): *OWASP Top 10 (A03:2021), CWE-89, SOX (Section 404)*

Explanation of Risk
The current system design allows raw SQL queries to be passed directly from the web portal through POST requests to the database processor. *The internal management portal builds SQL queries on the back-end from user input. Malicious actors could inject harmful commands. (i.e. Gain access, data manipulation)*

Recommendations **(Include at least two. Or, if only giving one, explain why that is the only feasible solution.)**	**How does the recommendation mitigate the risk?**

API Gateway with Input Validation Layer	*Enforces standardized data formats* *Eliminates direct SQL exposure* *Provides centralized security control* *Enables better monitoring and logging of requests* *Adds protection against abuse and malicious traffic*
requiring 8-10 weeks for full deployment	*Creates a security layer that prevents SQL injection, also provides improved security monitoring capabilities and standardized access control.*
Implement Parameterized Queries	*Separates SQL code from data* *Prevents malicious code execution* *Ensures proper query structure* *Maintains query efficiency while adding security*
The estimated timeline spans 4-6 weeks to review and modify all database interaction points	*Requiring thorough testing and verification.* *Significantly reduces the risk of SQL injection attacks.*

Risk 3: *Insufficient Access Controls and Audit Logging*

Risk Rating: *High*

Related Security Frameworks (if any): SOX (Section 404), PCI DSS (Requirements 7, 10), NIST SP 800-53 (AC, AU)

Explanation of Risk
The current system lacks proper access controls and audit logging capabilities, operating with default database configurations; Creating multiple vulnerabilities.

Recommendations **(Include at least two. Or, if only giving one, explain why that is the only feasible solution.)**	**How does the recommendation mitigate the risk?**
Audit Logging System	*Provides complete audit trail of all data access* *Enables security incident investigation* *Supports compliance requirements* *Allows detection of unauthorized access*
requires 4-6 weeks for proper configuration and testing	*Meets compliance requirements and protecting sensitive data*
Deploy Identity and Access Management (IAM)	Enforces principle of least privilege Controls and monitors all access

	Prevents unauthorized data access Ensures proper segregation of duties
needs 8-10 weeks for full deployment	*Standard enterprise security tools and practices.*

Final Architecture Recommendation

Provide a *final archi*tecture recommendation:

- Discuss each identified risk and provide the corresponding mitigating control.
- Explain how the proposed architecture meets the business requirements.
- Address the costs associated with each change, or clarify if there are no costs.
- Ensure the architecture remains logically consistent, avoiding interference between proposed changes.

The proposed architecture enhances security while fully supporting our core business operations. Customer self-service remains intact but is strengthened through the API Gateway and secure payment processing. CRM teams maintain their full management capabilities, now protected by role-based access controls. Data scientists keep their analytical access while complying with security protocols. These improvements achieve SOX and PCI/DSS compliance without disrupting essential business functions.

The implementation is designed to minimize operational impact through phased rollouts and proper training. By prioritizing both security and usability, this solution creates a foundation for secure business growth while protecting sensitive customer data.

The proposed security architecture requires strategic resource allocation across a 6-8 month implementation period:

Phase 1 - Payment Processor Migration (3-4 months)

- *2 Full-stack developers*
- *1 Security Engineer (part-time)*
- *QA team (3 weeks)*

Phase 2 - API Gateway & SQL Security (2-3 months)

