SHARED Information System

Software Requirements Specification

GCF Knuckles Project

Version 1.6

For client and expert review

This specification defines the required functions, information, interfaces, controls and acceptance checks for system planning, development and client review.

The seven TOR capability areas remain in scope. The companion coverage workbook is the detailed traceability, data dictionary, acceptance, release-option and NFR configuration annex to this SRS. Its retained baseline has 150 Design shown and 40 Technical only requirements; these labels are not implementation or acceptance totals.

Review decisions are listed in Chapter 13. This issue does not record client acceptance, scientific approval or operational acceptance. Institution review is the single place for prototype and SRS review comments.

All outputs and associated materials remain the property of the GCF Knuckles Project. Restricted source material must be handled under the applicable confidentiality and sharing terms.

Contents

1 Introduction 3
2 Data Providers 6
3 Stakeholders and System Management 31
4 Maps Dashboards and Geographic Information 37
5 Decision Support and Reporting 47
6 Project Implementation and Monitoring 55
7 Community Participation and Knowledge Services 61
8 Value Chains Markets and Ecosystem Services 65
9 Responsive and External Interfaces 69
10 Architecture Database and Data Governance 75
11 Service Quality Security and Operations 92
12 Implementation Testing and Acceptance 96
13 Review Decisions and Source References 101
14 Prototype Coverage and TOR Traceability 105

1 Introduction

How to read this specification: use the prototype and User guide to try a task. Use System diagrams for an overview, a focused workflow or the complete drawing. Use the requirement IDs below to check the exact obligation and acceptance condition. These reading aids do not change the requirements.

The SHARED Information System is being developed under the Green Climate Fund (GCF) Knuckles Project. The main aim of this system is to bring together information from different government institutions and other stakeholders to support better decision-making in land management, agriculture, water resources, climate adaptation, livelihoods and sustainable financing.

At present, different institutions maintain information related to their own areas. However, this information is not always available to other institutions when making decisions. Therefore, SHARED is expected to provide a common platform where relevant information can be collected, integrated, shared and used by different stakeholders based on their responsibilities and access permissions.

The system will help stakeholders identify problems, analyse available information, compare possible solutions and select suitable options based on the conditions of a particular location. It will also support stakeholder participation, monitoring of project interventions and evaluation of their results.

1.1 Purpose of the Document

The purpose of this Software Requirements Specification (SRS) document is to identify and describe the requirements of the SHARED Information System.

This document explains what the system is expected to do, what information is required, who will use the system and how it will support their activities and decision-making processes.

Keep three ideas separate. A definition states what a field means, its type and unit. An observation records a value for a place and period. Evidence identifies the source version and how the value was obtained or changed. Permission to use that evidence is checked separately.

It will provide a common understanding of the system requirements among stakeholders, the Project Management Unit (PMU) and the software development team. It will also serve as a reference for system design, development, testing, implementation and future improvements.

1.2 Scope of the System

The SHARED Information System will provide a common platform to collect, integrate, manage and share information from different institutions and other stakeholders involved in the GCF Knuckles Project.

The system will mainly focus on the following areas:

1. **Information Integration:** Collect and connect information from different institutions while maintaining appropriate data access and ownership.
2. **Information Visualization:** Present information through GIS maps, charts, dashboards and indicators at different geographical levels.
3. **Decision Support:** Help stakeholders identify problems, analyse information, compare different options and select suitable solutions.
4. **Stakeholder Participation:** Support information sharing, consultation and feedback among institutions, communities and other stakeholders.
5. **Project Intervention Monitoring:** Monitor project activities, implementation progress and expected outcomes.
6. **Sustainable Financing:** Provide information to support agricultural value chains, market opportunities and Payment for Ecosystem Services (PES).
7. **Knowledge and Advisory Services:** Provide relevant information, guidance and technical knowledge to different stakeholders.

The system will support decision-making from national level to local level, including districts, Divisional Secretariat divisions, Grama Niladhari divisions and sub-basin areas.

SHARED will mainly function as an information-sharing, monitoring and decision-support system. It is not intended to replace the existing operational systems of government institutions.

1.3 Intended Users and Stakeholders

The SHARED Information System will be used by different stakeholders who have different responsibilities and information requirements.

The main stakeholder groups are:

1. **Project Management and Governance:** PMU, project steering committees, executing entities and implementing partners.
2. **Government Institutions:** Departments and authorities responsible for agriculture, irrigation, forests, land use, environment, climate and other related areas.
3. **Provincial and Local Authorities:** Provincial departments, District Secretariats, Divisional Secretariats and relevant local government institutions.
4. **Research and Technical Institutions:** Universities, research organizations and technical experts providing scientific information and recommendations.

5. **Farmers and Communities:** Smallholder farmers, plantation workers, farmer organizations, community groups and other project beneficiaries.
6. **Private Sector and Financial Institutions:** Agricultural buyers, exporters, processors, plantation companies, investors and organizations involved in sustainable financing.
7. **System Administrators and Data Managers:** Authorized users responsible for system administration, data management, information quality and access control.

Each stakeholder will have access to relevant system functions and information based on their role, responsibilities and approved access permissions.

2 Data Providers

Data providers are the government institutions, research organizations, project implementing agencies, private organizations and other stakeholders who provide information to the SHARED Information System.

Different institutions maintain information related to their own responsibilities. For example, the Department of Agriculture maintains agricultural information, the Irrigation Department maintains water and irrigation information, and the Forest Department maintains forest-related information.

However, this information is not always available to other institutions when making decisions. SHARED is expected to provide a common platform to collect, connect, manage and share relevant information from these institutions.

The information provided to SHARED will be used for land-use planning, climate adaptation, agriculture, water management, sustainable financing, stakeholder coordination and monitoring of project interventions.

Data providers will be responsible for providing relevant information and maintaining its accuracy and updated status according to agreed responsibilities. SHARED will support different data collection methods, including file uploads, integration with existing systems and manual data entry.

The system will also maintain data ownership, access permissions and data quality to ensure that information is shared with authorized stakeholders in a reliable and secure manner.

2.1 Objectives

The main objectives of the data provider functions are to:

1. Identify the institutions and stakeholders who provide information to SHARED.
2. Identify the types of information available from each data provider.
3. Provide different methods to collect information from institutions and other stakeholders.
4. Support integration with existing institutional information systems.
5. Allow authorized data providers to add, update and maintain their information.
6. Validate information before making it available to other stakeholders.
7. Maintain data ownership, data sources, update history and access permissions.
8. Support sharing of information between institutions according to approved permissions.
9. Allow data providers to respond to information requests and provide clarifications.
10. Ensure that reliable and updated information is available for analysis, decision-making and project monitoring

2.2 Classification of Data Providers

Data providers are classified into three main groups.

2.2.1 Core Project Data Providers

These institutions are identified in the GCF Knuckles Project documentation as project partners, technical contributors or project coordination bodies.

ID	Institution	Information expected	Possible format
DP01	Land Use Policy Planning Department (LUPPD)	Land-use maps, classifications, sub-basin land-use information, planning areas and land management options	GeoPackage, GeoJSON, CSV, WMS/WFS
DP02	Natural Resources Management Centre (NRMC)	Soil types, soil health, erosion, land degradation and sustainable land management information	GeoPackage, GeoTIFF, CSV, XLSX
DP03	Department of Agriculture (DOA)	Crop varieties, cultivation practices, crop suitability, agricultural production and technical recommendations	CSV, XLSX, JSON/API
DP04	Department of Agrarian Development (DAD)	Minor irrigation, farmer organizations, village tanks and agrarian service information	CSV, XLSX, GeoJSON
DP05	Irrigation Department	Irrigation networks, reservoirs, water availability, water demand, sedimentation and rehabilitation	CSV, GIS, JSON/API
DP06	Mahaweli Authority of Sri Lanka (MASL)	Reservoirs, irrigation systems, water resources and catchment management	CSV, GIS, API
DP07	Forest Department	Forest boundaries, forest cover, forest types, degraded areas and restoration activities	GeoPackage, GeoTIFF, GeoJSON
DP08	Department of Meteorology	Rainfall, temperature, historical weather, forecasts and climate information	CSV, NetCDF, JSON/API
DP09	Department of Export Agriculture (DEA)	Export crops, production areas, suitability, value chains and market development	CSV, XLSX, JSON/API
DP10	Provincial Departments of Agriculture	Regional crop information, extension activities, farming constraints and production	CSV, XLSX, mobile forms
DP11	Project Management Unit (PMU)	Project activities, intervention locations, progress, indicators, monitoring and relevant beneficiary information	CSV, JSON/API, GeoJSON

ID	Institution	Information expected	Possible format
DP12	CIFOR-ICRAF and project research partners	Scientific assessments, baseline data, models, socioeconomic studies and land management options	CSV, GIS, NetCDF, PDF
DP13	Sub-Watershed Integrated Delivery Teams (SIDTs)	Local observations, stakeholder feedback, selected interventions and sub-basin monitoring	Mobile forms, CSV, GeoJSON

2.2.2 Additional Government and Research Data Providers

These institutions maintain information that may be useful to SHARED. Their participation and the availability of specific datasets must be confirmed.

ID	Institution	Information expected	Possible format
DP14	Survey Department of Sri Lanka	Administrative boundaries, topography, elevation and base maps	GeoPackage, GeoTIFF, WMS/WFS
DP15	National Spatial Data Infrastructure (NSDI)	Spatial data services, catalogues and metadata	WMS, WFS, OGC API
DP16	Disaster Management Centre (DMC)	Flood, drought, disaster events and vulnerability information	GeoJSON, CSV, API
DP17	National Building Research Organisation (NBRO)	Landslide hazard maps and slope stability assessments	GeoTIFF, GIS, PDF
DP18	Central Environmental Authority (CEA)	Environmentally sensitive areas, environmental monitoring and regulatory information	GeoJSON, CSV, PDF
DP19	Department of Wildlife Conservation	Protected areas, wildlife habitats and biodiversity information	GIS, CSV
DP20	Department of Census and Statistics (DCS)	Population, households, agriculture and socioeconomic statistics	CSV, XLSX, API
DP21	Water Resources Board	Groundwater, aquifers, water levels and groundwater quality	CSV, GIS, time series
DP22	National Water Supply and Drainage Board	Water sources, demand, supply and water-quality information	CSV, GIS, API
DP23	Geological Survey and Mines Bureau (GSMB)	Geological maps, formations and geological constraints	GIS, GeoTIFF, PDF
DP24	Land Commissioner General's Department	State land administration information and land restrictions	Restricted records, CSV, GIS

ID	Institution	Information expected	Possible format
DP25	Hector Kobbekaduwa Agrarian Research and Training Institute (HARTI)	Agricultural economics, commodity prices, market studies and socioeconomic research	CSV, XLSX, PDF
DP26	Export Development Board (EDB)	Export market information, products, demand and market requirements	CSV, XLSX, API
DP27	National Enterprise Development Authority (NEDA)	Enterprise development and business support programmes	CSV, XLSX
DP28	Industrial Development Board (IDB)	Processing facilities, industrial capabilities and enterprise support	CSV, GIS

2.2.3 Local, private-sector and operational data providers

These stakeholders provide local information, field observations, market information and project-related records.

ID	Data provider	Information expected	Collection method
DP29	District Secretariats	District priorities, development activities and coordination information	Web forms, CSV
DP30	Divisional Secretariats	Divisional priorities, community needs and interventions	Web forms, CSV, GIS
DP31	Grama Niladhari officers	Village-level observations, community information and field verification	Mobile forms
DP32	Farmer organizations	Cultivation constraints, irrigation problems and farmer observations	Mobile forms, assisted entry
DP33	Individual farmers	Crops, farming practices, observations and feedback	Mobile forms
DP34	Plantation companies	Plantation areas, crops, restoration and sustainability information	CSV, XLSX, API
DP35	Plantation workers and community groups	Livelihood issues, environmental problems and project feedback	Surveys, mobile forms
DP36	Agricultural buyers and traders	Commodity prices, purchasing demand and quality requirements	CSV, API, web forms
DP37	Processors and exporters	Processing capacity, product demand and market constraints	CSV, API
DP38	Banks and financing institutions	Financing products and authorized programme-level financing information	Secure API, CSV

ID	Data provider	Information expected	Collection method
DP39	PES intermediary organizations	PES schemes, participants, agreements and monitoring indicators	Secure forms, API
DP40	Universities and research institutes	Research datasets, scientific models and technical studies	CSV, GIS, PDF
DP41	Community-based organizations and NGOs	Community observations, surveys, local knowledge and feedback	Mobile forms, CSV, GeoJSON

2.3 Abstract Use Cases

The abstract use case diagram identifies the main functions required by data providers. The diagram uses stakeholder groups rather than showing every institution separately.

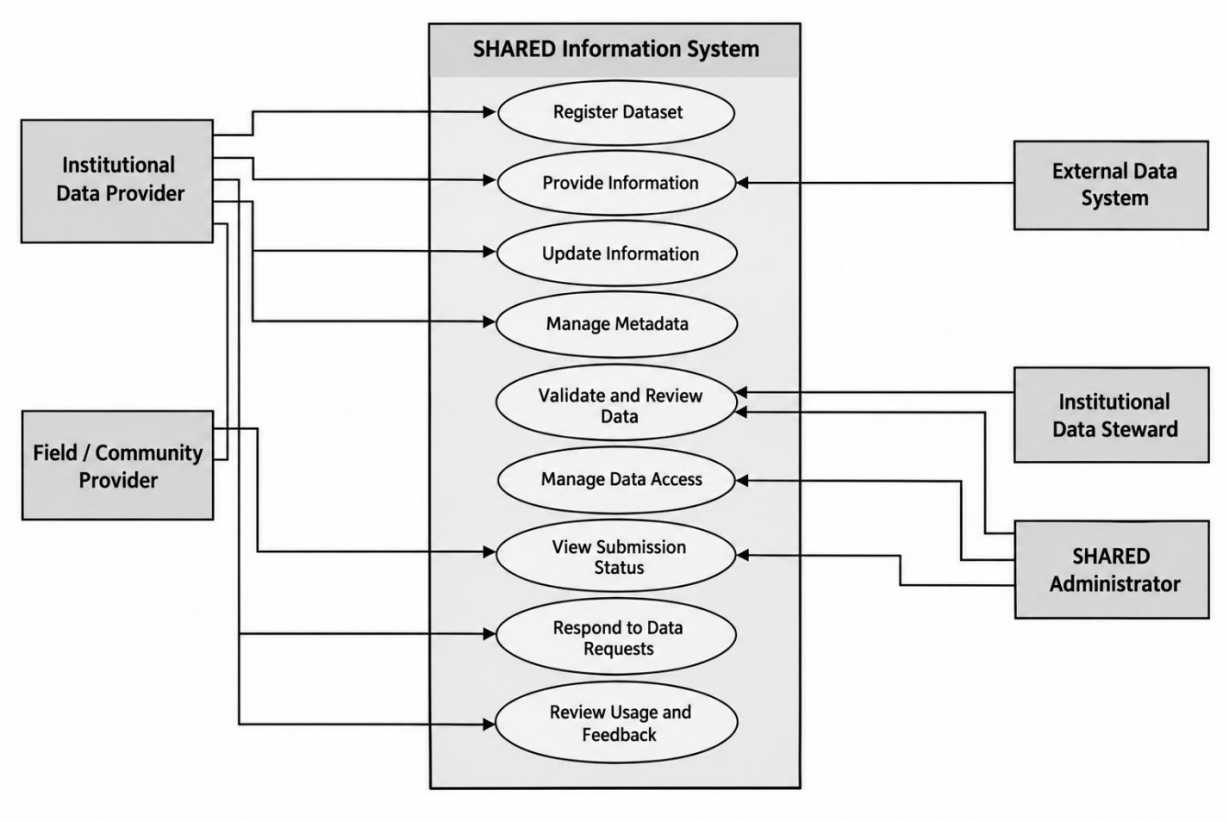


Figure 2 1 Abstract Use Case Diagram for Data Providers

2.3.1 Main use case descriptions

Use case ID	Use case	Description	Expected result
DP-UC01	Register Dataset	Register a dataset and its providing institution	Dataset registered

Use case ID	Use case	Description	Expected result
DP-UC02	Provide Information	Upload, connect or manually enter information	Information submitted
DP-UC03	Update Information	Add, correct or replace information	Updated dataset version
DP-UC04	Validate and Review Data	Check data quality and authorize release	Validated or rejected submission
DP-UC05	Manage Metadata	Maintain information about dataset source, ownership and coverage	Updated metadata
DP-UC06	Manage Data Access	Define approved access and sharing permissions	Access policy recorded
DP-UC07	View Submission Status	Check submission and validation progress	Status displayed
DP-UC08	Respond to Data Requests	Provide requested information or clarification	Response recorded
DP-UC09	Review Usage and Feedback	Review data usage, quality issues and comments	Feedback and improvement actions

2.4 Actors

The main actors are identified below.

Actor ID	Actor	Responsibility
DP-A01	Institutional Data Provider	Registers, submits and maintains institutional datasets
DP-A02	Field / Community Data Provider	Submits local observations, field records and supporting information
DP-A03	Research Data Provider	Supplies scientific datasets, assessments, models and technical information
DP-A04	Private-Sector Data Provider	Supplies relevant market, enterprise, plantation, financing or PES information
DP-A05	Institutional Data Steward	Reviews data quality, confirms ownership and authorizes sharing within delegated powers
DP-A06	SHARED Administrator	Manages technical configuration, user permissions, integration and system operations
DP-A07	External Data System	Supplies data through an approved machine-to-machine integration

Actor ID	Actor	Responsibility
DP-A08	Authorized Data Requester	Requests additional information or clarification from a data provider

One institution may act as both a data provider and a data user. For example, the Department of Agriculture may provide crop information and also use climate and water information from other institutions.

2.5 Sub-Use Cases

Some main use cases require several smaller functions.

2.5.1 DP-UC02 – Provide Information

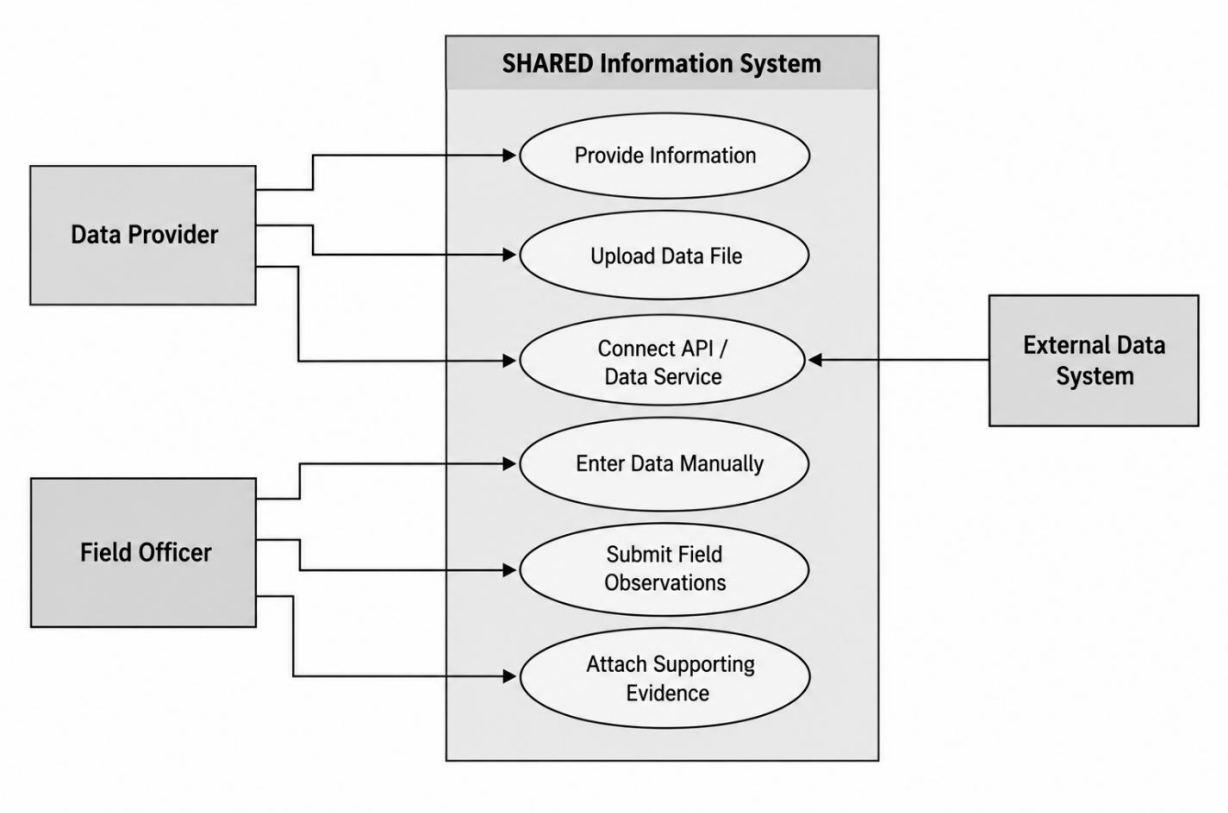


Figure 2 2 Provide Information

Sub-use case	Description	Example
Upload Data File	Upload structured information or GIS data	LUPPD uploads a land-use dataset

Sub-use case	Description	Example
Connect API / Data Service	Retrieve information from an external system	Approved rainfall data feed
Enter Data Manually	Enter records using SHARED forms	Field officer enters tank information
Submit Field Observations	Submit measurements and local observations	Forest restoration field inspection
Attach Supporting Evidence	Upload photographs or reports	Field photograph and inspection report

2.5.2 DP-UC03 – Update Information

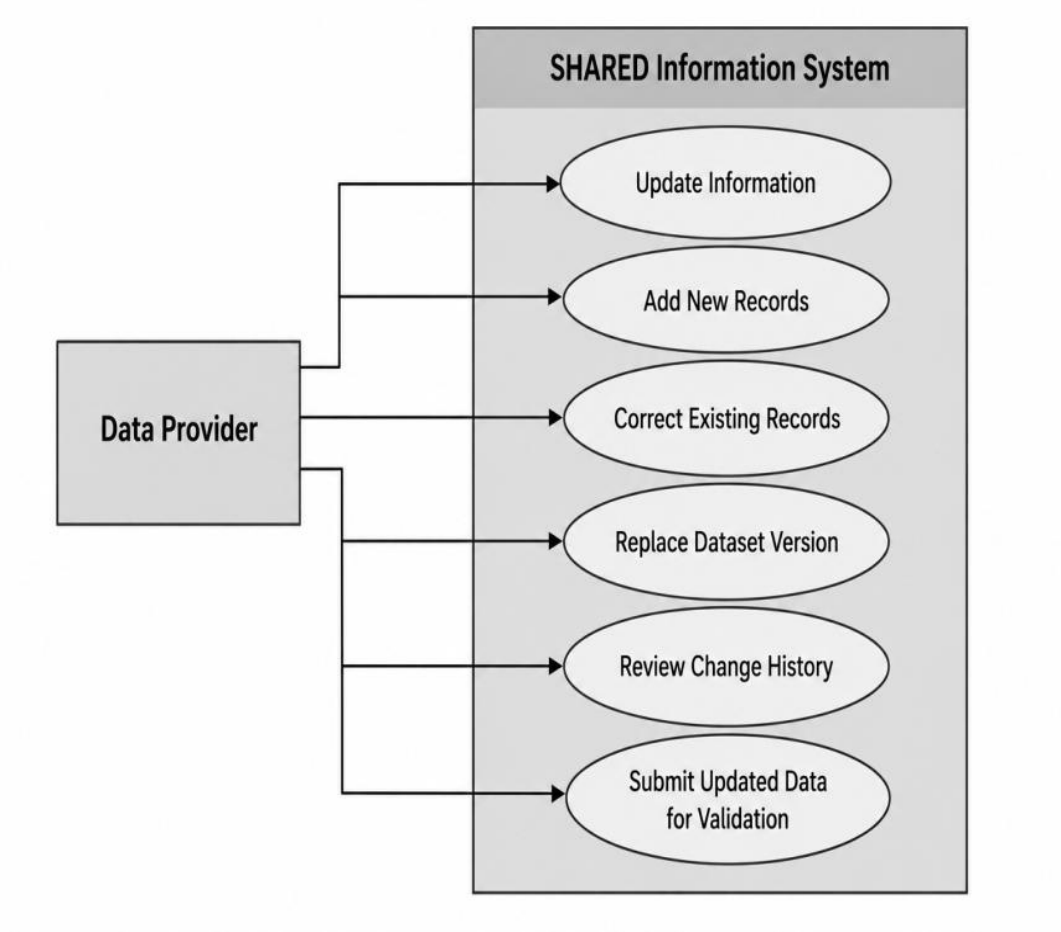


Figure 2 3 Update Information

2.5.3 DP-UC04 – Validate and Review Data

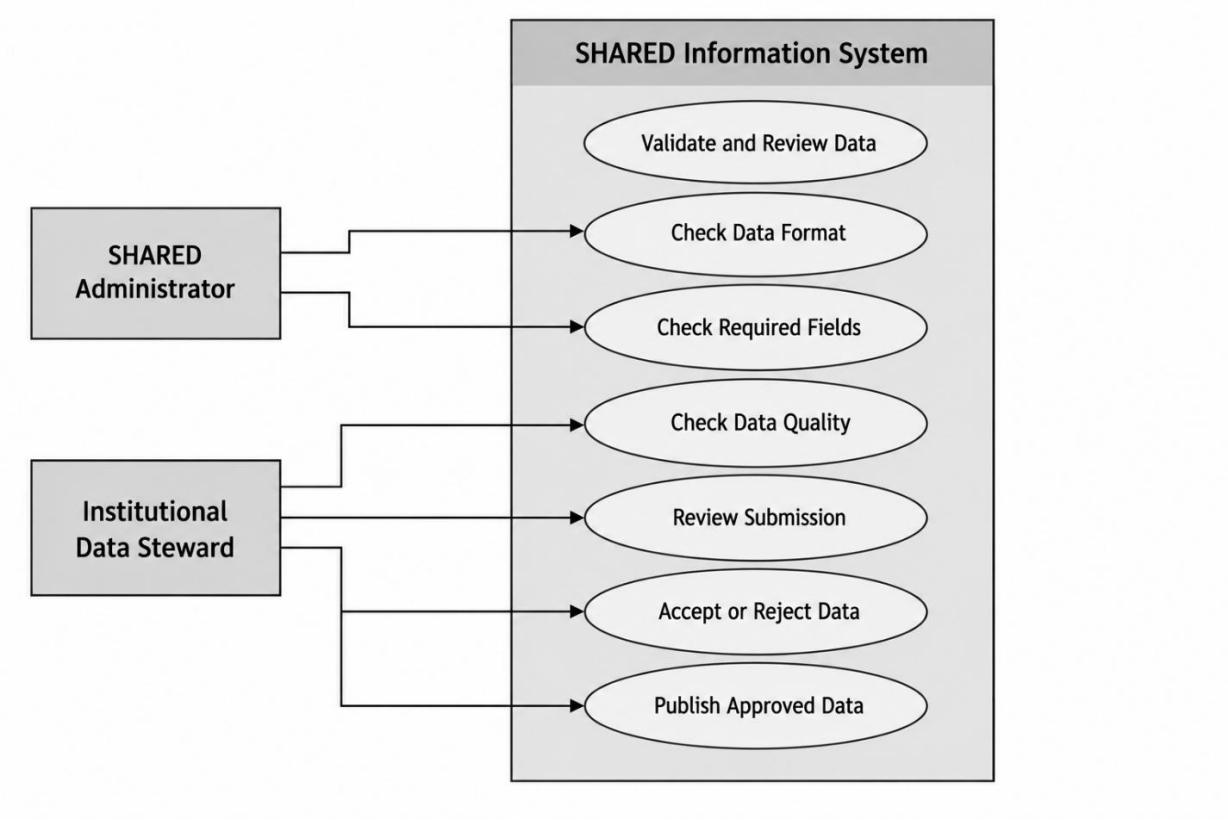


Figure 2 4 Validate and Review Data

Technical validation should be performed by the system where possible. Institutional validation should be performed by an authorized data steward.

