

SOL ENGINEERING SERVICES

The Daniel Group LLC

SUPPORTING DOCUMENTATION PACKAGE

ALICE: Adaptive Labor Intelligence and Capacity Engine

SBIR Topic DLA26BZ03-NV011 | Defense Logistics Agency

ARTIFACT 3 OF 11

Component Catalog

Document Version 1.0 | July 2026

Status: DRAFT — Pending Gate-3 Stakeholder Review

Classification: Unclassified

Document Control

Field	Value
Artifact ID	SDP-ART-03
Artifact Title	Component Catalog
Artifact Dependencies	SDP-ART-01 (Research Log) — Approved; SDP-ART-02 (ADR Register) — Approved Gate-2
Package	ALICE Supporting Documentation Package (SDP)
Source Documents	ALICE TNA v1.0 Sections 7, 10, 11, 14, 15, 18, 20; ALICE PRD v1.0; SDP-ART-01; SDP-ART-02
Prepared By	SOL Engineering Services | The Daniel Group LLC
Prepared For	Defense Logistics Agency | SBIR DLA26BZ03-NV011
Version	1.0 (Draft)
Date	July 2026
Classification	Unclassified
Status	Draft — Pending Gate-3 stakeholder approval before Artifact 4 is produced
Component Count	12 logical components (LC-01 through LC-12)
ID Convention	All IDs preserved from TNA v1.0 and SDP-ART-02. No IDs modified.

1. Purpose and Scope

This Component Catalog is Artifact 3 of the ALICE Supporting Documentation Package. It provides the authoritative, implementation-planning-ready description of each of the twelve logical service components that constitute the ALICE architecture, as established in TNA Section 10 and formalized through the ADR Register (SDP-ART-02).

For each component, the catalog provides: a stable identifier; the service layer it occupies; its deployment phase; its purpose and full responsibility list; all inputs and outputs with their data classification; all required interfaces with directionality, protocol class, and security controls; the data zones it is authorized to access and in what mode; performance and availability obligations; security and privacy considerations; NIST SP 800-53 control family coverage; ADRs that govern the component's design; functional domains it supports; operational workflows it participates in; and all PRD requirements to which it is traceable.

The catalog does not prescribe implementation technologies, vendors, programming languages, or hosting platforms. All capability descriptions use technology-neutral terminology consistent with TNA v1.0 and ADR-001 (Modular Service-Oriented Architecture). Items labeled [INFERRED] represent architecture requirements reasoned from PRD and CONOPS content not explicitly stated in the source but necessary for completeness. Items labeled [OPEN] identify unresolved questions requiring stakeholder resolution.

2. Component Architecture Overview

2.1 Layer Structure

The twelve components are organized into six service layers aligned to the ALICE OV-1 architecture plus a cross-cutting infrastructure and governance layer. Components within a given layer may not directly access the internal state of components in other layers; all cross-layer communication uses defined interface contracts.

Layer	Components	OV-1 Alignment	Phase
Layer 1 — Interface Control	LC-01	Data Ingestion and Enrichment (external boundary)	I and II
Layer 2 — Data Ingestion and Enrichment	LC-02, LC-03	Data Ingestion and Enrichment (internal pipeline)	I and II
Layer 3 — Organizational Ontology	LC-04	Organizational Ontology	I and II
Layer 4 — Synthetic Workforce Engine	LC-05	Synthetic Workforce Engine	I and II
Layer 5 — Agent-Based Simulation	LC-06	Agent-Based Simulation	I and II
Layer 6 — Decision Support Interface	LC-07	Decision Support Interface	I and II
Cross-Cutting — Infrastructure and Governance	LC-08, LC-09, LC-10, LC-11, LC-12	All layers (supporting)	I and II

2.2 Component Summary Index

ID	Name	Layer	Primary Purpose	Data Zone Access	Phase I MVP?	Governing ADR(s)
LC-01	Interface Control and API Management	Layer 1	Authenticate users; enforce access controls at the system boundary; route API requests.	None (session metadata only; no workforce data)	Yes	ADR-001, ADR-004
LC-02	Data Ingestion and De-Identification	Layer 2	Pull source data; detect and remove PII; write de-identified records to Processed Zone.	Raw (transient, in-flight); Processed (write)	Yes	ADR-001, ADR-002, ADR-009
LC-03	Schema Abstraction and	Layer 2	Translate DCPDS and DCHRMS source	None (pre-zone, in-	Yes	ADR-001,

ID	Name	Layer	Primary Purpose	Data Zone Access	Phase I MVP?	Governing ADR(s)
	Integration Adapter		schemas into the ALICE canonical data model.	flight translation)		ADR-003
LC-04	Organizational Ontology and Twin State	Layer 3	Maintain position/role graph; compute readiness indicators; archive historical state.	Processed (read); Analytical (write and read)	Yes	ADR-001, ADR-002
LC-05	Synthetic Workforce Engine	Layer 4	Generate, validate, and govern the privacy-preserving synthetic workforce population.	Processed (read); Synthetic (write)	Yes	ADR-001, ADR-002, ADR-007
LC-06	Agent-Based Simulation Engine	Layer 5	Execute ABM scenario simulations against the synthetic population; return readiness forecasts.	Synthetic (read); Analytical (write — results)	Yes	ADR-001, ADR-002, ADR-008
LC-07	Decision Support Interface	Layer 6	Render role-differentiated readiness dashboards; support scenario initiation and export.	Analytical (read)	Yes	ADR-001, ADR-002
LC-08	Identity and Access Management (IAM)	Cross-Cutting	Manage user identities, roles, activity scopes, session lifecycle, and service credentials.	None (identity metadata only)	Yes	ADR-001, ADR-004
LC-09	Immutable Audit Logging	Cross-Cutting	Receive, store, and protect all audit events from all services in an append-only log.	Audit Log Store (write — all services; read — authorized reviewers)	Yes	ADR-001, ADR-005
LC-10	Configuration Management	Cross-Cutting	Store, version, and serve all operational configuration parameters.	Configuration Store (write — System Administrator; read — all services)	Yes	ADR-001, ADR-010
LC-11	Observability and Health Monitoring	Cross-Cutting	Monitor service health; generate operational alerts for failures and anomalies.	Read from all service health endpoints; no	Yes	ADR-001

ID	Name	Layer	Primary Purpose	Data Zone Access	Phase I MVP?	Governing ADR(s)
				workforce data		
LC-12	Secrets Management	Cross-Cutting	Store and provide secure retrieval of all credentials and cryptographic key material.	Secrets Store (write — initial provisioning; read — authorized services)	Yes	ADR-001, ADR-004

2.3 Data Zone Access Matrix

The following matrix documents which component has read (R), write (W), or no access (—) to each of the four data zones defined in ADR-002. Access is enforced at the service account credential level per ADR-009.

Component	Raw Zone	Processed Zone	Synthetic Zone	Analytical Zone	Audit Log Store	Config Store	Secrets Store
LC-01	— (no persistent data)	—	—	—	W (access events)	R	R (session signing material)
LC-02	R (transient in-flight)	W	—	—	W (ingestion events)	R	R (source credentials)
LC-03	R (in-flight, pre-zone)	—	—	—	W (schema events)	R (schema mappings)	—
LC-04	—	R	—	W / R	W (ontology events)	R (thresholds)	R (zone credentials)
LC-05	—	R (training input)	W	—	W (generation events)	R (generation params)	R (zone credentials)
LC-06	—	—	R	W (results)	W (scenario events)	R (scenario params)	R (zone credentials)
LC-07	—	—	—	R	W (user action events)	R (display	R (session tokens)

Component	Raw Zone	Processed Zone	Synthetic Zone	Analytical Zone	Audit Log Store	Config Store	Secrets Store
						config)	
LC-08	—	—	—	—	W (IAM events)	R (role definitions)	W / R (service credentials)
LC-09	—	—	—	—	W / R (log service)	—	R (log signing keys)
LC-10	—	—	—	—	W (config change events)	W / R	—
LC-11	—	—	—	—	W (health alert events)	R (alert thresholds)	—
LC-12	—	—	—	—	W (secrets events)	—	W / R (master store)

