Project Report: Importing & Securing Data in ServiceNow

1. Introduction

This report outlines the process, tools, and security measures involved in importing data into ServiceNow and ensuring its secure handling within the platform. The goal of this project was to streamline data onboarding while complying with organizational security policies.

2. Objectives

Automate and manage data imports from various sources into ServiceNow.

Ensure data integrity, confidentiality, and access control.

Implement best practices for securing imported data.

3. Tools and Technologies Used

ServiceNow Instance (Orlando, Paris, or Tokyo, depending on your environment)

Data Sources: Excel/CSV files, REST APIs, JDBC connections

Import Sets

Transform Maps

Data Policies & Access Control Rules (ACLs)

Role-Based Access Control (RBAC)

Scheduled Data Imports

IntegrationHub (optional)

4. Data Import Process

4.1 Source Identification

Identified structured and unstructured data sources including legacy databases, Excel files, and third-party APIs.

4.2 Import Set Creation

Created Import Sets to temporarily store incoming data.

Mapped external data to ServiceNow tables (e.g., cmdb\_ci, incident, user).

4.3 Transform Maps

Used Transform Maps to convert and map import set records to target tables.

Implemented scripts for data normalization, deduplication, and validation.

4.4 Scheduled Imports

Created Scheduled Data Imports for recurring data updates (e.g., nightly syncs).

5. Data Security Measures

5.1 Access Control Rules (ACLs)

Defined table-level and field-level ACLs to restrict unauthorized access.

Applied conditions and scripts to enforce dynamic access logic.

5.2 Role-Based Access Control (RBAC)

Assigned roles based on user profiles to limit access to sensitive data.

Custom roles were created for data importers and transformers.

5.3 Data Policies

Enforced mandatory fields and validation rules during data input.

5.4 Encryption

Enabled encryption at rest for sensitive tables (e.g., PII, financial data).

Utilized Edge Encryption for enhanced data privacy where needed.

5.5 Audit & Logging

Enabled auditing on key tables to track changes.

Reviewed import logs and transformation history for traceability.

6. Testing and Validation

Conducted unit testing of transform maps with sample data.

Validated data integrity post-import.

Reviewed ACLs through impersonation testing.

7. Challenges & Mitigations

Challenge Mitigation

Data mismatch during transformation Applied data normalization scripts

Unauthorized data access risk Strengthened ACL rules and encryption

API rate limits during bulk import Implemented pagination and throttling

8. Outcomes

Efficient and accurate data imports into ServiceNow tables.

Controlled access to sensitive data through ACLs and RBAC.

Compliance with internal data governance and external regulatory standards.

9. Recommendations

Regularly audit imported data and ACL effectiveness.

Automate data quality checks in transform scripts.

Train import administrators on security protocols and best practices.

10. Conclusion

The project successfully implemented a robust data import and security framework in ServiceNow. It ensures scalable data integration while protecting sensitive business information.