**Internal Security Audit**

**Train Booking Reservation System**

**Audit Objective:**

The purpose of this audit is to evaluate the security posture of the Train Ticket Reservation System, identifying strengths, vulnerabilities, and areas for improvement in authentication, data protection, application, security and compliance.

**System Overview:**

The **Train Ticket Reservation System** is a web-based platform developed using **Java (J2EE), JDBC, and Oracle SQL**. It provides secure authentication, role-based access control (RBAC), and real-time train booking management for users and administrators. The audit examines security in **authentication, database protection, application vulnerabilities, and user session management**.

| **Control** | **Implemented? (Yes/No)** | **Remarks** |
| --- | --- | --- |
| **Least Privilege** | ✅ Yes | Role-Based Access Control (RBAC) ensures admins and users have different permissions. |
| **Disaster Recovery Plans** | ✅ Yes | Backup and recovery mechanisms are in place for database protection. |
| **Password Policies** | ✅ Yes | System enforces strong password complexity requirements. |
| **Separation of Duties** | ✅ Yes | Users can only book tickets; admins manage train data. |
| **Firewall** | ❌ No | Not implemented unless hosted on a secured cloud server. |
| **Intrusion Detection System (IDS)** | ❌ No | No IDS is in place for monitoring malicious activities. |
| **Backups** | ✅ Yes | Regular database backups are implemented. |
| **Antivirus Software** | ❌ No | Not applicable unless the system runs on an external server with malware threats. |
| **Manual Monitoring & Maintenance** | ❌ No | No active monitoring or intervention process is implemented. |
| **Encryption** | ✅ Yes | User passwords and sensitive data are encrypted. |
| **Password Management System** | ✅ Yes | Secure password storage and reset mechanisms are implemented. |
| **Physical Security (Locks, CCTV, etc.)** | ❌ No | Not applicable, as the system is software-based. |

**Compliance Checklist**

**Payment Card Industry Data Security Standard (PCI DSS)**

| **Best Practice** | **Implemented? (Yes/No)** | **Remarks** |
| --- | --- | --- |

|  |  |  |
| --- | --- | --- |
| Only authorized users have access to customers’ credit card information. | ✅ Yes | Role-based access prevents unauthorized access to user data. |

|  |  |  |
| --- | --- | --- |
| Credit card information is stored, accepted, processed, and transmitted securely. | ✅ Yes | Transaction data is encrypted and securely stored. |

|  |  |  |
| --- | --- | --- |
| Implement data encryption procedures to better secure credit card transactions. | ✅ Yes | Strong encryption mechanisms protect sensitive payment details. |

|  |  |  |
| --- | --- | --- |
| Adopt secure password management policies. | ✅ Yes | Passwords follow industry best practices for security. |

**General Data Protection Regulation (GDPR)**

| **Best Practice** | **Implemented? (Yes/No)** | **Remarks** |
| --- | --- | --- |
| Customers' personal data is kept private/secured. | ✅ Yes | Data is encrypted and stored securely. |
| A plan is in place to notify customers in case of a data breach. | ❌ No | No documented incident response plan is available. |
| Ensure data is properly classified and inventoried. | ✅ Yes | User data is categorized and protected accordingly. |
| Enforce privacy policies and procedures. | ✅ Yes | Privacy policies are in place for handling user data. |

**System and Organizations Controls (SOC Type 1 and Type 2)**

| **Best Practice** | **Implemented? (Yes/No)** | **Remarks** |
| --- | --- | --- |
| User access policies are established. | ✅ Yes | RBAC restricts user permissions. |
| Sensitive data (PII/SPII) is confidential/private. | ✅ Yes | Encryption and secure access controls protect user information. |
| Data integrity ensures data is consistent and accurate. | ✅ Yes | The system uses structured database management. |
| Data is available to authorized individuals. | ✅ Yes | Users and admins can access only relevant data. |

**Security Findings & Risk Assessment**

| **Risk Area** | **Issue Identified** | **Risk Level** |
| --- | --- | --- |
| Authentication | No Multi-Factor Authentication (MFA) | 🟠 Medium |
| Compliance | No incident response plan for data breaches | 🟠 Medium |
| Network Security | No IDS or firewall in place | 🔴 High |
| System Monitoring | No real-time monitoring system | 🟠 Medium |
|  |  |  |

**Conclusion:**

The Train Ticket Reservation System has a strong security foundation, with encryption, backup management, password security, and compliance with PCI DSS and GDPR standards. However, some key improvements are required in network security, incident response planning, and monitoring to ensure comprehensive protection against cyber threats.