3. Component Detail Records

LC-01: Interface Control and API Management Component

Layer: Layer 1 — Interface Control	**OV-1 Layer #**: 1	**Phase**: Phase I and II	**Status**	**Required**

Purpose	Controls all inbound access to ALICE services. Enforces authentication and authorization at the system boundary before any request reaches an application service. Routes authenticated requests to the appropriate downstream component.
Responsibilities	1. Validate DoD CAC-based authentication credentials against DoD PKI trust anchors, including certificate revocation status check. 2. Issue role-scoped session tokens encoding user identity, assigned role, assigned activity scope, and session expiration time. 3. Route authenticated requests to the appropriate service component based on request type. 4. Enforce API access controls; reject unauthenticated and unauthorized requests before they reach application services. 5. Enforce rate limiting to protect against denial-of-service conditions. 6. Write access audit events (login, logout, failed login, request denied) to LC-09. 7. Enforce TLS 1.2 or higher on all inbound connections.
Inputs	User authentication requests (CAC certificate + authentication challenge). API calls from authenticated users (with session token). Service-to-service calls with service identity credentials. Certificate revocation status from DoD PKI infrastructure.

Outputs	Authenticated session tokens (role-scoped, activity-scoped, time-limited). Routed API requests to downstream service components. Access denial responses to unauthorized requestors. Access audit events to LC-09.
Data Handled	Session credentials (transient, never persisted). Authentication tokens (transient). Request metadata (transient). No workforce data of any classification is handled by this component.
Data Zone Access	None. LC-01 does not access any of the four data zones defined in ADR-002.
Required Interfaces	→ DoD PKI / CAC Authority (INT-06): inbound certificate validation; encrypted; one per session. → LC-08 (IAM Service): role and scope resolution per authenticated identity; synchronous query. → LC-09 (Audit Logging): write-only; access events delivered on every authentication and authorization action. → All ALICE application services (LC-02 through LC-07): outbound routing of authenticated requests.
Performance Obligations	Maximum 200ms added latency to normal user request processing (Source-Derived from TNA LC-01 description). Must scale to support 20 or more concurrent users without degradation (REQ-NF-003).
Availability	Part of the critical path for all user-initiated operations. Availability obligation of LC-01 is subsumed in the system-wide 99.5% availability target during operational hours (REQ-NF-004). Failure of LC-01 blocks all user access.
Security Considerations	First enforcement point for role-based access control. Compromise of LC-01 would expose all downstream services. Certificate revocation check must occur on every session initiation, not only at initial registration. Rate limiting must apply before the authentication step to prevent credential brute-force attacks. Session tokens must be cryptographically signed using key material from LC-12. Token signatures must be verifiable by downstream services without contacting LC-01 on every request (to avoid LC-01 as a synchronous bottleneck on all service calls).
NIST SP 800-53 Controls	IA-2 (Identification and Authentication — Organizational Users): CAC validation at this boundary. IA-2(1) (Multi-Factor Authentication to Privileged Accounts): enforced here. AC-3 (Access Enforcement): deny-by-default; only authenticated, authorized requests pass. AC-12 (Session Termination): enforced via token expiration and active revocation signal from LC-08. SC-8 (Transmission Confidentiality and Integrity): TLS 1.2+ enforced at this boundary for all inbound connections. AU-2 / AU-3 (Event Logging / Content): access events written to LC-09 on every transaction.
Governing ADRs	ADR-001 (modular component; defined interface contract required); ADR-004 (identity-centric security — this component is the Policy Enforcement Point at the system boundary); ADR-009 (read-only external integration — this component enforces the user/service identity constraint at the entry

	point)
Functional Domains	FD-1 (User Access and Identity Management)
Operational Workflows	All four operational workflows (OW-1 through OW-4) — all user-initiated and system-initiated actions cross this boundary.
Phase I vs. Phase II	Phase I: CAC integration confirmed as required; ASM-008 documents the risk that CAC may not be available in the Phase I demonstration environment. If not available, an interim MFA mechanism shall be implemented with CAC targeted for Phase II. Phase II: Full ZTA enforcement including device trust evaluation integrated into this boundary per ADR-004.
PRD Requirements	REQ-SEC-001 (MFA / CAC); REQ-SEC-002 (RBAC); REQ-SEC-003 (least privilege); REQ-SEC-004 (activity-scoped access); REQ-NF-003 (concurrent users); REQ-NF-010 (response time)
Open Questions	[OPEN] ASM-008 / RISK-004: CAC integration feasibility in Phase I environment must be confirmed at contract award.

LC-02: Data Ingestion and De-Identification Service

Layer: Layer 2 — Data Ingestion and Enrichment	**OV-1 Layer #**: 2	**Phase**: Phase I and II	**Status**	**Required**

Purpose	Pulls workforce data from authoritative DLA source systems on a defined schedule, validates data against the canonical schema, detects and removes residual PII fields, applies de-identification transformation, and writes de-identified records to the Processed Zone. Provides the sole write pathway to the Processed Zone.
Responsibilities	1. Execute scheduled ingestion jobs on configured frequency (daily for position/person data; weekly for certification and workload metrics; annually for performance calibration data). 2. Authenticate to source systems using read-only service account credentials retrieved from LC-12. 3. Accept pre-translated canonical-model records from LC-03 for validation and de-identification. 4. Validate records against the canonical schema maintained in LC-10. 5. Detect residual PII fields using the PII detection capability. Reject records containing PII; log rejection with field identification; abort ingestion if PII is detected beyond configured tolerance. 6. Apply de-identification transformation: field removal of direct identifiers, tokenization of quasi-identifiers, and aggregation of sensitive attributes to aggregate bands. 7. Write validated, de-identified records to the Processed Zone. 8. Invoke LC-04 to trigger ontology refresh upon successful ingestion completion. 9. Fall back to OPM FWD proxy data when DLA-specific data is unavailable, setting proxy flag on all records sourced from proxy. 10. Log all ingestion events (schedule trigger, record counts, validation results, PII rejection events, completion status) to LC-09. 11. Alert LC-11 on ingestion failure or anomaly (record count delta

	exceeding 20% from prior day).
Inputs	Canonical-model records from LC-03 (pre-translated from DCPDS, DCHRMS, DLA TMS, DPMAP, or EBS). OPM FWD bulk data (public; when used as proxy). Schema registry from LC-10. Service account credentials from LC-12. Ingestion schedule configuration from LC-10.
Outputs	De-identified records written to the Processed Zone (CUI). Ingestion completion signal to LC-04. Ingestion audit events to LC-09. Schema validation error reports (configuration-logged). PII rejection records (audit-logged with field identifiers). Health status signals to LC-11.
Data Handled	Raw workforce records from LC-03: transient, in-flight only. Never persisted. May contain Privacy Act-protected PII. Transformation to de-identified form must complete before any persistence. De-identified records: persistent in Processed Zone. CUI. No individual identifying data.
Data Zone Access	Raw Zone: read (transient, in-flight only). Processed Zone: write. No access to Synthetic or Analytical Zones.
Required Interfaces	← LC-03 (Schema Abstraction): receives canonical-model records for validation and de-identification. → Processed Zone: write interface; encrypted; access credentials from LC-12. → LC-04 (Ontology Service): signals ingestion completion to trigger ontology refresh. → LC-09 (Audit Logging): write-only; all ingestion events. → LC-10 (Configuration Management): reads schema registry, schedule configuration, PII field definitions. → LC-11 (Observability): health status reporting; failure alert delivery. ← LC-12 (Secrets Management): retrieves source system service account credentials.
Performance Obligations	Full ingestion cycle must complete within the 24-hour data currency window from source extract availability (REQ-NF-001). DCPDS data latency of up to 48 hours is an upstream constraint outside ALICE control (RL-04).
Security Considerations	Raw records containing PII must never be written to any persistent storage. The in-flight transformation must be atomic: if the de-identification step fails, the record is discarded, not persisted. PII detection capability must be tested and validated before Phase I demonstration. Test cases must include records with known PII fields in expected and unexpected positions. Service account credentials for source system access must be stored exclusively in LC-12, never in configuration files or application code. Credentials must be rotated on the schedule defined in the System Security Plan. Schema validation must occur before de-identification. A schema mismatch may indicate a source system change that could affect de-identification correctness.

