Conduct an Application Security Review

*Security Assessment Template*

# Executive Summary

*Need to build secure and configure our network properly, by policy and communication between the systems in a good way, we need to mitigate the risk by some tools and ways how to protect our systems and network from attack or anything illegal*

# Risk 1: *Threats*

Risk Rating: *Critical*

Related Security Frameworks (if any): *PCI DSS*

|  |
| --- |
| **Explanation of Risk** |
| *A secure need to implement security design, the problem is no encryption between the communications system, assets, which can contain a vulnerability impact, and damage could be done in terms of time and money – helps to protect against potential losses of competitive advantage business opportunities and even legal risks* |

|  |  |
| --- | --- |
| **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?** |
| *Add SSL certificates* | *Create an encrypted link between a web server and a web browser* |
| *Add username and password* | *Using local administrator username and password combination* |
| *Add authentication on SSH* | *Allowing usernames and password authentication on SSH* |

# Risk 2: *Compromises*

Risk Rating: *Critical*

Related Security Frameworks (if any): *NIST , ISO 27001*

|  |
| --- |
| **Explanation of Risk** |
| *could be damaged or stolen devices. We must protect our devices in the data center and install CCTV Cameras to monitor our assets and give permission those to who have access to check everything has to value in the organization helps businesses avoid unforeseeable issues like hardware damage and significant data loss. Routine hardware maintenance of physical components and servers allows organizations to uphold their operational integrity and maintain a reliable IT infrastructure* |

|  |  |
| --- | --- |
| **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?** |
| *Add CCTV Cameras* | *Add CCTV Cameras to monitor scenarios and activities*  *Gather evidence also record anything happen* |
| *Add Access Card* | Gain access through the doors secured by the access control system Each access card is uniquely encoded and gives you data on who enters and exits a building or room |
| Add lock tube cable | Lock tube cable management for devices |

# Risk 3: *vulnerabilities*

Risk Rating: *Critical*

Related Security Frameworks (if any): *PCI DSS – SOX*

|  |
| --- |
| **Explanation of Risk** |
| *The potential for loss damage or destruction of assets or data threat is a negative event. We have to implement vulnerability assessment tools detection like Vectra AI detection system-- if the username and password the same or by defult or without any control (privilege ) – it will loses customer personal data by attacker or damage* |

|  |  |
| --- | --- |
| **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?** |
| Add a firewall at the perimeter | Firewalls can help restrict access to sensitive systems. A firewall will alleviate this risk by eliminating internet access to the affected system. This mitigates the potential database exposure. |
| Add secure portal | Security interface by encryption tools |
| *Add data protection SQL* | *We have to add and save all customer information in a database protected by dynamic data masking – different database schemas – row level security – transparent data encryption – encrypted columns* |

## Final Architecture Recommendation

Provide a final architecture recommendation that:

* Explains how the architecture changes in your final architecture remediate each of the identified risks
* Discusses how business requirements and customer needs are met by the proposed architecture
* Discusses any costs associated with the changes.

#### **1-Explanation of How the Architecture Changes Remediate Each Identified Risk**

##### **Risk 1: Threats**

* **Problem:** Lack of encryption in communication between systems increases the risk of data interception and unauthorized access.
* **Mitigation Actions:**
  1. **SSL Certificates:**
     + Creates an encrypted link between servers and clients, ensuring secure communication.
     + Prevents data interception during transmission.
  2. **Authentication on SSH:**
     + Enforces username-password combinations for secure access to systems.
     + Limits unauthorized access to critical assets.

##### **Risk 2: Compromises**

* **Problem:** Physical security risks (e.g., damaged/stolen devices) can result in data breaches and hardware failures.
* **Mitigation Actions:**
  1. **CCTV Cameras:**
     + Monitors physical activities in the data center, preventing unauthorized physical access and recording evidence.
  2. **Access Cards:**
     + Provides controlled access to critical areas by encoding user-specific permissions.
     + Tracks who enters and exits sensitive areas.

##### **Risk 3: Vulnerabilities**

* **Problem:** Default or weak credentials and insecure systems expose data to attackers.
* **Mitigation Actions:**
  1. **Firewalls:**
     + Restrict unauthorized access to systems by filtering inbound and outbound traffic.
     + Protects the database from external threats.
  2. **Dynamic Data Masking and Encryption:**
     + Implements advanced security measures like row-level security and column encryption to protect customer data in databases.
     + Ensures compliance with PCI DSS and SOX by safeguarding financial and personal data.