2.5.4 DP-UC06 – Manage Data Access

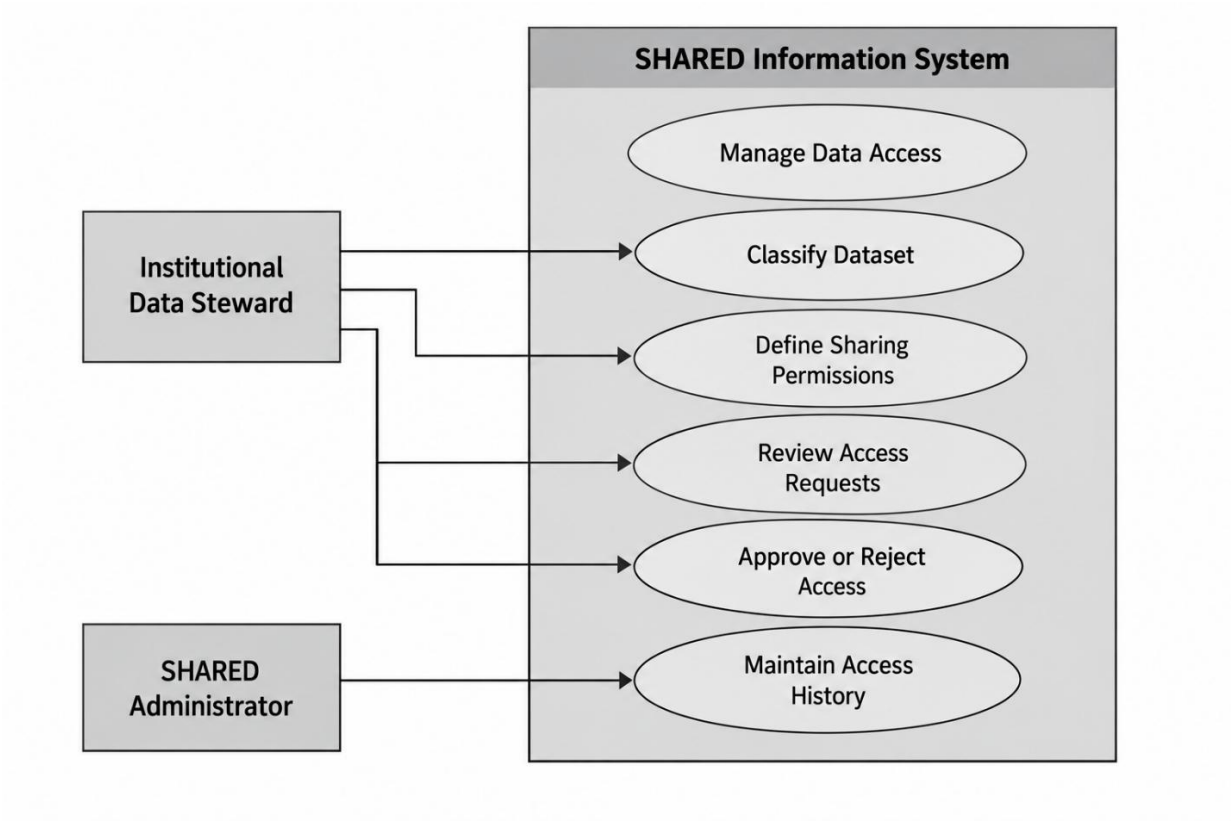


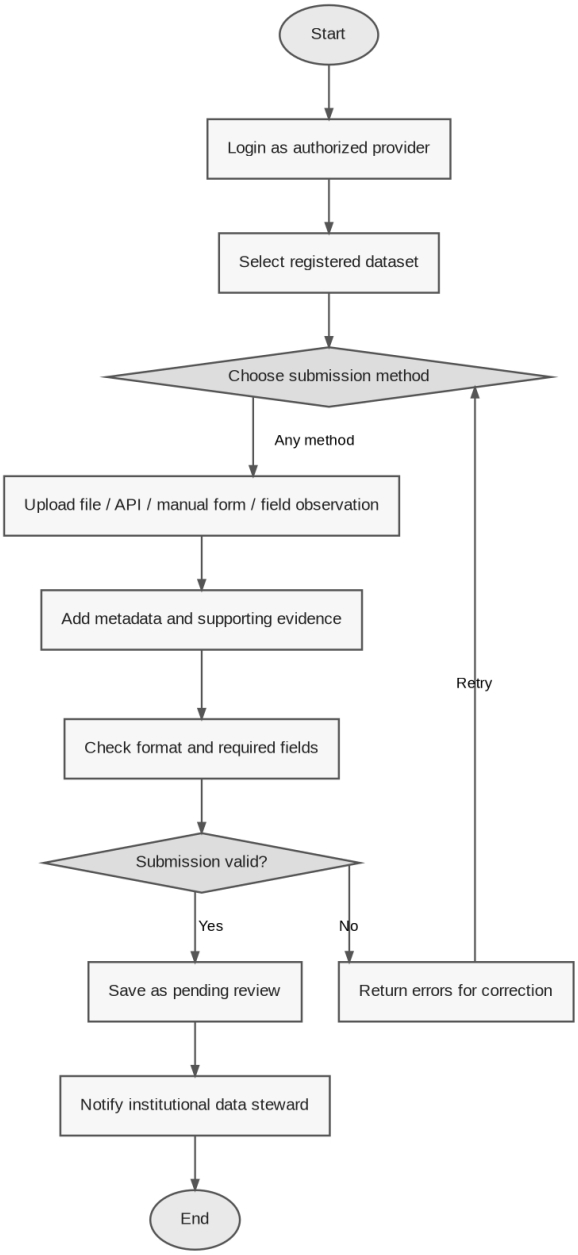
Figure 2 5 Manage Data Access

The system should allow institutions to protect restricted information while making approved information available to relevant stakeholders.

2.6 Activity Workflows – Data Providers

The following activity diagrams describe the proposed data-provider workflows. The responsible institutions will confirm the review roles and release rules.

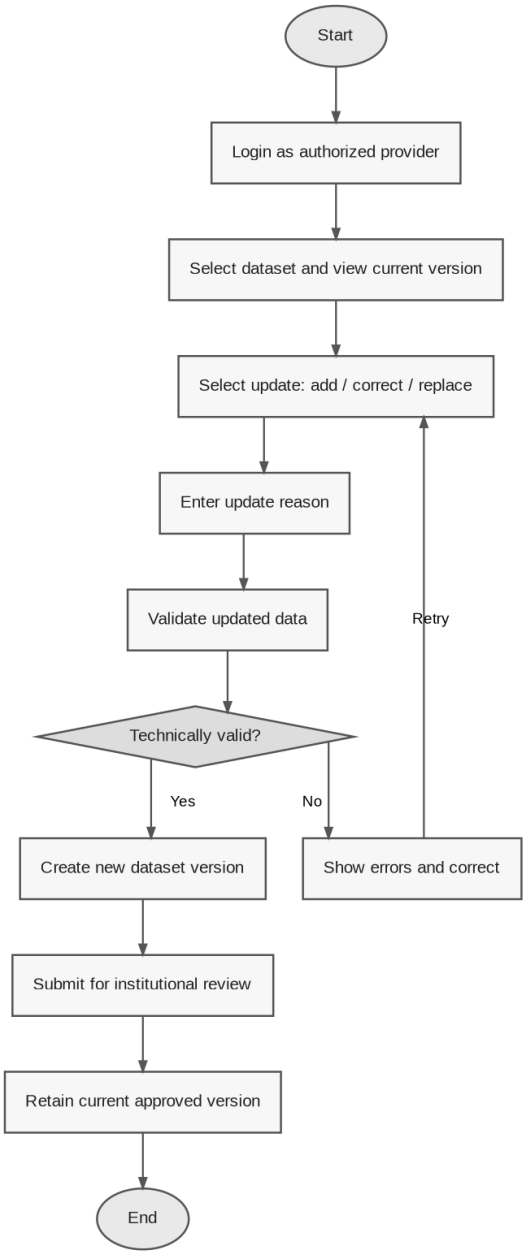
2.6.1 DP-UC02 – Provide Information



Scenario: A provider uploads a forest-cover dataset or a field officer submits observations. SHARED checks the submission and sends it for review.

Figure 2 6 DP-UC02 Provide Information

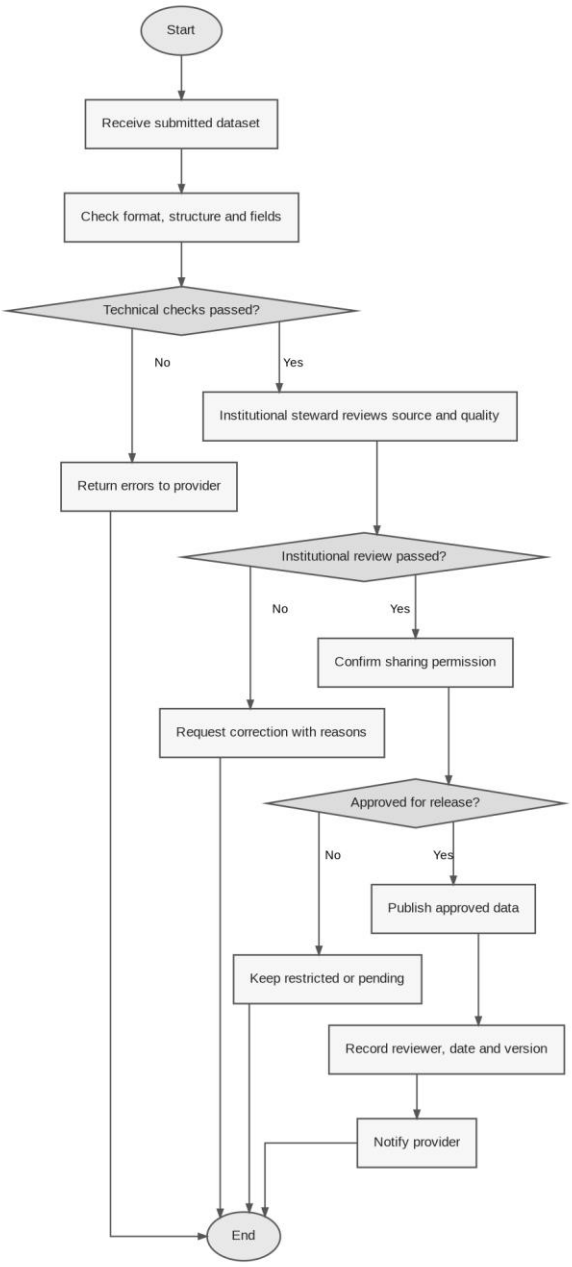
2.6.2 DP-UC03 – Update Information



Scenario: The Department of Agriculture updates seasonal cultivation information while SHARED keeps the current approved version available.

Figure 2 7 DP-UC03 Update Information

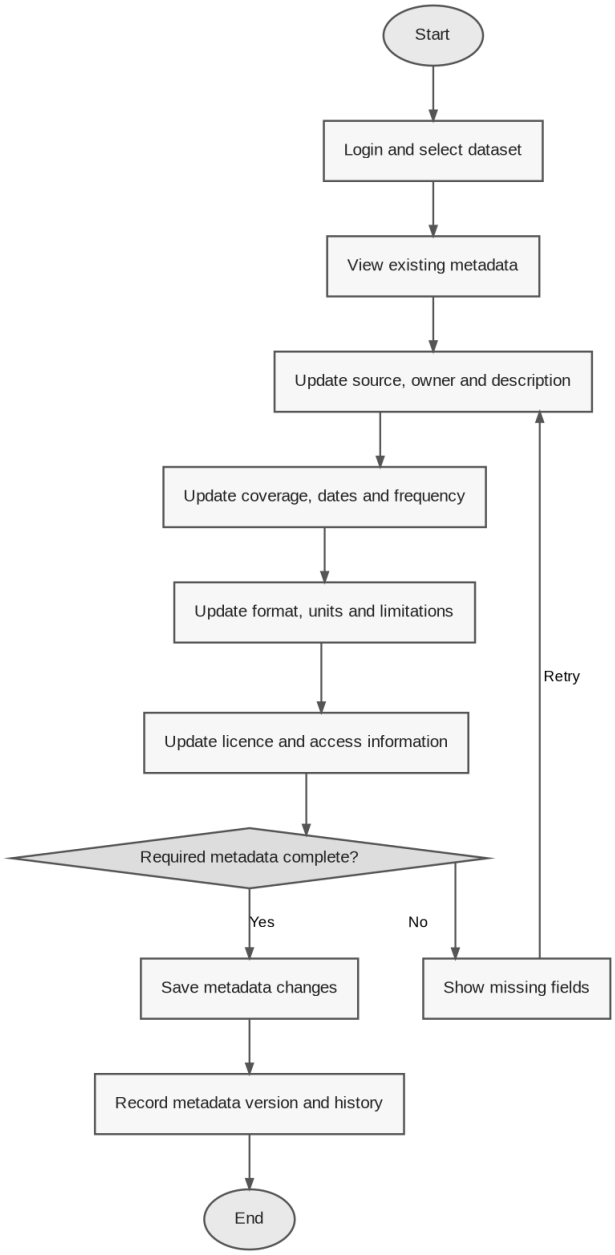
2.6.3 DP-UC04 – Validate and Review Data



Scenario: An NRMC data steward reviews updated soil information after technical validation. Approved data is released only under permitted access rules.

Figure 2 8 DP-UC04 Validate and Review Data

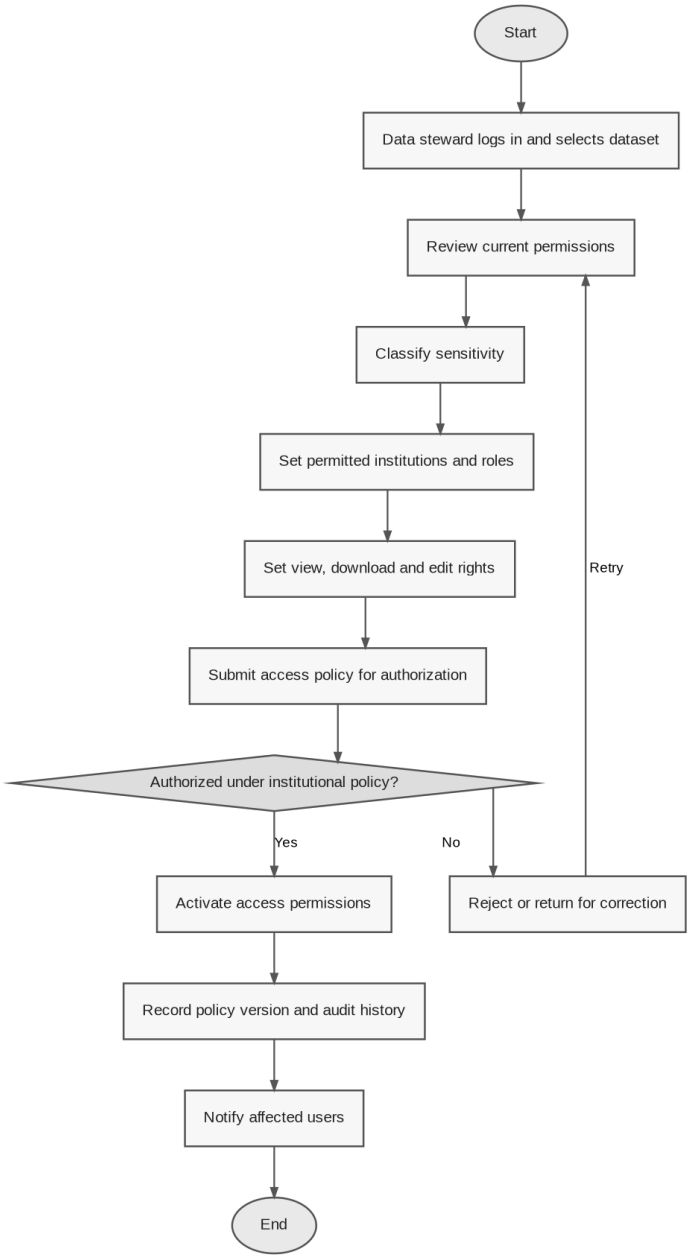
2.6.4 DP-UC05 – Manage Metadata



Scenario: The Survey Department records dataset coverage, source, coordinate reference system, accuracy and update date.

Figure 2 9 DP-UC05 Manage Metadata

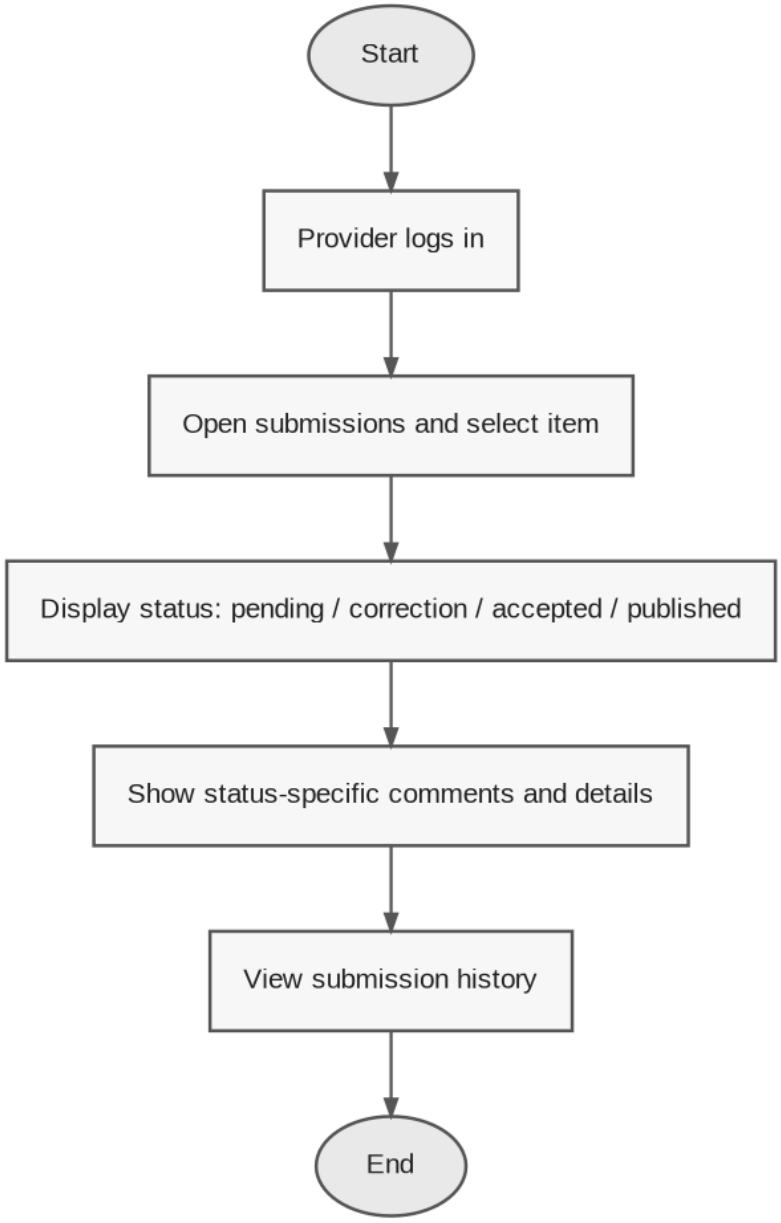
2.6.5 DP-UC06 – Manage Data Access



Scenario: The Forest Department shares general forest-cover information but restricts sensitive biodiversity locations.

Figure 2 10 DP-UC06 Manage Data Access

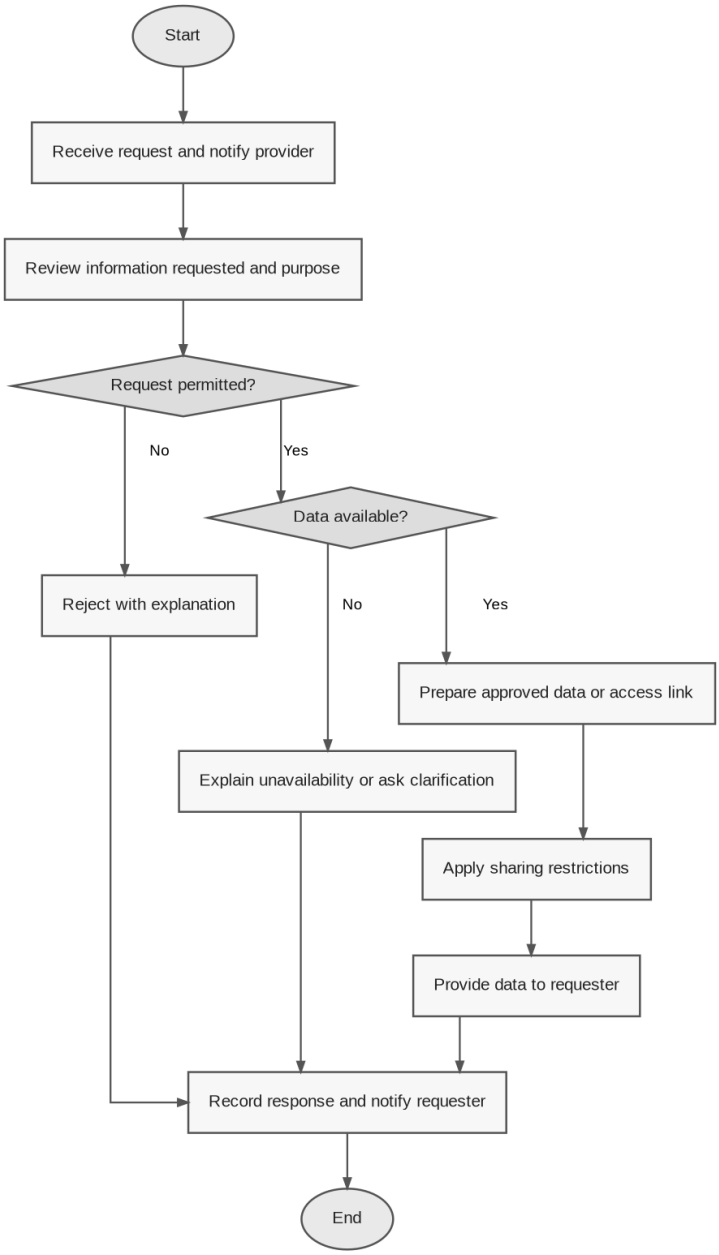
2.6.6 DP-UC07 – View Submission Status



Scenario: LUPPD checks whether an updated land-use map is pending, requires correction, has been accepted or has been published.

Figure 2 11 DP-UC07 View Submission Status

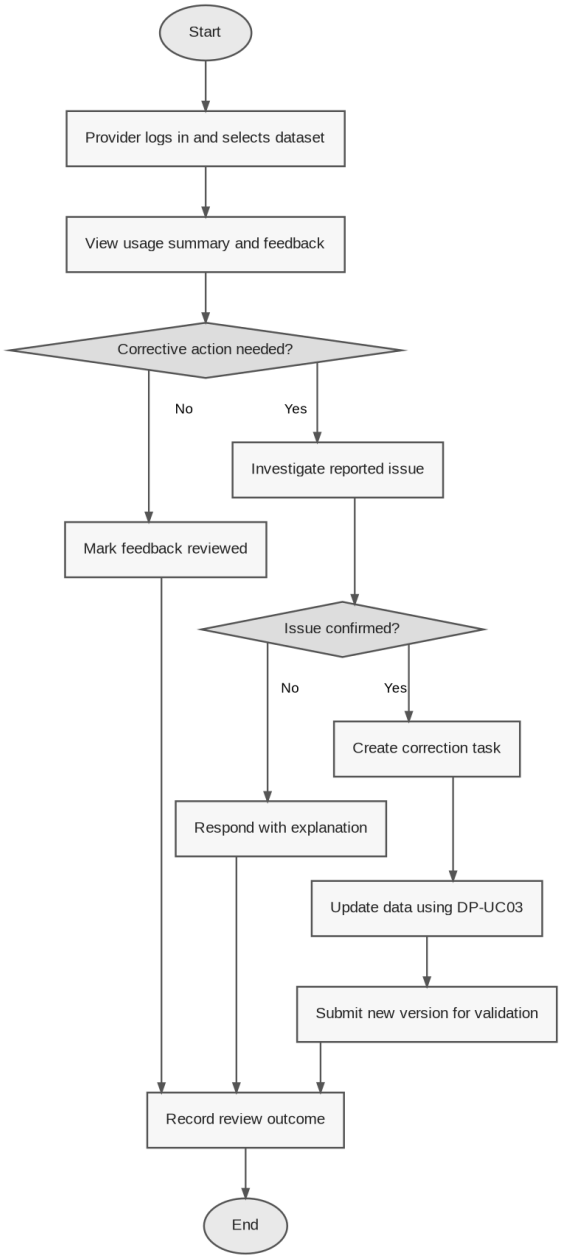
2.6.7 DP-UC08 – Respond to Data Requests



Scenario: An irrigation data steward checks an authorized planning officer's request for reservoir information and supplies only permitted data.

Figure 2 12 DP-UC08 Respond to Data Requests

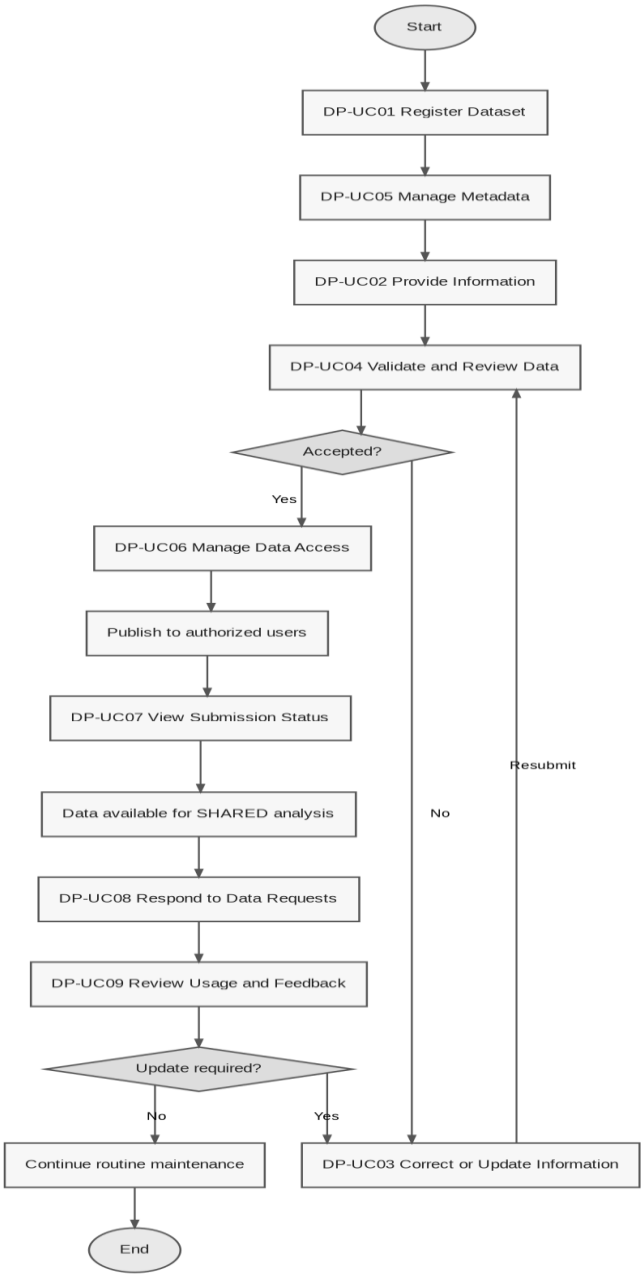
2.6.8 DP-UC09 – Review Data Usage and Feedback



Scenario: A planning officer flags outdated irrigation information. The responsible provider reviews the issue and submits a correction if needed.

Figure 2 13 DP-UC09 Review Data Usage and Feedback

2.6.9 Overall Data Provider Workflow



Scenario: The overall lifecycle connects registration, submission, validation, controlled sharing, requests, feedback and periodic updates.

Figure 2 14 Overall Data Provider Workflow

2 7 Functional Requirements

Data collection and review use the existing nine Data Provider use cases. The requirements below apply to manual forms, files, documents and approved feeds. Operational source contracts must state the actual update frequency and reviewer.

These requirements are proposed Must requirements in delivery package WP1. The client approves the release baseline and any deferral through C01. Optional intelligent processing, device adapters, additional field-access channels and offline operation require explicit scope confirmation. The acceptance checks are required tests, not recorded test results.