NIST SP 800-53 Controls	SI-12 (Information Management and Retention): data handling rules enforced here (raw records not retained). SC-28 (Protection of Information at Rest): Processed Zone encryption enforced at write. AU-2 / AU-3: all ingestion events logged with required content. AC-4 (Information Flow Enforcement): PII detection and de-identification enforce the Privacy Act boundary. IA-5 (Authenticator Management): source system credentials managed via LC-12.
Governing ADRs	ADR-001 (modular component); ADR-002 (sole write pathway to Processed Zone; Raw Zone records are transient); ADR-009 (read-only source system access enforced at service account level)
Functional Domains	FD-2 (Data Ingestion and Privacy Transformation)
Operational Workflows	OW-1 (Continuous Organizational Readiness Monitoring) — primary workflow actor
PRD Requirements	REQ-F-001 through REQ-F-006; REQ-NF-001; REQ-NF-013; REQ-INT-001 through REQ-INT-005
Open Questions	[OPEN] OQ-002 (GTPOC authority to execute data use agreement — determines when LC-02 can ingest DLA-specific data vs. OPM FWD proxy). [OPEN] OQ-009 (DLA operational hours — affects ingestion schedule window).

LC-03: Schema Abstraction and Integration Adapter Service

Layer: Layer 2 — Data Ingestion and Enrichment	**OV-1 Layer #**: 2	**Phase**: Phase I and II	**Status**	**Required**

Purpose	Provides a stable, schema-agnostic interface between ALICE and its upstream source systems. Translates native source system records (DCPDS schema or DCHRMS schema) into the ALICE canonical data model. Insulates all downstream ALICE components from source system schema changes, particularly the DCPDS-to-DCHRMS migration.
Responsibilities	1. Maintain versioned schema mapping definitions for both DCPDS and DCHRMS data structures. 2. Translate source system records from native schema into the ALICE canonical data model before handing records to LC-02. 3. Support dual-schema operation simultaneously: some DLA components may provide DCPDS-format data while others provide DCHRMS-format data during the transition period. 4. Detect source schema deviations (fields not matching expected schema) and alert LC-11 before attempting translation. 5. Maintain schema mapping configuration in LC-10 as version-controlled configuration data. 6. Log all schema translation events (source schema version, translation result, deviation flags) to LC-09.
Inputs	Source system data extracts or API responses in native DCPDS or DCHRMS schema.

	DLA TMS certification export data. Schema mapping configuration from LC-10.
Outputs	Records in ALICE canonical data model format, delivered to LC-02 for validation and de-identification.
Data Handled	Source system records in native schema (transient, pre-zone). These records may contain PII and are treated as Raw Zone data. They are never persisted in ALICE storage at this stage.
Data Zone Access	Pre-zone: handles raw source records in-flight before any zone boundary is crossed. Records in this component are considered Raw Zone data per ADR-002 classification.
Required Interfaces	← INT-01 (DCPDS / DCHRMS): receives source system data extracts or API responses. ← INT-02 (DLA TMS): receives certification data exports. → LC-02 (Data Ingestion): delivers canonical-model records for processing. → LC-09 (Audit Logging): schema translation events. → LC-10 (Configuration Management): reads and writes schema mapping configuration. → LC-11 (Observability): schema deviation alerts.
Performance Obligations	Schema translation must not add material latency to the ingestion pipeline. Translation is a synchronous, in-memory operation per record; it is not a blocking I/O operation. [INFERRED: translation throughput must be sufficient to process a full daily delta within the 24-hour currency window.]
Security Considerations	Schema mapping configuration is a security-relevant artifact: an incorrect mapping could cause PII fields to be mislabeled as non-identifying, bypassing the de-identification step in LC-02. Schema mapping changes must require administrator authorization and must be logged as configuration change events. Source system records handled by this component are Raw Zone data and carry the same handling requirements as in LC-02: no persistence, in-flight only.
NIST SP 800-53 Controls	CM-3 (Configuration Change Control): schema mapping configuration is version-controlled and change-logged. SI-7 (Software and Firmware Integrity): schema mappings must be integrity-checked before use.
Governing ADRs	ADR-001 (modular component; dedicated to schema abstraction); ADR-003 (this component is the decision implementation); ADR-010 (schema mappings stored as configuration in LC-10)
Functional Domains	FD-2 (Data Ingestion and Privacy Transformation)
Operational Workflows	OW-1 (Continuous Organizational Readiness Monitoring) — upstream pipeline stage
PRD Requirements	REQ-INT-001 (integration abstraction for DCPDS/DCHRMS transition); REQ-NF-014 (standard data exchange formats)
Open Questions	[OPEN] OQ-004 (DCHRMS migration schedule for pilot sub-component — determines Phase I scope of DCHRMS schema mapping). [OPEN] OQ-008 (DLA TMS extract format — determines whether TMS schema mapping is standard or requires custom development).

LC-04: Organizational Ontology and Twin State Service

Layer: Layer 3 — Organizational Ontology	**OV-1 Layer #**: 3	**Phase**: Phase I and II	**Status**	**Required**

Purpose	Maintains the ALICE organizational model as a directed graph of positions, roles, workflow dependencies, and readiness indicators. Updates the model on each successful ingestion cycle. Archives historical twin states for trend analysis and backtesting. Serves ontology data to authorized services through role-scoped and activity-scoped query interfaces.
Responsibilities	1. Maintain position nodes with defined attributes: occupational series, grade, fill status, required certifications and currency status, mission function assignment, workflow dependencies, and the five leading workforce degradation indicators identified in RL-06. 2. Maintain role nodes with defined workflow dependency relationships: prerequisite roles, dependent roles, and single-point-of-failure identification. 3. Compute and update readiness indicators for each mission function area on each ingestion cycle. 4. Evaluate readiness indicators against threshold values configured in LC-10; generate alert events when thresholds are crossed. 5. Maintain historical snapshots of twin state at a defined archival frequency for trend analysis and backtesting (minimum 12 months of snapshots). 6. Serve ontology data to LC-07 (Decision Support Interface) through a role-scoped, activity-scoped read interface. 7. Serve synthetic population training scope data to LC-05 through a read interface limited to position and role structural data. 8. Log all ontology updates, readiness indicator computations, threshold crossing events, and historical snapshot creation events to LC-09.
Inputs	Ingestion completion signal from LC-02. De-identified records from the Processed Zone. Threshold configuration from LC-10. Readiness computation rules from LC-10. Ontology read requests from LC-07 and LC-06 (structural data for agent model).
Outputs	Updated organizational graph in the Analytical Zone. Readiness indicator values (Analytical Zone). Alert events (to LC-11 for delivery to users). Historical state snapshots (Analytical Zone). Ontology read responses to LC-07 (role-scoped, activity-scoped). Audit events to LC-09.
Data Handled	Position data (CUI); role data (CUI); readiness indicators (CUI internal analytical output). No Privacy Act records; all data is derived from de-identified Processed Zone records.
Data Zone Access	Processed Zone: read. Analytical Zone: read and write (ontology graph, readiness indicators, historical snapshots).
Required Interfaces	← LC-02: ingestion completion signal. ← Processed Zone: reads de-identified records for ontology update.

