

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 6 OF 11

Risk Register

Document Version 1.0 | July 2026

Status: DRAFT — Pending Gate-6 Stakeholder Review

Classification: Unclassified

Document Control

Field	Value
Artifact ID	SDP-ART-06
Artifact Title	Risk Register
Artifact Dependencies	SDP-ART-01 through SDP-ART-05 — all approved
Package	ALICE Supporting Documentation Package (SDP)
Source Documents	ALICE TNA v1.0 Section 23; ALICE PRD v1.0 Sections 25–26; SDP-ART-01 through SDP-ART-05
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-6 stakeholder approval before Artifact 7 is produced
Risk Count	18 risks (RISK-001 through RISK-018)
ID Convention	RISK-001 through RISK-010: carried from TNA v1.0 Section 23 without modification. RISK-011 through RISK-018: identified during SDP cross-artifact analysis. All IDs will be carried forward into all remaining SDP artifacts.

1. Purpose and Scope

This Risk Register is Artifact 6 of the ALICE Supporting Documentation Package. It consolidates all architecture, program, integration, security, privacy, and adoption risks identified across the TNA, PRD, and prior SDP artifacts into a single authoritative register. It provides the complete risk record required for Phase I program planning, Phase II ATO preparation, CMMC assessment readiness, and stakeholder decision-making.

The register covers 18 risks. RISK-001 through RISK-010 are carried directly from TNA Section 23, expanded with additional cross-reference data from the SDP artifact series. RISK-011 through RISK-018 are new risks identified during SDP analysis of artifacts 1 through 5 that were not formally captured in the TNA. Each risk record includes: a stable identifier; a risk statement; the cause; the impact if the risk materializes; likelihood and severity ratings; current mitigation actions; residual risk after mitigation; the risk owner; all affected components and interfaces; related requirements and ADRs; the decision or action needed; and the SDP artifact where the risk was first identified or confirmed.

Likelihood and severity ratings use a three-point scale (High, Medium, Low) consistent with the TNA. No quantitative probability estimates are provided; ratings reflect the collective judgment of the architecture team based on available evidence. Ratings marked [INFERRED] represent assessments derived from source document analysis where the TNA or PRD did not assign explicit ratings.

2. Risk Summary

2.1 Risk Heat Map

The following table summarizes all 18 risks by likelihood and severity for prioritization purposes. Risks in the High Severity / Medium or High Likelihood quadrant represent the highest-priority items for Phase I program management attention.

Risk ID	Statement (abbreviated)	Likelihood	Severity	Origin	Owner	Decision Needed?
RISK-001	Data sharing agreement not executed within Phase I.	Medium	High	TNA; PRD	DLA GTPOC	Yes — DUA initiation at contract award
RISK-002	DCHRMS migration begins for pilot sub-component during Phase I.	Low	High	TNA; PRD	DLA GTPOC	Yes — confirm migration schedule at kickoff
RISK-003	Synthetic population fidelity below 5% threshold.	Medium	High	TNA; PRD	SOL	Yes — pilot sub-component selection (OQ-001)
RISK-004	CAC authentication not available in Phase I demonstration environment.	Medium	Medium	TNA	SOL / DLA GTPOC	Yes — confirm CAC feasibility at contract award
RISK-005	Simulation execution exceeds 5-minute threshold under concurrent load.	Medium	Medium	TNA; PRD	SOL	No — mitigated through Phase I design; monitor
RISK-006	CMMC Level 2 C3PAO assessment not completed before November 10, 2026.	Medium	High	TNA; PRD	SOL	Yes — initiate gap assessment at contract award
RISK-007	Membership inference attack success rate exceeds 50%.	Low	High	TNA; PRD	SOL	No — mitigated by conservative epsilon design
RISK-008	Phase II hosting model not resolved before ATO initiation.	Medium	High	TNA	DLA GTPOC / DLA CIO	Yes — hosting model decision before Phase I Month 2
RISK-009	Phase II user adoption failure — Activity Directors do not complete independent scenario runs.	Medium	Medium	TNA; PRD	SOL / DLA GTPOC	No — mitigated through Phase I UX evaluation
RISK-010	Synthetic data classification ambiguity delays Phase II export governance.	Medium	Medium	TNA	DLA CDO / SOL Privacy Officer	Yes — initiate PIA in Phase II Month 1
RISK-	Interface contract drift	Mediu	Mediu	SDP-ART-	SOL	No — mitigated