FR029 Describe each source and dataset

SHARED must keep source ownership, custody, licence, update frequency, coverage, quality, classification, dataset versions and available distributions in the shared catalogue.

Acceptance check: Open a source's rights, period and current version.

FR030 Describe versioned fields

SHARED must expose each dataset version's field definitions, types, units and supported integration method.

Acceptance check: A new file format uses the correct contract version.

FR031 Define indicators before results

SHARED must record each indicator definition's unit, owner, frequency, disaggregation, baseline and target descriptive information, and required sources. Observations require approved contracts.

Acceptance check: Do not create an indicator result from a label alone.

FR032 Separate original input from curated data

SHARED must keep unchanged or versioned staged input, then use the approved defined data structures for accepted records. Do not create a single store of values without defined types and meanings.

Acceptance check: An import preserves its original and its typed destination.

FR033 Follow up with the provider

SHARED must use shared assigned work, responses, evidence and review for dataset requests and quality feedback. Show permitted usage relationships without claiming complete view/download telemetry.

Acceptance check: A provider can explain unavailable data through the assigned workflow.

FR034 Connect usable fields to sources

SHARED must retain reviewed links from domain fields to dataset fields that identify the shared field and version, permitted area and period, and actual source availability. A field link must not copy values or approve observations.

Acceptance check: Show a missing source or unpublished binding clearly.

FR035 Use controlled entry routes

SHARED must require external contributors to use authenticated web, mobile or API workflows. They must not read or write database tables directly.

Acceptance check: Reject direct database use by the runtime user.

FR036 Follow configured transitions

SHARED must enforce the configured workflow for draft, submission, validation, review, return, approval, publication and archive steps. Invalid transitions must fail atomically.

Acceptance check: A returned submission needs correction before resubmission.

FR037 Keep submission context

SHARED must retain source, submitter, organization, time, reporting period, schema version, rights, owner, sensitivity and validation outcomes as unchanged or versioned evidence.

Acceptance check: Reopen the submitted form with its original context.

FR038 Keep manual source details

SHARED must store the supplied source resources, source rows and measured location accuracy with the shared observation. Reject unsupported precision, overflow and excessive text instead of silently changing it.

Acceptance check: Save zero with its source row and reopen it unchanged.

FR039 Keep missing values distinct

SHARED must use configured field types and checks. Missing values, zero and false must remain different. Unknown observation time and GN must not be guessed.

Acceptance check: A missing date does not become the upload date.

FR040 Reuse detailed field forms

SHARED must reuse published forms for surveys, trials, training and field feedback. When a form value is used in a report field, keep the approved mapping and the link back to the submitted evidence.

Acceptance check: Trace a reported field value back to its submitted form.

FR041 Validate a batch before confirmation

SHARED must process every structured dataset import, including project and deliverable onboarding, through a published CSV, Excel, JSON or restricted XML contract, a quarantined original, row validation and a preview.

Acceptance check: Show invalid rows before any accepted business records are created.

FR042 Approve and save the batch safely

SHARED must bind independent import approval to the exact list of included rows and target schema.

Acceptance check: A failed confirmation leaves no partly accepted project batch.

FR043 Keep the import history

SHARED must retain auditable batches, rows, validation decisions, source evidence and corrective follow-up, protected by their access scope.

Acceptance check: A correction links to the earlier import outcome.

FR044 Recover repeated upload results safely

SHARED must keep the same identifier when an upload or command is retried. If the response is lost, retain the protected original and check the saved outcome before trying again. Never change the earlier evidence to make the retry appear successful.

Acceptance check: Changed bytes under the same command identity are rejected.

FR045 Provide one common file parser

SHARED must support CSV, XLSX, JSON arrays of scalar-valued records and restricted XML row documents through one versioned mapping and validation workflow. Reject unsupported nesting and oversized content. Never execute spreadsheet formulas, macros, XML DTDs or external entities.

Acceptance check: Reject unsafe XML and oversized rows clearly.

FR046 Register the original purpose

SHARED must record original checksum, owner, classification and source purpose. Reuse matching sources only within compatible scope; requirements or guidance must not become observations automatically.

Acceptance check: A design prompt stays reference material, not a measured fact.

FR047 Gate real AI processing

SHARED must require approved provider configuration, processing permission and genuine clean scanning before document processing. Missing setup must be visible; never invent a scan or extraction result.

Acceptance check: An uncleared document cannot proceed as successful extraction.

FR048 Keep extraction evidence

SHARED must retain the original passage, table or page, uncertainty and processing record with each extraction suggestion. Values must use allowed shared data types and destinations.

Acceptance check: Trace a proposed value to the source passage.

FR049 Review several domains from one document

SHARED must require permitted users to verify every proposed base domain, subject, attribute and value. Route approved mappings through the relevant shared dataset batches and independent reviews.

Acceptance check: Review rainfall and cultivation without duplicating the original report.

FR050 Keep mapping approval separate from acceptance

SHARED must record the mapping decision separately from the review of extracted values. Keep rejected suggestions and corrections. Before saving, check permission and the current destination version again.

Acceptance check: Accept one mapping while leaving other values pending.

FR051 Register a controlled source feed

SHARED must bind each feed's source and dataset version to approved fields, keys, units, location context and origin designation. Disabled feeds cannot acquire or ingest new events. Configuration changes preserve history and invalidate affected approvals.

Acceptance check: A feed cannot write another dataset's field.

FR052 Review provider mappings

SHARED must record source-event, observation-time, applicable device and value-field mappings for provider messages. An independent reviewer approves them; a mapping or governing-field change invalidates approval.

Acceptance check: Editing an accepted mapping blocks its unreviewed use.

FR053 Decode supported provider formats

SHARED must provide adapters for institutional data services and device gateways using approved message contracts. An unsupported source or message format requires an accepted adapter contract before connection.

Acceptance check: Reject unsupported content instead of reporting a connection success.

FR054 Keep honest row outcomes

SHARED must retain the source message identity, observed and received times, mapping version, staged-pending rows and rejected-row reasons in each intake receipt.

Acceptance check: A mixed valid/invalid message does not appear wholly successful.

FR055 Prevent repeated source events

SHARED must reuse unchanged source events and require an explicit correction for changed content. Keep out-of-order arrival distinct from revision. Retained archive batches must use their documented all-or-none saving and duplicate checks.

Acceptance check: Replay an archive without creating a second series.

FR056 Keep live activation explicit

SHARED must keep connections inactive until a real endpoint, protected machine identity, rights and mapping review have been supplied.

Acceptance check: Show a missing live connection rather than a fabricated reading.

FR057 Track quality issues and corrections

SHARED must retain versions, reasons, source references and permitted history for quality issues and observation corrections.

Acceptance check: Reopen a returned issue and its correction evidence.

FR058 Apply published field rules

SHARED must use the same published checks for numeric values, text, required dates and source identifiers on every entry route. Changing a rule already used by records requires a reviewed new version.

Acceptance check: A correction cannot bypass a required field rule.

FR059 Review candidate identity links

SHARED must prevent candidate identity suggestions from approving themselves. Link source keys to a permitted registered object only through the reviewed workflow, preserving source-specific scope.

Acceptance check: A similar reservoir name alone does not create a confirmed match.

FR060 Keep differing values from each source

SHARED must retain both originals and their units, places, dates, methods, review and origin when comparing source-reported values. Do not silently average or overwrite conflicting claims.

Acceptance check: Retain both illustrative 100-acre and 110-acre claims.

FR061 Limit preferred source decisions

When a reviewer chooses a source, record the purpose and evidence for that choice. Check that units, place, period, field mapping and review are suitable. Recheck the choice after a source changes.

Acceptance check: An old preference cannot override a changed unreviewed revision.

FR062 Reuse the quality worklist

Provide one worklist for reviewing values, correcting errors and comparing sources. Keep versions of field and related-field rules. Experts must approve scientific plausibility checks, calibration and specialist rules before those checks are used.

Acceptance check: An unresolved scientific check remains explicit.

2 8 Register Dataset Workflow

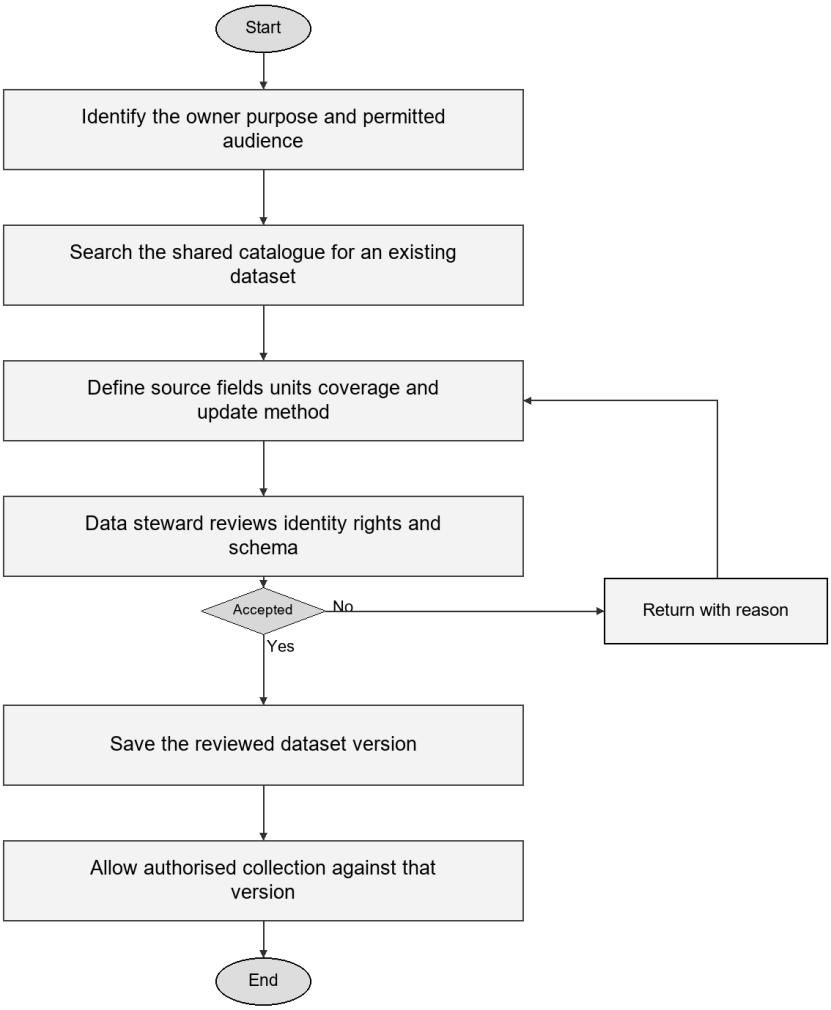


Figure 2 15 Register Dataset

Scenario: An institution proposes a rainfall dataset. The steward checks its source, period, place, units and sharing rights before a feed or file mapping can be used.

3 Stakeholders and System Management

Each participating institution keeps responsibility for its information. SHARED connects the institutions through common records, agreed roles and controlled sharing. An institution may provide information, use information and review work in different contexts.

3 1 Objectives and Actors

The main objectives are to complete the use cases below, retain source and review history, and show the next permitted action clearly. The main actors are Institutional administrator, Data steward, Authorised user, Platform administrator.

3 2 Abstract Use Cases

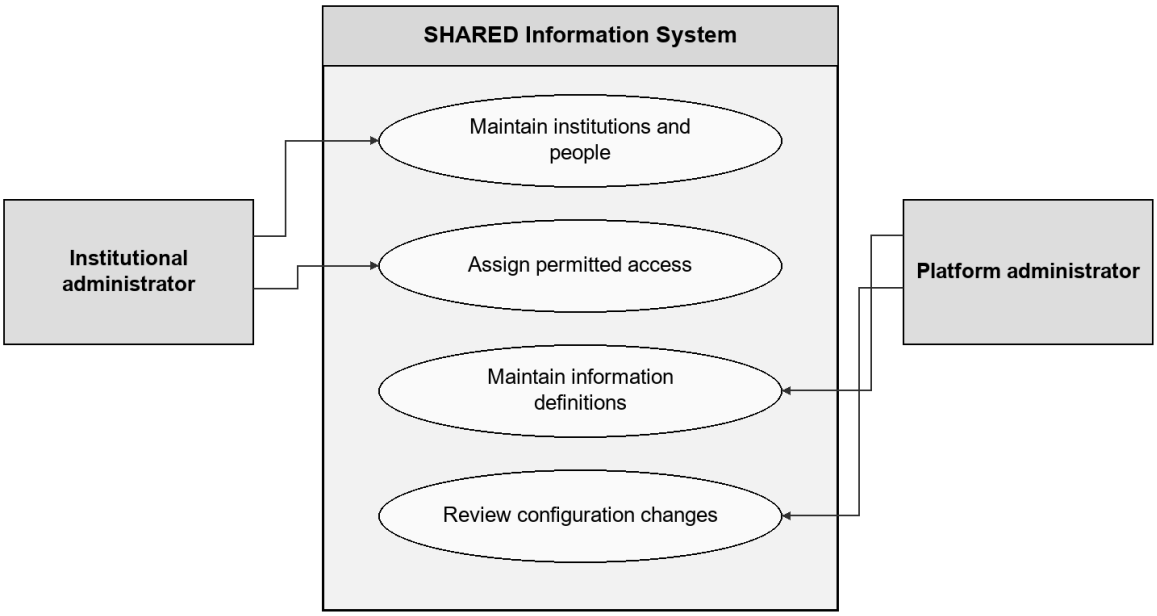


Figure 3 1 Abstract Use Cases

Use case	Main function	Expected result
SM-UC01	Maintain institutions and people	Register an institution once and link its units, people and responsibilities.
SM-UC02	Assign permitted access	Invite the intended user and assign time-limited roles within an approved scope.
SM-UC03	Maintain information definitions	Review domains, fields, units, choices and form versions.
SM-UC04	Review configuration changes	Check affected records before publishing a new definition or access rule.

3 3 Activity Workflow

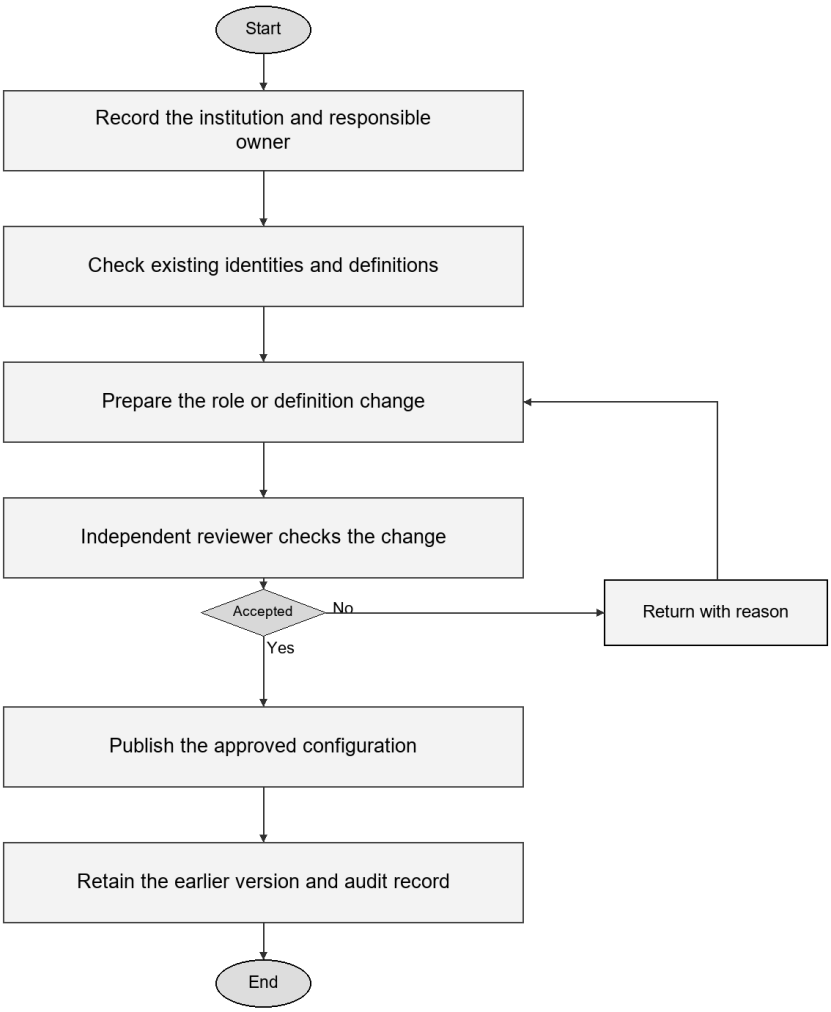


Figure 3 2 Proposed Activity Workflow

Scenario: An appointed steward adds a new crop choice. Existing crop records keep their earlier meaning. Adding the choice does not grant the steward access to another institution.

3 4 Responsibilities and Access

Role	Responsibility
Data provider	Create and correct information within the assigned source and scope.
Data steward	Review metadata, quality, identity links and proposed data releases.
Analyst or researcher	Use permitted evidence, prepare reports and compare options.

Role	Responsibility
Domain expert	Review an appointed method or advice within their competence.
Decision maker	Record an institutional choice within an evidenced mandate.
PMU or implementing partner	Plan, assign, monitor and report programme work.
Farmer or community user	Read released guidance and use permitted personal or feedback functions.
Platform operator	Operate the service and support users without gaining data approval authority.

Permissions apply to the whole allowed combination of action, organisation, domain, project, place, classification and record state. Separate incomplete grants must not combine into a wider grant. Creating data, reviewing it, publishing it and making an institutional decision remain distinct powers.

3 5 Functional Requirements

These requirements are proposed Must requirements in delivery package WP1. The client approves the release baseline and any deferral through C01. Optional intelligent processing, device adapters, additional field-access channels and offline operation require explicit scope confirmation. The acceptance checks are required tests, not recorded test results.

FR001 Maintain organizations and people

SHARED must allow authorized administrators to maintain organizations, units, stakeholders and contacts. They must keep these records separate from login accounts and retain deactivation history.

Acceptance check: Deactivate an organization without erasing its earlier records.

FR002 Manage accounts and roles

SHARED must allow authorized administrators to manage account state, groups, memberships, roles and permissions through audited workflows. Open self-registration must remain disabled unless separately approved.

Acceptance check: Reject an unauthorized attempt to add a privileged user.

FR003 Limit delegated powers

SHARED must apply the permitted scope and effective dates to every delegation and assignment. A delegate must not grant powers beyond those they may delegate.

Acceptance check: An expired assignment no longer gives access.

FR004 Use standard secure sign in

SHARED must provide secure sign-in through an authentication service, including standard password hashing, lockout, expiring tokens and revocable sessions. Require multi-factor

authentication for platform administrators, privileged access reviewers and other roles identified by the approved security policy.

Acceptance check: Disable an account and reject its later protected requests.

FR005 Use the signed in user identity

SHARED must identify the acting user from validated sign-in on the server. An identity or scope supplied in a request must not be accepted as proof of permission.

Acceptance check: Changing a submitted actor identifier does not widen access.

FR006 Invite the intended user

SHARED must issue expiring, single-use invitations that activate only the intended account. Keep delivery, use and recovery states truthful; do not print invitation secrets in logs.

Acceptance check: Reject a reused or expired invitation.

FR007 Keep the user identity when changing workspace

SHARED must let an authorized administrator select a shared stakeholder context. SHARED must retain the actual acting account and check the chosen context's permissions.

Acceptance check: Switch context without granting access to another owner's private records.

FR008 Use one connected platform

SHARED must connect organizations, domains, geography, projects, evidence, contributions and discovery through shared identities and workflows.

Acceptance check: Open a project's permitted source and location without creating another project.

FR009 Check the full access scope

SHARED must deny access unless permitted for the action, organization, stakeholder, domain, project, geography, record, classification and workflow state. Lists, counts, maps, files and exports must follow the same rule.

Acceptance check: A copied private link remains inaccessible to an unauthorized user.

FR010 Let owners control sharing

SHARED must allow appointed sharing managers to choose owner-only or selected-stakeholder audiences within shared rules, including dataset overrides. Audit changes and prevent recipient re-sharing or self-delegation.

Acceptance check: Withdraw an allowed audience and recheck the next read.

FR011 Place all stakeholders correctly

SHARED must retain the approved stakeholder branches and related participants through shared identities. The prototype currently groups these into 15 main branches. This is an editable starting configuration. Adding a participant must not create legal ownership, a login account or access automatically.

Acceptance check: Place a research partner without duplicating its identity.

FR012 Keep separate owned base domains

SHARED must allow each owner to maintain its permitted base domains, subjects, attributes and connections. Forest and Wildlife must retain separate ownership. Shared subjects must use reviewed relationships.

Acceptance check: Link a watershed subject without merging department ownership.

FR013 Configure useful workspaces

SHARED must provide configurable dashboard definitions, audiences and saved preferences. Register proposed products with their purpose, inputs, coverage, approval and acceptance needs; leave proposals inactive.

Acceptance check: A proposed chart does not appear as a working analysis.

FR014 Maintain versioned domain packs

SHARED must allow appointed stewards to maintain reviewed domain packs containing schema definitions, vocabularies, units and project or deliverable templates.

Acceptance check: Reopen a submission with the exact form version it used.

FR015 Allow safe configuration only

SHARED must limit configuration to reviewed field types, components, validation, vocabulary, geography and evidence definitions. Reject scripts, executable expressions and unknown properties.

Acceptance check: Reject a form definition that attempts to run supplied code.

FR016 Keep the original form version

SHARED must keep the exact field definitions and form version used to validate each submitted section. Later template edits must not rewrite that submission.

Acceptance check: Changing a draft template does not rewrite a submitted form.

FR017 Separate editable settings from software changes

SHARED must allow new domains, subjects and attributes that use published supported storage profiles to be configured without deployment.

Acceptance check: Add another decimal field through configuration; reject an unsupported geometry-valued attribute until its required extension is delivered.

FR018 Maintain editable vocabularies

SHARED must support hierarchy, translations, effective dates, ordering, aliases and retirement in reference lists. Used identities and meanings must remain stable.

Acceptance check: Retire a value without breaking earlier records.

FR019 Allow several domain classifications

SHARED must link a controlled record to its primary domain and secondary classifications without copying its core record.

Acceptance check: One project can be found under farming and irrigation.

FR020 Keep business terms in configuration

SHARED must store the initial domain names, field descriptions and allowed choices as editable settings. They must not be fixed in screen code or supplied as sample business records.

Acceptance check: Change an allowed display label without a code deployment.

FR021 Review meanings and impacts

SHARED must reuse existing meanings, fields and units where they are truly the same. Before merging definitions or publishing a change, an authorized reviewer must check possible duplicates and affected records. Similar labels do not prove equal meaning.

Acceptance check: Keep gross and effective reservoir capacity distinct.

4 Maps Dashboards and Geographic Information

Maps and dashboards help users understand where a problem occurs, what information is available and how results differ between places and periods. Every figure must show its unit, source, period, level of detail and review state.

4 1 Objectives and Actors

The main objectives are to complete the use cases below, retain source and review history, and show the next permitted action clearly. The main actors are Policy maker, Researcher or GIS specialist, Farmer or field officer, Geographic data steward.

4 2 Abstract Use Cases

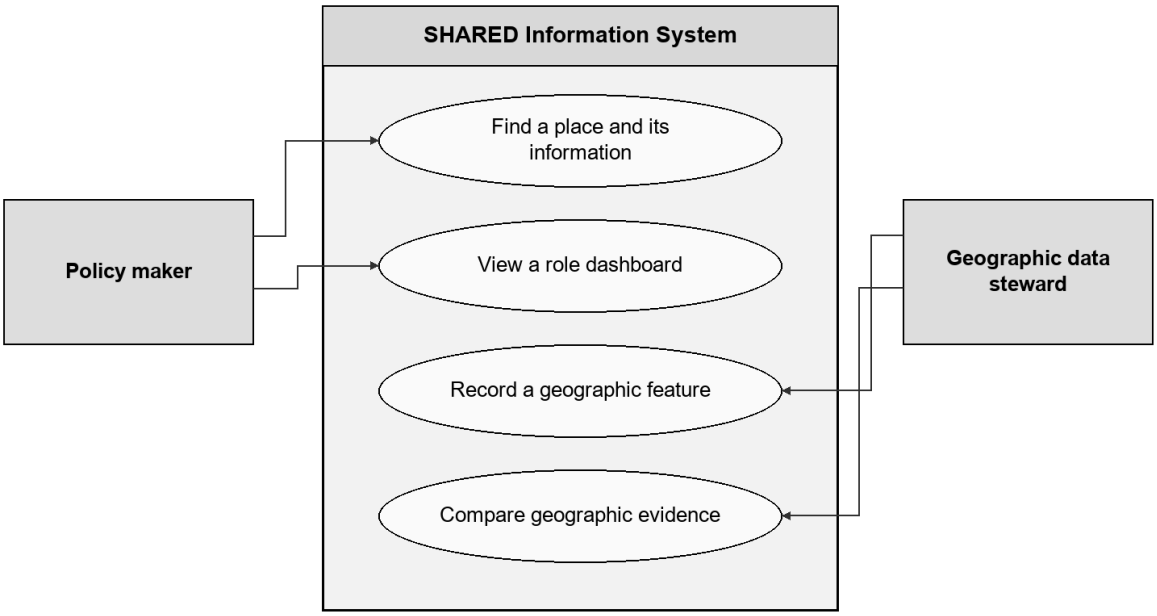


Figure 4 1 Abstract Use Cases

Use case	Main function	Expected result
GI-UC01	Find a place and its information	Search an approved place, open a permitted layer and inspect its source.
GI-UC02	View a role dashboard	Choose the relevant measures, period and area without changing the underlying records.
GI-UC03	Record a geographic feature	Use an approved feature type, location role and field definition.
GI-UC04	Compare geographic evidence	Run a supported comparison with compatible sources and stated limits.

4 3 Activity Workflow

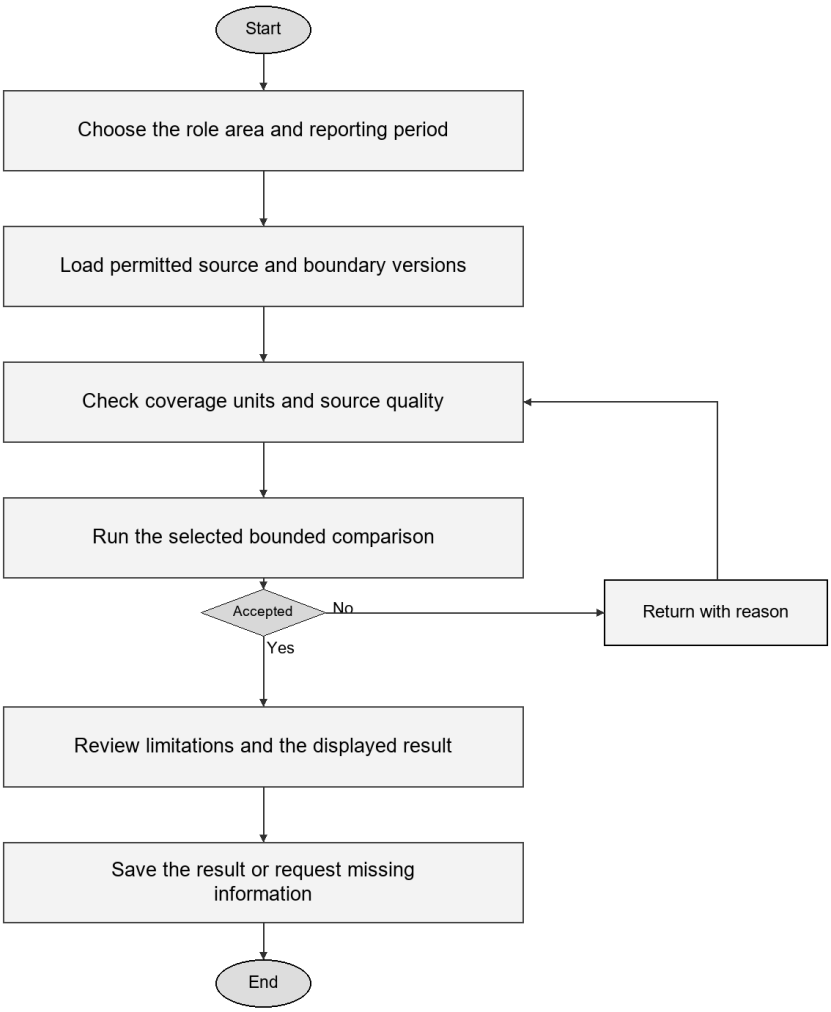


Figure 4 2 Proposed Activity Workflow

Scenario: A researcher compares two forest-cover releases for the same area. SHARED identifies changed class definitions or boundary editions before showing a change result. A farmer sees simpler released information for the selected local area.