	← LC-10: reads threshold configuration and computation rules. → Analytical Zone: writes ontology graph, readiness indicators, historical snapshots. → LC-07: serves role-scoped, activity-scoped ontology read requests. → LC-09: writes ontology update and threshold event audit records. → LC-11: delivers health status and threshold alert events.
Performance Obligations	Full ontology refresh (readiness indicator recomputation) must complete within the 24-hour data currency window for an organizational scope of up to 30,000 positions (REQ-NF-001; REQ-NF-006). Ontology read responses to LC-07 must return within a timeframe that does not contribute materially to the 5-minute scenario execution threshold. [INFERRED: Graph query complexity must be evaluated at Phase II design for enterprise scale; $O(n^2)$ query patterns are not acceptable at 30,000 positions.]
Security Considerations	Activity scope enforcement must occur at the query level within this service, not at the LC-07 presentation layer. A query that exceeds the requesting user's activity scope must be rejected at the source. Historical snapshot data is CUI and must be stored with the same encryption and access controls as current ontology data. Threshold configuration values must be readable by this component but writable only by authorized administrators through LC-10.
NIST SP 800-53 Controls	AC-4 (Information Flow Enforcement — activity scope); AC-3 (Access Enforcement — scope-limited query responses); AU-2 (Event Logging — readiness updates and threshold events).
Governing ADRs	ADR-001 (modular component); ADR-002 (reads from Processed Zone, writes to Analytical Zone — distinct zone credentials per ADR-002)
Functional Domains	FD-3 (Organizational Ontology Management)
Operational Workflows	OW-1 (Continuous Organizational Readiness Monitoring) — primary actor; OW-4 (backtesting — historical snapshot provider)
PRD Requirements	REQ-F-007; REQ-F-008; REQ-F-009; REQ-F-019; REQ-F-020; REQ-F-021; REQ-F-022; REQ-NF-001; REQ-NF-006
Open Questions	[OPEN] OQ-001 (pilot sub-component selection — determines initial ontology scope and Phase I position count). [INFERRED] Five leading degradation indicators from RL-06 must be explicitly included in ontology attribute specification.

LC-05: Synthetic Workforce Engine Service

Layer: Layer 4 — Synthetic Workforce Engine	**OV-1 Layer #**: 4	**Phase**: Phase I and II	**Status**	**Required**

Purpose	Generates a statistically faithful, privacy-preserving synthetic workforce population from de-identified records in the Processed Zone. Validates the population for distributional fidelity and differential privacy compliance before promoting it to the Synthetic Zone. Governs all synthetic data export requests through a workflow requiring Data Steward authorization.

Responsibilities	1. Load de-identified records from the Processed Zone as generative model training input. 2. Apply a privacy-preserving generative model with differential privacy noise injection during training, targeting epsilon not exceeding 1.0. 3. Generate the synthetic workforce population. 4. Execute fidelity validation: KS test for continuous variables; chi-squared test for categorical variables. Target: distributional deviation within 5% across all tracked attributes. 5. Execute privacy validation: membership inference attack simulation. Target: attack success rate not exceeding 50% (random chance). 6. If both validations pass, promote the synthetic population to the Synthetic Zone with generation metadata (epsilon applied, fidelity results, privacy results, training dataset version, generation timestamp). 7. If either validation fails, quarantine the candidate population; log the failure; do not promote. Preserve the prior validated population as active. 8. Support the synthetic data export workflow: receive export requests, route to Data Steward authorization, generate export file from current validated population, deliver via authorized channel, attach provenance metadata, log export event to LC-09. 9. Log all generation, validation, and export events to LC-09.
Inputs	De-identified records from the Processed Zone (training input). Generation configuration from LC-10 (epsilon target, training parameters, generation schedule). Validation threshold configuration from LC-10. Export requests from authorized requesters (via LC-07 or administrative interface). Data Steward authorization decisions (from export authorization workflow).
Outputs	Validated synthetic population written to the Synthetic Zone (CUI). Generation metadata record written to Synthetic Zone (compliance artifact). Fidelity and privacy validation reports. Synthetic data export files with provenance metadata (CUI). Audit events to LC-09 for all generation, validation, and export events. Quarantine records for failed generations (logged, not promoted).
Data Handled	Processed Zone records (read; training input; transient within the training environment). Synthetic population (write; persistent; CUI per ADR-007). Generation metadata (compliance artifact; retained per audit schedule).
Data Zone Access	Processed Zone: read (training input). Synthetic Zone: write (validated populations and metadata). No access to Raw or Analytical Zones.
Required Interfaces	← Processed Zone: reads de-identified records for model training. → Synthetic Zone: writes validated synthetic populations and generation metadata. ← LC-10: reads generation and validation configuration. → LC-09: writes all generation, validation, and export audit events. → LC-11: reports generation health status and failure alerts. ← LC-12: retrieves zone access credentials. Export delivery channel: outbound to authorized requester via approved secure transfer mechanism.
Performance	Synthetic population regeneration must complete without data loss or corruption (REQ-NF-005). Atomicity is required: the prior population

Obligations	remains active until the new population passes both validations. [INFERRED: Generation cycle duration is not formally specified in the PRD. For Phase I, generation on demand plus scheduled monthly cycle is the expected pattern. Phase II schedule must be defined before Phase II deployment.]
Security Considerations	The generative model training environment must be isolated from LC-06 and LC-07. Training input data (de-identified records) must not be accessible to simulation or decision support services during or after training. Generation metadata is a compliance artifact required for RMF assessment, CMMC audit, and PIA support. It must be retained for the audit retention period applicable to the Synthetic Zone. Export files carry CUI marking per ADR-007 pending formal PIA classification determination. All export files must have cryptographic hash generated and logged at the time of export. The hash is the primary integrity verification mechanism for exported data.
NIST SP 800-53 Controls	SC-28 (Protection at Rest — synthetic zone encryption); AU-2 (Event Logging — generation and export events); AC-4 (Information Flow — export governance workflow); SI-12 (Information Management — quarantine and retention of failed generations).
Governing ADRs	ADR-001 (modular component); ADR-002 (reads Processed Zone, writes Synthetic Zone — distinct credentials); ADR-007 (synthetic population treated as CUI pending PIA — enforced here by CUI marking on export)
Functional Domains	FD-4 (Synthetic Population Generation and Governance)
Operational Workflows	OW-3 (Synthetic Data Export — primary actor); OW-4 (Synthetic Population Regeneration — primary actor)
PRD Requirements	REQ-F-015; REQ-F-016; REQ-F-017; REQ-F-018; REQ-NF-005; REQ-NF-008; REQ-COMP-004
Open Questions	[OPEN] OQ-006 (NIST SP 800-188 finalization — may affect export marking and PIA framework). [OPEN] OQ-001 (pilot sub-component selection — determines training corpus size; must meet ASM-003 minimum of 300 positions).

LC-06: Agent-Based Simulation Engine Service

Layer: Layer 5 — Agent-Based Simulation	**OV-1 Layer #**: 5	**Phase**: Phase I and II	**Status**	**Required**

Purpose	Executes agent-based simulations of workforce disruption scenarios against the current validated synthetic population. Returns time-series readiness forecasts with confidence intervals derived from Monte Carlo sampling. Supports preset and custom scenario types.
Responsibilities	1. Accept validated scenario parameters from LC-07 (Decision Support Interface) for authorized users. 2. Retrieve the current validated synthetic population from the Synthetic Zone. 3. Instantiate agents from synthetic population attributes, with each agent carrying its occupational series, grade band, certification profile, tenure