Risk ID	Statement (abbreviated)	Likelihood	Severity	Origin	Owner	Decision Needed?
011	between service components undermines integration correctness.	m	m	02 (ADR-001)		by interface contract governance process
RISK-012	LC-12 secrets management credential rotation causes service outage during Phase II.	Low	High	SDP-ART-02 (ADR-004); SDP-ART-03 (LC-12)	SOL	Yes — rotation test required before Phase II deployment
RISK-013	Activity scope not precisely encoded in session tokens — Activity Directors access out-of-scope data.	Low	High	SDP-ART-02 (ADR-004); SDP-ART-03 (LC-01, LC-08)	SOL	No — mitigated by token specification design task
RISK-014	Audit log event volume at enterprise scale causes LC-09 storage or throughput failure.	Low	Medium	SDP-ART-02 (ADR-005); SDP-ART-03 (LC-09)	SOL	Yes — storage provisioning estimate required in Phase I
RISK-015	DPMAP aggregate-only schema not formally defined in data use agreement — individual records delivered.	Low	High	SDP-ART-04 (DE-03); SDP-ART-05 (INT-03)	DLA HRMS / SOL	Yes — DUA schema definition required before INT-03 ingestion
RISK-016	De-identification specification not completed before DCPDS data delivery — raw Privacy Act records ingested.	Medium	High	SDP-ART-04 (DE-03, DE-05); SDP-ART-05 (INT-01)	SOL Privacy Officer / DLA Privacy Officer	Yes — de-identification specification must be approved before any DLA data flows to ALICE
RISK-017	OPM FWD proxy data format schema not mapped before DLA data decision point — Phase I blocked.	Low	Medium	SDP-ART-04 (DE-01); SDP-ART-05 (INT-05)	SOL	No — mitigated by Phase I Month 1 schema development
RISK-018	Phase I acceptance standard for proxy-based validation not confirmed — GTPOC rejects deliverable.	Medium	High	SDP-ART-05 (INT-05); SDP-ART-04 (OQ-010)	DLA GTPOC	Yes — confirm acceptance standard at Phase I kickoff

2.2 Risk Count by Severity and Likelihood

	High Severity	Medium Severity	Low Severity	Total
High Likelihood	0	0	0	0
Medium Likelihood	7 (RISK-001, 003, 006, 008, 016, 018; RISK-004 medium/medium)	3 (RISK-005, 009, 010)	0	10
Low Likelihood	4 (RISK-002, 007, 012, 013, 015; see note)	3 (RISK-011, 014, 017)	0	8 (approx)
Total High + Medium Severity	11	6	0	18 (all risks)

Note: The table groups are approximate due to mixed-cell risks. All 18 risks are detailed in Section 3. No risk in this register has been assessed as Low Severity; all identified risks carry at minimum Medium Severity given the program context.

3. Risk Detail Records

RISK-001 Data sharing agreement with DLA not executed within Phase I period.				
Likelihood: Medium	**Severity:** High	**Origin:** TNA Section 23; PRD Section 26	**Status:** Open	**Artifact:** SDP-ART-06

Cause	DLA data governance process requires CDO involvement; MOU execution may extend beyond 60 days from contract award. Competing priorities within DLA governance chain may delay review and signature.
Impact	Phase I synthetic model trained on OPM FWD proxy data only. DLA-specific fidelity and organizational accuracy not validated during Phase I. Phase II funding case weakened if Phase I results cannot demonstrate DLA-specific representational fidelity.
Mitigation	Initiate DUA coordination at contract award — do not wait for formal program kickoff meeting. Document the OPM FWD proxy path explicitly in the Phase I performance plan; position it as a planned parallel track, not a contingency. Socialize the DUA requirement with the DLA GTPOC before contract award to establish expectations and identify CDO involvement requirements. Engage DLA Data Decrees authority (CDAO-directed access) as an enabling pathway per TNA Section 17 governance architecture.
Residual Risk	Medium. The proxy fallback path (INT-05, OPM FWD) operationally mitigates schedule risk but does not mitigate fidelity validation risk against DLA-specific data.
Risk Owner	DLA GTPOC (DUA execution authority); SOL Program Manager (initiation and tracking).
Affected Components / Interfaces	LC-02 (Data Ingestion — delayed from INT-01 to INT-05 fallback); INT-01 (DCPDS — blocked until DUA executed); INT-05 (OPM FWD — activated as proxy).