#### **How Business Requirements and Customer Needs are Met by the Proposed Architecture**

* **Enhanced Usability:**
  + SSL certificates and secure communication ensure that customers and employees can access systems safely without interruptions or security risks.
  + Access cards maintain a balance between security and ease of access for authorized personnel.
* **Customer Data Protection:**
  + By encrypting sensitive data and implementing row-level security in databases, customer information remains secure.
  + These measures build customer trust and help the organization avoid reputational damage.
* **Operational Integrity:**
  + CCTV and physical security measures safeguard critical IT infrastructure, ensuring continued operations and reliability.
  + Routine vulnerability detection and firewall configurations keep systems updated against potential threats.

**Costs Associated with the Changes:**

SSL Certificates

Time: Initial Phase 1-2 weeks

Maintenance requirement with regular update and renewal needed

Money : Low to Moderate

The cost of SSL certificates ranges from $200 to $600annually, with potential upgrades to infrastructure required to manage encryption overhead

Complexity : Moderate- Needs adjustments to database configuration and thorough testing to verify that all connections are secured with SSL.

**Time:**

* **Initial setup:** Estimated to take 1-2 weeks.
* **Ongoing maintenance:** Moderate, involving regular token management and periodic security updates.

**Money:**

* **Development costs:** Range from $7,000 to $25,000 depending on project scope and complexity.
* **Licensing costs:** Possible expenses for authentication libraries or third-party services.

**Complexity:**

* High. Involves integrating with existing authentication systems, updating user management processes, and conducting thorough testing to ensure both security and functionality.

CCTV Cameras

**Time:**

* **Initial setup:** Estimated to take 2-3 weeks, including installation and configuration.
* **Ongoing maintenance:** Minimal, involving periodic inspections and occasional software updates for the monitoring system.

**Money:**

* **Installation costs:** Range from $5,000 to $10,000 depending on the number of cameras and system complexity.
* **Additional costs:** Possible expenses for maintenance contracts or software licensing for video management systems.

**Complexity:**

* Moderate. Requires proper placement of cameras, integration with existing security systems, and testing to ensure coverage, functionality, and compliance with organizational policies.

**Access Cards**  
**Time:**

* **Initial setup:** Estimated to take 2-3 weeks, including installation of card readers and configuration of the access control system.
* **Ongoing maintenance:** Minimal, involving periodic audits, system updates, and card replacements as needed.

**Money:**

* **Installation costs:** Range from $3,000 to $8,000 depending on the number of entry points and system complexity.
* **Additional costs:** Possible expenses for system maintenance contracts or purchasing additional access cards.

**Complexity:**

* Moderate. Requires proper installation of card readers, integration with the existing security infrastructure, and testing to ensure reliable functionality and compliance with organizational policies.

**Firewall**  
**Time:**

* **Initial setup:** Estimated to take 2-3 weeks, including deployment, configuration, and integration with the existing network infrastructure.
* **Ongoing maintenance:** Moderate, involving regular updates, rule adjustments, and periodic performance monitoring.

**Money:**

* **Installation costs:** Range from $15,000 to $20,000 depending on the type of firewall (hardware or software) and network complexity.
* **Additional costs:** Possible expenses for subscription services, support contracts, or advanced security features.

**Complexity:**

* Moderate. Requires proper configuration of rules and policies, integration with the existing network setup, and thorough testing to ensure functionality and protection against unauthorized access.

**Dynamic Data Masking and Encryption**

**Time:**

* **Initial setup:** Estimated to take 3-4 weeks, including configuring masking rules, encryption protocols, and testing database integration.
* **Ongoing maintenance:** Moderate, involving periodic updates to masking rules, key rotation, and monitoring for compliance.

**Money:**

* **Implementation costs:** Range from $7,000 to $15,000 depending on the database size and complexity.
* **Additional costs:** Potential expenses for licensing encryption tools or data masking solutions, as well as ongoing support and updates.

**Complexity:**

* High. Requires detailed configuration of data masking policies, integration with existing databases, and rigorous testing to ensure compatibility and secure handling of sensitive information.

#### **1. SSL Certificates**

* **Purpose**: Secure communication across applications and databases.
* **Architecture Change**:
  + Implement SSL/TLS across all web and application servers.
  + Update database configurations to enforce encrypted connections.
  + Upgrade infrastructure (if needed) to handle encryption overhead.
  + Establish automated certificate renewal processes using tools like Let’s Encrypt or enterprise-grade solutions.
* **Impact**: Improved data security during transmission, reducing vulnerability to interception.