	band, and performance tier. 4. Apply the initiating scenario event to the agent set: departure of a target position agent (Key Departure), workload demand increase (Workload Surge at 25%, 50%, or 100%), certification pipeline shortfall (Pipeline Shortfall), or geographic redistribution (Geographic Reallocation). 5. Execute ABM simulation for the defined time horizon (default 90-day; configurable per scenario library). 6. Run Monte Carlo sampling across the synthetic population to generate confidence intervals for all forecast outputs. 7. Compute time-series readiness forecast: projected mission capacity as percentage of baseline, by mission function area. 8. Compute ranked at-risk position list. 9. Compute response option comparison if multiple response options are specified in the scenario parameters. 10. Return structured results to LC-07. 11. Write scenario run record (user, scenario type, parameters, duration, output reference) to LC-09. 12. Write simulation results to the Analytical Zone for historical reference.
Inputs	Validated scenario parameters from LC-07 (scenario type, target position, timeline, response options). Current validated synthetic population from the Synthetic Zone. Scenario library configuration from LC-10.
Outputs	Time-series readiness forecast with confidence intervals. Ranked at-risk position list. Response option comparison table. Scenario run record to LC-09 (audit artifact). Simulation results to Analytical Zone (for historical review and backtesting).
Data Handled	Synthetic population data: read from Synthetic Zone; not persisted within the simulation service after scenario execution. Scenario results: CUI; written to Analytical Zone.
Data Zone Access	Synthetic Zone: read-only. Analytical Zone: write (simulation results). No access to Raw or Processed Zones per ADR-008.
Required Interfaces	← LC-07 (Decision Support Interface): receives scenario initiation requests with validated parameters. ← Synthetic Zone: reads current validated synthetic population. → LC-07: returns structured scenario results. → Analytical Zone: writes scenario run results. → LC-09: writes scenario run audit records. ← LC-10: reads scenario library configuration and parameter ranges. ← LC-12: retrieves Synthetic Zone access credentials. → LC-11: reports simulation health status.
Performance Obligations	Preset scenario results must be returned within 5 minutes at the 95th percentile under normal load (REQ-NF-002; REQ-F-012). Custom scenario results must be returned within 15 minutes at the 95th percentile (REQ-F-013). Must support 20 or more concurrent users without degrading preset scenario execution time (REQ-NF-003). Horizontal scaling or parallel execution architecture is required.

	If a scenario exceeds the time limit, the user must be notified of expected completion time and offered a cancellation option (CONOPS Workflow 2 exception handling).
Security Considerations	The simulation engine has no access to the Raw or Processed Zones (ADR-008). Simulation engine service account credentials must not be provisioned to those zones. Scenario results must not contain data that could re-identify any individual from the underlying de-identified or source datasets. Results report aggregate population-level outcomes only. User's activity scope must be enforced on the scenario parameter validation step: a user may not initiate a scenario against a position in an activity outside their assigned scope.
NIST SP 800-53 Controls	AC-4 (Information Flow Enforcement — synthetic-zone-only access); AC-3 (Access Enforcement — activity scope on scenario parameters); AU-2 (Event Logging — scenario run records); SC-28 (simulation results encrypted at rest in Analytical Zone).
Governing ADRs	ADR-001 (modular component); ADR-002 (Synthetic Zone read, Analytical Zone write); ADR-008 (Candidate — Synthetic Zone only; no Processed Zone access)
Functional Domains	FD-5 (Scenario Simulation)
Operational Workflows	OW-2 (Scenario Planning — primary actor)
PRD Requirements	REQ-F-010; REQ-F-011; REQ-F-012; REQ-F-013; REQ-F-014; REQ-NF-002; REQ-NF-003
Open Questions	[OPEN] CON-011 / ASM-005: ABM framework license must be confirmed before Phase I Month 2. [INFERRED] Parallel execution architecture for concurrent user support must be specified in Phase I technical design.

LC-07: Decision Support Interface Service

Layer: Layer 6 — Decision Support Interface	**OV-1 Layer #**: 6	**Phase**: Phase I and II	**Status**	**Required**

Purpose	Presents readiness assessments, scenario results, and threshold alerts to authenticated, role-differentiated operational users through a web-based interface. Supports scenario initiation, results review, result export, and alert acknowledgment. The primary human-facing output layer of the ALICE architecture.
Responsibilities	1. Render enterprise readiness heat map by mission function and geographic region for Enterprise Decision-Maker role. Update on each ingestion cycle without user action. 2. Render activity-level position risk register for Activity Director role. Scope data to the user's assigned activity. Display fill status, certification currency, and fragility rating per position. 3. Provide investment prioritization panel for Human Capital Planner role showing training, hiring, and cross-training interventions ranked by modeled readiness impact. 4. Present scenario planning workflow for scenario initiation using preset

	scenario library. Workflow must be completable without knowledge of ABM model internals. 5. Display scenario results: time-series readiness forecast chart with confidence band; sortable at-risk position list; response option comparison table. 6. Display alert notifications on user login if unacknowledged threshold alerts exist. Alert display must include type, affected function, severity, and timestamp. 7. Show data currency timestamp on all readiness indicators. 8. Support export of scenario results in PDF summary format and structured data (CSV or JSON) format, accessible within two interactions from the primary results view. 9. Display historical analysis view allowing authorized users to compare predicted vs. actual readiness outcomes. 10. Validate all user inputs in real time with actionable error messages. 11. Log all user actions (dashboard access, scenario initiation, export requests, alert acknowledgment) to LC-09.
Inputs	Role-scoped, activity-scoped ontology and readiness indicator data from LC-04. Scenario results from LC-06. Alert events from LC-04 (via LC-11 delivery). User session and role from LC-01.
Outputs	Rendered interface views (enterprise heat map, position risk register, scenario results). Scenario initiation requests to LC-06 (with validated parameters). Export files (PDF and structured data). User action audit events to LC-09.
Data Handled	Readiness indicators (CUI); scenario results (CUI); alert notifications (CUI). No Privacy Act records. No Processed Zone or Synthetic Zone data is handled directly by this component.
Data Zone Access	Analytical Zone: read-only. No access to Raw, Processed, or Synthetic Zones.
Required Interfaces	← LC-01 (Interface Control): user session and role for all requests. ← LC-04 (Ontology Service): role-scoped readiness data. ← LC-06 (Simulation Engine): scenario results. → LC-06 (Simulation Engine): scenario initiation requests. → LC-09 (Audit Logging): user action events. → LC-11: health status reporting. ← LC-10: display configuration parameters.
Performance Obligations	Enterprise readiness dashboard must load and display current data within a response time that does not add material delay above the LC-01 maximum of 200ms for routing. [INFERRED: dashboard render target is under 3 seconds from authenticated request.] Must support 20 or more concurrent users without degradation (REQ-NF-003). Scenario initiation must pass parameters to LC-06 and return a confirmation to the user within the routing time budget; it does not block on simulation completion.
Security	All data displayed to users is CUI. Role and scope enforcement must be

Considerations	applied to every data query to LC-04 before rendering. The interface must not be engineerable to return data outside the user's authorized scope. Data currency timestamp is a mandatory display element on all readiness indicators. Absence of this timestamp creates a risk of decision errors on stale data. Export files must carry CUI marking. Export actions must be logged as user action events with the file reference. Section 508 / WCAG 2.1 Level AA compliance is a legal obligation (CON-009; REQ-NF-011). Accessibility must be designed in from inception.
Usability Obligations	An Activity Director must complete a preset scenario run from login to results export within 15 minutes following a single 30-minute orientation (REQ-NF-010). The dashboard must display current readiness state without requiring any user configuration (REQ-UX-001). Scenario planning workflow must be completable using only the preset scenario library, without requiring knowledge of ABM model, ontology structure, or simulation parameters (REQ-UX-002). Desktop optimization for minimum 1280×800 resolution is required (REQ-UX-007). Mobile access is a Phase III consideration.
NIST SP 800-53 Controls	AC-3 (Access Enforcement — scope-restricted data rendering); SC-8 (Transmission Confidentiality — TLS 1.2+ for all interface communications); AU-2 (Event Logging — user action events).
Governing ADRs	ADR-001 (modular component); ADR-002 (Analytical Zone read-only access)
Functional Domains	FD-6 (Decision Support and Reporting)
Operational Workflows	OW-1 (Continuous Monitoring — readiness display); OW-2 (Scenario Planning — user initiation and results display); OW-3 (Synthetic Data Export — export request submission for Data Steward workflow)
PRD Requirements	REQ-F-019; REQ-F-020; REQ-F-021; REQ-F-022; REQ-F-023; REQ-NF-010; REQ-NF-011; REQ-UX-001 through REQ-UX-010
Open Questions	[OPEN] OQ-009 (DLA operational hours — affects auto-refresh cycle timing for the readiness dashboard).