4 4 Geographic Rules

Administrative units, catchments, parcels, infrastructure and ecological areas are separate schemes. Their overlap does not establish administrative authority or programme eligibility. Use an approved coded programme roster. Source studies contain different GN totals, including 1,533 and 1,584; these figures must not be reconciled by guessing exclusions. A district-only observation remains district-level information.

Keep measured station data, satellite or model-grid data, forecasts, expert assessments and official warnings identifiable. A grid value must not be presented as a GN measurement. Raster comparisons require compatible coordinate systems, cells, units, class definitions and NoData rules. Public map availability does not establish a licence for storage, analysis or redistribution.

4 5 Functional Requirements

These requirements are proposed Must requirements in delivery package WP2. The client approves the release baseline and any deferral through C01. Optional intelligent processing, device adapters, additional field-access channels and offline operation require explicit scope confirmation. The acceptance checks are required tests, not recorded test results.

FR022 Support several geography schemes

SHARED must allow appointed stewards to configure independent geography schemes and levels rather than force all places into one hierarchy.

Acceptance check: Administrative divisions and catchments coexist.

FR023 Keep place identity and source

SHARED must retain each place's stable codes, names, aliases, translations, geometry, source, accuracy, dates, version and status for supported point, line and polygon forms.

Acceptance check: A recorded river line keeps its own source and dates.

FR024 Link overlapping places

SHARED must support reviewed hierarchy, containment, overlap and many-to-many links between schemes.

Acceptance check: A catchment can overlap several GN divisions.

FR025 Preserve boundary history

SHARED must preserve historical references and prevent deletion of used meanings when a place is replaced, split, merged or retired.

Acceptance check: An old project still points to its earlier boundary version.

FR026 Validate spatial input

SHARED must check coordinate system, bounds, type, validity, topology, complexity and safe query limits. Unsupported input must fail clearly.

Acceptance check: Reject an invalid or oversized geometry without partial saving.

FR027 Review boundary changes

SHARED must enforce the configured Draft, Review, Active and Retired lifecycle for boundaries. High-impact changes need impact preview and independent approval.

Acceptance check: Reject self-approval of a protected boundary change.

FR028 Search GN divisions within safe limits

SHARED must search GN areas through the shared paged geography reader. Keep timeout, missing and denied responses distinct from a valid empty list.

Acceptance check: A failed GN search shows a recoverable error.

FR063 Describe spatial sources

SHARED must retain each spatial layer version's source type, geometry or raster descriptive information, coordinate system, scale or resolution, coverage, owner and classification.

Acceptance check: Open a layer's source and coverage before using it.

FR064 Save permitted map settings

SHARED must make approved map styles, legends, layer groups and saved map workspaces refer to the shared permitted layers. Recheck withdrawn source access.

Acceptance check: A saved map does not reveal a now-private layer.

FR065 Reuse one spatial catalogue

SHARED must connect layers to domains, datasets, documents, projects, interventions and geographies without another GIS registry.

Acceptance check: The same layer appears in its permitted project and domain views.

FR066 Protect location disclosure

SHARED must enforce device, volume and location-disclosure limits in web and mobile maps. Sensitive exact locations must be hidden or generalized according to approved rules.

Acceptance check: A restricted species location is not exposed by identify or export.

FR067 Exclude known demonstration features

SHARED must exclude positively identified test and demonstration features from operational maps while preserving their history. Unknown origin must not be relabelled real.

Acceptance check: A demonstration marker cannot appear as an operational observation.

FR068 Keep navigation and large maps simple

SHARED must use the shared grouped menu, context and progressive layer loading. Cancel old requests and distinguish missing, denied, failed and valid empty results.

Acceptance check: Changing a layer does not leave an obsolete response on screen.

FR069 Provide bounded vector exploration

SHARED must support the specified approximate buffer, loaded-feature proximity, selected-polygon overlap and area tools with method, units, inputs and limits.

Acceptance check: An approximate distance is not labelled a road route or legal survey.

FR070 Use genuine points for point methods

SHARED must use actual points and retain scale, denominators and non-estimable states for clustering, record-density grids and exploratory hotspot counts. Do not invent point centres or risk classes.

Acceptance check: Reject a polygon input where actual points are required.

FR071 Compare compatible raster cells

SHARED must check coordinate system, grid alignment, units, class meaning and missing cells before supported raster preview, swipe, native-cell summary or change analysis.

Acceptance check: Reject change between incompatible grids instead of silently resampling.

FR072 Retain an exploratory receipt

SHARED must keep source versions, context, parameters, fingerprints, limits and outputs. Bound background work, support cancellation and invalidate results after source change.

Acceptance check: A changed input requires a new exploration.

FR073 Retain normalized spatial sources

SHARED must use the shared source and version workflow for exact lawful originals and supported normalized points or native raster cells. Preserve coordinates, source dates and missing cells.

Acceptance check: Reopen the retained original and its source receipt.

FR074 Review spatial release separately

SHARED must keep a pending spatial layer unpublished during ingestion. Apply archive, geometry, extent and supported transformation controls. General conversion, national tiling or every GIS file type must not be claimed.

Acceptance check: A local preview does not automatically upload or approve a layer.

FR075 Keep weather source identities

SHARED must retain source product, variable, location, unit, observation period, receipt time, issue time and forecast validity where supplied.

Acceptance check: A forecast issue date is not presented as its observation date.

FR076 Show missing and stale weather honestly

SHARED must show overdue or failed source acquisition and expired retained forecasts in source-refresh views. Unknown source or period must remain unknown.

Acceptance check: Opening an old forecast does not label it current.

FR077 Keep retained rainfall at its actual scale

SHARED must retain the original grid location, period, units, references and origin of retained rainfall source series. Do not invent a GN assignment or new station.

Acceptance check: A model grid point remains model-grid context on the map.

FR078 Do not invent the GN time series

SHARED must require suitable dated records or an approved allocation method for a complete GN rainfall and cultivation comparison. An undated classification or district statistic cannot supply five annual GN totals.

Acceptance check: The report identifies the exact missing years and geographic detail.

FR079 Separate evidence from warnings

SHARED must require the relevant accepted method, inputs and authority before presenting operational hazard, drought, adaptation or warning outputs. Recorded context must not become an official warning automatically.

Acceptance check: A thermal detection is not labelled a confirmed fire.

FR080 Keep farming identities and plots

SHARED must reuse society or farmer-group profiles, members, farm plots and plot-crop records with their owner, source, area and permitted review states.

Acceptance check: One participant does not become another login or duplicate farmer record.

FR081 Record farm work and issues

SHARED must link farming activities, problems, actions and evidence to the relevant plot, crop, project and workflow.

Acceptance check: A returned farm issue retains its reason and corrective action.

4 6 Geographic Record Requirements

The following existing prototype requirements specify geographic business records. They reuse the common catalogue, forms and review workflow. Detailed current fields are retained in the coverage workbook. All are proposed Must requirements in WP2.

SH-GEO-FEAT-001 Register Geographic Information Types

Each geographic record type must identify its owning institution, domain, subject, business object, allowed geometry, required and optional fields, place and time rules, source and evidence, validation, review workflow, map style, classification and access. Authorised stewards configure the type through the shared definitions.

Acceptance check: Publish a reviewed type and create a record using its exact field and geometry rules.

SH-GEO-FEAT-002 Create Geographic Records from a Map

Authorised users must select the domain and record type, then choose an existing area or feature, enter coordinates, drop a point, or draw a line, polygon or supported multipart feature. Show only applicable fields and save the geometry or reference as a draft with the related business information.

Acceptance check: Save a point and polygon for permitted types; reject a geometry that the selected type does not allow.

SH-GEO-FEAT-003 Record Unknown or Approximate Locations

Keep a known administrative area separate from the actual occurrence or affected extent. Allow an area-only record when a precise location is unknown. Retain positional accuracy, uncertainty and source description for approximate points. Never invent coordinates, centroids or polygons to satisfy a field.

Acceptance check: Save a GN-only record without creating a point or an affected-area polygon.

SH-GEO-FEAT-004 Support Different Geographic Roles

One record may have several geographic representations: reported location, observed extent, surveyed footprint, investigation area, model assessment, proposed intervention and monitoring area. Each representation must retain its role, source, applicable period, accuracy and version. Do not silently combine these roles.

Acceptance check: Retain a reported point and a later surveyed footprint as distinct representations of one record.

SH-GEO-FEAT-005 Use Domain-Specific Attributes

Use the domain owner's published field definitions and reuse equivalent fields. Incident, wildlife, crop suitability and other record types may need different attributes and review rules. The owner confirms the field meanings, required state, units and allowed values before publication.

Acceptance check: A wildlife incident and crop assessment show their own approved fields without creating duplicate definitions.

SH-GEO-FEAT-006 Accept Multiple Geographic Data Sources

Support approved manual drawing, field and mobile surveys, coordinate entry, existing feature selection, GIS imports, institutional APIs and remote-sensing products. AI-suggested geographic references require the approved document-processing route. Every route uses shared source registration, mapping, validation and review.

Acceptance check: Import and manually enter the same supported geometry type through the common validation and review controls.

SH-GEO-FEAT-007 Validate Geographic Information

Validate coordinate system, axis order, ranges, geometry type, empty shapes, polygon closure, self-intersection, topology, extent, time, units, required fields, duplicate submissions, object relationships and source version. Apply complexity limits and return clear correction details.

Acceptance check: Reject an invalid ring, incorrect coordinate order and duplicate source event without a partial accepted record.

SH-GEO-FEAT-008 Review Geographic Records

Reviewers must inspect the submitted geometry, original source, field mappings, accuracy, related records, existing layers, validation, earlier versions and evidence. Record acceptance, return,

rejection or required correction under the approved workflow. Technical validity alone cannot approve a geographic feature.

Acceptance check: A valid polygon stays pending until the appointed reviewer records the required decision.

SH-GEO-FEAT-009 Preserve Source Ownership

Preserve the source institution, custodian, classification and permitted audience of every geographic claim. Different institutions may report on the same occurrence. Reviewed matching may link the reports without deleting originals or transferring ownership.

Acceptance check: Link two institutional reports of one event while retaining both sources and their separate sharing rules.

SH-GEO-FEAT-010 Maintain Geographic History

Preserve corrections, earlier geometry versions and reasons. A later surveyed footprint links to the original approximate record. Authorised users can inspect the historical evidence and change history.

Acceptance check: Correct an approximate location and reopen the earlier geometry and correction reason.

SH-GEO-FEAT-011 Support Geographic Time Periods

Keep occurrence, observation, reporting, survey, assessment, validity, entry and revision times distinct where relevant. Allow historical and reporting-period filters. A past flood extent must not be displayed as a current flood simply because its record is opened.

Acceptance check: Filter an event by its occurrence period without substituting the upload or revision time.

SH-GEO-FEAT-012 Reuse Existing GIS Layers

Expose permitted accepted records through the shared Map Explorer and spatial catalogue. Reuse existing layers, styles, geography references and services. Use governed feature collections where appropriate rather than a new catalogue, engine or physical layer for every institution or event.

Acceptance check: Open the same permitted record from its project and shared map without copying the feature.

SH-GEO-FEAT-013 Configure Map Symbols and Legends

Configure symbols, legends and styles for record types and geographic roles. Distinguish incidents, surveyed extents, suitability assessments, proposed interventions and unreviewed observations. Colour alone must not communicate approval, severity, hazard or suitability.

Acceptance check: Read each state through its label or symbol as well as colour, including in a monochrome view.

SH-GEO-FEAT-014 Support Geographic Analysis

Permit supported area, distance, overlap, intersection, containment, proximity, administrative aggregation, temporal comparison, counts and overlay analyses. Retain the actual source geometry, method, units, limits and derived-result evidence. Do not imply unsupported scientific accuracy.

Acceptance check: Reproduce a bounded area or overlap result and show the original geometry and calculation limits.

SH-GEO-FEAT-015 Connect Geographic Records to Other Modules

Reuse the same accepted geographic identity across permitted map, location profile, domain dashboard, expert, planning, decision, project and PMU views. Links must preserve the governed source, version and access rules.

Acceptance check: Open one feature through its dashboard and decision case with the same source identity and permissions.

SH-GEO-FEAT-016 Support Data Maintenance

Provide the appropriate authorised edit, field survey, API, GIS import or source-synchronisation route for each record or layer. Preserve source and geometry history. Operational users must not edit database records directly.

Acceptance check: Correct a feature through its approved route while retaining the earlier source and geometry version.

SH-GEO-FEAT-017 Support responsive geographic collection

Within the agreed responsive field journey, allow authorised users to capture geographic points, accuracy, permitted geometry, photographs and actual observation time where the selected device supports them. An additional field-access channel and offline drafts are proposed options under C01, C06 and C07. If selected, protect drafts and synchronise through the common authenticated service interfaces. Synchronisation alone must not publish an unreviewed record.

Acceptance check: Submit a permitted field observation through the selected journey and retain it as pending until the required review; test offline retry only when that option is selected.

SH-GEO-FEAT-018 Show Geographic Data Quality and Status

Show source, actual observation or occurrence time, geometry role, accuracy, review and approval state, version and real, reference or demonstration origin in maps and record details. Keep unavailable information explicitly unknown.

Acceptance check: A missing accuracy or observation time stays unknown; a demonstration feature remains labelled as such.

SH-GEO-FEAT-019 Protect restricted geographic information

Apply complete institutional ownership and permission rules to geographic features, service responses, maps, search, counts and exports. Protect sensitive wildlife locations, personal information and restricted records. For fresh public access, use one shared eligibility rule for publication state, classification, audience, required source identity, exact permitted source version, approved use rights, expiry and source or citation dependencies. Re-evaluate on read and export,

including dependent cached outputs. Suppress public access when a required dependency is withdrawn, expired, restricted, missing, cyclic or no longer authorised for the requested use. Do not assume the newest version is approved or reject an older version that remains explicitly permitted. Preserve authorised internal records, provenance and history. Previously downloaded copies outside SHARED cannot be recalled.

Acceptance check: Publish a synthetic observation, then withdraw, expire or restrict its required source or change its exact-version rights. Fresh list, detail, map, count, cache and export paths suppress the dependent output while permitted internal provenance remains available; permitted older versions and cycle or missing-reference denial are tested.

SH-GEO-FEAT-020 Distinguish Facts from Assessments and Warnings

Distinguish reported from verified landslides, thermal detections from confirmed fires, forecasts from observed flood extents, suitability scores from legal land-use decisions, proposed from implemented activities, and exploratory from accepted scientific results. Official warnings, regulatory decisions and expert conclusions require their own authority and approval.

Acceptance check: A thermal detection, forecast or exploratory result cannot acquire a confirmed-event or official-warning state without the required evidence and authority.

5 Decision Support and Reporting

SHARED helps an authorised person prepare and record a decision. The system brings together the problem, evidence, alternatives, analysis, expert advice and stakeholder responses. The institution with authority remains responsible for the selected action.

5 1 Objectives and Actors

The main objectives are to complete the use cases below, retain source and review history, and show the next permitted action clearly. The main actors are Decision officer, Analyst, Domain expert, Authorised decision maker.

5 2 Abstract Use Cases

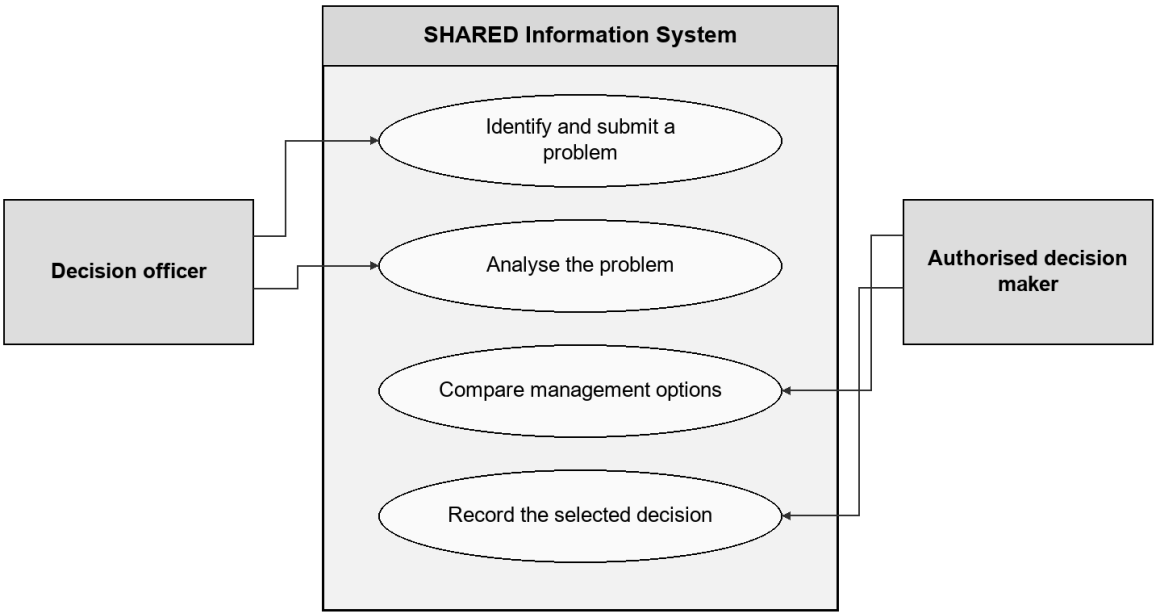


Figure 5 1 Abstract Use Cases

Use case	Main function	Expected result
DM-UC01	Identify and submit a problem	Record the problem, affected places and evidence needed.
DM-UC03	Analyse the problem	Use permitted information and a reviewed calculation or report definition.
DM-UC04	Compare management options	Show benefits, costs, risks, assumptions and missing evidence for each option.
DM-UC07	Record the selected decision	Record the selected option, reason, authority, conditions and follow-up.

5 3 Activity Workflow

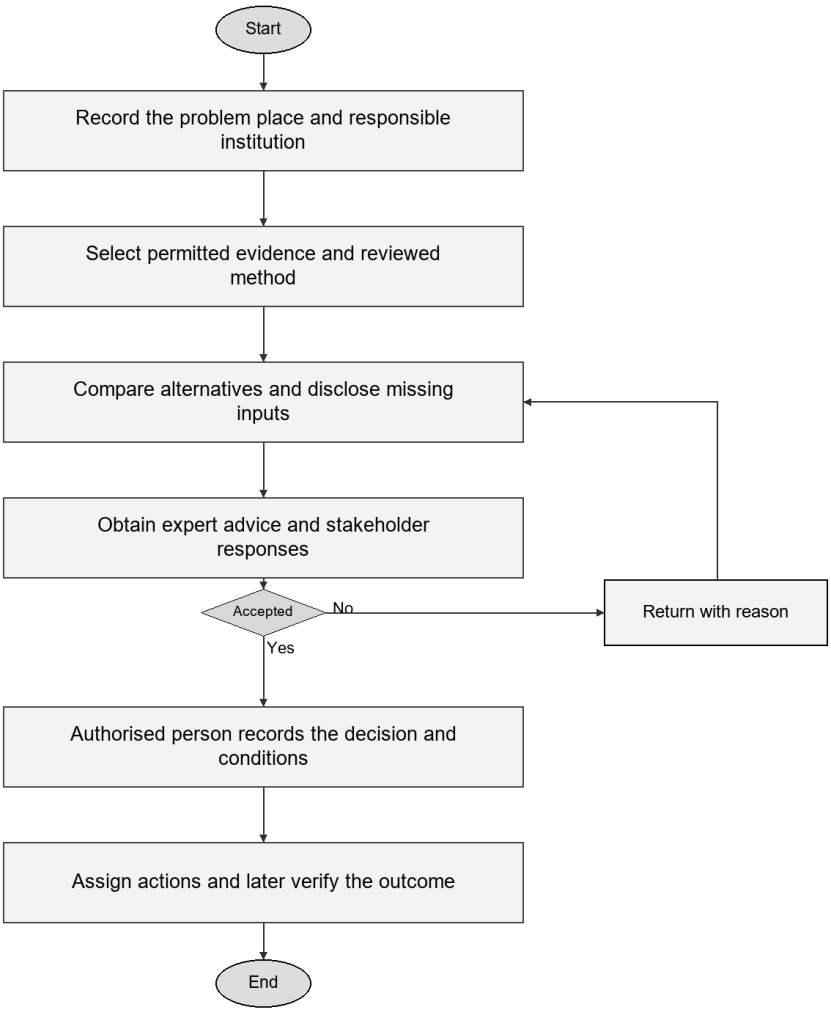


Figure 5 2 Proposed Activity Workflow

Scenario: A proposed reservoir rehabilitation is compared with maintenance and demand-management options. Engineering advice supports the comparison. Funding and institutional approval remain separate recorded decisions.

5 4 Analysis and Statistical Rules

Use the companion Calculations and Decision Rules appendix, Version 1.6, for formulas, inputs, units, sources and limits. Its categories are Government publication, Institution publication, and Validation required. Published methods name the publisher and source section. All approvals remain pending in Institution review.

Check joins before aggregation. An unresolved identity or many-to-many join must not multiply a total. Do not average percentages without the correct weights. A before-and-after difference does not establish causal impact. Survey estimates need their sample frame, sampling design, weights, non-response and uncertainty. Sensitive small groups require the approved suppression rule. Predictive methods need independent validation and documented limits before operational use.

Calculation	Detailed rule in the appendix	What needs agreement
Distinct count	Shared rule Counts and source coverage	Agree the entity, identity key and population.
Weighted average	SURVEY and Shared rule Weighted means and pooled rates	Agree weights, denominators, design and uncertainty.
Yield	YIELD and Shared rule Basic crop yield	Use the matching output and harvested or resource input.
Gross margin	MARGIN	Separate variable cost, fixed cost, profit and cash.
Break even price	Shared rule Break even and margin ratios	State the cost scope and excluded costs.
Plan variance	VARIANCE and Shared rule Percentage variance and target progress	Agree units, period, direction and zero denominator handling.
Target progress	Shared rule Percentage variance and target progress	Distinguish progress from baseline and achievement against target.
Criteria score	Shared rule Reviewed weighted criteria	Approve anchors, weights, exclusions, precision and ties.
Cost effectiveness	Shared rule Cost per additional observed outcome	State the outcome direction and attribution limits.

The design catalogue contains 820 candidate decision examples, 57 calculation families and 139 retained method references. These are design references, not accepted scientific models. The appendix and its controlled registers preserve the detailed logic and source mapping. The coverage workbook shows design coverage. The client selects operational priorities; appointed experts approve selected methods and input definitions through Institution review. Approve the main SRS and appendix as one version.

Read the appendix and its source register at https://sharedproto.wkslabs.com/reviews/dashboard-portfolio-20261027/srs-document/Calculations_and_Rules.html. Its Word and PDF editions and the Decision Register, Method References and Calculation Sources files are controlled parts of this SRS package. A source link alone does not validate a formula; project proposed rules and unconfirmed external methods are labelled separately.

5 5 Functional Requirements

These requirements are proposed Must requirements in delivery package WP3. The client approves the release baseline and any deferral through C01. Optional intelligent processing, device adapters, additional field-access channels and offline operation require explicit scope confirmation. The acceptance checks are required tests, not recorded test results.

FR094 Build reusable report questions

SHARED must allow permitted users to select bounded approved templates, fields, filters and aggregations. Do not accept raw database commands, scripts or arbitrary executable formulas.

Acceptance check: Change supported area, subject, measure and period selections without a crop-specific rule.

FR095 Keep report sources and access rules

SHARED must retain source and version, time, scope and reproducible inputs for queries and executions. Export and later reads must recheck permission.

Acceptance check: A withdrawn source cannot be obtained through an old export link.

FR096 Review how datasets will be combined

SHARED must retain a versioned join plan identifying exact input versions, keys, number of matching records, time alignment, meaning of one output row, missing-row policy, purpose and evidence.

Acceptance check: Block execution of an unapproved or stale plan.

FR097 Show unmatched and invalid inputs

SHARED must preserve unmatched rows and mapping or approval checks when joining datasets. Reject duplicate keys, unsupported joins, changed approval state and work beyond limits.

Acceptance check: A missing match does not become a zero-valued observation.

FR098 Save report definitions and results

SHARED must reuse private versioned report definitions and saved report runs, retaining exact source values, units, filters, review and calculation. Editing or refreshing creates a new version or execution.

Acceptance check: Reopen the original captured numbers after the source changes.

FR099 Use suitable visuals and source maps

SHARED must use suitable comparisons, date series and distributions with units and source coverage.

Acceptance check: A current source map does not rewrite saved report values.

FR100 Export reports with sources and review history

SHARED must retain source and review evidence in supported spreadsheet, CSV, JSON and print outputs. Formal report versions use saved results, list of supporting evidences and reviewed publication.

Acceptance check: A new published report version preserves its predecessor.

FR101 Show what a decision needs

SHARED must show each decision question, exact context, required data, method, authority and outcome-monitoring needs. Missing data, expert decisions and governance approval must have named owners.

Acceptance check: A guidance page does not label a scenario scientifically ready.

FR102 Calculate an approved criteria score

SHARED must use explicit reviewed weights, best/worst anchors, exact source units and required values in the criteria calculation within defined limits. Missing evidence blocks the score; equal scores keep equal rank.

Acceptance check: An omitted criterion cannot silently improve a candidate's score.

FR103 Check differences and thresholds safely

SHARED must check compatible unit, place and period before plan/actual arithmetic and withhold percentage variance when the plan is zero. Numeric rule checks require explicit reviewed thresholds and output meaning.

Acceptance check: A positive variance is not automatically labelled favourable.

FR104 Route a reviewed finding only when configured

SHARED must allow an approved enabled routing policy to create a shared review case with named people, severity and deadline. Case creation and result publication must succeed or fail together.

Acceptance check: A routing failure cannot leave a partly published result.

FR105 Record the human decision

SHARED must retain each case's problem, evidence, assignment, options, consultation, recommendation, authority, rationale, actions, outcome verification and closure or reopening history.

Acceptance check: A recommendation remains distinct from the approved decision.

FR106 Use actual evidence and current guidance

SHARED must use actual permitted records for decision preparation. When considering which option fits the local circumstances, SHARED must reuse current independently reviewed published knowledge and exact case citations.

Acceptance check: An expired or restricted guidance source is no longer offered as current.

FR107 Require independent review and approved methods

SHARED must enforce required independence between decision roles. Generic scoring and policy checks must not claim scientific suitability, legal eligibility, entitlement or payment authority.

Acceptance check: The creator cannot fill every required independent decision role.

5 6 Land Use Change Investigation

Help a land-use planner find important changes inside the project area, assess the evidence and choose the next investigation. The main users are the land-use planner and spatial data custodian. This scenario refines FR026, FR029, FR063, FR099, FR100, FR101, FR156 without adding a separate module or requirement ID.

Analysis area. Use a fixed analysis boundary inside each division. Keep the project portion separate from the full administrative division. The three prototype areas and their shapes are fictional.

Workflow. Select the area, earlier and later observation years and land-use class. Read the annual trends and coverage. Compare net hectares, percentage and average annual change. Inspect the from/to transitions when compatible spatial evidence is available.

Review order. Choose absolute hectares or absolute percentage, and any change, decreases or increases. Show both metrics and the class used for sorting. A zero baseline has no percentage. The selected order explains the list; it is not a material-change threshold or a scientific confidence result.

Inputs and safeguards. Keep source and observation details, fixed area and classification versions, original units, missing values and quality evidence. Reject conflicting source categories. Keep ambiguous mappings unresolved. Class areas plus unclassified area must equal the analysis area. Incomplete endpoints withhold whole-area change and transitions.

Map and data consistency. The example input, annual charts, map images, transition table and decision record use the same versioned dataset. A balanced explicit edit updates the in-page example; no balancing value is invented. Official-source records and file selections remain previews. The prototype saves or uploads no institutional records.

