SPR MARKET-SOUNDING PACKAGE

Annex B

Case Management / Back Office

High-Level, Outcome-Based Requirements

Technology-neutral market sounding	Non-binding	Vendor solution approach requested

Document field	Value
Version	2.0
Related document	SPR Market-Sounding Master Document
Issuing organization	Information Systems Agency of Armenia (ISAA)

Contents

How to read this annex / This annex intentionally defines business outcomes and non-negotiable boundaries rather than prescribing screens, queue layouts, workflow diagrams, routing algorithms, status catalogues, API schemas or technical products. Vendors are expected to propose a coherent implementation approach and explain assumptions, dependencies and alternatives.

1. Purpose and document status

This annex describes the required outcomes for the SPR Case Management / Back Office capability. It supports market sounding and is not a final solution design or procurement specification.

- **Technology-neutral.** No specific low-code platform, product or architecture is mandatory for this annex.
- **Self-contained.** Vendors should be able to prepare an indicative response without receiving internal source documents.
- **Outcome-based.** The annex defines what the capability must achieve and the boundaries it must respect.
- **Non-binding.** The market-sounding exercise does not constitute a tender or commitment to procure.

2. Business objective

The objective is to provide authorized staff with a controlled internal workspace for receiving, routing, reviewing, validating, deciding and resolving SPR-related cases, while preserving the authority of SPR Core and ensuring full traceability.

Core business outcome / A case must reach the correct responsible unit, receive the required review and decision, and produce a traceable result - without direct editing of the SPR database or creation of a PSN outside SPR Core.

3. Scope and boundaries

3.1 Mandatory baseline scope

- Secure access for authorized internal users and approved operational roles.
- Automatic case creation and routing by default for supported digital submissions and exception triggers.
- Controlled manual case creation for approved offline and exceptional situations.
- Work queues, assignment, prioritization, task handling, deadlines and escalation.
- Review of submitted data, proposed changes, evidence references and validation outcomes.
- Duplicate review, clarification, correction, approval, rejection and case closure.
- Preparation and submission of approved requests to SPR Core and handling of Core outcomes.
- Exception handling for failed integrations, unmatched persons, conflicts, duplicates and rejected transactions.
- Subject- and provider-facing status/communication triggers where applicable.
- Full case history, audit, operational monitoring, reporting and controlled administration.

3.2 Separately priced optional scope

- Back Office functionality required for an optional document or certificate issuance module.
- Back Office functionality required for optional Authorized Representative processing.
- OCR-assisted evidence review or automatic extraction where separately proposed under the evidence-document scope.
- Other optional functionality explicitly identified by the vendor and excluded from the baseline price.

3.3 Out of scope

- Direct editing of the SPR database.
- Creation, selection or modification of a PSN outside SPR Core.
- Construction of SPR Core itself.
- Construction of the SPR Portal, Provider Interface or Evidence Document Management Service, except for required integrations.
- Full automation of the internal processes of external organizations.
- Generic government correspondence or enterprise-wide document management.

4. Users and required outcomes

User group	Required outcome
Back Office officer	Receive and process assigned cases; review information; request clarification; record actions and recommendations.
Reviewer / validator	Validate data, evidence and duplicate results within assigned authority.
Approver	Make or confirm an authorized decision where separation of duties is required.
Supervisor	Monitor workload, routing, overdue work, reassignment and escalation.
Auditor / operational reviewer	Review authorized case and transaction history without modification rights.
Administrator / support user	Manage approved configuration and support activities without unrestricted business-data access.

5. High-level capability areas

Capability area	Required business outcome
Case intake	Create or receive a case from approved channels, integrations or exception events with a clear source and purpose.
Routing and ownership	Route work to the responsible unit or queue based on approved ownership and business rules; allow controlled reassignment.
Work management	Provide staff with usable queues, priorities, tasks, deadlines, waiting states and escalation visibility.
Review and validation	Support review of submitted and existing data, evidence references, completeness, authority and duplicate/conflict indicators.
Clarification and correction	Request additional information or evidence and preserve the history of returned and resubmitted information.
Decision and approval	Support recommendation, approval, rejection, return for correction and recording of reasons and authority.
SPR Core interaction	Prepare and submit approved requests; receive outcomes; route failures or conflicts to the appropriate process.
Exception management	Handle manual intake, integration failures, unmatched persons, duplicate risk, Core rejection and other mandatory-review conditions.
Status and communication	Maintain consistent internal status and trigger permitted subject/provider-facing updates and notifications.
Audit, reporting and administration	Provide traceability, operational oversight, controlled configuration and reporting without weakening access controls.