LC-08: Identity and Access Management (IAM) Service

Layer: Cross-Cutting — Infrastructure and Governance	**OV-1 Layer #**: Cross-Cutting	**Phase**: Phase I and II	**Status**	**Required — Critical Security Dependency**

Purpose	Manages user identities, role assignments, activity scope mappings, session lifecycle, and service identity credentials. Issues and validates role-scoped authorization tokens used by all ALICE services to enforce least-privilege access. Integrates with DoD PKI for CAC-based user authentication.
Responsibilities	1. Integrate with DoD PKI / CAC infrastructure to validate user identity certificates presented at LC-01. 2. Maintain user account records: identity, assigned role (one of four: Enterprise Decision-Maker, Activity Director, Human Capital Planner, System Administrator), and assigned activity scope.

	3. Issue role-scoped, activity-scoped, time-limited authorization tokens upon successful authentication. 4. Validate token integrity for service-to-service calls. 5. Enforce session timeout and revocation. Revocation must propagate to all services holding the revoked token within a defined window. 6. Maintain service identity credentials for all service-to-service communication. Coordinate with LC-12 for credential storage. 7. Provide user provisioning and de-provisioning workflows accessible to the System Administrator role. 8. Log all IAM events (user provisioning, role assignment, session creation, token issuance, revocation, failed authentication) to LC-09.
Inputs	CAC certificate and authentication challenge result from LC-01. User provisioning and role assignment requests from System Administrator. Token validation requests from downstream services. Session revocation signals from System Administrator or session timeout mechanism.
Outputs	Role-scoped, activity-scoped session tokens to LC-01 (for forwarding to authenticated users and services). Token validation responses to requesting services. User account provisioning confirmations. IAM audit events to LC-09.
Data Handled	Identity metadata: user IDs, role assignments, activity scope mappings. No workforce data of any classification. IAM data is sensitive operational data requiring protection at the confidentiality level of the systems it controls.
Data Zone Access	None of the four workforce data zones. IAM data is stored in a dedicated identity store separate from all data zones.
Required Interfaces	← INT-06 (DoD PKI / CAC Authority): certificate validation queries per user session. ← LC-01: receives authentication results; provides token issuance response. ← All services: token validation requests. → LC-09: IAM audit events. ← LC-12: service credential management for service-to-service tokens.
Security Considerations	Compromise of LC-08 results in compromise of the entire ALICE authorization model. This component must receive the highest available security controls and operational monitoring priority. No shared administrative credentials. Each System Administrator account must be individually provisioned and individually attributable in audit records. Token signing material must be stored exclusively in LC-12 and rotated on the schedule defined in the System Security Plan. Session revocation must take effect within a defined time window after the revocation event. The time window must be specified in the System Security Plan and tested as part of Phase I acceptance.
NIST SP 800-53 Controls	IA-2 (MFA); IA-3 (Device Identification — service identity); IA-5 (Authenticator Management — CAC integration); AC-2 (Account Management); AC-5 (Separation of Duties); AC-6 (Least Privilege); AC-12 (Session Termination).
Governing ADRs	ADR-001 (modular component); ADR-004 (this component is the Policy Engine and Policy Administrator in the ZTA model; LC-01 is the Policy

	Enforcement Point)
Functional Domains	FD-1 (User Access and Identity Management)
Operational Workflows	All workflows — IAM underlies every authenticated operation
PRD Requirements	REQ-SEC-001 through REQ-SEC-005; REQ-ADM-001
Open Questions	[OPEN] ASM-008 / RISK-004: CAC integration feasibility in Phase I environment. [INFERRED] Token format specification (identity claims, role claim, scope claim, expiration) must be defined as a Phase I design artifact before LC-01 and LC-08 integration testing.

LC-09: Immutable Audit Logging Service

Layer: Cross-Cutting — Infrastructure and Governance	**OV-1 Layer #**: Cross-Cutting	**Phase**: Phase I and II	**Status**	**Required — Compliance Critical**

Purpose	Receives structured audit events from all ALICE service components and stores them in an immutable, append-only log store. Supports authorized review, query, and export of audit records. Provides tamper-detection capability through hash-chain or equivalent integrity mechanism. Is the sole component with write access to the audit log store.
Responsibilities	1. Receive structured audit events from all ALICE services via a write-only service-to-service interface. 2. Assign each received event an entry ID and a receipt timestamp in UTC. 3. Append events to the immutable log store. Reject any request to modify or delete existing log entries, regardless of the requesting identity. 4. Generate integrity verification records (hash-chain or equivalent) enabling tamper detection on any log entry. 5. Enforce authorized read access: System Administrator and designated Auditor roles may search and review log records; no other role has read access. 6. Support log search by user identity, event type, and date range. 7. Support export of log record sets for external compliance review. 8. Enforce retention policy: minimum 7-year retention for all log entries, enforced by automated policy, not manual deletion. 9. Buffer incoming events in a durable queue when the log store is temporarily unavailable; deliver buffered events on store restoration.
Inputs	Structured audit event records from all ALICE service components (LC-01 through LC-12) via write-only authenticated service interfaces.
Outputs	Immutable log entries in the Audit Log Store. Hash-chain integrity records. Log search results to authorized reviewers. Log export files for external review.
Data Handled	Audit log entries (CUI — sensitive). May include user identity references, event types, timestamps, and data access descriptions. Retained for minimum 7 years. Log entries must not contain raw workforce data content

	(e.g., position salary data or individual performance ratings); they contain references to events and outcomes only.
Data Zone Access	Audit Log Store: write (from services); read (authorized reviewers). No access to Raw, Processed, Synthetic, or Analytical Zones for data content.
Required Interfaces	← All ALICE services (LC-01 through LC-12): write-only event delivery interfaces. → Authorized reviewers (System Administrator, Auditor): read interface for log search and export. ← LC-12: log signing and integrity key material.
Performance Obligations	[INFERRED: Event ingestion must not create a bottleneck on service operations. Asynchronous event delivery with durable queuing is the required pattern. Delivery confirmation must be provided to sending services.]
Security Considerations	Technical isolation from all other ALICE services is the primary security requirement for this component. No service other than LC-09 has write capability to the Audit Log Store. The System Administrator role has read-only access to audit logs. The System Administrator must not have delete capability. Hash-chain integrity must be computable and verifiable independently — without access to any ALICE application service — for compliance assessment purposes.
NIST SP 800-53 Controls	AU-2 (Event Logging); AU-3 (Content of Audit Records); AU-9 (Protection of Audit Information — write isolation); AU-11 (Audit Record Retention — 7-year minimum); AU-12 (Audit Record Generation — all services).
Governing ADRs	ADR-001 (modular, dedicated service); ADR-005 (this component is the decision implementation)
Functional Domains	FD-8 (Governance, Audit, and Compliance)
Operational Workflows	All four operational workflows — audit events generated in every workflow
PRD Requirements	REQ-NF-012; REQ-SEC-009; REQ-SEC-010; REQ-F-018; REQ-ADM-006
Open Questions	[INFERRED] Storage provisioning for 7-year retention at enterprise scale must be estimated during Phase I technical design. Log volume depends on event frequency at full enterprise scale (30,000 positions, daily refresh, 20+ concurrent users).

LC-10: Configuration Management Service

Layer: Cross-Cutting — Infrastructure and Governance	**OV-1 Layer #**: Cross-Cutting	**Phase**: Phase I and II	**Status**	**Required**

Purpose	Stores, versions, and serves all operational configuration parameters that control ALICE system behavior. Ensures that operational adjustments — readiness thresholds, alert conditions, scenario parameter ranges, ingestion schedules, export workflow settings — can be made through the administrative interface without modifying application code.