#### **2. Authentication System**

* **Purpose**: Enhance authentication mechanisms for better security and user management.
* **Architecture Change**:
  + Integrate an advanced authentication system such as OAuth2, OpenID Connect, or SAML.
  + Update existing applications to support token-based authentication.
  + Implement multi-factor authentication (MFA) for all critical systems.
  + Reconfigure user access policies and establish role-based access controls (RBAC).
* **Impact**: Increased security and better management of user identities and access levels.

#### **3. CCTV Cameras**

* **Purpose**: Strengthen physical security and monitoring.
* **Architecture Change**:
  + Install a network of IP-based CCTV cameras with centralized video management.
  + Integrate the camera system with existing physical security systems (e.g., access control).
  + Configure secure access to camera feeds for monitoring and data storage.
* **Impact**: Enhanced physical security and real-time surveillance capabilities.

#### **4. Access Cards**

* **Purpose**: Control and monitor physical access to sensitive areas.
* **Architecture Change**:
  + Deploy modern access control readers with secure card authentication.
  + Integrate the access control system with a centralized database for monitoring and auditing.
  + Enable periodic system audits and implement a process for issuing/revoking access cards.
* **Impact**: Improved control over physical entry points and enhanced accountability.

#### **5**

#### **. Firewall**

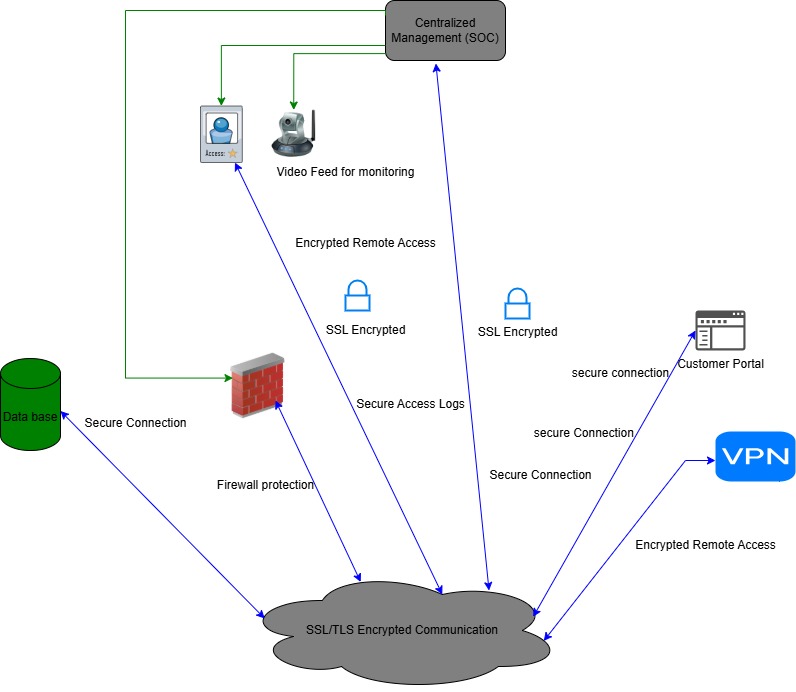
* **Purpose**: Protect the network from unauthorized access and cyber threats.
* **Architecture Change**:
  + Deploy next-generation firewalls (NGFWs) capable of deep packet inspection (DPI).
  + Configure rules and policies tailored to organizational needs.
  + Enable features like intrusion prevention, content filtering, and advanced threat detection.
  + Regularly review and update firewall configurations.
* **Impact**: Enhanced network security and protection against external and internal threats.

#### **6. Dynamic Data Masking and Encryption**

* **Purpose**: Protect sensitive data within databases.
* **Architecture Change**:
  + Implement dynamic data masking to hide sensitive data from unauthorized users.
  + Configure encryption protocols (e.g., TDE or column-level encryption) for databases.
  + Integrate encryption tools with key management solutions for automated key rotation.
  + Conduct regular compliance checks to ensure adherence to data protection standards.
* **Impact**: Enhanced data confidentiality and compliance with regulatory requirements.

### **Overall Proposed Architecture**

1. **Centralized Management**:
   * Consolidate monitoring and management of security systems (CCTV, access cards, firewalls) into a centralized security operations center (SOC).
2. **Integration**:
   * Ensure interoperability between physical and digital security systems (e.g., firewalls, access cards, CCTV).
   * Utilize SIEM (Security Information and Event Management) for real-time monitoring and response.
3. **Automation and Scalability**:
   * Automate processes like SSL renewal, key rotation, and access provisioning.
   * Build a scalable architecture to accommodate future needs and expansions.
4. **Compliance and Testing**:
   * Conduct thorough testing after each phase of implementation to ensure reliability and functionality.
   * Regularly review configurations to comply with industry standards and regulations.



# 