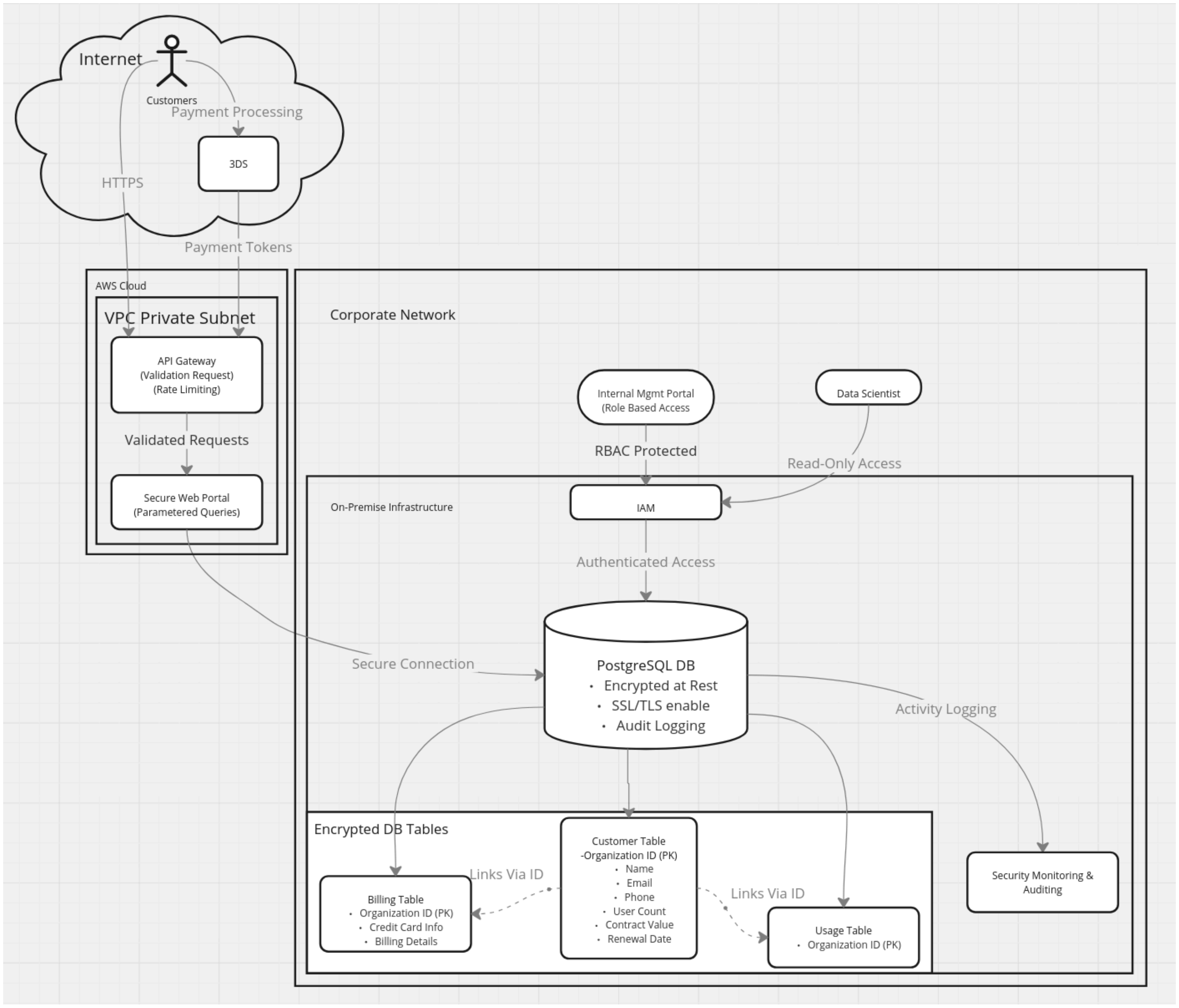
- *2 Backend developers*
- *1 DevOps engineer (2 weeks)*
- *Security Engineer (review cycles)*