Responsibilities	1. Store configuration parameters as version-controlled data items. 2. Enforce write access restriction: only the System Administrator role may modify configuration values through the administrative interface. 3. Log all configuration changes to LC-09 with: administrator identity, parameter changed, prior value, new value, and timestamp. 4. Serve current configuration values to all requesting services on demand. 5. Support rollback to a prior configuration version through the administrative interface. 6. Support configuration backup per REQ-ADM-007.
Inputs	Configuration update requests from System Administrator (via administrative interface). Configuration read requests from all ALICE services.
Outputs	Current configuration values to requesting services. Configuration change audit events to LC-09. Configuration backup exports.
Data Handled	Configuration parameters: threshold values, schedule settings, role definitions, scenario library parameters, export workflow settings. Sensitivity: operational data; not workforce CUI. Schema mapping data (used by LC-03) is stored here as a special configuration category.
Data Zone Access	Configuration Store: read and write. No access to any workforce data zone.
Required Interfaces	← System Administrator: write access for configuration updates. → All services: configuration read responses. → LC-09: configuration change audit events.
Security Considerations	Configuration parameters that govern threshold values and alert conditions are operationally sensitive. Write access must be restricted to System Administrator role. Configuration store must be access-controlled with the same rigor as operational data stores. Changes to schema mappings (used by LC-03) must trigger a review flag given their privacy implications.
NIST SP 800-53 Controls	CM-2 (Baseline Configuration); CM-3 (Configuration Change Control); CM-6 (Configuration Settings); AU-2 (Event Logging — configuration changes).
Governing ADRs	ADR-001 (modular component); ADR-010 (Candidate — this component is the decision implementation); ADR-003 (schema mapping stored here)
Functional Domains	FD-7 (Administration and Configuration)
PRD Requirements	REQ-ADM-002; REQ-ADM-004; REQ-ADM-006; REQ-ADM-007
Open Questions	None specific to this component.

LC-11: Observability and Health Monitoring Service

Layer: Cross-Cutting — Infrastructure and Governance	**OV-1 Layer #**: Cross-Cutting	**Phase**: Phase I and II	**Status**	**Required**

Purpose	Monitors the operational health of all ALICE service components. Generates alerts for failures, anomalies, and performance degradation. Provides the System Administrator with operational visibility required to maintain system

	availability and respond to incidents.
Responsibilities	1. Collect health status signals from all ALICE services via health check endpoints. 2. Monitor ingestion pipeline execution status: completion, failure, and anomaly (record count delta exceeding 20% from prior day). 3. Monitor simulation engine performance against the 5-minute preset scenario time threshold. 4. Monitor authentication failure rates from LC-01; alert on threshold breach. 5. Generate and deliver operational alerts to the System Administrator for: ingestion failures; simulation engine errors; authentication failure threshold breach; synthetic population expiration; data source connectivity failures. 6. Alert delivery must occur within 5 minutes of event detection (REQ-NF-015). 7. Report health status summary to the System Administrator dashboard.
Inputs	Health status signals and metrics from all ALICE service components.
Outputs	Operational alert notifications to System Administrator. Health status dashboard data. Health event records to LC-09.
Data Handled	Operational metrics and health status signals. No workforce data. Health data is internal operational data; it does not carry a CUI classification but must be protected as operationally sensitive.
Data Zone Access	No access to any workforce data zone. Accesses service health endpoints only.
Required Interfaces	← All services: health endpoint polling or push-based health signals. → System Administrator: alert delivery and health dashboard. → LC-09: health event audit records.
Security Considerations	Health monitoring data could reveal operational patterns useful to an adversary (e.g., ingestion schedule, simulation load patterns). Access to health monitoring outputs must be restricted to the System Administrator role.
NIST SP 800-53 Controls	SI-4 (System Monitoring); IR-6 (Incident Reporting — health alerts support incident detection); AU-2 (health events logged to LC-09).
Governing ADRs	ADR-001 (modular component)
Functional Domains	FD-7 (Administration and Configuration); FD-8 (Governance, Audit, and Compliance — health evidence for RMF continuous monitoring)
PRD Requirements	REQ-NF-015; REQ-ADM-005
Open Questions	[INFERRED] Specific alert threshold values (e.g., authentication failure rate trigger) must be defined in the System Security Plan and configurable via LC-10.

LC-12: Secrets Management Service

Layer: Cross-Cutting — Infrastructure	**OV-1 Layer #**: Cross-Cutting	**Phase**: Phase I and II	**Status**	**Required**

and Governance				

Purpose	Stores and manages all ALICE credentials, service account passwords, API keys, authentication tokens, and cryptographic key material. Provides secure, authenticated retrieval of secrets to authorized services without exposing secrets in configuration files, environment variables, or application code.
Responsibilities	1. Store all source system service account credentials (for INT-01 through INT-04) in encrypted, access-controlled storage. 2. Store all inter-service credentials and data zone access credentials. 3. Store encryption keys for each of the four data zones and the Audit Log Store. 4. Store token signing material for LC-08. 5. Provide secret retrieval to authorized services using service identity verification. 6. Enforce credential rotation: support automated rotation on configured schedule; ensure services receive rotated credentials without manual intervention. 7. Log all secrets access events (retrieval, rotation, provisioning) to LC-09. 8. Alert LC-11 on rotation failures or credential access anomalies.
Inputs	Secrets provisioning requests from System Administrator (initial provisioning). Secret retrieval requests from authorized services (using service identity credential). Rotation schedule configuration from LC-10.
Outputs	Secret values to authorized requesting services (encrypted in transit). Rotation confirmations. Secrets access audit events to LC-09. Rotation failure alerts to LC-11.
Data Handled	Cryptographic key material, service account credentials, and API keys. All at the highest sensitivity level within the ALICE operational environment. Exposure of any credential stored here is a critical security incident.
Data Zone Access	Secrets Store: read and write. No access to workforce data zones.
Required Interfaces	← System Administrator: initial provisioning of secrets. ← All services: secret retrieval requests (authenticated by service identity). ← LC-10: rotation schedule configuration. → LC-09: secrets access and rotation audit events. → LC-11: rotation failure alerts.
Security Considerations	This component is a high-value attack target. Compromise of LC-12 exposes all credentials across all ALICE zones. All secrets must be encrypted at rest using FIPS 140-3 validated encryption (REQ-SEC-007). Secret retrieval must be authenticated: each service must prove its identity before receiving credentials. This requires a bootstrap mechanism (a root secret or certificate) that itself must be protected as the highest-sensitivity item in the system. No secret value must ever appear in log files, configuration files, or error messages.

	Annual key rotation minimum is required per REQ-SEC-008. The rotation process must be tested before Phase II deployment to confirm that rotation does not cause service outages.
NIST SP 800-53 Controls	SC-12 (Cryptographic Key Establishment and Management); SC-28 (Protection of Information at Rest — secrets encrypted); IA-5 (Authenticator Management — service credential lifecycle); AU-2 (secrets access events logged to LC-09).
Governing ADRs	ADR-001 (modular component); ADR-004 (service identity credentials managed here — integral to ZTA service-to-service authentication)
Functional Domains	FD-1 (User Access and Identity Management — service credential dimension); FD-8 (Governance — key lifecycle evidence)
PRD Requirements	REQ-SEC-006; REQ-SEC-007; REQ-SEC-008
Open Questions	[INFERRED] Bootstrap mechanism for LC-12 itself (the root of trust) must be designed and documented as a Phase I security architecture task. This is a common implementation challenge for secrets management systems.

4. Component Dependency Map

The following table documents the directional dependencies between components. A dependency exists when Component A requires Component B to function. This map is the basis for deployment sequencing, failure impact analysis, and integration test order determination.