Not prescribed at market-sounding stage / Exact screens, queue layouts, task allocation algorithms, workflow steps, status lists, dashboard widgets, report layouts, API schemas and technical products are not fixed by this annex. Vendors should propose a coherent approach and explain how it meets the required outcomes.

6. Processing model and logical context

The Back Office must support a default automated intake and routing model, while retaining controlled manual handling for situations that cannot be completed automatically or legally require human review.

Processing pattern	High-level use
Automatically created case	Created from a Portal application, case-based provider submission, Core/provider exception or another approved event.
Automatically routed work	Sent to the responsible unit or queue using approved ownership, data-category and operational rules.
Human-review case	Used where evidence assessment, approval, duplicate resolution, conflict handling or another legal/business decision is required.
Manual / offline case	Created only for approved offline channels, failed integrations, unmatched persons, archival/foreign evidence or similar exceptions.
Straight-through transaction monitoring	Successful approved provider-to-Core transactions may remain outside full case processing but must be visible for audit and monitoring.
Exception case	Created or routed when validation fails, a conflict/duplicate appears, Core rejects a transaction or human judgment is required.

6.1 Non-negotiable processing principles

- SPR Core remains the authoritative source of truth and performs the final registration or data update.
- Back Office users and CMS components must not directly edit the SPR database or generate a PSN.
- Automatic case creation and routing are the default where rules and ownership are known.
- Manual creation, manual assignment and routing override are controlled exception mechanisms.
- Every decision, status change, reassignment, Core interaction and evidence access must remain traceable.