Affected Data Entities	DE-01, DE-03 (DLA-specific instances unavailable until DUA executed; proxy-derived versions used).
Related Requirements	ASM-002; REQ-F-001; REQ-F-005; DEP-001.
Related ADRs	ADR-006 (Phase-Gated Security Posture — proxy operation during Phase I is architecturally supported).
Decision or Action Required	DUA initiation must occur at contract award, not at Phase I kickoff. Program Manager must have a DUA draft ready before contract execution begins.
SDP Origin	TNA Section 23 (RISK-001); confirmed in SDP-ART-04 (OQ-002); SDP-ART-05 (INT-01 open questions).

RISK-002 DCHRMS migration begins for pilot sub-component during Phase I performance period.

Likelihood: Low	**Severity:** High	**Origin:** TNA Section 23; PRD Section 26	**Status:** Open	**Artifact:** SDP-ART-06

Cause	The DoD-wide DCHRMS (Oracle HCM) migration is proceeding on a rolling schedule by component. The migration timeline for any specific DLA activity is not publicly documented. If the Phase I pilot sub-component's DCHRMS migration is imminent or begins during the 6-month Phase I period, the DCPDS schema used for LC-03 mapping will change mid-program.
Impact	The LC-03 schema mapping for DCPDS would require update to the DCHRMS schema mid-Phase I, adding unplanned development scope within a $100,000 fixed-price ceiling. If the abstraction layer (LC-03) is not designed from the outset to support both schemas, the impact is substantially greater: the entire ingestion pipeline would require redesign.
Mitigation	ADR-003 is the primary mitigation: LC-03 is designed as a dedicated schema abstraction layer that supports dual-schema operation (DCPDS and DCHRMS) from Phase I start. Maintain both DCPDS and DCHRMS schema mappings in LC-10 (Configuration Management) from the beginning of Phase I, even if DCHRMS mapping is not yet exercised. Confirm DCHRMS migration schedule for the pilot sub-component at Phase I kickoff (OQ-004). If migration is imminent, prioritize DCHRMS schema mapping over DCPDS mapping.
Residual Risk	Low. The LC-03 abstraction layer is the architectural mitigation. If the abstraction is implemented correctly from Phase I Month 1, a mid-program schema change impacts only LC-03 configuration, not core services.
Risk Owner	SOL Lead Architect (LC-03 design); DLA GTPOC (DCHRMS migration schedule information).
Affected Components / Interfaces	LC-03 (Schema Abstraction — primary impact); INT-01 (DCPDS/DCHRMS — schema change source).
Related Requirements	REQ-INT-001; ADR-003; DEP-007; ASM-004.
Decision or Action Required	Confirm DCHRMS migration schedule for pilot sub-component at Phase I kickoff. This information must be requested from the DLA GTPOC before LC-03 Phase I schema mapping scope is finalized.

SDP Origin	TNA Section 23 (RISK-002); SDP-ART-03 (LC-03 open questions); SDP-ART-05 (INT-01 open questions).

RISK-003 Synthetic population fidelity does not meet the 5% distributional deviation threshold with Phase I dataset.

Likelihood: Medium	**Severity:** High	**Origin:** TNA Section 23; PRD Section 26	**Status:** Open	**Artifact:** SDP-ART-06

Cause	Two compounding factors: (1) If the pilot sub-component contains fewer than 300 positions (below ASM-003 minimum), the training corpus is insufficient for the generative model to learn stable distributional patterns. (2) Differential privacy noise injected at epsilon ≤ 1.0 can dominate the signal in small populations, degrading synthetic fidelity.
Impact	Phase I deliverable acceptance criterion not met (PRD Section 12.2 requires synthetic fidelity within 5%). Phase II funding case is materially weakened if the Phase I synthetic generation prototype cannot demonstrate the required fidelity. DLA GTPOC may decline to recommend Phase II.
Mitigation	Confirm pilot sub-component position count at Phase I kickoff (OQ-001). If count is below 300, pursue one of: (a) augment with OPM FWD proxy data to expand the training corpus; (b) expand the pilot scope to include an adjacent sub-function; or (c) negotiate with DLA GTPOC to accept proxy-based fidelity demonstration for Phase I. Target a working epsilon of 0.5 (more conservative than the 1.0 acceptance threshold) to allow headroom for noise effects on small populations. Document the augmentation approach and its implications for fidelity interpretation in the Phase I performance plan.
Residual Risk	Medium. The residual risk depends on pilot sub-component selection (OQ-001) and remains unresolvable until that decision is made.
Risk Owner	SOL Lead Architect / Data Scientist (synthetic engine design); DLA GTPOC (pilot sub-component selection).
Affected Components / Interfaces	LC-05 (Synthetic Engine — fidelity validation); IF-08 (training input scope determines corpus size).
Affected Data Entities	DE-08 (Synthetic Person — fidelity is the quality attribute at risk); DE-12 (Generation Metadata — validation results document the fidelity outcome).
Related Requirements	REQ-F-015; REQ-F-016; ASM-003; PRD Section 12.2 (MVP success criteria).
Decision or Action Required	OQ-001 (pilot sub-component selection) is the blocking decision. Must be resolved at Phase I kickoff.
SDP Origin	TNA Section 23 (RISK-003); SDP-ART-04 (DE-08 open questions).