Decision output. Review a division, state the reason, choose a field check, a source-data check or waiting for better evidence, and record the proposed responsible role and follow-up. Incompatible evidence forces a data check. The decision example and exports retain the selected scope, years, figures, source versions and method LAND-CHANGE-1. No assignment is sent by the prototype.

Detailed fields, formulas, sources and the matching fictional example are in section 6 2 of the calculation appendix. Project boundaries, suitable source years, rights, local mapping and quality, decision roles and action thresholds are confirmed through Institution review only.

Scenario	Expected result
LU A1	Native Dense Forest cannot be assigned to Paddy land. Ambiguous classes remain unresolved rather than receiving a false success result.
LU A2	A 20 ha loss from 8000 ha precedes a 10 ha loss from 100 ha when sorting hectares; the order reverses for percentages. No priority policy is silently selected.
LU A3	Loss and gain reproduce the net result. Equal loss and gain can leave zero net change. Transition margins reproduce both dated class totals.
LU A4	An explicit balanced example edit changes the annual chart, map images, transition table and decision record consistently; an unbalanced edit is rejected.
LU A5	Missing or incompatible endpoints withhold change and transitions. No missing result is displayed as zero; the proposed next action becomes a data check.
LU A6	A downloaded decision example contains only its selected division and period, the same figures as the screen, method/source versions, reason, action, proposed role and follow-up state.

5 7 Domain Decision Analysis

Published formula verification. “Verified published formula” means its formula and transcription match the cited recognised publication. “Verified published component” covers only the named part. Source categories, publisher and exact locator remain visible. Local adaptations stay “Validation required”. Confirm local inputs, settings and intended use through Institution review.

The 819 remaining candidate decisions use the same area and period selection, typed source preview, editable sample and proposed follow-up workflow as the completed land-use example. The existing 820 IDs and 41 institution profiles remain. These are decision examples under the existing requirements, not 820 accepted project deliverables.

The rule must match the question. Keep physical and cash balances separate; show the denominator for productivity; compare quality against a matching parameter, unit, use and limit edition; retain unknown cohort follow-up; distinguish point forecasts from probabilities; and keep survey weights and design-based uncertainty explicit. A complete checklist alone cannot grant suitability, safety, permission or eligibility.

Each decision records its required source evidence, field units, observation period, scope, original dataset and revision, boundary and definition versions, method version, result limits and proposed responsible role. Missing evidence stays visible. Incompatible records cannot produce

a decision result. Charts, example edits, review examples and exported decision records use the same versioned evidence.

Published figures are used only with their actual place, period, unit and source locator. Where suitable records have not been obtained, realistic sample records use meaningful place, crop, land-use or service names and remain clearly labelled. DCS district paddy-yield references are separate from illustrative Knuckles records; no district result is represented as a project result.

The existing decision route offers Analysis, Example input and Source input. Source files remain selection previews; no institutional data is uploaded or saved by this component. Exports retain the selected scope and period. A suggested action is not dispatched or treated as an authorized decision.

The calculation appendix describes the shared families and explicit domain variants. Decision_Register.csv and the web decision register give all 820 input and rule bindings. Government and institution publications identify only the stated published components. Confirm local scope, data rights, parameters and responsible roles through Institution review only. The shared-form inventory excludes these decision-analysis previews; their fields are controlled separately in the decision register.

Check	Expected behavior
Domain meaning	Correct physical, money, count, area, time and probability units; no generic score substitutes for domain evidence.
Data integrity	Missing versus zero, valid dates, matching versions, distinct eligible counts and balance/component closure are checked.
Consistent output	The same sample edit changes its chart, review figure and selected exported result; source previews remain separate.
External decisions	No scientific, legal or institutional approval is inferred; retain existing pending review decisions.

6 Project Implementation and Monitoring

The project functions connect plans, activities, assigned work, evidence and results. The monitoring functions distinguish expected targets, reported progress and verified outcomes. The same project identity is reused across domains and places.

6 1 Objectives and Actors

The main objectives are to complete the use cases below, retain source and review history, and show the next permitted action clearly. The main actors are PMU officer, Implementing partner, Monitoring specialist, Independent reviewer.

6 2 Abstract Use Cases

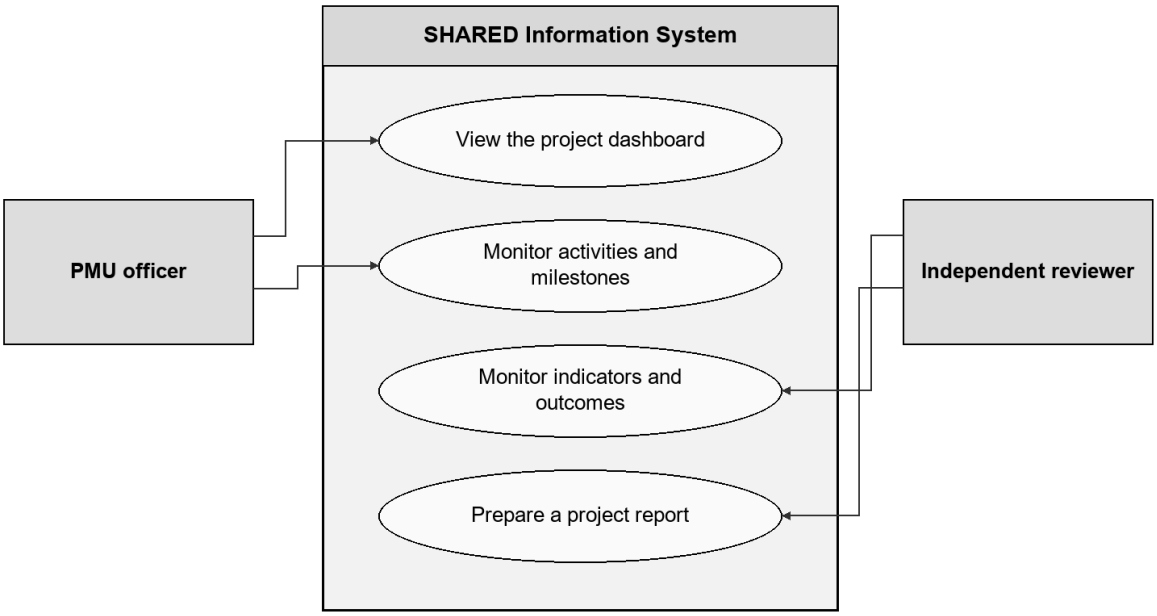


Figure 6 1 Abstract Use Cases

Use case	Main function	Expected result
PM-UC01	View the project dashboard	View planned and verified progress with missing information identified.
PM-UC03	Monitor activities and milestones	Track recurring work, dependencies, due items and corrective actions.
PM-UC04	Monitor indicators and outcomes	Compare accepted actual values with the approved baseline and target.
PM-UC10	Prepare a project report	Save the exact reporting period, source versions and reviewed results.

6 3 Activity Workflow

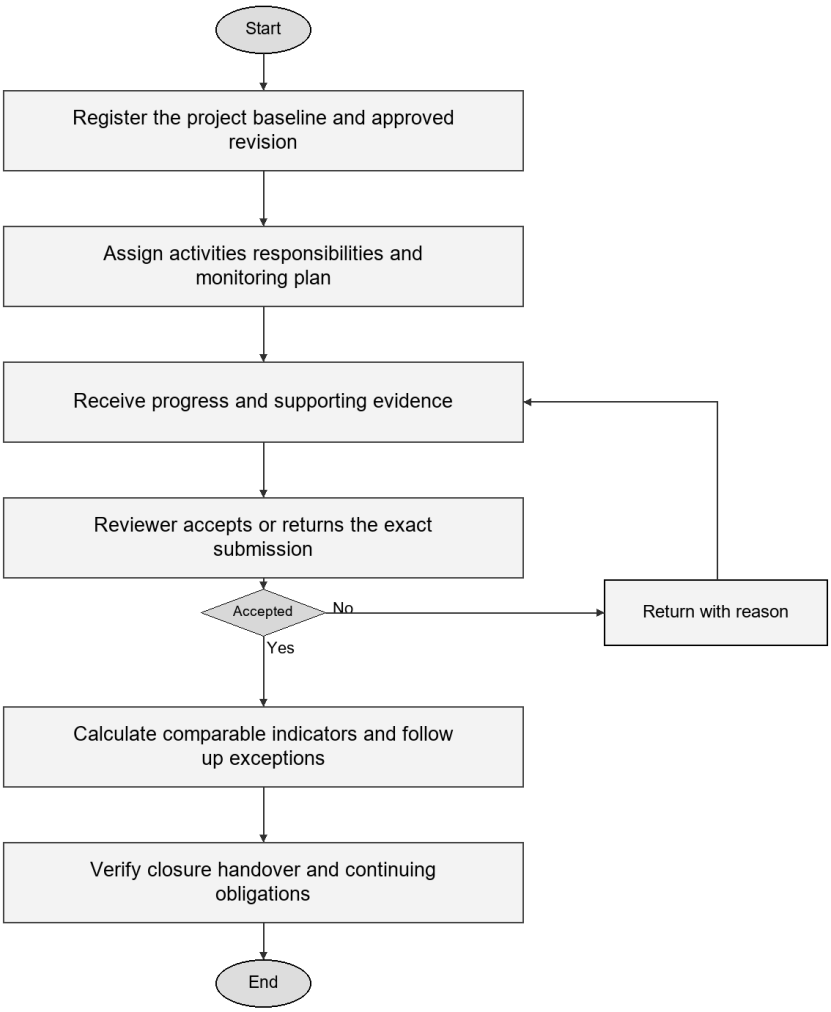


Figure 6 2 Proposed Activity Workflow

Scenario: An implementing partner reports a completed restoration activity. The reviewer checks its evidence. The planted area, surviving trees and later livelihood outcome remain different measures.

6 4 Monitoring Rules

Use impact, outcome, output and activity indicators at their stated level. Each indicator needs an owner, definition, unit, numerator and denominator where relevant, baseline state, dated target, frequency, disaggregation, source and means of verification. Unknown and descriptive baselines are allowed when the indicator contract permits them. Targets never become actual observations.

Record implementation, verification and outcome separately. Completion requires the specified evidence and independent review. Recurring obligations are generated once. Asset condition, maintenance, handover and receiving-institution acceptance link to the same project and asset identities. C12 resolves the boundary with other project-management tools.

6 5 Functional Requirements

These requirements are proposed Must requirements in delivery package WP4. The client approves the release baseline and any deferral through C01. Optional intelligent processing, device adapters, additional field-access channels and offline operation require explicit scope confirmation. The acceptance checks are required tests, not recorded test results.

FR108 Register the programme or project

SHARED must keep project type, funder, lead, partners, objectives, dates, lifecycle state and reporting obligations within permitted scope.

Acceptance check: Reject an invalid or cross-scope project change.

FR109 Connect domains and areas once

SHARED must link one project to several domains and places through explicit applicability relationships tied to that project revision.

Acceptance check: Do not duplicate the project for each GN or department.

FR110 Organize implementation

SHARED must maintain components, activities, interventions, sites, responsible organizations, schedules and implementation state.

Acceptance check: A stale edit cannot overwrite newer activity details.

FR111 Link project evidence

SHARED must preserve source and access rules when linking projects or interventions to documents, datasets, indicators, layers, submissions and evidence.

Acceptance check: A project link cannot release a private source.

FR112 Onboard ongoing and completed projects

SHARED must retain a reviewed source baseline, original project identifier, baseline date and known quality findings when onboarding an ongoing or completed project. The import must preserve known history without inventing milestones.

Acceptance check: Do not invent historic completion milestones.

FR113 Keep versions of major project changes

SHARED must create linked revisions for material changes to active projects instead of overwriting approved project or domain profiles.

Acceptance check: Reopen the earlier approved revision unchanged.

FR114 Follow the project from setup to closure

SHARED must use one persisted plan from intake and configuration through review, activation, execution, monitoring, decision, reporting, closure and archive.

Acceptance check: Show the next allowed action and earlier completion evidence.

FR115 Record each project step and its owner

SHARED must distinguish setting up a new project from importing an ongoing or completed project. Each applicable step must keep status, owner, due date, dependencies, validation and completion evidence.

Acceptance check: Unmet dependencies block an invalid activation.

FR116 Keep task submissions and review records linked

SHARED must keep obligation definition, occurrence, fixed submitted version, schema section, artifact and review decision separately linked.

Acceptance check: Correcting a submission does not replace its earlier version.

FR117 Generate scheduled tasks once

SHARED must support one-time and recurring obligations. Generate occurrences repeatably and derive overdue from the actual due date and state.

Acceptance check: Repeating schedule generation does not create duplicate work.

FR118 Record who must deliver each item

SHARED must record each assignment's responsible organization, group or person, component, domain, geography, dates, dependencies, acceptance criteria, authority and evidence needs.

Acceptance check: Reject an assignee or place outside the permitted project scope.

FR119 Return and correct with a reason

SHARED must validate against the original form version. Retain review findings, return reasons, corrected versions and resubmission. Blocking findings must prevent acceptance.

Acceptance check: Retrying review does not change a previous deterministic validation outcome.

FR120 Show only permitted assigned work

SHARED must prevent My work and review queues from disclosing differently scoped work through lists, counts, maps, files or exports.

Acceptance check: Another department cannot infer the private survey queue.

FR121 Keep required review independent

SHARED must use configured reviewer assignments and retained decisions. Protect high-impact publication, role, geography, taxonomy and import changes with independent approval.

Acceptance check: The same creator cannot satisfy a protected maker-checker decision.

FR122 Connect protected feedback to action

SHARED must link an exact permitted feedback submission to the shared decision case with compatible revision, domain and place. Keep original content, review and later response evidence.

Acceptance check: A feedback link does not copy private content into another audience.

FR123 Approve the monitoring plan

SHARED must retain reviewed indicators, baseline, target, period, place, responsibility, sources, calculation, quality and approval for each active project-domain monitoring context.

Acceptance check: An unapproved plan cannot produce an accepted operational result.

FR124 Allow honest baseline and target states

SHARED must support unknown or descriptive baselines where permitted, dated targets, denominators, assumptions and verification needs. Keep targets separate from observed results.

Acceptance check: An unknown baseline does not become zero automatically.

FR125 Execute a repeatable reviewed method

SHARED must generate monitoring results only through approved versioned calculations. Keep exact input and output history, steps, units, parameters, review and execution evidence.

Acceptance check: Later source changes do not rewrite a published calculation.

FR126 Reconcile closure across the project

SHARED must reconcile delivery, monitoring, decisions, data, access, knowledge, handover, retention and post-project obligations during required closure.

Acceptance check: Outstanding required actions remain visible before closure.

FR127 Verify or waive each closure check properly

SHARED must record each closure check's owner, deadline, evidence and independent verification or permitted reasoned waiver. Retain unchangeable status history.

Acceptance check: Reject a stale, unauthorized or self-verified closure transition.

FR128 Allow closure only after required checks

SHARED must enforce the approved closure plan and frozen list of required closure checks before a project becomes Closed or Archived. This gate applies through every supported service operation.

Acceptance check: A direct lifecycle request cannot bypass the closure gate.

FR090 Reuse asset and connection records

SHARED must extend shared structure or intervention records with asset profiles. Keep condition, capacity, custody and directed source-reported connections with evidence.

Acceptance check: A drawn water connection is not treated as verified hydrology.

FR091 Retain handover and maintenance evidence

SHARED must link asset handover and maintenance responsibilities to the required receiving-institution evidence and shared closure process.

Acceptance check: A draft handover cannot complete an accepted closure check.

7 Community Participation and Knowledge Services

Farmers, community groups and other beneficiaries need simple access to relevant information and a clear way to ask questions or provide feedback. Personal participation records and sensitive concerns require more protection than published guidance.

7 1 Objectives and Actors

The main objectives are to complete the use cases below, retain source and review history, and show the next permitted action clearly. The main actors are Farmer or community member, Field facilitator, Knowledge editor, Receiving institution.

7 2 Abstract Use Cases

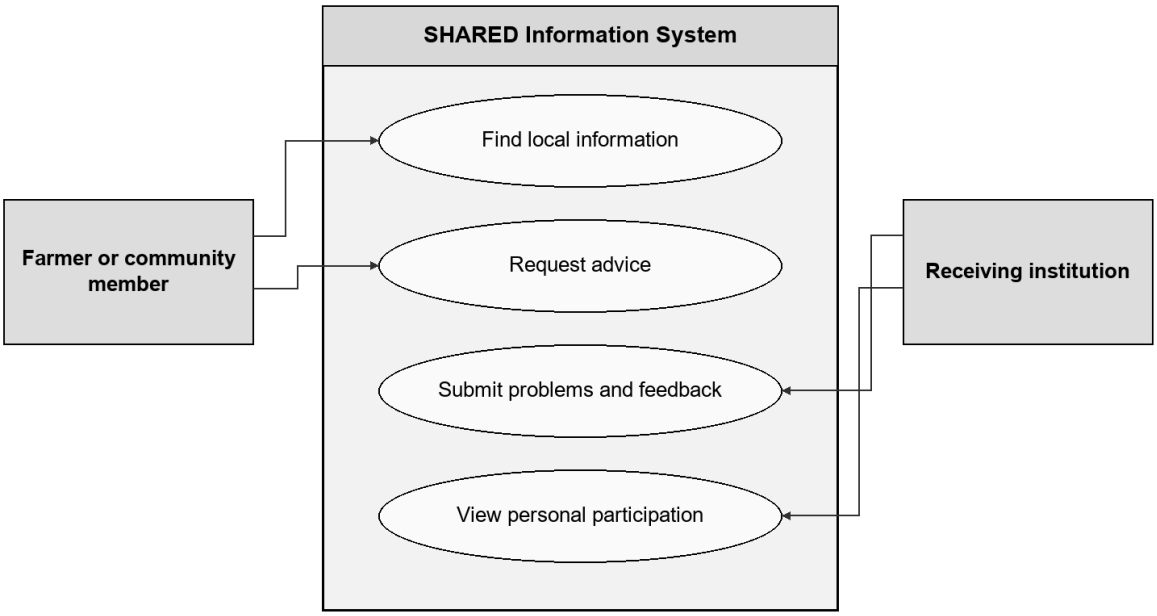


Figure 7 1 Abstract Use Cases

Use case	Main function	Expected result
BF-UC01	Find local information	Find released guidance, project activities and opportunities for a chosen area.
BF-UC05	Request advice	Record a question and route it to the responsible institution.
BF-UC06	Submit problems and feedback	Keep the concern, response and follow-up within the permitted audience.
BF-UC10	View personal participation	Allow a verified participant to view only the history they may access.

7 3 Activity Workflow

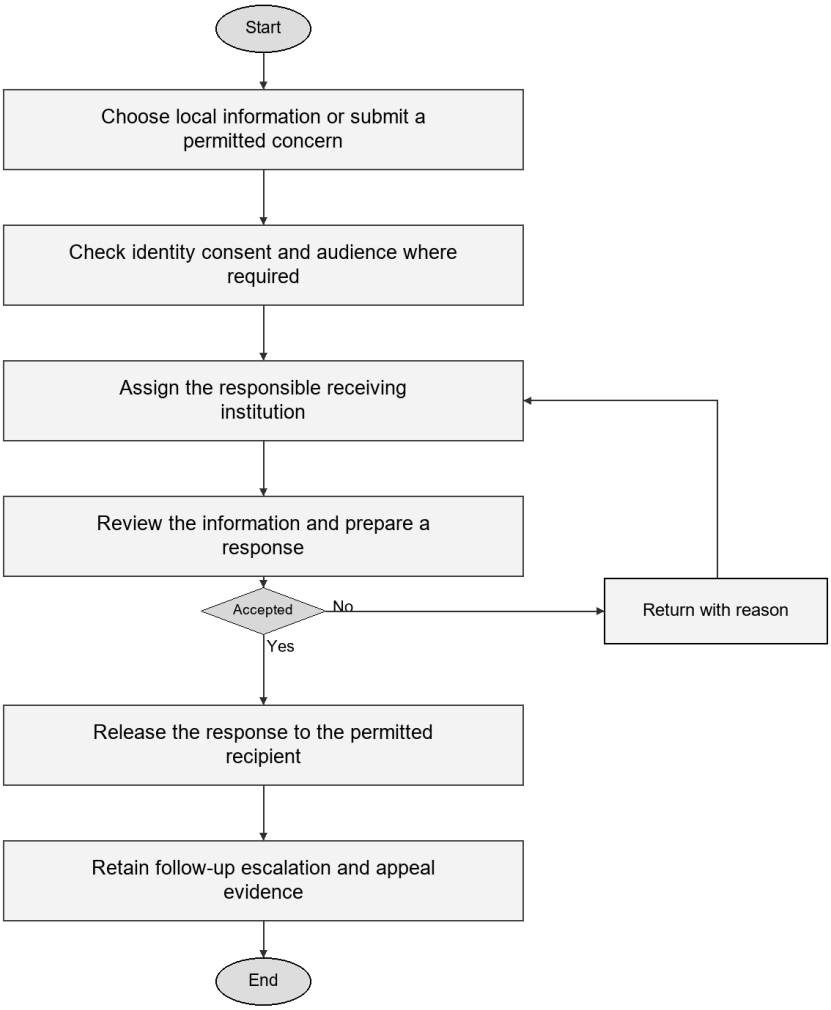


Figure 7 2 Proposed Activity Workflow

Scenario: A farmer asks about a reported irrigation problem. The field facilitator records the concern once. A public update contains only approved information and does not expose the farmer or a private complaint.

7 4 Participation and Knowledge Rules

Register the same person once and retain programme-specific support episodes. Household size, account count, attendance and distinct beneficiaries are different measures. Access to a person record does not automatically permit access to every support or feedback record. Programme training attendance is an ordinary activity record. Use the approved task-specific forms.

Published advice needs an accountable author, sources, intended audience, language, review state and replacement policy. Public or anonymous grievance intake needs C09 before activation.

Keep the original concern, response, escalation and independent appeal protected. A public page displays only approved non-sensitive information.

7 5 Functional Requirements

These requirements are proposed Must requirements in delivery package WP4. The client approves the release baseline and any deferral through C01. Optional intelligent processing, device adapters, additional field-access channels and offline operation require explicit scope confirmation. The acceptance checks are required tests, not recorded test results.

FR086 Reuse participant identities

SHARED must extend shared identities with programme participant profiles and retain their owner, domain, geography, source and origin. Keep shared departmental accounts separate from individual beneficiaries.

Acceptance check: Find the same participant's earlier support without another identity.

FR087 Record support and training history

SHARED must retain support episodes with their programme, provider, type, source-reported status and known amounts, currency, quantities and dates. Prior-assistance checks must respect lawful access.

Acceptance check: Unknown assistance dates remain unknown.

FR088 Connect products producers and buyers

SHARED must reuse shared product, production, producer and named buyer-demand records, retaining their source, units, period and place.

Acceptance check: Show a recorded relationship without predicting a sale.

FR089 Keep livelihood outcomes separate

SHARED must record the definition, period, evidence and denominator for each employment, income, training, women/youth participation or other outcome. A population count is not programme participation.

Acceptance check: A training target is not reported as completed attendance.

FR129 Catalogue documents and media

SHARED must keep evidence descriptive information, checksum, classification, version and review/publication state with controlled project, domain and location links.

Acceptance check: One image can be referenced without duplicating its original.

FR130 Protect originals and derived files

SHARED must store originals that cannot be changed and controlled previews outside public web folders. Replacement must create a new version.

Acceptance check: An old original remains traceable after replacement.

FR131 Scan and authorize file use

SHARED must enforce size, type, signature, renamed storage, quarantine and genuine malware checks before publication. Reauthorize preview, download and export; expire temporary links where relevant.

Acceptance check: A failed scan or expired link cannot expose the original.

FR132 Review knowledge publication

SHARED must enforce knowledge authoring, independent review, publication, replacement by a newer version, retention and archive stages. Keep earlier versions unchanged.

Acceptance check: An unpublished draft is not publicly searchable.

FR133 Retain eligible citations

SHARED must link knowledge to permitted projects, areas, sources, evidence, results, decisions and deliverables. Recheck restricted or withdrawn citations without leaking descriptive information.

Acceptance check: An ineligible required source removes the public item from current view.

FR134 Offer a simple beneficiary view

SHARED must let public readers find eligible local information, options, opportunities and project activities without an account. Signed-in readers must retain an uncomplicated public view.

Acceptance check: A public reader cannot see internal participant or case histories.

FR135 Keep anonymous intake closed until approved

SHARED must keep protected feedback separate from public grievances. Public activation needs a recorded policy covering receiver, deadlines, independent appeal, privacy, safeguarding and abuse controls.

Acceptance check: Without approved policy, anonymous complaint intake stays closed.

8 Value Chains Markets and Ecosystem Services

These functions help stakeholders understand production, demand, costs and ecosystem-service arrangements. The system records evidence and supports appraisal. The responsible institution must approve scheme rules, financial authority and any commitment.

8 1 Objectives and Actors

The main objectives are to complete the use cases below, retain source and review history, and show the next permitted action clearly. The main actors are Producer or enterprise, Market information provider, PES scheme coordinator, Appointed verifier.

8 2 Abstract Use Cases

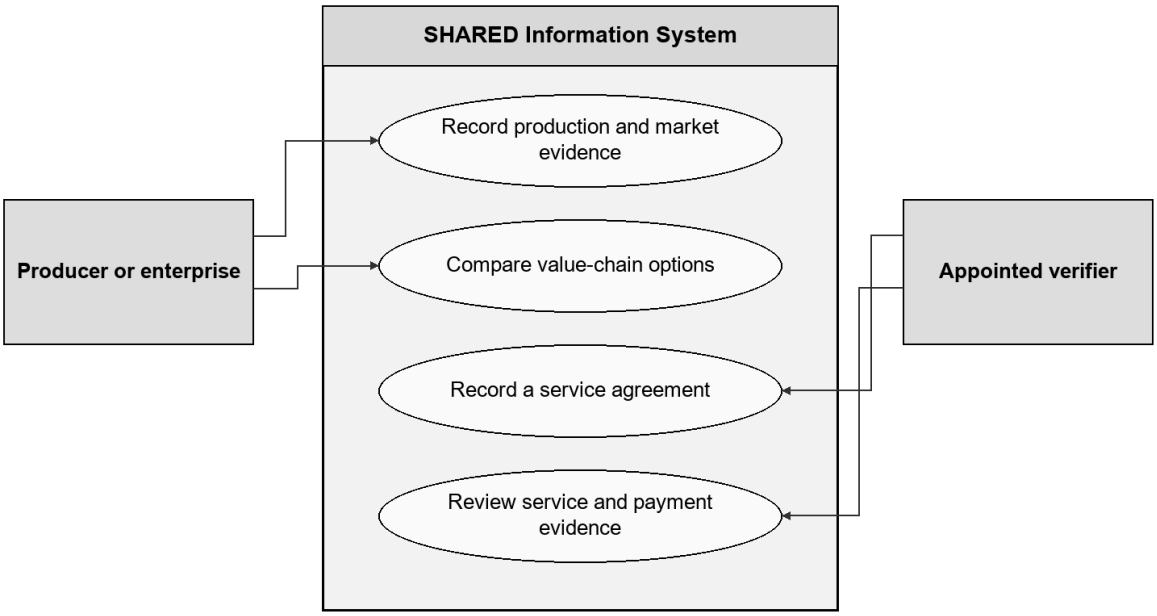


Figure 8 1 Abstract Use Cases

Use case	Main function	Expected result
VC-UC01	Record production and market evidence	Record the product, grade, quantity, unit, market, currency and period.
VC-UC02	Compare value-chain options	Compare compatible production, demand and costs with their assumptions.
ES-UC01	Record a service agreement	Link the scheme, parties, service area, conditions and verification method.
ES-UC02	Review service and payment evidence	Keep agreement, verification, funding and reported payment states separate.