6.2 Preliminary logical context

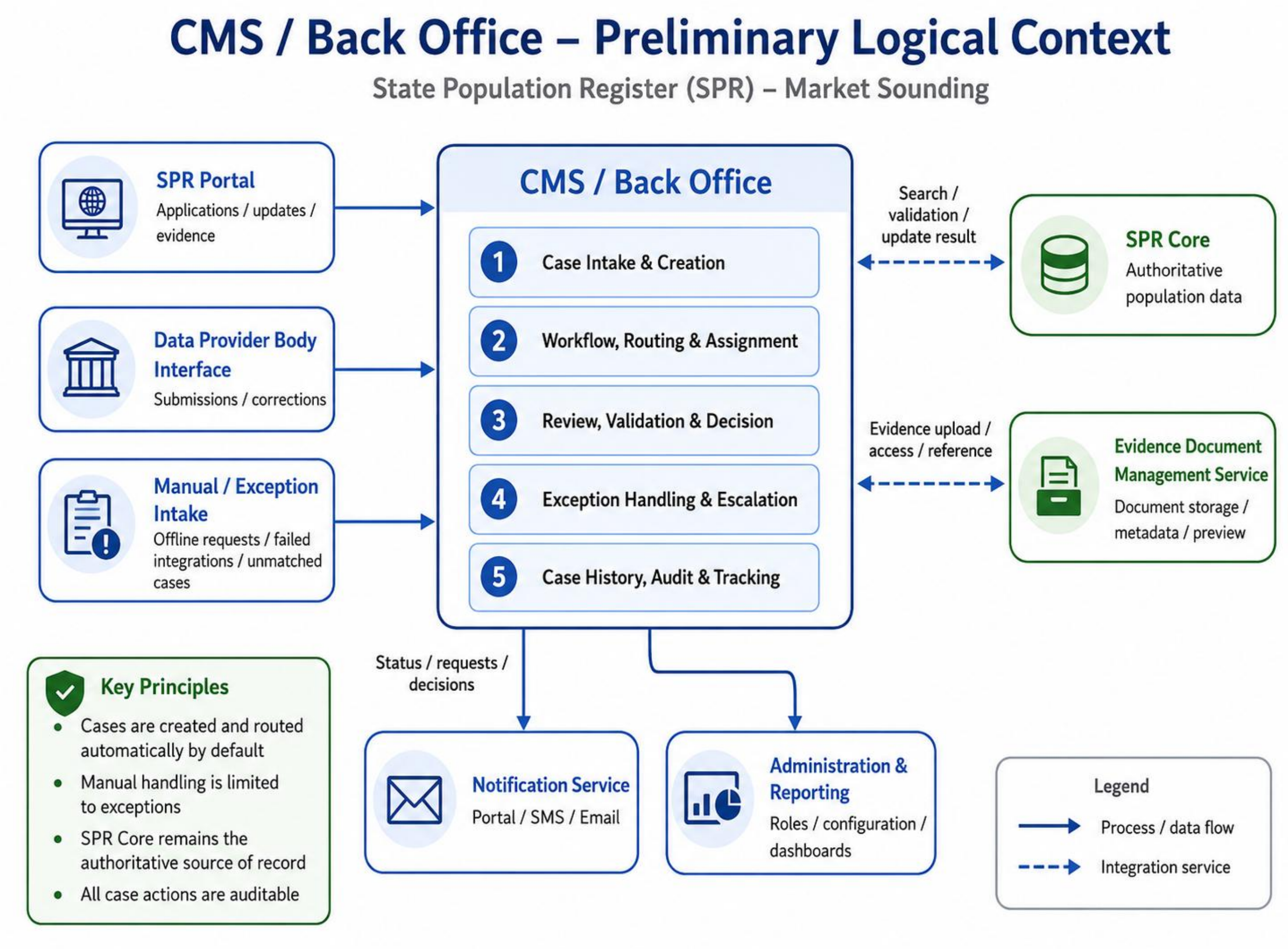

Figure 1. Preliminary logical context. The diagram is illustrative and does not prescribe a final technical architecture.

> **Interpretation /** The diagram shows the main sources, internal Back Office capability areas and external services. It does not define exact screens, queues, workflow steps, deployment components or API designs.

7. Shared requirements

Area	High-level expectation
Security and privacy	Role-, organization-, case- and task-based access; least privilege; protection of personal and restricted information.
Audit and accountability	Traceable actor, action, object, time, reason and outcome for significant case and administrative activity.
Usability and accessibility	Efficient officer workspace, understandable validation/errors, consistent navigation and practical support for high-volume work.
Configurability	Case types, ownership, routing, roles, statuses, deadlines, checklists and communication triggers should be configurable where appropriate.
Reliability and recoverability	Controlled error handling, retries, reconciliation, recovery and prevention of duplicate processing.
Maintainability	Documented interfaces, supportable components, controlled releases and minimal dependency on undocumented custom logic.
Observability	Operational monitoring of queues, integrations, exceptions, SLA, errors and capacity with actionable alerts.
Data protection by design	Data minimization, need-to-know access, protected exports and controlled evidence access.

8. Integrations and dependencies

System / service	Purpose
SPR Portal	Receive applications and responses; synchronize permitted subject-facing status, required actions and results.
Data Provider Body Interface / systems	Receive case-based submissions and exception triggers; exchange correction requests and permitted status.
SPR Core	Search/matching, duplicate check, validation, registration, authoritative update, PSN generation, transaction status and outcome handling.
Evidence Document Management Service	Secure preview/access, metadata, verification status, case linkage and audit.
IAM / SSO	Authentication, organization/role context and access control.
Notification service	Trigger and track approved Portal, SMS, email or other notification channels.
Address and other authoritative services	Approved lookup, validation or reference-data support.
Audit / monitoring platform	Security events, operational monitoring, alerting and centralized traceability where applicable.

Integration detail / Detailed API contracts, protocols, credentials, message patterns, retry rules and error catalogues are design-stage decisions. Vendors must state assumptions and propose a secure, supportable integration approach.