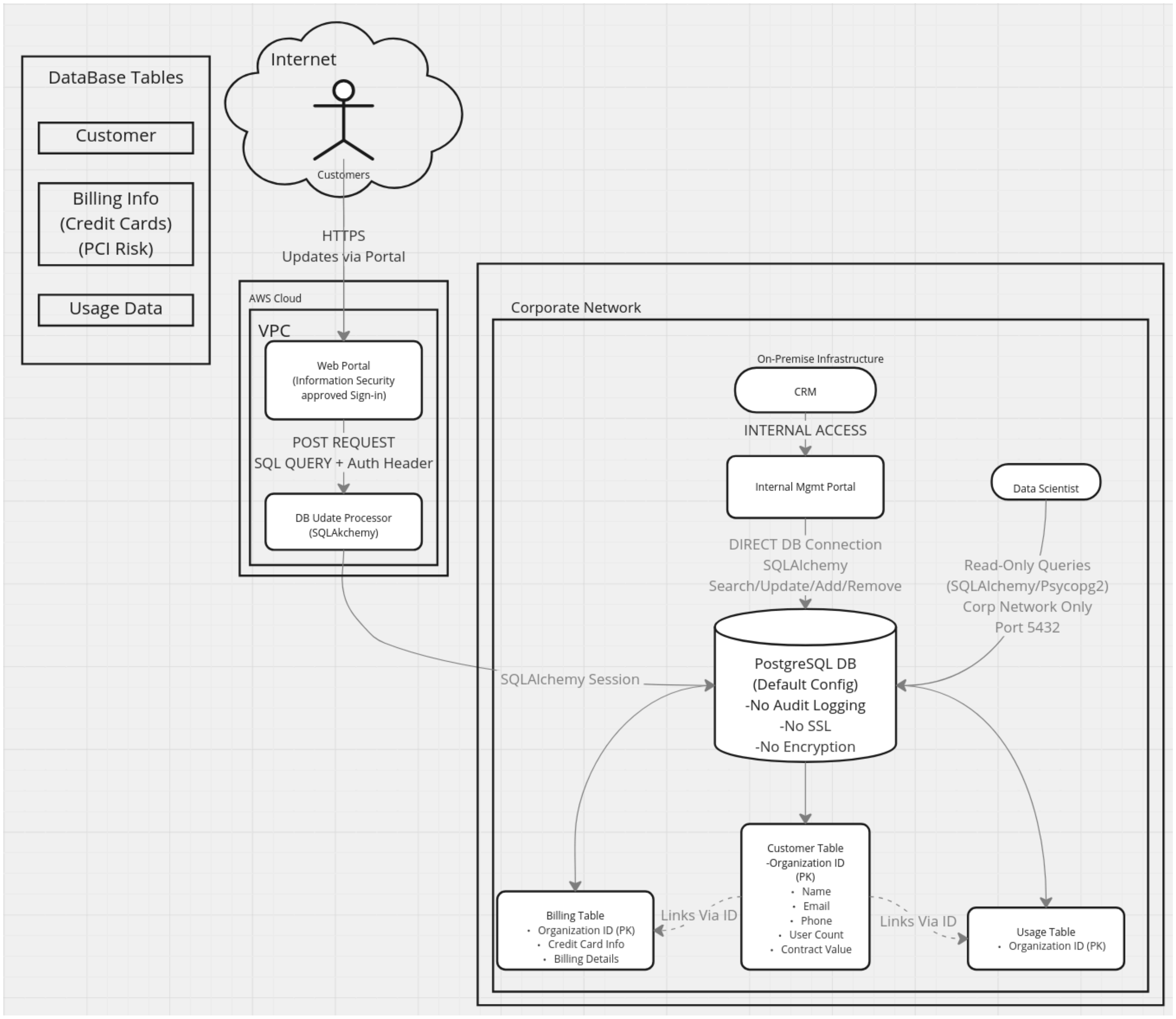
Phase 3 - Access Controls & Audit (2-3 months)

- *1 Security Engineer*

- *1 Database Administrator (3 weeks)*
- *1 System Administrator (4 weeks)*
- *Training resource (1 week)*

Total core team requirement: 4-6 dedicated engineers for 6 months, with additional specialized resources for shorter durations. Implementation can be adjusted based on resource availability and business priorities.


Internet
Customers
Payment Processing
3DS
HTTPS
Payment Tokens
AWS Cloud
VPC Private Subnet
API Gateway (Validation Request) (Rate Limiting)
Validated Requests
Secure Web Portal (Parametered Queries)
Corporate Network
Internal Mgmt Portal (Role Based Access
Data Scientist
RBAC Protected
Read-Only Access
On-Premise Infrastructure
IAM
Authenticated Access
Secure Connection
PostgreSQL DB
• Encrypted at Rest
• SSL/TLS enable
• Audit Logging
Activity Logging
Encrypted DB Tables
Customer Table -Organization ID (PK) • Name • Email • Phone • User Count • Contract Value • Renewal Date
Links Via ID
Billing Table • Organization ID (PK) • Credit Card Info • Billing Details
Links Via ID
Usage Table • Organization ID (PK)
Security Monitoring & Auditing


DataBase Tables
Customer
Billing Info (Credit Cards) (PCI Risk)
Usage Data
Internet
Customers
HTTPS
Updates via Portal
AWS Cloud
VPC
Web Portal (Information Security approved Sign-in)
POST REQUEST
SQL QUERY + Auth Header
DB Udate Processor (SQLAkchemy)
SQLAlchemy Session
Corporate Network
On-Premise Infrastructure
CRM
INTERNAL ACCESS
Internal Mgmt Portal
DIRECT DB Connection
SQLAlchemy
Search/Update/Add/Remove
Data Scientist
Read-Only Queries
(SQLAlchemy/Psycopg2)
Corp Network Only
Port 5432
PostgreSQL DB
(Default Config)
-No Audit Logging
-No SSL
-No Encryption
Customer Table
-Organization ID (PK)
• Name
• Email
• Phone
• User Count
• Contract Value
Links Via ID
Billing Table
• Organization ID (PK)
• Credit Card Info
• Billing Details
Links Via ID
Usage Table
• Organization ID (PK)