8 3 Activity Workflow

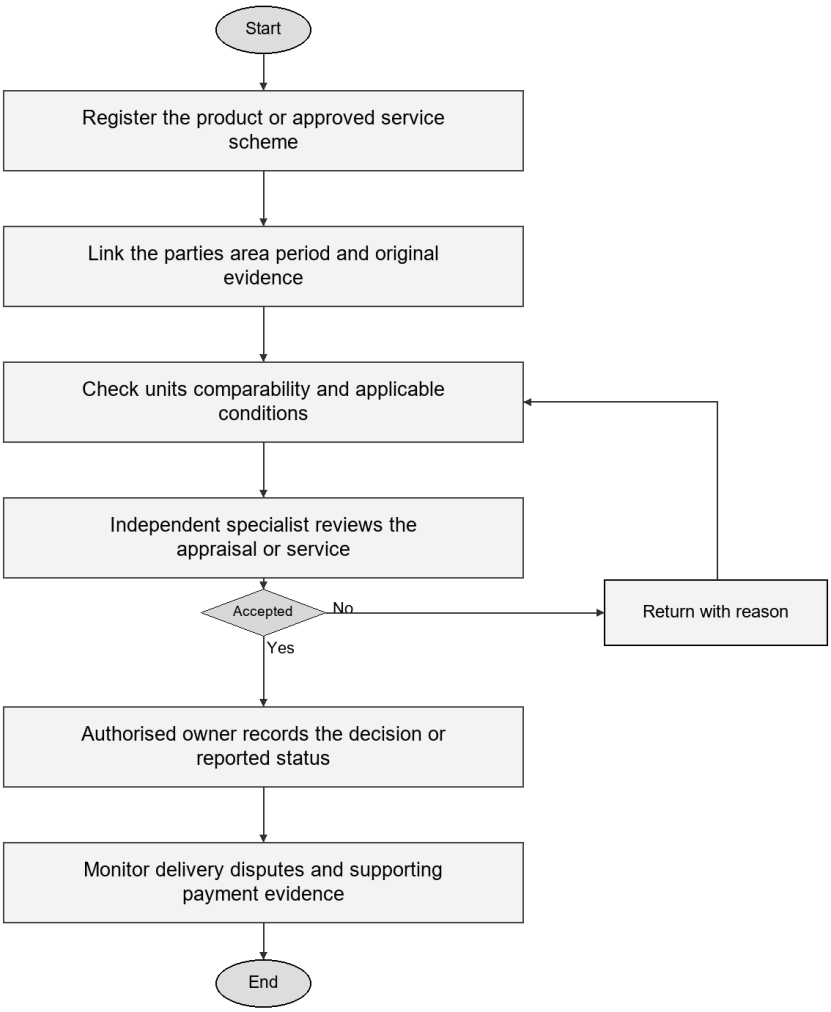


Figure 8 2 Proposed Activity Workflow

Scenario: A farmer group proposes riverbank protection under a PES scheme. The agreement defines the service and verification conditions. A verified service record and a source-reported payment record remain separate. Saving either record does not transfer money.

8 4 Domain Rules

Market comparisons must match product and grade, market or channel, quantity unit, currency and period. Keep historic, quoted, realised and forecast prices distinct. A recorded buyer demand does not prove a purchase commitment. Currency conversion needs an accepted rate source and applicable period. Revenue, gross margin, net profit and cash received have different meanings.

For sustainable land management, record the local context, constraints, proposed options, selected treatment, trial or implementation evidence and repeated monitoring. Soil and land-health datasets require the applicable site or plot reference, sampling method, depth where relevant, laboratory or field method, unit, observation period and quality state. The responsible expert approves these dataset fields and methods; ordinary forms stay focused on their business task.

A PES scheme needs the environmental service, baseline, additionality, eligible parties and rights, service area and period, conditions, safeguards, verification method, funding, rates and dispute process. The scheme owner names proposer, coordinator, service provider, beneficiary or buyer, verifier, approver and financial recorder roles as applicable. No generic score grants entitlement. The baseline records source-reported payment evidence; bank payment execution requires a separately approved scope change.

8 5 Functional Requirements

These requirements are proposed Must requirements in delivery package WP3. The client approves the release baseline and any deferral through C01. Optional intelligent processing, device adapters, additional field-access channels and offline operation require explicit scope confirmation. The acceptance checks are required tests, not recorded test results.

FR082 Keep harvest and sale evidence

SHARED must retain product, quantity, unit, dates, currency, source and scope for harvest batches, buyers, sales and recorded sale-payment evidence. Recording evidence is not executing a payment.

Acceptance check: A source-reported sale can be traced to its original evidence.

FR083 Keep origin and currency explicit

SHARED must retain a source-supported origin assertion for the particular record and expire the assertion when the supporting facts change. Complete unknown currency through authorized evidence without changing amounts or an established currency silently.

Acceptance check: Confirming a person does not confirm every later transaction.

FR084 Compare only compatible market evidence

SHARED must retain exact product, unit, origin, periods, row versions and comparison time when comparing production and demand. Different periods must not produce a misleading quantity difference.

Acceptance check: Different-period demand stays separate from current production.

FR085 Use accepted seasonal arithmetic

SHARED must use reviewed formula versions and exact compatible inputs for seasonal production, cost, revenue, margin and break-even outputs. Unknown costs, yield assumptions, currencies and season definitions must block the affected result or appear as explicitly incomplete.

Acceptance check: A missing production cost makes the margin incomplete; it does not become zero cost.

FR092 Keep PES frameworks controlled

SHARED must retain the owner and authority of PES schemes, agreements, service verification and source-reported payment-stage evidence. Missing rates, eligibility, appeals or legal approval must not be invented.

Acceptance check: No relationship creates an automatic PES entitlement or bank payment.

FR093 Trace programme connections

SHARED must connect permitted support, product, asset, market, outcome and evidence records in analysis while preserving source versions and original scope.

Acceptance check: Trace a claimed outcome to its project and dated evidence.

8 6 Payments for Ecosystem Services

Payments for ecosystem services (PES) are agreed payments for work or results that protect an ecosystem. Providers do the work, a payer funds the agreement, an intermediary manages records and an independent checker assesses the agreed conditions. These are proposed roles, not appointed institutions.

The PES workflow is: agree the work and payment conditions; record and check the work; calculate a payment proposal; then record separate authorisation and payment evidence. Keep the agreement version, provider, payer, area, year, checking protocol, rights, rate, cap, funding and payment references together. This refines FR092 and FR093.

Fictional annual example: 24 ha are agreed, 22 ha are checked, 20 ha meet the conditions, 2 ha need correction and 2 ha still need a visit. At LKR 12,500 per accepted hectare per year, the proposal is LKR 250,000 under a LKR 300,000 annual cap. Funding evidence is missing; no amount is ready for authorisation. Authorised and paid amounts are both zero.

PES decision views use plain questions, area and year filters, editable examples and the required source fields. Keep hectares separate from rupees. Checked hectares do not establish cleaner water or an additional environmental benefit. Compare matching environmental observations and investigate other causes. Appendix section 6 4 explains the examples and sources; scheme rules and local use are handled in Institution review.

9 Responsive and External Interfaces

The responsive core interface and any separately approved field-access channel follow the same data definitions, permissions and review rules. Offline operation and additional channels remain proposed options under C01, C06 and C07. Connections to other institutions use approved contracts. An unavailable source remains visible without creating a reading or a successful exchange.

9 1 Objectives and Actors

The main objectives are to complete the use cases below, retain source and review history, and show the next permitted action clearly. The main actors are Web user, Field officer, External source system, Integration operator.

9 2 Abstract Use Cases

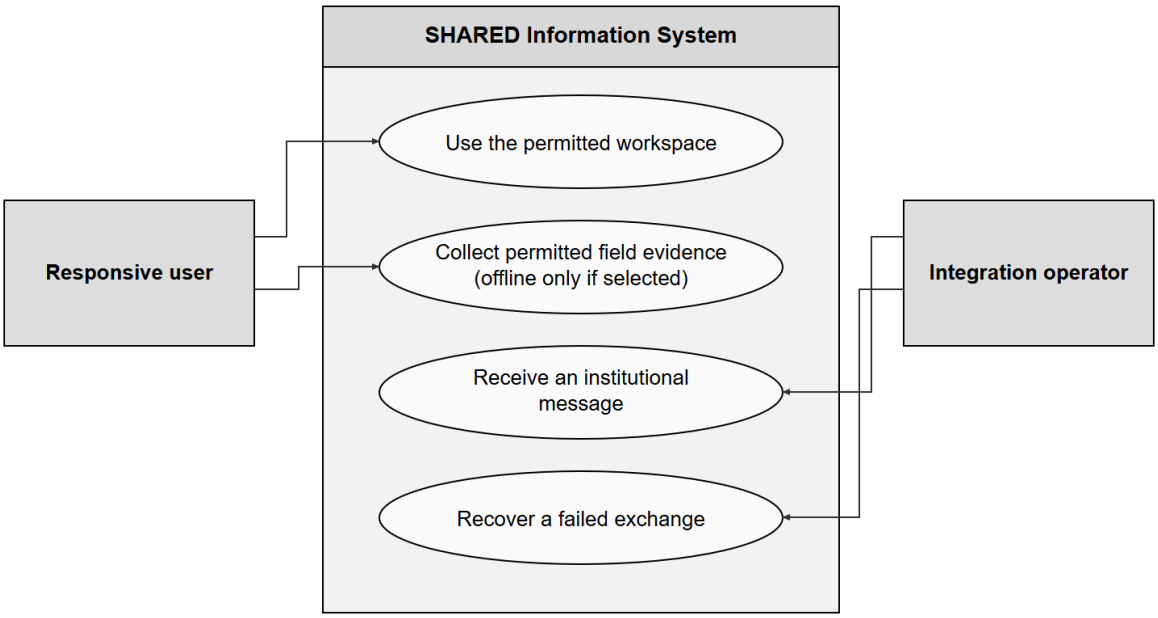


Figure 9 1 Abstract Use Cases

Use case	Main function	Expected result
IF-UC01	Use the permitted workspace	Open assigned functions through the shared API and approved reference data.
IF-UC02	Collect permitted field evidence	Use the responsive core journey. If offline operation is selected, protect authorised drafts and show their sending, rejection and conflict states.

Use case	Main function	Expected result
IF-UC03	Receive an institutional message	Check source identity, mapping version and every row outcome.
IF-UC04	Recover a failed exchange	Retry safely or resolve a conflict without a duplicate committed result.

9 3 Activity Workflow

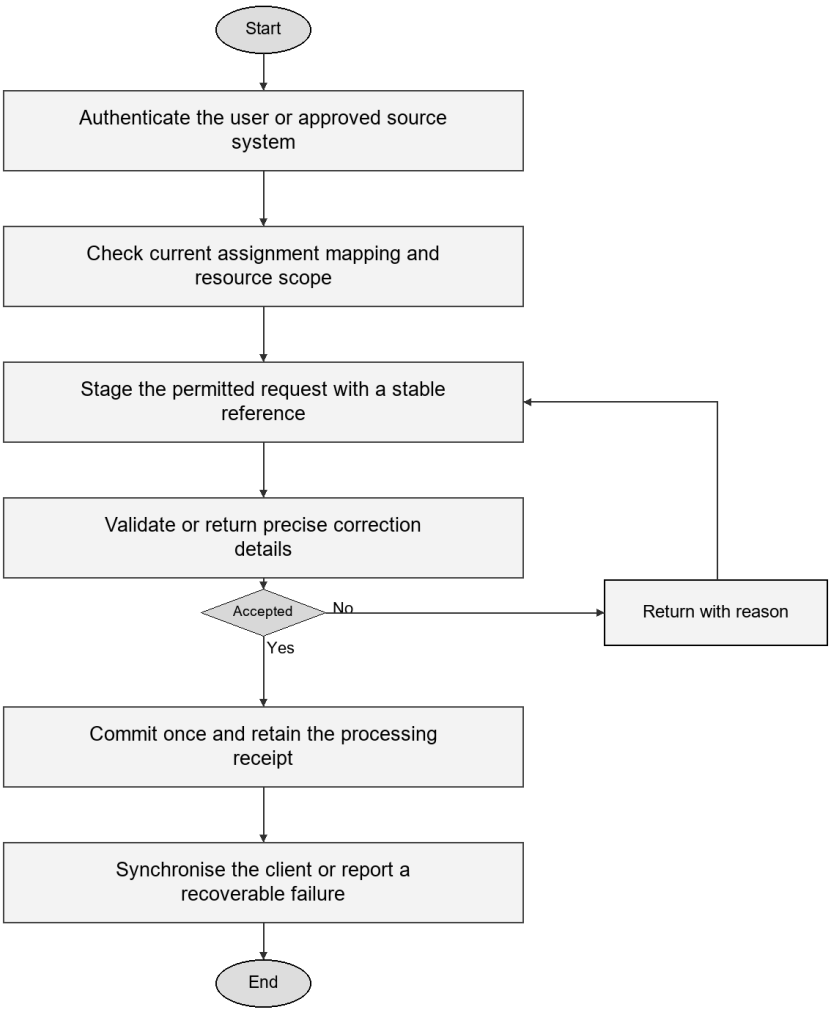


Figure 9 2 Proposed Activity Workflow

Scenario: A field officer submits a permitted observation through the responsive journey. If the client selects offline operation, the officer may keep a protected draft while disconnected. After reconnection, shared services check current access and exact record versions; a conflict requires resolution instead of overwriting an accepted record.

9 4 Interface Contracts

Interface group	Required contract
Identity and assignments	Account state, current scopes, session expiry and revocation. Client-supplied actor IDs never establish permission.
Catalogue and source versions	Typed metadata, schema, rights and permitted distributions. Search and detail obey the same resource checks.
Submissions and reviews	Original reference, mapping version, exact included rows, expected version, decision and reason. Approval cannot survive a protected content change.
Geographic services	Approved spatial layer contracts, coordinate systems, bounded extents, paging, legends and permitted feature details.
Results and decisions	Method version, input references, parameters, frozen result, limitations, consultation and institutional decision records.
Institutional and device feeds	Approved machine identity, event key, observed and received times, calibration where relevant, correction semantics and explicit row outcomes.
Documents and exports	Authorised preview, download and export, classification, safe file handling and permission checks at delivery time.
Background work	Accepted job reference, durable status, bounded retries, cancellation rules and stable receipt after worker or network failure.

The development company must supply exact request and response schemas in an agreed OpenAPI version before coding each interface. Include resource identifiers, field types, required and optional values, units, validation, paging, permission requirements, expected-version checks, safe retry keys, error codes and representative success and failure examples. Errors must distinguish invalid input, denied scope, conflict, unavailable dependency and a valid empty result.

Source protocols may include approved HTTPS JSON APIs, structured files, WMS for image display and WFS or OGC API Features for permitted vector exchange. Declare supported formats and operations for each provider. Do not imply that a map image supplies analytical source cells. Source credentials remain on the protected server side. External URLs must be allowlisted and requests bounded against malicious destinations and redirects.

Responsive, low-bandwidth access is the required core. If an additional field-access channel or offline capability is selected under C01, C06 and C07, download only permitted assignments and minimum necessary reference data. Protect local drafts, evidence and access material under approved encryption, retention and privacy rules. Recheck access on synchronisation and show expiry, revocation, conflict and lost-reply states. Device and measurement conditions also require C08. A browser role preview is not operational authentication.

9 5 Functional Requirements

These requirements are proposed Must requirements in delivery package WP4. The client approves the release baseline and any deferral through C01. Optional intelligent processing, device adapters, additional field-access channels and offline operation require explicit scope confirmation. The acceptance checks are required tests, not recorded test results.

FR136 Use the API for all web actions

SHARED must provide a web application that uses the published service contracts, secure server-side sessions, anti-forgery protection and secure cookies. It must never access database tables directly.

Acceptance check: A forged form request fails without changing a record.

FR137 Keep workflows simple and accessible

SHARED must use guided steps, searchable choices, progressive details and clear loading, empty, error and denied states. Validate responsive, keyboard and accessibility behaviour on the agreed matrix.

Acceptance check: Correct a form error without losing valid entered values.

FR138 Use approved choices and language resources

SHARED must obtain approved choices from authorised API reference data. It must support English, Sinhala and Tamil resources for the agreed delivery scope. Client-appointed reviewers must accept terminology and translations before release.

Acceptance check: Unreviewed translation is not presented as accepted institutional wording.

FR139 Protect sign in across approved access channels

SHARED must use environment-safe configuration and the same authenticated service interfaces across approved access channels. Each channel must protect credentials and session material using approved secure facilities and enforce rotation, revocation, expiry and logout. An additional field-access channel is a proposed option under C01, C06 and C07, not an accepted first-release commitment.

Acceptance check: A revoked session cannot continue an authenticated action through any approved access channel.

FR140 Capture permitted field evidence

Through the responsive core interface, SHARED must allow permitted users to browse assigned projects, domains, places and maps and capture authorised location, source, accuracy, observation time and evidence. An additional field-access channel or local draft-storage capability is conditional on C01, C06 and C07. When local drafts are permitted, protect them under the approved encryption, retention and privacy rules.

Acceptance check: An unauthorised user cannot capture or export a restricted location through the selected field journey.

FR141 Control optional offline submission

If offline operation is selected under C01, C06 and C07, SHARED must protect downloaded authorised assignments, local drafts and evidence under the agreed retention and privacy rules. Show pending, sending, received, rejected and conflict states. Synchronise through the common authenticated service interfaces using stable retry identifiers. Offline operation remains a proposed option until the client accepts its scope.

Acceptance check: When offline operation is selected, network loss, restart and retry do not create duplicate submissions; a rejected or unreviewed submission does not become published.

FR142 Explain the architecture through real workflows

SHARED must retain a clear system explanation and role-based user guidance linked to the relevant permitted workflow. The prototype presentation and diagrams support this explanation. A demonstration link does not grant access or establish operational acceptance.

Acceptance check: A presentation example does not become a completed programme transaction.

FR143 Expose controlled API contracts

SHARED must use versioned API routes and explicit request/response contracts with an accurate API description. Reject unsupported request properties.

Acceptance check: A client cannot submit arbitrary database fields.

FR144 Bound work and return safe errors

SHARED must return consistent safe errors without internal database commands, stack traces or secrets. Lists must use deterministic paging, limits, cancellation and timeouts.

Acceptance check: A timeout is not returned as a successful empty report.

FR145 Prevent duplicate requests and conflicting edits

Use request references, expected-version checks and stable retry identifiers. Limit retries so repeated failures do not overload the service. Health checks must use approved service operations.

Acceptance check: A stale edit cannot overwrite a newer correction.

FR146 Protect transport and endpoints

SHARED must use HTTPS, secure headers, approved origins, rate limits, input checks and endpoint plus permission checks for the requested record.

Acceptance check: An unapproved browser origin cannot bypass protected access.

FR155 Separate interface and hosting responsibilities

SHARED must keep user-interface responsibilities separate from authenticated application services, shared business rules and controlled data access. Clients must not access data-store tables directly. Protect configuration, files and process permissions. A separate deployment or hosting topology is a

proposed option under C07; select it only after reviewing isolation, operations, recovery, cost and portability.

Acceptance check: A user-interface request cannot bypass the shared permission and controlled data-access boundary. The selected hosting option has an explicit C07 decision and corresponding isolation tests.

10 Architecture Database and Data Governance

10 1 Logical Architecture

Use an API-first modular application as the proposed starting architecture, with shared business rules and one coherent service boundary. Keep domain rules independent of user interfaces, storage products and external providers. Separate interface responsibilities, authenticated application services, module rules, controlled persistence, protected document/object storage and background integration logically. Separate deployment units are optional and require a documented C07 isolation, operating, recovery, cost and portability decision.

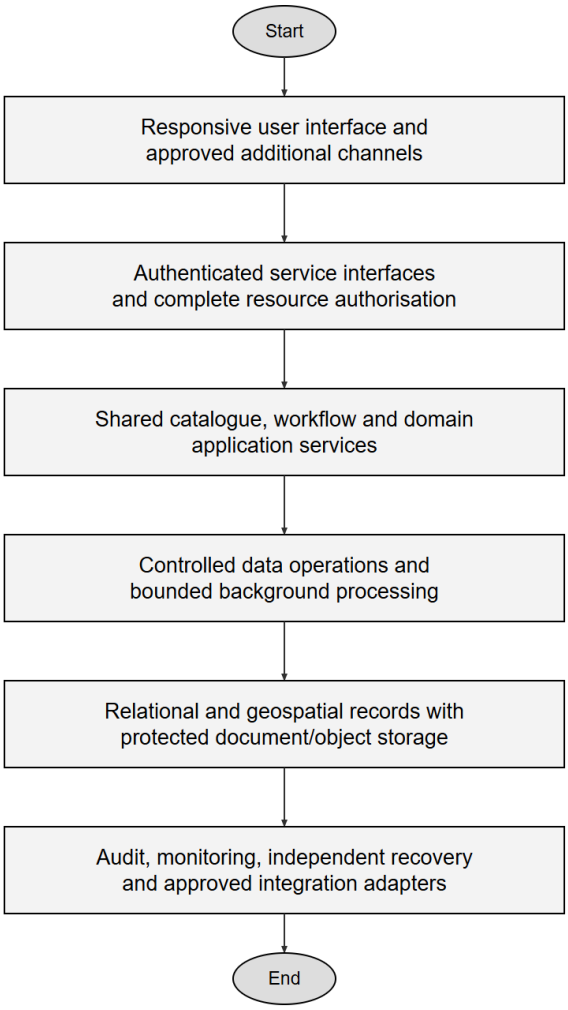


Figure 10 1 Logical Service and Data Flow

10 2 Logical Data Model

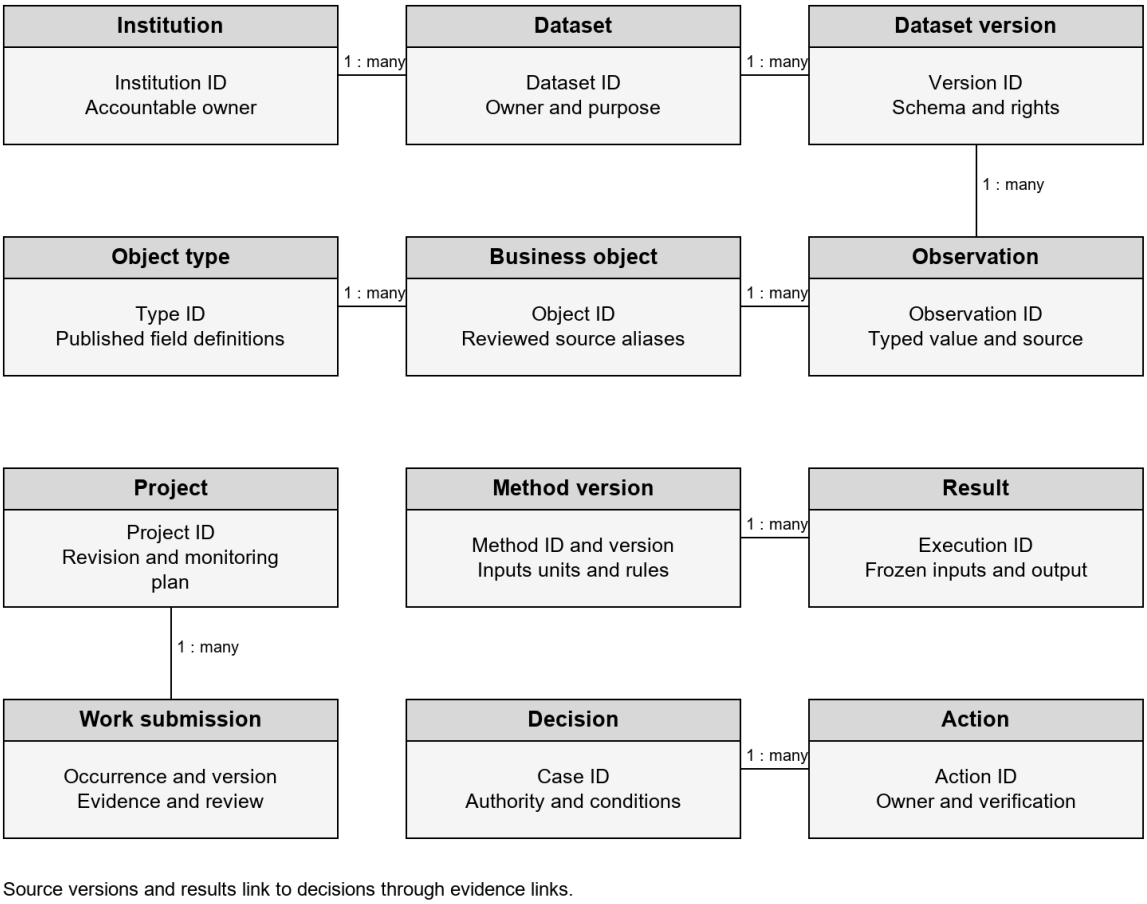


Figure 10 2 Main Record Relationships

Each box represents a record type. One to many means one record can relate to several records of the next type. An observation may describe a declared subject without a business-object link. The diagram shows principal links; the dictionary below includes additional records and version constraints. Source versions, observations and results link to decisions through controlled evidence relationships.

Record group	Minimum content and relationships
Organisation and person	Stable identity, name, type, active state and permitted contact details. Membership links people to organisations. Accounts remain separate.
Account and assignment	Account state, framework identity reference, role, complete permitted scope, effective period and revocable session. Never store plain passwords.
Domain subject and attribute	Owner, parent, meaning, version, type, unit, vocabulary, validation, sensitivity and permitted aggregation. One primary parent; reviewed related links.

Record group	Minimum content and relationships
Business object and source alias	Object type, stable identity, names, custody and state. A provider namespace plus its external key is unique within the declared contract.
Geography and boundary version	Scheme, level, stable code, name, geometry, coordinate system, source, accuracy, effective period and review state. Historical links stay valid.
Source dataset and version	Owner, custodian, purpose, rights, classification, source reference, schema version, coverage, update frequency and quality. A current release is explicit.
Observation and revision	Object or declared subject, field version, typed value or missing reason, unit, actual place and period, source row or passage, method and review.
Document and resource version	Protected original, file type, size, integrity reference, owner, source page or row, classification, derived-file links and publication state.
Project and revision	Purpose, funder, lead, parties, component, activities, domains, places, schedules and applicability. Material changes create a new revision.
Work occurrence and submission	Obligation, occurrence key, assignee, due period, exact form version, frozen submission, evidence, review and correction history.
Indicator method and result	Definition version, baseline, target, numerator, denominator, calculation version, exact inputs, result, uncertainty, reviewer and evidence.
Decision consultation and action	Problem, options, evidence versions, advice, responses, mandate, selected option, reasons, conditions, assigned actions and outcome verification.
PES and market evidence	Scheme or product reference, parties, area, period, conditions, quantities, currency, source-reported state and supporting evidence. Distinct legal and payment states.
Audit and processing receipt	Authenticated actor, action, resource, scope, result, reason, standard time and correlation reference. Receipts identify pending, rejected and committed outcomes.

One organisation has many dataset definitions. One dataset has many immutable versions. One version has many typed fields and source rows. One business object can have many source-specific observations and dated geographic links. One project has many revisions, activities and monitoring plans. Each accepted result identifies the exact method and source versions. These relationships use foreign keys or equivalent enforced referential constraints; a relationship never broadens access.

10 3 Database Design Rules

Use typed curated structures for accepted high-value records, decimal precision appropriate to each quantity, stable identifiers and uniqueness constraints at the declared grain. Preserve immutable source input separately. A configurable form definition does not justify one untyped

value table for all business data. Store geometry with a declared coordinate system and use suitable spatial indexes. Binary originals belong in protected file or object storage with controlled metadata and reference integrity.

The dictionary retains 34 operational forms with 280 baseline fields and three knowledge publication controls (audience, public use and permitted versions): 283 current fields. It also retains 359 source intake schemas with 3,928 source fields and configured domain definitions. These are prototype definitions for review. Field mapping, source-use permission, data acceptance and scientific approval remain separate decisions. Use each source field key, label, type, unit and required state in the detailed contracts.

Define atomic transaction boundaries for submission, review, acceptance, publication, source correction, closure and safe retry receipts. Enforce expected-version checks and uniqueness for repeated source events and scheduled work. Do not silently overwrite conflicting claims. A database migration is ordered, versioned, reviewed, rerunnable or safely detectable, and supported by reconciliation and recovery guidance.

The physical design deliverable must include entities, keys, field types, precision, nullability, constraints, indexes, relationships, audit strategy, partition or archive policy, retention and migration rules. Every runtime read and write uses approved server-side operations under a least-privilege runtime identity. The selected relational or geospatial data store must demonstrate controlled access, transaction integrity and enforcement evidence. Data-store deployment is a separately authorised operation.