Component	Depends On (Hard)	Depends On (Soft)	Is Required By	Failure Impact if Unavailable
LC-01	LC-08 (token issuance); LC-12 (signing material); INT-06 (CAC validation)	LC-09 (audit — degrades to buffered)	LC-07 (user access); All user-initiated workflows	All user access blocked. System-automated workflows (OW-1, OW-4) continue unaffected.
LC-02	LC-03 (canonical records); LC-12 (source credentials); LC-10 (schema, schedule)	LC-09 (audit); LC-11 (health)	LC-04 (ingestion completion trigger)	Data ingestion stops. Ontology and twin state freeze at last successful refresh. Readiness indicators become stale after 24 hours.
LC-03	INT-01 (DCPDS/DCHRMS); INT-02 (DLA TMS); LC-10 (schema mappings)	LC-09 (audit); LC-11 (health)	LC-02 (canonical records)	Source data cannot be ingested. Same impact as LC-02 failure.
LC-04	Processed Zone (read); LC-10 (thresholds); LC-12 (zone credentials)	LC-09 (audit); LC-11 (health)	LC-07 (readiness data); LC-05 (structural scope data)	Readiness indicators not updated. Dashboard shows stale data. Threshold alerts not generated.
LC-05	Processed Zone (read); Synthetic Zone (write); LC-10 (generation params); LC-12 (zone credentials)	LC-09 (audit); LC-11 (health)	LC-06 (synthetic population)	Synthetic population cannot be regenerated. LC-06 continues to use last validated population until it expires.

Component	Depends On (Hard)	Depends On (Soft)	Is Required By	Failure Impact if Unavailable
LC-06	Synthetic Zone (read); LC-10 (scenario config); LC-12 (zone credentials)	LC-09 (audit); LC-11 (health)	LC-07 (scenario results)	Scenario simulation unavailable. Readiness monitoring (OW-1) continues; scenario planning (OW-2) blocked.
LC-07	LC-04 (readiness data); LC-06 (scenario results); LC-01 (session); LC-12 (session material)	LC-09 (audit); LC-11 (health)	Operational users (all roles)	User interface unavailable. All user-initiated workflows blocked. Automated OW-1 and OW-4 continue.
LC-08	INT-06 (CAC validation); LC-12 (token signing material)	LC-09 (audit)	LC-01 (token issuance); All services (token validation)	Critical: all authentication fails; all user access blocked. Equals LC-01 failure impact.
LC-09	Audit Log Store	LC-12 (log signing)	All components (audit event destination)	Audit trail interrupted. Service operations continue. Compliance gap accumulates. Alert LC-11 immediately.
LC-10	Configuration Store	LC-09 (config change audit)	All services (configuration reads)	Services operate on last-loaded configuration until LC-10 is restored. Configuration changes cannot be applied.
LC-11	Health endpoints of all services	LC-09 (health event audit)	System Administrator (alerts)	Operational alerting unavailable. System administrator loses automated incident detection. Manual monitoring required.
LC-12	Secrets Store	LC-09 (secrets access audit)	All services (credential retrieval)	Critical: all services that require credential rotation or new credential retrieval will fail. Services using cached credentials may continue temporarily. Full service degradation on next credential rotation cycle.

5. Phase I MVP Component Scope

All twelve components are required in Phase I, though their scope is bounded to the MVP use case. The following table documents the Phase I scope for each component versus the full Phase II scope.

Component	Phase I Scope	Phase II Additions / Extensions
LC-01	CAC or interim MFA authentication; RBAC for four roles; routing to Phase I components.	Full ZTA enforcement with device trust; enterprise-scale concurrent user support.
LC-02	Scheduled ingestion from de-identified DCPDS extract or OPM FWD proxy for pilot sub-component; PII detection; de-identification.	Live API integration with DCPDS, DLA TMS, DPMAP, EBS; enterprise-wide scope; real-time delta processing.
LC-03	DCPDS schema mapping for pilot sub-component. DCHRMS schema mapping if migration reaches pilot during Phase I.	Full dual-schema support across all DLA activities; additional source adapters as required.
LC-04	Ontology for pilot sub-component only; readiness indicators for pilot function areas; 12-month historical snapshot archive.	Enterprise-wide ontology (all DLA activities, 30,000 positions); full alert delivery integration.
LC-05	Synthetic population generation for pilot sub-component; fidelity and privacy validation; export governance workflow prototype.	Enterprise-scale generation; scheduled regeneration cycle; full PIA-informed export governance.
LC-06	Minimum 3 preset scenario types (Key Departure, Workload Surge, Pipeline Shortfall); Monte Carlo confidence intervals; preset scenario execution within 5 minutes.	All 5 preset scenario types; custom scenario builder; horizontal scaling for 20+ concurrent users.
LC-07	Activity-level position risk register; preset scenario planning workflow for Activity Director and HC Planner roles; scenario results display with export.	Enterprise readiness heat map; investment prioritization panel; full alert notification system; historical analysis view; mobile access (Phase III).
LC-08	CAC or interim MFA; four RBAC roles; session management; System Administrator provisioning workflow.	Full ZTA service identity management; device trust integration; enterprise user population management.
LC-09	Immutable audit logging for all Phase I operations; 7-year retention policy configured; hash-chain integrity; basic log search.	Enterprise-scale log volume management; compliance reporting automation; external audit export.
LC-10	Configuration management for Phase I operational parameters: pilot thresholds, ingestion schedule, generation parameters, Phase I scenario library.	Full enterprise configuration management; advanced rollback; configuration compliance reporting.
LC-11	Phase I health monitoring: ingestion, simulation, authentication failure, synthetic population expiration alerts.	Full enterprise observability; RMF continuous monitoring integration; automated incident response triggers.

Component	Phase I Scope	Phase II Additions / Extensions
LC-12	Phase I secrets management for source system credentials, zone keys, and token signing material.	Enterprise key management at IL4; annual rotation automation; integration with government-authorized key management infrastructure.

6. Gate-3 Summary and Decision Required

What Was Created

Artifact 3 (Component Catalog) provides complete, implementation-planning-ready specifications for all twelve ALICE logical service components. Each component record includes: a purpose statement; full responsibility enumeration; all inputs, outputs, and data handled; data zone access rights (per ADR-002 and ADR-008); required interface directionality, protocol class, and security controls; performance and availability obligations; security considerations; NIST SP 800-53 control family coverage; governing ADR cross-references; functional domain and operational workflow participation; all PRD requirements; and Phase I versus Phase II scope differentiation. The component dependency map in Section 4 documents directional dependencies, failure impact, and the basis for deployment sequencing and integration test ordering.

Major Assumptions in This Artifact

- All twelve components are described at the technology-neutral capability level per TNA v1.0 and ADR-001. Technology selection for each component is deferred to Phase I technical design.
- LC-01 assumes CAC integration per DoDI 8520.02. ASM-008 / RISK-004 documents the risk that CAC may not be available in the Phase I demonstration environment. If unavailable, interim MFA is the required fallback.
- LC-05 training corpus size assumes a minimum of 300 positions per ASM-003. If the pilot sub-component is smaller, augmentation with OPM FWD data is required.
- LC-06 component descriptions assume open-source or commercially licensed ABM framework availability per ASM-005. License confirmation is a Phase I Month 2 prerequisite (CON-011).
- The LC-12 bootstrap mechanism — the root-of-trust for secrets management itself — is flagged as an inferred design task requiring resolution in Phase I security architecture planning.

Open Issues

- **[Critical]** OQ-001: Pilot sub-component selection determines the scope of LC-04 (ontology), LC-05 (training corpus size), and LC-06 (scenario parameter calibration). Must be resolved at Phase I kickoff.
- **[High]** ASM-005 / CON-011: ABM framework license confirmation must be completed before Phase I Month 2 to avoid blocking LC-06 implementation.
- **[High]** ASM-008 / RISK-004: CAC integration feasibility in Phase I environment must be confirmed at contract award to determine whether interim MFA is required.
- **[Medium]** OQ-004 / OQ-008: DCHRMS migration schedule and DLA TMS extract format must be confirmed to finalize LC-03 Phase I scope.
- **[Inferred]** The LC-12 root-of-trust bootstrap mechanism and the LC-01 token format specification are both inferred Phase I design tasks not explicitly covered in the PRD or TNA. They must be addressed in Phase I security architecture documentation.

Decision Required

Gate-3 Decision: Please approve Artifact 3 (Component Catalog) to proceed to Artifact 4 (Data Catalog), or provide specific revision instructions. If any component scope, responsibility, interface, or access right requires modification, please identify the component ID and the specific change required. Once approved, Artifact 4 will be produced using consistent IDs and cross-references to this catalog.