RISK-004 DoD PKI / CAC authentication infrastructure not available for Phase I demonstration environment.

Likelihood: Medium	**Severity:** Medium	**Origin:** TNA Section 23	**Status:** Open	**Artifact:** SDP-ART-06

Cause	SOL's Phase I development and demonstration environment is a non-federal contractor system. DoD PKI integration (INT-06) requires access to the DoD PKI trust anchor and OCSP/CRL infrastructure. This integration may not be technically feasible or authorized within the Phase I demonstration environment constraints and timeline.
Impact	Phase I demonstration cannot satisfy REQ-SEC-001 (CAC as required authentication mechanism). An alternative multi-factor authentication mechanism must be implemented as an interim substitute. This does not affect the architecture design (LC-01 and LC-08 are designed for CAC), but it creates a gap in Phase I security acceptance evidence.
Mitigation	Initiate CAC integration feasibility assessment at contract award — technical and authorization questions must be resolved before Phase I Month 1 development begins. If CAC integration is not feasible in Phase I: implement an alternative MFA mechanism (software-based or hardware token equivalent) as an interim measure, with explicit documentation that CAC integration is a Phase II requirement. Confirm with DLA GTPOC whether alternative MFA is acceptable for Phase I deliverable acceptance, or whether CAC is a mandatory Phase I demonstration requirement.
Residual Risk	Medium. Alternative MFA operationally addresses the authentication function. The residual risk is a gap in Phase I security posture documentation relative to DoDI 8520.02 requirements.
Risk Owner	SOL Security Lead (integration planning); DLA GTPOC (acceptance standard clarification).
Affected Components / Interfaces	LC-01 (Interface Control — authentication enforcement point); LC-08 (IAM — identity resolution); INT-06 (DoD PKI integration).
Related Requirements	REQ-SEC-001; ASM-008; DEP-003.
Decision or Action Required	Confirm CAC integration feasibility at contract award. If not feasible, document the interim MFA approach and confirm GTPOC acceptance before Phase I demonstration.
SDP Origin	TNA Section 23 (RISK-004); SDP-ART-03 (LC-01 and LC-08 open questions); SDP-ART-05 (INT-06 open questions).

RISK-005 Simulation execution time exceeds the 5-minute preset scenario threshold under concurrent user load.

Likelihood: Medium	**Severity:** Medium	**Origin:** TNA Section 23; PRD Section 26	**Status:** Open	**Artifact:** SDP-ART-06

Cause	ABM simulation complexity grows non-linearly with population size and scenario complexity. Under concurrent user load (20+ users), resource contention in the simulation execution environment may extend execution times beyond the 5-minute threshold for preset scenarios.
Impact	KPP REQ-NF-002 not met. Users require analyst support to schedule simulation runs. Objective O-2 (scenario simulation in under 15 minutes) at risk. Field adoption friction increases.