Declare a unique observation grain for each contract, including provider, object or subject, field, place, period and replicate or sampling-depth keys where applicable. A duplicate test must not erase independent samples. Preserve external codes as text, retain zero and false, and store unknown values with an explicit missing reason. Use exact decimal arithmetic for money and governed precision for measurements; reject unsupported overflow rather than round silently. Record time standard and the supplied observation precision; received time cannot fill an unknown observation time.

Index permitted-scope and common search paths, source-event keys, dataset versions, dated observations and spatial queries. Validate plans against the approved workload. Source, review and publication references must be enforced consistently. Versioned audit records and protected originals remain linked after archival. Business transaction records and their durable processing or notification receipts must commit together.

10 4 Data Governance and Update Contracts

The source institution remains accountable for its data. Name the dataset owner, steward, sharing approver, technical custodian and operating processor. Agree the permitted purpose, audience, licence, quality rules, refresh method, frequency, late-data policy, retention and correction route. Each feed contract defines observed time, received time, issue time where relevant, expected update and stale status. Real-time is claimed only for a verified source contract.

Source group	Proposed update arrangement	Required confirmation
Administrative boundaries and reference codes	Versioned official releases; periodic change review.	Custodian, code edition, effective period and programme crosswalk.
Institutional statistics and project registers	Monthly, quarterly, annual or event-driven according to the source.	Reporting grain, revision rules and accountable updater.
Weather climate and device observations	Provider schedule with explicit observation and receipt time.	Product, station or grid, calibration, time standard, access and failure rules.
Markets and value chains	Source-specific daily, weekly or seasonal releases.	Product grade, market, unit, currency and price type.
SLM PES and field evidence	Agreement or monitoring-plan schedule.	Sampling protocol, verifier, scheme terms and disclosure limits.
Knowledge and advice	Author review and controlled replacement when guidance changes.	Competent author, citations, language reviewer and review trigger.

Use a common minimum metadata profile: stable source and dataset IDs; title and purpose; owner and custodian; format and schema; coverage and grain; actual time and time standard; unit and method; coordinate system and accuracy where relevant; quality and review; rights, sensitivity, frequency, retention and lineage. Use UTF-8 for text and explicit international encodings in exchange contracts. Unknown source values remain unknown.

10 5 Privacy and Sharing

Confirm the applicable national requirements and institutional policies with a qualified reviewer under C05. Do not infer a legal basis or controller role from technical hosting. Record the purpose and lawful basis for each personal-data category. Where consent is used, retain its scope, evidence and withdrawal state; do not use preselected consent. Minimise identifiers and coordinates, restrict household and complaint information, and apply approved retention and disclosure rules.

Sharing approval identifies purpose, recipient, scope, expiry and onward-sharing restrictions. A recipient cannot grant wider rights. Withdrawal blocks future access, cached delivery and saved-result export where rights require it; it cannot claim to erase copies already lawfully exported. Record correction, restriction, deletion or retention decisions and any lawful hold. Apply the policy to backups and recovery without destroying required audit evidence.

10 6 Technology and Platform Options

The TOR prefers open-source options. The client selects the final supported stack through C07 using requirements fit, skills, support life, security, interoperability, licence, total cost and exit. Product names below identify options for evaluation; none is an awarded procurement choice.

Option	Potential fit	Proof needed before selection
Landscape Portal and later government mirror	The PMU work template identifies this route for initial dashboard hosting and later government publication.	Custodian demonstration, hosting terms, identity, private workflows, APIs, backup, migration and scope fit. Current capability is not established by the planning note.
Configurable spatial catalogue with a geospatial service and data store	Open-source spatial catalogue, map publication and controlled resource sharing.	Demonstrate project review, DSS, M&E and PES workflows or a governed extension. A spatial portal alone does not prove the whole SRS.
Supported open application services with relational and geospatial stores	A candidate for the shared API, workflows and curated spatial data.	Compare supported framework versions, operational skills, identity, transaction controls, backup and lifecycle cost.
Supported application and relational data-store option	A candidate where the receiving institution can support its licensing and database operations.	Demonstrate approved server-side operations, least privilege, transaction integrity, spatial capability, support, licence terms, portability and cost.
Existing institutional tools and approved adapters	Reuse a source of record rather than duplicate its operational register.	Field-level fit and rights, exchange contract, ownership, reconciliation and failure tests.

Run a fit-gap exercise against every approved Must requirement with the same demonstration data and acceptance criteria. Record native fit, configuration, extension, integration or unmet need, with evidence, cost and owner. Do not assign unsupported numerical vendor scores. Select only after the pilot workflow, security, recovery and exit tests are reviewed.

10 7 Hosting and Long Term Operation

Compare cloud, on-premises and hybrid operation. The PMU portal-to-government-mirror route must be reconciled with the proposed Sri Lanka primary site and independent recovery site. A mirror of published data is different from a disaster-recovery service. Select the operator, jurisdiction, residency, network boundaries, identity, storage, key custody, backup location, monitoring, support and funding before procurement.

The deployment design places public channels behind HTTPS controls, keeps application and job services within approved boundaries, and protects the database, originals and keys from

public access. Replication or publication across boundaries sends only the approved data class and schema. A backup is independently recoverable. The exit plan includes complete data and metadata export, source and build handover, dependency licences, key transfer under authority, migration rehearsal and termination of old access.

10 8 Functional Requirements

These requirements are proposed Must requirements in delivery package WP1. The client approves the release baseline and any deferral through C01. Optional intelligent processing, device adapters, additional field-access channels and offline operation require explicit scope confirmation. The acceptance checks are required tests, not recorded test results.

FR147 Use approved operations to access data

SHARED must perform runtime data access through a controlled server-side data access layer and approved operations, including identity and health checks. Runtime principals receive only the necessary permissions. Clients never access database tables. The selected database plan must specify the operation catalogue and enforcement evidence.

Acceptance check: Architecture and native permission checks reject table access.

FR148 Keep action history and source links

SHARED must record significant actor, action, resource, scope, result, reason, standard time and request reference. Trace published data back through source, validation and review.

Acceptance check: Reopen the chain from report result to original evidence.

10 9 Connected Data Architecture

Start with the existing API-first modular application, controlled operational and geographic data, protected files and bounded analytical views. Add specialist stores only when measured volume, query latency, retention or research requirements justify their operating cost. These are logical responsibilities. Several may share one deployment and store. This section extends the existing architecture and uses the same Institution review decisions.

Source authority and the lifecycle

An institution remains authoritative for its own source records unless an agreed mandate says otherwise. SHARED can hold an authorised reference, snapshot or derivative. Record the custodian, exact dataset release, rights, classification, geography, period and update policy before intake. Information follows controlled intake, protected evidence, parsing, versioned mapping, validation, review, curated records, rebuildable projections, Expert Hub and monitoring. An observation, an institutional decision and a published result are separate records.

Common capture contract

Manual forms, field evidence, spreadsheets, structured files, document tables, scans, GIS layers, institutional APIs, scheduled imports, webhooks, device telemetry and approved remote-sensing products use one intake contract with source-specific adapters. Every receipt retains a batch or packet key, source release, checksum where applicable, adapter and mapping versions, arrival time, counts and an observable outcome. Keep original, normalised and curated values distinct. Parse reliable structured rows deterministically before considering AI. The controlled capture matrix identifies actual prototype domains, source ownership, staging, duplicates, exceptions, replay and consumers for all twelve routes.

Separate progress quality review and access

Track ingestion progress, data quality, institutional or scientific review, and publication eligibility independently. A parsed reading can pass technical checks while remaining provisional or restricted. A previously authorised feed can run configured automated quality checks without a person approving each reading. Feed authority, calibration, exceptions and finalisation remain controlled. Extracted document candidates follow the applicable human review policy before an authorised commit. Never turn an unknown status into approved or public.

Operational meaning and record envelope

Reuse the current institution branches, domain definitions, field contracts, source mappings, work records and geographic references. The envelope maps their existing identifiers to a record, institution, domain and definition version, dataset release, feature of interest, observation interval, receipt time, raw and normalised values, unit, method, geometry version, quality, review, access, evidence, run, mapping and supersession. A packet containing ten properties produces ten scalar observations linked to one protected packet. The packet identifier is not a replacement for individual property identity.

Data structure and compatibility

Separate semantic definitions, operational entities, observations, source claims and derived products. Prefer typed relational entities for identities and high-integrity relationships. Use validated flexible extensions for sparse domain fields with a versioned contract, typed indexes and explicit query limits. A typed attribute-value model can support heterogeneous observations, but requires type and unit enforcement, query planning and meaningful keys. Do not create a physical table for every field, merge similar labels, or accept uncontrolled text as a numeric observation. Preserve institution-owned claims and reviewed equivalence mappings.

Definition change and geography

A label edit preserves meaning. A new optional field does not backfill history. A unit conversion retains the original unit and conversion version. A meaning change creates a new definition. A breaking structural change needs impact analysis, compatible adapters, migration design and rollback or forward repair. Release definitions through draft, impact analysis, validation, authorised release, mapping update and compatible projection refresh. Maintain overlapping administrative, catchment, ecological, project and community schemes through many-to-many relationships and boundary versions. Sensitive sites and species locations require restricted precision and audiences.

Storage and projections

Operational relational records and approved geography remain the controlled core. Protected object storage holds source files, photos, audio, raster objects and report artifacts with versions and retention. Partitioned operational observation tables may meet initial time-series needs. Analytical views or a mart provide reconciled facts and conformed dimensions. An OLAP cube supports dimension-based aggregates; an earth-observation cube holds gridded arrays by space, time, variable and resolution. A keyword or vector index is a rebuildable retrieval projection, not the numerical or approval authority. Relationship graphs, specialist time-series engines, analytical files and federated queries remain optional until a measured need exists.

Refresh correction withdrawal and recovery

Use a committed change receipt or outbox where reliable prompt refresh is needed; compare it with a simpler scheduled incremental watermark for bounded workloads. Consumers deduplicate using source identity and version, acknowledge progress and permit replay. Do not promise exactly-once delivery or make uncontrolled dual writes. Each projection records its source of truth, authoritative keys, watermark, lag, rebuild steps and retention. Corrections and rights withdrawal invalidate affected maps, aggregates, search results, caches and new exports. Recheck rights when serving cached results. Restricted historical retention is separate from public access. Previously downloaded external copies cannot be recalled by the prototype.

AI extraction and retrieval

Keep file safety, native parsing, optional vision or OCR, constrained extraction, mapping, deterministic checks and human review as separate steps. A candidate includes definition IDs, original values and units, periods, place candidates, exact page/table/row/span evidence, missing or ambiguous states and validation messages. Schema-valid output can still be wrong. Verify evidence locations, totals, units, duplicates and cross-field consistency before commit. Treat

source text as untrusted data. No model can execute arbitrary queries, change definitions or permissions, or publish records. Preserve source checksum, parser, model, template, schema and mapping versions, evidence anchors and reviewer edits.

Optional provider boundary

OpenAI is one replaceable adapter for file input, constrained extraction, retrieval or report assistance. Exact model capabilities, input limits, retention, residency and deletion must be checked for the selected account and implementation. Use deterministic whole-table processing for spreadsheets rather than assuming a file interface reads every row. Compare external processing, local or private processing and manual entry. Obtain institutional permission before transmitting private documents. Evaluate representative field-level correctness and reviewer effort, including Sinhala and Tamil only where representative samples are available. Model-generated confidence is not a calibrated probability.

Retrieval and reporting assistance

Chunk authorised source versions into meaningful sections with source/page anchors, embedding and parser versions, access metadata and rebuild lineage. Apply permissions before retrieval where supported, then recheck current rights before returning text or supplying context to a model. Withdraw stale chunks and invalidate cached answers when a source changes. Keep document retrieval separate from numerical execution. AI may propose a report definition or explain verified results. Numeric answers come from deterministic calculations over authorised records, not document similarity or model memory.

Devices and observation time

Support a direct sensor, logger or edge gateway, permitted network and common intake route, or a provider-managed station, authorised API adapter and the same intake route. A sensor is not a complete station or necessarily Internet-connected. Map OGC SensorThings concepts as a reference model without claiming protocol conformance. Distinguish measurement time, aggregation interval, transmission, ingestion and display times, and observed, forecast, reanalysis, estimated and simulated values. Retain deployment, location, elevation or depth, datum, calibration, clock drift, battery and connectivity health, duplicates, late arrivals, resets, corrections and freshness. Offline recording does not establish real-time telemetry.

Quality and official warnings

Configure plausibility, range, rate-of-change, stuck-value, duplicate and completeness checks for each authorised stream and reviewed method. Quality exceptions enter an observable queue. Preserve late valid readings and correction history without silently replacing accepted values. A threshold crossing or forecast is not an official hazard warning. Keep the official warning issuer, issue time, validity and affected area separately. Device, logger, network, API access and local siting choices remain researched options rather than procurement or deployment commitments.

Expert Hub execution

The ordinary wizard remains usable without AI. It selects permitted domains, subdomains, datasets, attributes, places, periods, measures, comparisons and outputs from the existing Domain Studio definitions. A saved report definition records versions, filters, joins, grain, calculations, missing-data policy, visual choices and access context. Validate this configuration

before execution. Reject ambiguous definitions, incompatible units or periods, unsafe joins and restricted sources. A bounded modular planner chooses curated rows, observation aggregates, analytical views, cubes or spatial processing. Retrieve documents separately for supporting evidence.

Report jobs and reproducibility

Run versioned deterministic methods with previews, progress, cancellation, timeout and safe retry. Record the run ID, dataset and schema versions, geography snapshot, method versions, watermark and artifact fingerprints. Recheck permissions for caches and exports. Provide charts with clear units, coverage and supporting rows. Reproduction requires retained authorised snapshots or reproducible provider references. If an external source is not retained or changes independently, state that the earlier run cannot be reproduced exactly. A visual comparison alone does not establish causation.

Cultivation and weather example

The architecture demonstration compares annual rice cultivation categories for Polonnaruwa with rainfall and temperature using explicitly synthetic data. Declare crop-category-season-area grain and weather-property-interval-cell or station grain separately. Gross seasonal cultivated hectares can count the same land in successive seasons; unique physical land area requires feature identity and spatial union. Aggregate each compatible fact set independently before joining by year and approved geography. Apply an explicit station or grid weighting method, rainfall accumulation and coverage-aware temperature averaging. Do not multiply rainfall by crop rows, average ratios blindly, sum temperature or add reservoir storage across time.

Capacity and acceptance

For an illustrative 100 stations with ten properties and 1,440 one-minute samples, there are 1,440,000 scalar observations and 144,000 ten-value packets per day. Neither count alone states database row count or bytes. Size original evidence, normalised records, indexes, projections, document chunks, embeddings and backups separately. Use measured ingestion lag, query concurrency, retention and recovery to decide upgrades. No current local simulation establishes production throughput or uptime. The linked executed architecture tests are separate from the retained institutional case plans. Institutional definition and method acceptance stays in Institution review.

Controlled architecture views

The existing architecture explorer contains thirteen linked views, the capture and storage matrices, the AS-IS inventory, current field mappings and five guided simulations. Each component separates implementation maturity, data provenance and decision status. Each interface states payload, trigger, direction, validation, failure handling and owner. Open https://sharedproto.wkslabs.com/reviews/dashboard-portfolio-20261027/system-diagrams/#data-context

Capture method matrix

All routes use the same versioned receipt, protected evidence, mapping, typed checks, quarantine and replay contract. Keep rejected rows and reasons, bound retries, retain checkpoints and monitor counts, lag and unresolved exceptions. The full route records retain owner, rights, exact

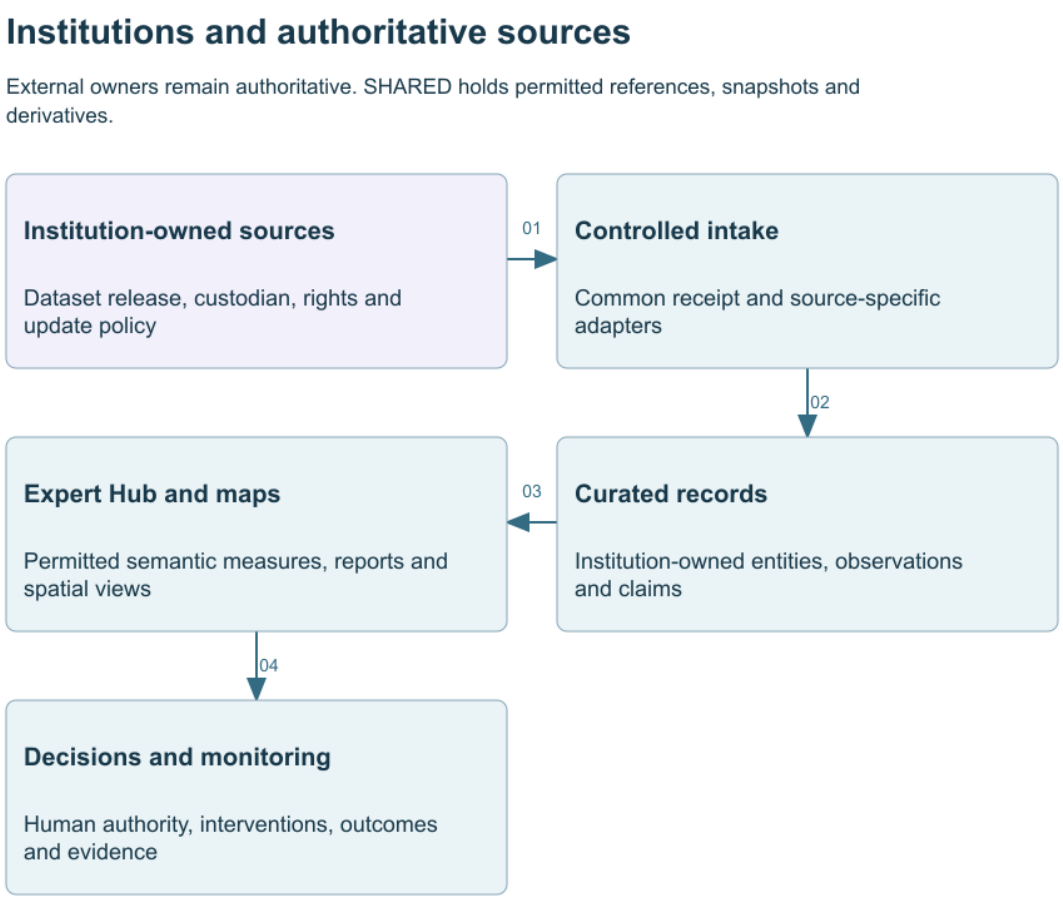
dataset and field references, adapter version, mapping version, replay policy, failure queue and downstream consumers. They supplement the existing Domain Studio catalogue.

Capture route	Source and validation	Destination and review
Manual forms	Owning institution / DP03. Agriculture, irrigation and operational forms. Typed form values. Trigger: Explicit save/submit. Checks: Type, required fields, vocabulary and relationships. Replay key: Record ID and expected revision.	Existing provider Draft rows / SrsDemonstration records. Independent record review as applicable. Field examples: Crop; District; Measure; Value; Unit; Season.
Field evidence	Field team / institutional custodian. Site, project, soil and geographic evidence. Permitted photos, observations and coordinates. Trigger: User capture; offline exchange only if selected. Checks: File safety, time/location accuracy, sensitivity and evidence links. Replay key: Capture identity and evidence checksum.	Protected evidence references and candidates. Field verification under approved policy. Field examples: OBJECTID; Tank_Code; Res_Name; soil_classification_1; geometry.
Spreadsheets	Owning source institution. Crop, soil, market and monitoring schemas. CSV/XLSX with sheet/header/unit contracts. Trigger: Approved import or schedule. Checks: Deterministically read all required sheets/rows; reconcile totals. Replay key: Dataset release, sheet and source row key.	Common intake batch / mapping preview. Batch review with rejected-row corrections. Field examples: Crop; District; Measure; Value; Unit; Season.
Structured files	Source custodian. Existing typed source contracts. Configured CSV/JSON/XML. Trigger: Upload or permitted file exchange. Checks: Schema, encoding, units, period, size and row outcomes. Replay key: Source event identity and exact release.	Raw evidence + normalized staging + quarantine. Per-source batch policy. Field examples: Crop; District; Measure; Value; Unit; Season.

Capture route	Source and validation	Destination and review
Document tables	Document owner / reviewer. Crop, project and reservoir statements. Native text/tables with page/table/row locators. Trigger: Selected permitted document. Checks: Native parse first; unit/period/place/total reconciliation. Replay key: Source checksum/version, row and definition identity.	Evidence version and extraction candidates, not approved facts. AI/OCR candidates require applicable human review. Field examples: Crop; District; Measure; Value; Unit; Season.
Scanned pages	Document owner / reviewer. Scanned institutional statements. PDF/image pages with resolution and anchors. Trigger: Selected pages requiring OCR/vision. Checks: Check anchors; preserve ambiguous/missing values; no guessed totals. Replay key: Source checksum, page, span and extraction schema.	Protected originals + extraction-run issue queue. Human review and correction before commit. Field examples: Crop; District; Measure; Value; Unit; Season.
GIS layers	GIS custodian. IRR_CATALOG and INST_CATALOG layers. GeoJSON/GeoPackage/GeoTIFF or approved adapter. Trigger: Versioned release / authorised refresh. Checks: CRS, topology, bounds, geometry, generalization and sensitivity. Replay key: Source feature ID, release and geometry version.	Spatial staging and reviewed geometry versions. Official boundary/crosswalk acceptance separate. Field examples: OBJECTID; Tank_Code; Res_Name; soil_classification_1; geometry.
Institutional APIs	Provider / connector owner. Existing source connector contracts. Documented JSON/XML/GeoJSON. Trigger: Authorised bounded polling. Checks: Schema/version, pagination, rate limits, totals, freshness and rights. Replay key: Native source/event key and release watermark.	Common run; native fields retained with normalized values. Explicit feed activation; feed policy governs ordinary rows. Field examples: stationid; date; rainfall_mm; station_id; latitude; longitude.

Capture route	Source and validation	Destination and review
Scheduled imports	Source owner / operator. Approved periodic releases. Permitted files/API pages and manifest. Trigger: Configured authorised schedule. Checks: Completeness, availability, nonoverlapping checkpoint ranges. Replay key: Release/watermark and row identity.	Resumable common run/checkpoints and quarantine. Approved batch/feed policy with exception review. Field examples: stationid; date; rainfall_mm; station_id; latitude; longitude.
Webhooks	Provider / connector owner. Proposed event-triggered source contracts. Signed bounded event payload where supported. Trigger: Provider event at an authorised boundary. Checks: Signature/replay/clock, schema and safe routing. Replay key: Provider delivery ID and source revision.	Proposed durable receipt; isolated replay model. Approved feed policy; anomalous events held. Field examples: stationid; date; rainfall_mm; station_id; latitude; longitude.
Device telemetry	Station custodian / calibration lead. DP08 weather / DP05 hydrology / DP02 soil needs. Multi-property packet with event time and raw units. Trigger: Logger interval, store-forward or provider polling. Checks: Deployment, calibration, duplicates, late, clock, range, stuck and missing checks. Replay key: Datastream/event time/property/revision; packet identity retained.	Raw packet + scalar observations + exception queue. Approve feed and automatic QC policy; provisional states; exceptions reviewed. Field examples: stationid; date; rainfall_mm; station_id; latitude; longitude.
Approved remote-sensing products	Product/licence custodian / GIS expert. Land, weather and vegetation rasters. Raster release and product/grid/time metadata. Trigger: Approved published product refresh. Checks: CRS/resolution, masks, band units, nodata and provenance. Replay key: Edition, tile/grid, time, variable and processing version.	Protected raster/reference + rebuildable zonal products. Product rights and extraction/masking policy accepted separately. Field examples: OBJECTID; Tank_Code; Res_Name; soil_classification_1; geometry.

Connected information lifecycle



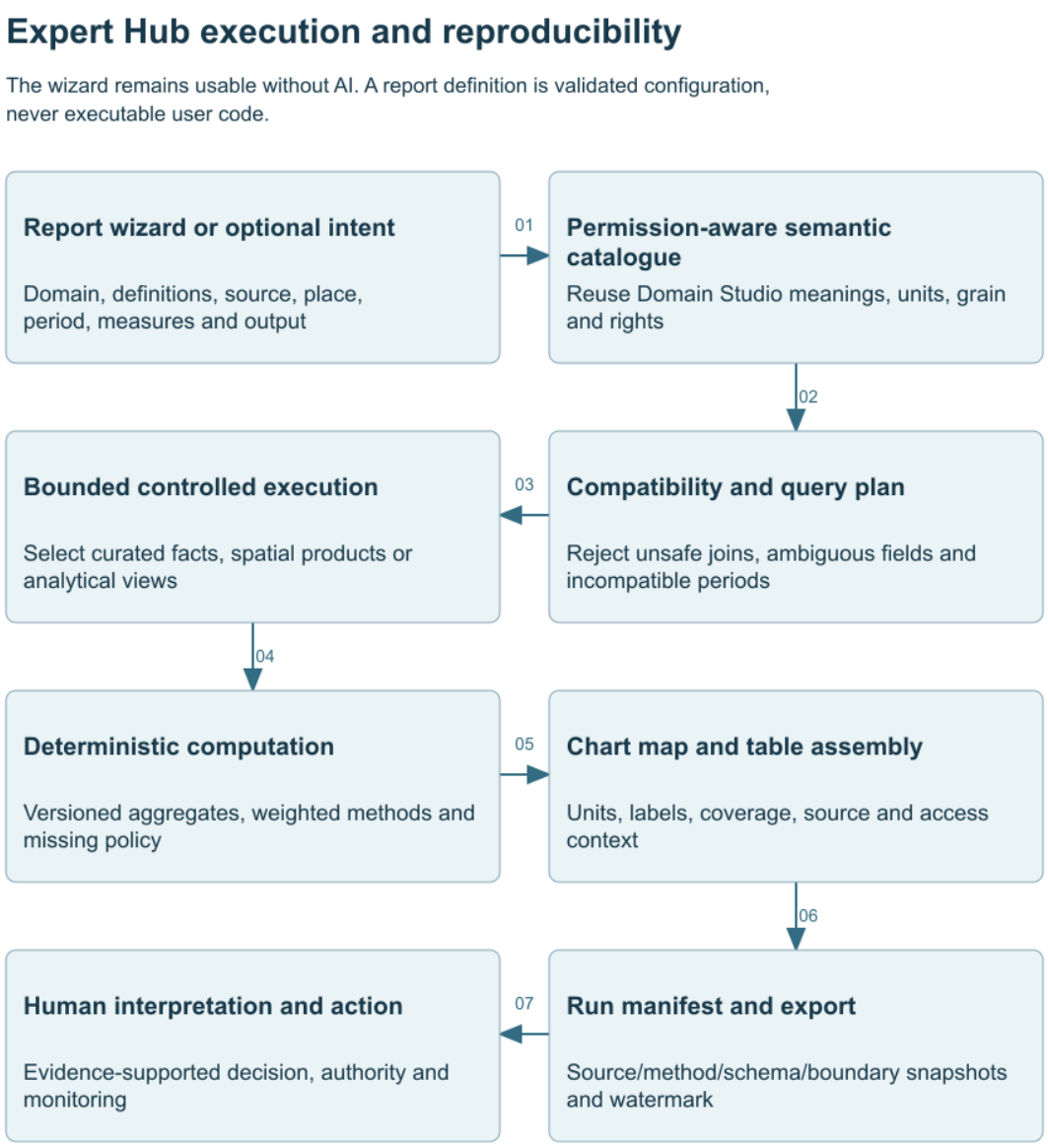
Proposed logical architecture. Synthetic demonstrations and external dependencies are identified separately. Full-size vector and editable source: https://sharedproto.wkslabs.com/reviews/dashboard-portfolio-20261027/system-diagrams/#data-context

Domain records evidence and derived products



Proposed logical architecture. Synthetic demonstrations and external dependencies are identified separately. Full-size vector and editable source: https://sharedproto.wkslabs.com/reviews/dashboard-portfolio-20261027/system-diagrams/#data-model

Expert Hub execution and reproducibility



Proposed logical architecture. Synthetic demonstrations and external dependencies are identified separately. Full-size vector and editable source: https://sharedproto.wkslabs.com/reviews/dashboard-portfolio-20261027/system-diagrams/#data-expert

11 Service Quality Security and Operations

The requirements below define measurable service outcomes. The availability minimum comes from the TOR. Other numeric targets are proposals for C08. They become contractual commitments only after the client approves their workload, measurement and acceptance conditions.

