



Enterprise Data Analytics and Reporting System

Attachment A

Enterprise Data Analytics & Reporting System

Baseline Functional Requirements
Attachment A

1. Purpose

This document defines the **baseline functional requirements** for an **Enterprise Data Analytics and Reporting System (EDARS)** delivered as a **Software-as-a-Service (SaaS)** solution. These requirements ensure the solution establishes a common "Language of Truth" across disparate systems while allowing the agency to **Modernize-in-Place** without the risk of mass data migration.

2. Scope

The EDARS Solution will:

- Securely connect to and query disparate data sources (Cloud, On-Prem, Legacy) in their original environment.
- Establish a **Semantic Governance Layer** to align metrics and definitions across sovereign programs.
- Provide **Explainable AI** grounded in governed context and auditable lineage.
- Integrate with the agency's existing identity and audit ecosystems.
- Operate **solely as a cloud-hosted SaaS solution**.

3. Baseline Functional Requirements

3.1 General SaaS & Platform Requirements

The Solution **must**:

- Operate as a **cloud-hosted SaaS platform**, fully managed by the Contractor.
- Provide a centralized **administrative console** for managing data connections, semantic models, and user permissions.
- Support **Role-Based Access Control (RBAC)** for administrative and data-stewardship functions.
- Provide a **multi-tenant or logically isolated** architecture to ensure secure data separation.
- Deliver **continuous updates** to the semantic engine and connectors without requiring customer-side infrastructure changes.
- Support **scaling** to thousands of concurrent users across multiple agency departments.

3.2 Semantic Governance & Logic Management

The Solution **must** provide a logic-abstraction layer independent of underlying data storage, including:

- **Unified Business Logic Model:** Ability to define a business metric (e.g., "Total Eligibility") once and deploy it to all dashboards and AI endpoints.
- **Definition Reconciliation Tools:** Identify and reconcile conflicting definitions (e.g., "Active Case") across different program silos.
- **Statutory Mapping:** Ability to encode legislative definitions and policy rules directly into the semantic logic to ensure audit defensibility.
- **Logic Versioning:** Maintain an immutable history of all changes made to metric calculations and business rules.

3.3 Federated Architecture & Data Sovereignty

The Solution **must** enable cross-system insights while respecting existing ownership boundaries, including:

- **Read-In-Place Connectivity:** Connect to disparate sources (e.g., SQL, Oracle, Snowflake, Mainframes) and query them without requiring physical ingestion or data duplication.
- **Security Pass-Through:** Inherit and respect existing permissions (AD/LDAP) from the source system to preserve data sovereignty.
- **Push-Down Optimization:** Delegate calculation workloads to the underlying database to minimize data transfer and latency.

3.4 AI Readiness & Explainability

The Solution **must** provide the context required for safe, non-hallucinatory AI:

- **AI with Lineage:** Provide an auditable "Click-to-Source" trace for any AI-generated insight, showing the exact metrics and logic used.
- **Contextual Guardrails:** Restrict AI models to answer only from governed metrics within the metadata layer to prevent "Black Box" errors.
- **Transparent Logic:** Display the underlying SQL or logic generated by the AI for verification by oversight bodies.

3.5 Identity, Access & Session Management

The Solution **must**:

- Integrate with the agency's **Identity Provider (IdP)** for **Single Sign-On (SSO)** via SAML 2.0 or OIDC.
- Support **Multi-Factor Authentication (MFA)** as enforced by the agency's security platform.
- Support **user and group-based policy enforcement** leveraging directory attributes (e.g., role, department).

3.6 Compliance & Security Standards

The Solution **must**:

- Follow **industry-standard security practices**, including encryption in transit (TLS 1.2+) and at rest.
- Provide **Governance Audit Logs** detailing every change to a metric, definition, or administrative permission.
- Support alignment with frameworks such as **NIST CSF, FedRAMP, CJIS, or HIPAA** as selected by the agency.

3.7 Integration & Compatibility

The Solution **must** support integration with:

- **Audit & Monitoring (SIEM):** Export of administrative and semantic change logs to central monitoring platforms.
- **Workflow Overlays:** Delivery of governed metrics directly into existing web-based applications (e.g., case management) via non-disruptive extensions.

- **Third-Party Visualization:** Provide governed data feeds to other tools (e.g., Excel, Tableau) to ensure they use the same centralized business logic.

3.8 Performance & Availability

The Solution **must**:

- Support **monthly uptime** consistent with the selected SLA (e.g., 99.99% or higher).
- Ensure query performance allows a reasonable end-user experience even when federated across multiple disparate sources.
- Document a formal approach for **service restoration** following any degradation.

3.9 Training & Support

The Solution **must** include:

- **Administrator Training:** On semantic design, federation configuration, and governance reporting.
- **Support Services:** Access to vendor support during business hours at a minimum, with documented escalation paths.
- **End-User Materials:** Documentation explaining the "governed" reporting experience and the use of lineage tools.

3.10 Optional & Value-Added Services

- **Policy Advisory Services:** Assistance in designing and tuning semantic policies tailored to specific agency risk profiles and statutory use cases.
- **Managed Administration:** Vendor or partner-provided ongoing administration and semantic model management under defined Statements of Work (SOW).
- **Advanced AI Risk Scoring:** Enhanced insights into definition inconsistencies and lineage gaps, providing a quantitative risk score for datasets prior to AI deployment.
- **Non-Production Sandbox:** An optional test environment for modeling new business logic and policy rules before they are deployed enterprise-wide.
- **Quarterly Modernization Reviews (QMR):** Regular strategic meetings to review platform adoption, performance, and recommendations for incremental modernization pathways.
- **Legacy Acceleration Workshops:** Professional services aimed at mapping high-value logic within 20+ year-old "un-replaceable" legacy systems.

4. Vendor Response Matrix

Ref ID	Requirement Summary	Mandatory	Vendor Response (Meets / Partial / No)	Notes / Reference
BR-1.1	SaaS-only, cloud-hosted delivery model	Y		
BR-1.2	Centralized administrative console for configuration	Y		
BR-2.1	Reusable Business Logic Layer/MetadataModel	Y		
BR-2.2	Automated versioning and audit trail for logic changes	Y		
BR-3.1	Federated "Read-In-Place" query capability	Y		
BR-3.2	Native, high-performance connectors for diverse sources	Y		
BR-4.1	AI answers grounded in governed metrics	Y		
BR-4.2	Click-to-source auditable lineage for AI insights	Y		
BR-5.1	Non-disruptive workflow overlays (Zero-Click)	Y		
BR-6.1	Support for Identity Standards (SSO/MFA/SAML)	Y		
BR-7.1	Uptime target consistent with defined RFQ SLA	Y		
BR-8.1	Comprehensive Admin and Data Steward training	Y		
OR-9.1	Optional: Policy Advisory/Mapping Services	N		
OR-9.2	Optional: Advanced AI Risk/Readiness Scoring	N		
OR-9.3	Optional: Managed Administration/Ongoing SOW	N		