

FSC Readiness Scanner — Solution Architecture and Usage

Publisher: Atlas Advisory LLC (namespace `atlasys`) | Package: FSC Readiness Scanner, 2GP managed package | Version under review: 0.5.0 (04tfn000005ucSjAAI) | Contact: chase@atlasys.io

1. Solution Overview

FSC Readiness Scanner is a 100% Salesforce-native managed package that inventories a subscriber org's dependencies on the legacy Financial Services Cloud managed package (`FinServ` namespace) and produces a scored, actionable migration plan for the move to FSC Core. The solution contains no web application, no external service, no callouts, and no off-platform components of any kind. All processing, storage, and presentation occur inside the subscriber org.

2. Components

Component	Technology	Purpose
ScannerService	Apex (@AuraEnabled)	Service layer for the UI: start scans, read dashboard/finding data as plain DTOs, triage findings, export support.
ScanOrchestrator	Apex Queueable + Finalizer	Runs scanner modules sequentially with checkpoint chaining to respect governor limits; Finalizer marks scans Failed on unhandled exceptions.
ApexBodyScanner	Apex	Reads ApexClass/ApexTrigger bodies (subscriber code only, <code>NamespacePrefix = NULL</code>) and finds FinServ token references, ignoring comments and string literals.
SchemaScanner	Apex	Uses Schema describe calls to find subscriber fields on managed objects and lookups/formulas referencing FinServ objects.

DataFootprintScanner	Apex	Row counts per FinServ object (COUNT queries capped at 9,999) to size data migration.
RuleCatalog / FindingRule__mdt	Apex + Custom Metadata	Maps FinServ tokens to severity, FSC Core equivalents, and remediation steps.
Scan__c, Finding__c	Custom Objects	Scan runs and de-duplicated findings with triage status.
scannerConsole	Lightning Web Component	Readiness console: score, severity filters, findings table, remediation detail, CSV export (client-side only).
FSC_Scanner_Admin	Permission Set	Sole access path to the app, its objects, and its Apex.

3. Information Flow

1. An admin with the `FSC_Scanner_Admin` permission set opens the FSC Readiness Console (Lightning tab) and clicks Run Scan.
2. The LWC calls `ScannerService.startScan()` (@AuraEnabled), which inserts a `Scan__c` record and enqueues `ScanOrchestrator`.
3. The orchestrator runs the three scanner modules in sequence. Each module reads org metadata/data via SOQL and Schema describe calls executed in `USER_MODE`, and returns findings. Long-running modules checkpoint and re-enqueue.
4. Findings are upserted into `Finding__c` (de-duplicated by a SHA-256 natural key) with severity and remediation guidance resolved from `FindingRule__mdt`.
5. The LWC polls the dashboard while the scan runs and renders results. CSV export is generated entirely client-side from data already displayed.

All data flow is intra-org: Salesforce database → Apex (user mode) → LWC. No step transmits data outside the Salesforce Platform.

4. Authentication and Authorization

- No authentication is implemented by the solution; users are standard Salesforce users in the subscriber org. There are no Connected Apps, Named Credentials, External Client Apps, or stored tokens/secrets of any kind.
- Authorization: every SOQL query runs `WITH USER_MODE` or `AccessLevel.USER_MODE`; every DML statement uses `insert/update/upsert as user`; every class is declared

with sharing . CRUD pre-checks in the service layer return actionable errors when the permission set is missing.

- The packaged permission set is the only access path; the package modifies no profiles and ships no default access.

5. Encryption and Data in Transit

No data leaves the Salesforce Platform, so no transport channels exist beyond the standard Salesforce UI (HTTPS enforced by the platform). The solution performs no callouts and stores no data off-platform. At-rest encryption is inherited from the subscriber org (including Shield Platform Encryption where enabled; the package does not preclude it).

6. Data Touchpoints

Data	Access	Storage
ApexClass / ApexTrigger bodies (subscriber-authored only)	Read-only, USER_MODE	Not stored; only component name, matched FinServ token, and occurrence count are persisted to <code>Finding__c</code> .
Schema metadata (object/field describes)	Read-only describe calls	Only qualified field names and referenced object names persisted to findings.
FinServ object row counts	COUNT() queries, USER_MODE, capped at 9,999	Aggregate counts only, stored on <code>Scan__c</code> . No record contents are ever read.

No PII, customer records, or credentials are read, stored, or transmitted.

7. Basic Usage Instructions

1. Install the package (install URL or `sf package install --package 04tfn000005ucSjAAI`).
2. Assign the permission set: `sf org assign permset --name atlasys__FSC_Scanner_Admin` (or via Setup → Permission Sets).
3. Open the **FSC Readiness Scanner** app from the App Launcher and go to the **FSC Readiness Console** tab.
4. Click **Run Scan**. Progress displays per module (Apex → Schema → Data Footprint); results refresh automatically.

5. Review the readiness score, filter findings by severity/status, click **View** on any finding for severity rationale, the FSC Core equivalent, and remediation steps. Export CSV for the full inventory, and use the triage actions (In Progress / Resolved / Ignore) to manage the migration plan.