NFR01 Availability

The service shall achieve at least 99 percent availability. This is the TOR minimum. Proposed measurement is a calendar month of agreed service minutes, including planned maintenance until an exclusion policy is approved.

Acceptance check: Availability equals successful service minutes divided by agreed service minutes. Retain monitoring and incident evidence.

Approval needed: Client and operator confirm measurement boundary.

NFR02 Interactive performance

Proposed target: 100 concurrent authenticated users; standard bounded API reads p95 at most 750 ms and p99 at most 1.5 seconds; error rate below 0.5 percent.

Acceptance check: Run the approved workload after documented warm-up in a representative isolated environment. Measure server duration separately from network time.

Approval needed: Client confirms workload and budgets.

NFR03 Spatial performance

Proposed target: bounded spatial queries p95 at most 2 seconds and p99 at most 4 seconds.

Acceptance check: State geometry count, complexity, extent, coordinate system, caching and query type with the result.

Approval needed: GIS expert and client.

NFR04 Capacity and scaling

Proposed sizing: 250 organisations and one million vector features at the agreed workload. Test twice the interactive load for controlled saturation.

Acceptance check: Reject or queue excess work without corruption, leaked records or unbounded memory. Agree storage growth and larger limits before procurement.

Approval needed: Client data custodians and operator.

NFR05 Low bandwidth and responsive use

Proposed profile: 1.5 Mbps down, 750 Kbps up, 300 ms round trip and 1 percent packet loss. Essential initial transfer at most 1.5 MiB compressed. The system shall support mobile-compatible use of the agreed core journeys on client-agreed devices.

Acceptance check: Complete sign-in, list, detail, form and retry tasks on the agreed devices under the approved network profile.

Approval needed: Client confirms field profile.

NFR06 Accessibility and language

Proposed web target is WCAG 2.2 AA. Provide keyboard operation, visible focus, labelled controls, readable error messages, text alternatives, accessible tables and text scaling. English, Sinhala and Tamil coverage requires client agreement.

Acceptance check: Check agreed user journeys with keyboard, screen reader and manual review. Language reviewers accept terms and translations.

Approval needed: Client and appointed language reviewers.

NFR07 Security verification

Use threat modelling and an agreed OWASP ASVS control set, proposed Level 2. Protect sessions, inputs, files, exports, transport and secrets.

Acceptance check: No unresolved critical or high security finding at release. Record disposition and owner for other findings. Tests need an authorised isolated scope.

Approval needed: Security specialist and client.

NFR08 Data protection

Collect only information needed for an approved purpose. Apply classification, disclosure limits, retention and rights handling to originals, results, exports and backups.

Acceptance check: Test list, detail, count, map, preview and export against each denied scope. No private content or secrets appear in diagnostic output.

Approval needed: Data owners and qualified privacy reviewer.

NFR09 Recovery

Proposed recovery point objective is 24 hours and recovery time objective is 8 hours. Include database, protected files, configuration, keys and spatial resources.

Acceptance check: Rehearse restoration to an isolated environment. Reconcile committed records and referenced files and prove usable sign-in and access checks.

Approval needed: Operator and client approve recovery targets.

NFR10 Reliability

Commands shall use expected versions and safe retry references. Save a business change and its delivery request reliably together.

Acceptance check: Test duplicate requests, lost replies, stale edits, worker crashes, provider outage and cancellation without duplicate or partial committed outcomes.

Approval needed: Solution and database reviewers.

NFR11 Interoperability

Publish versioned API and data contracts. Declare supported geospatial protocols, encodings, units, coordinate systems and export formats.

Acceptance check: Contract tests include unsupported versions, malformed messages, mapping changes, pagination and source failure.

Approval needed: Provider technical owners.

NFR12 Maintainability and portability

Keep business definitions configurable, modules separated and dependencies supported. Supply reproducible builds, migrations, operation contracts and complete export.

Acceptance check: An appointed maintenance team installs an isolated copy and reuses the supplied build, restore and migration guidance.

Approval needed: Client operating institution.

NFR13 Audit and observability

Retain protected business audit separately from redacted diagnostics. Proposed correlation target is at least 99 percent of API requests; significant events queryable within five minutes.

Acceptance check: Trace a publication to its actor, exact source and review. Test denied access and log redaction. Agree audit retention and alert delivery.

Approval needed: Security and operations.

NFR14 Support and sustainability

Name the service owner, support levels, escalation, funding, renewal obligations and patch responsibility before operational acceptance.

Acceptance check: Handover includes a costed support plan, dependency inventory, incident route, continuity rehearsal and knowledge transfer evidence.

Approval needed: Client and receiving operator.

11 1 Operational Controls

Keep development, test, staging and production isolated. Inject secrets through approved protected settings. Use supported dependencies and a controlled patch process. Record service health without exposing private content. Agree alert recipients, severity, escalation, response and incident closure. Recovery, credential rotation and release work follow reviewed runbooks.

The service test plan must state upload and archive limits, page sizes, query limits, file types and retention. Proposed early limits are a 50 MiB single upload, no more than 10 files or 100 MiB in a batch, and explicit limits on decompression, feature counts and vertices. Larger datasets use a reviewed asynchronous import contract. Security and data owners approve the final limits and representative tests.

11 2 Functional Requirements

These requirements are proposed Must requirements in delivery package WP5. The client approves the release baseline and any deferral through C01. Optional intelligent processing, device adapters, additional field-access channels and offline operation require explicit scope confirmation. The acceptance checks are required tests, not recorded test results.

FR149 Protect discovery and notification delivery

SHARED must protect private people and sensitive locations from disclosure through search, counts and exports. If an action creates a notification, save the action and delivery request reliably together. Retry delivery without duplicating the message.

Acceptance check: A notification failure does not erase the business action or leak its content.

FR151 Separate environments and secrets

SHARED must separate development, test, staging and production configuration and inject secrets through protected settings. Do not publish credentials or private data in code, documents, logs or exports.

Acceptance check: A test configuration cannot silently target production.

FR152 Monitor service health without exposing private data

SHARED must monitor service availability, failures and background processing. Retain safe diagnostic details and a request reference so an authorised operator can investigate an error. Health responses and logs must not expose credentials, personal records or original source content.

Acceptance check: An error can be traced without exposing the source payload.

FR153 Release through controlled runbooks

SHARED must support reviewed procedures for deployment, migration, rollback or forward repair, credential rotation, incidents and continuity. Do not upgrade the database at application startup.

Acceptance check: A release preserves shared configuration and records a recovery path.

FR154 Prove coordinated recovery

SHARED must back up the database and protected files under agreed security and retention rules. Confirm recovery targets through an authorized restore exercise, not backup creation alone.

Acceptance check: Restore a consistent database and evidence-file set in isolation.

12 Implementation Testing and Acceptance

Build and accept complete information journeys in five dependent work packages. Each package delivers the relevant software, data contracts, tests and guidance. The consultancy delivers the specification and mock screens; future developer delivery and operational acceptance are separate from consultancy acceptance.

12 1 Work Packages and Dependencies

Package	Required outputs	Entry and acceptance gate
WP1 Foundations and data	Identity and scope; owned definitions; source catalogue; typed data model; intake, quality, review and audit.	Approved SRS and design decisions. Demonstrate one full source-to-accepted-data journey.
WP2 Maps and dashboards	Geography, layer contracts, role dashboards, data discovery and source-aware reporting.	WP1 and approved source geometry. Reconcile map, table and exported values.
WP3 Decision and domain functions	Reviewed calculations, options, advice, SLM, PES and value-chain appraisal.	WP1 and WP2; accepted operational methods and scheme rules for their activation.
WP4 Participation and implementation	Project work, M&E, community feedback, knowledge, field workflows and approved integrations.	Shared identity and data foundations; agreed receiver, project-tool boundary and field scope.
WP5 Acceptance and handover	Cross-module UAT, security, accessibility, load, recovery, migration, support and complete handover.	All approved release requirements pass; external gates have authorised evidence.

12 2 Module Outputs and KPIs

Each module must pass 100 percent of its approved Must acceptance cases. Numeric programme targets remain the PMU monitoring plan. The following KPIs measure delivered system behaviour and do not invent programme achievements.

TOR module	Quantifiable output and acceptance KPI
Data integration and management	All approved contracts identify owner, fields, units, grain, rights and frequency. Every tested input has a truthful row outcome and traceable source. Replaying an unchanged event creates no duplicate accepted record.
Decision support	Every accepted execution retains method and input versions, assumptions and limits. All approved numerical fixtures match their expected results. Every operational decision retains the required authority and conditions.

TOR module	Quantifiable output and acceptance KPI
Multi-scale dashboards	All approved role and scale views reconcile with the same source data, filters and exports. Zero restricted values or locations leak through a denied view.
Monitoring and evaluation	Every active indicator has its definition, baseline state, target, denominator where relevant, source and verification. All tested plan-versus-actual figures reconcile; missing actuals remain missing.
SLM and PES coordination	All approved options and scheme records retain context, protocol, parties, authority and verification. Zero agreement uploads or generic scores generate an unsupported entitlement.
Value-chain and market information	Every accepted comparison states product, grade, unit, currency and period. All approved margin and break-even fixtures reconcile; incompatible evidence is flagged.
Stakeholder interaction	Every permitted concern or advice request has a receiving role, status, response history and protected audience. Zero unanswered consultations become consent.

12 3 Acceptance Journeys

Journey	Required evidence and failure checks
A Source to decision	Register a dataset; submit a source; reject an invalid row; correct and independently approve; use the accepted version in a dashboard and saved report; obtain advice; record the institutional decision and action. Repeat with denied scope, missing method, changed approval and withdrawn source.
B Field work to project outcome	Assign work; capture authorised evidence; recover from disconnection and conflict; review the exact submission; calculate an approved indicator; respond to an exception; verify asset handover and closure. Repeat with stale edits, duplicate occurrences, missing baseline and incomplete closure.
C Market or PES evidence	Record compatible production, demand and costs or a proposed service agreement. Review the applicable method and authority. Retain verification and source-reported payment evidence separately. Test missing costs, mismatched periods, absent rules and an unauthorised approver.
D Operational recovery	Install from the handover package, migrate a reviewed batch and reconcile totals. Restore database and protected files together. Demonstrate current access, source traceability and service recovery within the approved targets.

For every acceptance case, record the stable requirement and clause IDs, actor and scope, configuration, isolated input data, preconditions, steps, expected result, evidence type, actual result and disposition. The coverage workbook and acceptance annex provide the single clause-to-case mapping, shared suites, output paths and permission dimensions. Future service cases

remain Not executed until authorised evidence exists. Local prototype checks are design evidence and do not prove authentication, secure storage, live interfaces or availability.

12 4 Developer Milestone Payment Proposal

The following weights are a proposal for developer procurement under C10. They are separate from consultancy fees and payment terms. Payment requires the accepted deliverables and evidence, rather than a screen count or a demonstration alone.

Milestone	Proposed share	Acceptance evidence
Design and contracts	10 percent	Approved baseline, architecture, data dictionary, interface contracts, security model and detailed acceptance plan.
Core data and geographic views	25 percent	WP1 and WP2 end-to-end tests, source reconciliation and role-based dashboard checks.
Decision and specialist modules	25 percent	WP3 tests and accepted method contracts for selected operational uses.
Implementation and user acceptance	25 percent	WP4 and cross-module UAT, security, accessibility, performance and corrected defects.
Recovery and handover	15 percent	WP5 recovery evidence, complete source and data export, operator guidance and signed receiving acceptance.

12 5 Migration Handover and Sustainability

Inventory and preserve authorised sources before migration. Keep source aliases, mapping, rejected and unresolved records, loaded counts and reconciliation. A trial import must not create production records. The custodian accepts each approved batch. Retain rollback or forward-repair guidance without overwriting an existing unknown database.

Handover includes controlled source code, reproducible builds, supported dependency and licence inventory, ordered database migrations, approved operation catalogue, API descriptions, data dictionary, source and method registers, test evidence, deployment and recovery runbooks, user and administrator guidance, configuration without secrets, maintenance plan and authorised transfer of custody. Demonstrate installation and recovery by the receiving team.

12 6 Consultancy Deliverables

Deliverable	Required closure evidence
D1 Inception and inventory	Agreed approach, source inventory, stakeholder map and consultation plan.
D2 Needs and workflows	Actual stakeholder findings, roles, use cases, workflow feedback and prototype revisions.
D3 Structured requirements	Functional and non-functional requirements, architecture, data and governance draft.
D4 Validation package	Draft SRS, phasing, module KPIs, acceptance and payment proposal, mock screens, validation presentation, comments and agreed revisions.
D5 Final SRS and handover	Approved final issue, final presentation, source and deliverable package, resolved comment log and client acceptance.

This completed SRS and the prototype can support D4 and D5 review. Preparing a document does not establish that interviews, presentations, agreed revisions or final acceptance have occurred. C11 remains open until the authorised evidence is recorded. Only then can the consultancy be closed according to the TOR.

12 7 Risks and Mitigation

Risk	Effect	Mitigation
Source availability	Unavailable or changed endpoints delay operational feeds.	Build the contract and isolated tests; assign the source owner and preserve a manual approved route.
Unapproved methods	A plausible chart may be mistaken for a scientific recommendation.	Record the published basis separately. Obtain specialist review of local assumptions, adaptations and intended use; retain inputs and limits.
Geographic mismatch	Different boundaries or GN rosters distort coverage and eligibility.	Use versioned official keys and a reviewed crosswalk; retain unresolved matches.
Sensitive disclosure	Counts, maps, exports or public feedback can expose people or locations.	Apply the same complete scope to every output and test indirect disclosure.
Scope growth	Hundreds of candidate decisions can become an uncontrolled delivery commitment.	Approve priorities and packages while retaining the full candidate catalogue and change history.

Risk	Effect	Mitigation
Operating cost	Hosting, licences, data services and maintenance may become unfunded.	Compare lifecycle costs and exit options before selection and name an accountable operator.
Field connectivity	Poor connectivity interrupts capture and creates repeated submissions.	Use protected drafts, explicit sending states, conflict checks and safe retries.
Acceptance evidence	Screens or technical checks may be mistaken for programme or consultancy acceptance.	Retain separate records for mock review, software acceptance, scientific acceptance and client sign-off.

12 8 Functional Requirements

These requirements are proposed Must requirements in delivery package WP5. The client approves the release baseline and any deferral through C01. Optional intelligent processing, device adapters, additional field-access channels and offline operation require explicit scope confirmation. The acceptance checks are required tests, not recorded test results.

FR150 Govern change and trace requirements

SHARED must keep business settings editable and dated. Register proposed products before claiming delivery. Link requirements to design, work, implementation, tests and evidence, with controlled change history.

Acceptance check: A newly proposed product stays Proposed until its required delivery and acceptance are recorded.

FR156 List software gaps and missing external decisions separately

SHARED must track unfinished software separately from missing data, expert decisions and governance approval.

Acceptance check: A missing policy cannot be closed with a developer-created approval.

13 Review Decisions and Source References

Use published methods as their documented basis. Check the exact source and the copied calculation once. Ask the client or expert to confirm only local use, project choices and new or changed rules. Review each shared method once and list where it is used.

Published methods and software checks

Category	Check needed
Government publication	Record the government publisher, publication, edition and exact page or section. Confirm local inputs and settings where needed.
Institution publication	Record the institution, publication, edition and exact page or section. Keep draft and historical status visible. Confirm local inputs and settings where needed.
Validation required	Review new or changed domain rules, incomplete source matches and local assumptions. A data table or background page alone does not support a formula.
Software check	The developer tests the copied formula, arithmetic, units and invalid or missing inputs. Ordinary arithmetic does not need separate scientific approval.

The calculation appendix lists the published methods, exact sources and local settings to confirm. Published methods do not need separate approval on each screen. Use the same recorded review wherever a method is repeated.

Client and expert decisions

These decisions remain pending in Institution review. Each decision should state what was checked, who checked it, the outcome and any conditions. One review can cover the same method used by several screens.

Topic	What to confirm	Who
Scope and institutions C01, C02, C12	Confirm the final features, proposed decisions, participating institutions and what stays in existing tools.	Client
Responsibilities C02	Name who owns data, submits records, reviews them and approves sharing.	Client and institutions
Maps and boundaries C03	Confirm official boundaries and area codes. Resolve the different GN totals.	Data custodian and GIS expert

Topic	What to confirm	Who
Data sources C04	Confirm datasets, fields, units, update frequency and access or sharing conditions.	Source institutions
Privacy C05	Confirm access to personal records, sensitive locations and retention periods.	Client and privacy specialist
New or changed calculations E01	Review proposed scores, weights, thresholds, missing-value rules and method changes. For published methods, confirm local inputs, units, settings and intended use.	Relevant expert or statistician
Land soil and water methods E02	Confirm local suitability, sampling, laboratory methods and model factors.	Relevant domain experts
Ecosystem services and PES E03	Confirm eligibility, rights, rates, safeguards, verification and payment authority.	Client and relevant experts
Indicators and payments C10	Confirm indicator definitions, acceptance measures, milestones and payment weights.	Client and monitoring or finance specialists
Languages and access needs C06	Confirm wording, supported devices and accessibility requirements.	Client and representative users
Technical choices and service targets C07, C08	Agree architecture, hosting, operator, costs, performance, security and recovery targets.	Client and technical adviser
Complaints and appeals C09	Confirm receiving officers, response times and the appeal process.	Client
Final SRS acceptance C11	Confirm consultation comments, agreed revisions, validation, final presentation and final acceptance.	Authorized client representative

Source details to confirm

LUPPD: the alternative publications provide planning context. The applicable local planning procedure still needs confirmation under C04 and E02.

HARTI: the published prices support the quoted observations. They do not automatically support proposed volatility, spread or other analysis; review these under C04 and E01.

Live-system security, load and recovery tests belong to implementation. The SRS needs agreed requirements and a test plan. No separate expert approval is needed for each mock screen or repeated calculation.

Record decisions in Institution review only. Keep the source reference, method and affected uses with the decision. A changed method or changed local settings needs a new review of the change; an unchanged shared method can reuse the recorded decision.

13 1 Source Baseline

Source	Use in this SRS	Authority or remaining check
Supplied GCF Knuckels document	Introduction, 41 provider references, nine provider use cases and original grayscale diagrams.	Retained as the writing and diagram baseline; the original file remains unchanged.
Final ToR SRS SHARED IS	Seven modules, architecture, data governance, mock screens, phasing, KPIs, acceptance, developer payment framework and consultancy deliverables.	Controlling requirements baseline subject to confirmation of contract amendments under C01.
PMU SRS work template and consultation workbook	Source inventory, priorities, responsibilities, platform fit, hosting and acceptance structure.	Working inputs; proposed answers and colour coding are not signed consultation evidence.
Concept note GCF framework GIS and PES studies	Project context, intervention logic, candidate data, methods and governance questions.	Project studies support requirements; official boundaries, current values and operational rules need custodian or expert acceptance.
Earlier SHARED SRS chapters and addenda	FR001 to FR156, 49 use cases, 20 decision pathways, 33 PMU topics and geographic additions.	Consolidated without repeating module stores. Later design additions remain reviewable under C01.
Current isolated review prototype	Screens, 34 forms with 283 fields (280 baseline + 3 publication controls), structures, 820 decision examples, charts, methods, guides and diagrams.	Design and mock evidence only. No real-system implementation comparison or change is part of this issue.
Primary external references	Technical standards, provider descriptions, source methods and public information catalogues.	Calculation Sources links the checked LUPPD, FAO and HARTI alternatives. The local planning procedure, source use and method approvals remain pending.

13 2 Technical Reference Standards

W3C Web Content Accessibility Guidelines 2 2. Proposed accessibility acceptance baseline. https://www.w3.org/TR/WCAG22/

OWASP Application Security Verification Standard. Security control selection and verification; no certification claim. https://asvs.owasp.org/

OpenAPI Specification. Interface descriptions; pin the agreed supported version in the technical plan. https://spec.openapis.org/oas/latest.html

OGC API Features. Candidate standard for permitted vector exchange. https://www.ogc.org/standards/ogcapi-features/

Open spatial catalogue documentation. A reference for platform fit-gap; no product choice is mandated. https://geonode.org/

NASA POWER daily API. Source-specific time standard, grid and request-limit considerations. https://power.larc.nasa.gov/docs/services/api/temporal/daily/

CHIRPS rainfall products. Preserve product version, preliminary or final state, grid and temporal meaning. https://www.chc.ucsb.edu/data/chirps3

NASA FIRMS active fire data. Preserve product state and distinguish detections from confirmed events. https://firms.modaps.eosdis.nasa.gov/content/active_fire/

GCF Knuckles implementation. Project Options by Context and adaptive-management context. https://gkp.lk/implementation/

Keep publication versions and observation periods with the source evidence.

14 Prototype Coverage and TOR Traceability

The comparison runs in both directions. The SRS-to-prototype direction checks every retained requirement and use case against the mock design. The prototype-to-SRS direction inventories views, forms, fields, decisions, panels, methods, institution reviews and domain definitions and assigns an SRS location. The companion workbook is the detailed crosswalk. It retains the current prototype IDs instead of creating a competing register.

14 1 Coverage Meaning

Coverage label	Meaning
Design shown	A relevant screen, field, diagram or local workflow is present. This does not establish production or institutional acceptance.
Partial demonstration	The prototype shows part of the requirement. Remaining data, method, role, interface or workflow evidence is identified.
Technical only	The requirement concerns a real service, device, security, hosting or operating control beyond mock screens.
Review needed	A required source, mandate, parameter, translation or specialist decision remains unconfirmed.
Unmapped	An inventory item has no SRS location or a requirement has no identified design or technical rationale. This is a traceability gap to correct.

14 2 Current Prototype Inventory

Inventory	Count	SRS location
Functional requirement identities	156	Chapters 2 to 12
Geographic requirement identities	20	Chapter 4
Retained stakeholder use cases	49	Chapters 2 and 5 to 8; detailed workbook
Institutional decision examples	820	Chapter 5 and domain requirements
Record forms and current fields	34 forms and 283 fields	Chapters 2 to 10; workbook field dictionary
Source intake schemas and fields	359 schemas and 3,928 fields	Chapters 2 and 10; workbook field dictionary
Institution references	41	Chapter 2 and Institution review

Inventory	Count	SRS location
Decision panel definitions	164	Chapter 4 with domain and method links
Public-data chart definitions	158	Chapter 4 with original source contracts
Calculation families and method references	57 families and 139 references	Chapter 5 and the workbook catalogue
Retained external-reference library	2,037 links	Chapters 2 and 10; workbook Sources
PMU consultation topics	33	Chapters 2 to 13; detailed workbook
Role and system views	18 main views checked	Chapters 3 to 9
Retained baseline local checks	129	Design evidence; required service acceptance remains Chapter 12

The retained pre-correction audit opened all 34 record forms, the 18 main views and 53 static HTML pages, including the legacy redirect. It found no added TOR controls and passed 129 local checks. This is historical design and mapping evidence, not current acceptance of every clause. Version 1.6 correction checks are recorded separately. The prototype retains Institution review as its single review entry point.

14 3 What Still Needs Evidence

All 190 retained functional, geographic and nonfunctional IDs have a place in this SRS and a prototype or technical explanation. The retained coverage labels remain 150 Design shown and 40 Technical only. Some controls have only a partial local demonstration. Operational authentication, server-side permissions, permanent shared storage, file-safety checks, provider interfaces, conditional field-channel protection and synchronisation, load, security, recovery and handover require future service evidence. They are not extra mock-screen deliverables.

Version 1.6 author revision records the corrections dated 2026-11-01. It preserves the original review as historical evidence. It updates public-source eligibility, disputed PMU scope labels, traceability and acceptance annexes, conditional field access, generic architecture descriptions and the seed-category example. Client, expert and operational acceptance remain pending.

DP11-PNL02 and DEC-DP11-002, DEC-DP11-006, DEC-DP11-007, DEC-DP11-008 and DEC-DP11-016 remain proposed finance or procurement examples awaiting scope confirmation under C01/C02/C10/C11/C12. They are not accepted first-release scope. Keep physical progress, project milestones and evidence functions available while the client decides the disputed examples.

The annex records exact source class and passage, stakeholder need, proposed owner and appointment status, release or work package, decision reference and validation state for each requirement. A documented consultation, proposed owner or broad TOR paragraph does not establish individual institutional acceptance. The needs-to-requirements view checks the reverse direction.

The release view retains the five work packages and seven TOR capability areas. The 820 decision examples remain a candidate catalogue grouped under reusable families. Proposed, accepted, conditional and formally deferred totals are separate; no unknown acceptance becomes a completion percentage. NFR01 to NFR14 use one configuration annex with proposed targets and explicit pending workload, devices, network, languages, measurement windows, exclusions, owners and pass/fail conditions.

Open the current acceptance annex and controlled downloads.

Open the existing Institution review for the 15 pending decisions.

Operational use also depends on accepted institution data, scientific methods, source rights, official geography, PES rules and mandates. The exact client and expert decisions are in Chapter 13. Consultancy completion additionally requires actual consultation and validation evidence, agreed revisions, the final presentation and client acceptance. It is not yet supported to say that only signatures remain.

14 4 TOR Crosswalk

TOR requirement group	SRS coverage	Acceptance or decision
Stakeholders consultations roles and national-to-GN use cases	Chapters 2 to 9; 49 retained use cases and institution catalogue.	C02 C03 C11 and validated consultation record.
Data integration and management	Chapters 2 and 10; source, typed data, quality and review requirements.	WP1 source-to-accepted-data journey.
Decision support	Chapter 5; evidence, methods, options, advice and human decisions.	WP3 numerical fixtures and E01.
Multi-scale dashboards	Chapter 4; role, place, period, map, accessible table and export.	WP2 reconciliation and denied-scope tests.
Monitoring and evaluation	Chapter 6; indicator plans, baselines, targets, actuals and verification.	WP4 monitoring journey and C10.
SLM and PES coordination	Chapters 5 6 and 8; context, options, monitoring and service evidence.	E02 E03 and WP3 domain journey.
Value-chain and market information	Chapter 8; compatible production, demand, price and appraisal.	WP3 market fixtures and source acceptance.

TOR requirement group	SRS coverage	Acceptance or decision
Stakeholder interaction	Chapter 7; guidance, advice, participation, protected response and appeal.	WP4 user journey and C09.
Workflows data flows and logic	Source provider workflows and Chapters 3 to 10.	Use-case and end-to-end acceptance checks.
Performance uptime scalability and modularity	Chapters 10 and 11 including at least 99 percent availability.	C08 and WP5 measured service evidence.
National interoperability and security	Chapters 9 to 11.	Approved provider contracts, security tests and C04 C05.
Mobile low-bandwidth access and roles	Chapters 3 9 and 11.	C06 C08 and device, network and scope tests.
High-level and detailed architecture options	Chapter 10; logical components, records, interfaces, controls and platform fit-gap.	C07 and reviewed physical design before development.
Data formats metadata governance sharing and update frequency	Chapters 2 9 and 10.	Source contracts, schema and sharing acceptance.
Wireframes mock screens and role dashboards	Chapter 14 and the existing prototype.	Institution review and client feedback closure; no separate UI-reviewer gate.
Phasing dependencies priorities risks and sustainability	Chapters 10 and 12.	Five work packages, operating plan and C01 C07.
Module KPIs measurable acceptance and developer payments	Chapter 12.	Approved test cases, milestone evidence and C10.
Validation final SRS presentation ownership and handover	Chapters 12 and 13.	D4 D5 evidence and C11 client acceptance.

14 5 Reading the Coverage Workbook

Start with Summary. Coverage links both requirements and prototype items to their SRS chapter and prototype entry. Form fields retains the operational form and source schema fields. Domain dictionary retains the configured definitions and their source status. Sources combines the core method references and retained external-reference library without duplicate URLs; earlier access

status is labelled as a retained audit. Pending review decisions remain in Chapter 13. A mapped row means the item has a documented home; it does not mean its complete behaviour has passed acceptance.