9. Sizing and assumptions

Parameter	Current market-sounding baseline
Registered persons	300,000+ programme population baseline.
Back Office users	1,000+.
Provider organizations	10-30.
Concurrent users	200.
Cases / transactions	100,000+ cases per year programme baseline.
Growth	Vendor should explain scaling approach and principal capacity drivers.

Sizing instruction / Unknown peak loads, document volumes and notification volumes shall not be guessed by the Customer. Vendors shall state and justify assumptions, identify capacity drivers and explain how the solution can be scaled after the design-stage sizing model is approved.

10. Preliminary MVP and full implementation

10.1 Preliminary MVP

The vendor should propose a practical MVP that demonstrates end-to-end case processing while preserving the non-negotiable boundaries in this annex. The proposed MVP should cover, at minimum:

- authorized staff access and role separation;
- automatic case intake and routing for representative digital submissions;
- controlled manual case creation for approved exceptions;
- work queues, assignment, task handling and basic SLA visibility;
- review, validation, clarification, decision and audit;
- one end-to-end correction/update case and one manual person-registration or exception case;
- SPR Core submission and outcome/exception handling;
- basic reporting, monitoring and administration.

10.2 Full implementation

The full implementation should support the approved case catalogue, all agreed operator roles, configurable routing and approval rules, provider exceptions, Core integration patterns, inter-agency review where required, operational reporting, monitoring and scalable support for the confirmed baseline.

11. Design-stage decisions

The following details are intentionally not finalized for market sounding. The required capability is part of the baseline; the exact configuration will be confirmed during analysis and design.

Decision area	To be confirmed
Final case catalogue	Priority case types, sources, closure/reopening rules and MVP sequencing.
Operator organizations and roles	Participating units, role catalogue, access scope and support responsibilities.
Data Ownership and Approval Matrix	Responsible body/unit, provider, reviewer, approver and authority by data category.
Routing and assignment rules	Ownership, data category, organization, workload, specialization, location and override rules.
Human-review and automation rules	Transactions requiring approval versus those eligible for automated processing.
Segregation of duties	Case types where the same person may not review and approve.
Manual intake channels	Approved offline sources, initiation reasons, required evidence and supervision rules.
SLA and legal deadlines	Case-specific deadlines, pause/resume conditions, warnings and escalation thresholds.
Status models and mappings	Internal, subject-facing and provider-facing terminology and permitted transitions.
SPR Core interface contracts	Detailed services, errors, retry/idempotency, asynchronous patterns and reconciliation.
Evidence review rules	Required evidence, verification responsibility, visibility, download and retention exceptions.
Reporting and performance visibility	Final report catalogue, filters, export rules and whether individual officer metrics are used.
Operational support model	Monitoring ownership, incident handling, maintenance, release and post-go-live responsibilities.

12. Vendor response requirements

The vendor response should be concise but sufficiently detailed to support market comparison. Vendors should provide:

Response area	Requested information
Understanding of need	Summary of the business problem, intended outcomes and important boundaries.
Proposed solution approach	High-level architecture, major components, configuration approach and technology choices.
Case-processing approach	Automatic intake/routing, queues, task management, review, approval, exception and audit approach.
Integration approach	SPR Core, Portal, Provider Interface/systems, evidence service, IAM, notifications and monitoring assumptions.
Security and access	Role/case/task/evidence access, segregation of duties, data protection and audit protection.
Sizing and performance	Capacity model using the confirmed baseline and justified assumptions for unknown peaks.
MVP proposal	Recommended MVP scope, sequencing, calendar duration, person-days, team and total price in AMD with VAT treatment.
Full implementation	Calendar duration, person-days, team composition and total price in AMD with VAT treatment.
Optional scope	Separate effort, duration and price for optional module impacts.
Warranty and support	Separate 12-month service description and price, including incident assumptions.
Risks and dependencies	Key Customer, Core, provider, infrastructure, legal and decision dependencies; risks and mitigation.
Deviations and alternatives	Any unsupported requirement, proposed alternative, exclusion or condition affecting price or timeline.

Market-sounding principle / Vendors are not expected to reproduce a predefined solution. They are expected to demonstrate that their proposed approach can achieve the required business outcomes, respect programme boundaries and provide credible assumptions, effort and cost information.

End of Annex B