Mitigation	Profile ABM execution time during Phase I prototype development with realistic population sizes and scenario configurations. Identify computational bottlenecks before Phase II design. Design LC-06 (Simulation Engine) with horizontal scaling and parallel execution capability from Phase I, even if Phase I deployment operates at single-instance scale. Set computational bounds on preset scenario complexity in the scenario library configuration (LC-10). Preset scenarios that are overly complex should be simplified to meet the 5-minute threshold. Concurrent user load test during Phase I usability evaluation to validate execution time under realistic multi-user conditions.
Residual Risk	Low to Medium. Profiling and horizontal scaling design substantially reduce the risk, but execution time under full enterprise-scale load cannot be fully validated until Phase II.
Risk Owner	SOL Lead Architect (simulation engine design); LC-06 implementation team.
Affected Components / Interfaces	LC-06 (Simulation Engine — primary risk component); IF-10 (synthetic population read — performance of this flow contributes to total execution time).
Related Requirements	REQ-NF-002; REQ-NF-003; REQ-F-012; Objective O-2.
Decision or Action Required	No stakeholder decision required at Gate-6. Mitigation is a Phase I design and implementation task. Execution time profiling results should be reported in the Phase I technical deliverable.
SDP Origin	TNA Section 23 (RISK-005); PRD Section 26 (RISK-004 — same risk, different PRD numbering); SDP-ART-03 (LC-06 performance obligations).

RISK-006 **CMMC Level 2 C3PAO assessment not completed before November 10, 2026.**				
Likelihood: Medium	**Severity:** High	**Origin:** TNA Section 23; PRD Section 26	**Status:** Open	**Artifact:** SDP-ART-06

Cause	CMMC Phase 2 mandatory C3PAO assessments begin November 10, 2026 (32 C.F.R. Part 170). C3PAO scheduling lead times are typically 3 to 6 months. If gap assessment and C3PAO scheduling are not initiated immediately at contract award, the November 2026 deadline may not be achievable within the Phase I performance period.
Impact	SOL cannot process DLA CUI in non-federal systems after November 10, 2026, without a completed CMMC Level 2 C3PAO assessment. Phase II operational pilot — which requires processing live DLA workforce data — would be blocked. This is a regulatory compliance failure with direct legal consequence under 32 C.F.R. Part 170.
Mitigation	Initiate CMMC Level 2 readiness gap assessment immediately upon contract award. Do not defer to Phase I Month 2 or later. Schedule C3PAO assessment for Q2 2026 (targeting completion by Q3 2026 to provide margin before the November 10 deadline). Treat CMMC assessment as a critical-path item independent of the ALICE technical development schedule. Budget for C3PAO assessment costs within SOL's operating budget, not from the SBIR Phase I ceiling.

Residual Risk	Medium. The assessment schedule is tight but achievable if initiated immediately. The November 10 deadline is firm; no extension mechanism exists under current regulation.
Risk Owner	SOL Privacy Officer / Security Lead (CMMC readiness); SOL Program Manager (scheduling and budget).
Affected Components	All SOL systems that process DLA CUI — the entire ALICE Phase II operational environment.
Related Requirements	REQ-COMP-003; CON-005; 32 C.F.R. Part 170; NIST SP 800-171 Rev 3.
Decision or Action Required	Gap assessment must begin at contract award. This is a Phase I Month 1 action item (TNA N-06). No stakeholder approval required to initiate; stakeholder notification is appropriate.
SDP Origin	TNA Section 23 (RISK-006); PRD Section 26 (RISK-006); SDP-ART-01 (RL-15, RL-19).

RISK-007 **Membership inference attack success rate exceeds 50% threshold during privacy validation.**				
Likelihood: Low	**Severity:** High	**Origin:** TNA Section 23; PRD Section 26	**Status:** Open	**Artifact:** SDP-ART-06

Cause	Insufficient differential privacy noise during generative model training (epsilon applied too close to or above 1.0), or training corpus too small (below 300 positions), increases the probability that an attacker can infer whether a specific individual's record was used to train the model.
Impact	Synthetic population fails privacy validation (REQ-F-017). Population is quarantined; it cannot be used for simulation or exported. Core privacy architecture fails. If this failure occurs and an unvalidated population were mistakenly used, ALICE would be processing Privacy Act-derived outputs without formal privacy guarantees — a compliance failure.
Mitigation	Apply a conservative working epsilon target of 0.5 during Phase I development (acceptance threshold is 1.0; working margin provides headroom for small population effects). Test synthetic population against established membership inference attack frameworks (e.g., the Yeom et al. shadow model attack or equivalent) before any population is promoted to active status. The atomic promotion design in LC-05 (IF-09) ensures that a failed population is quarantined and the prior validated population remains active — preventing operational disruption from a failed generation cycle.
Residual Risk	Low. Conservative epsilon and mandatory testing before promotion substantially reduce the probability that a non-compliant population reaches the Synthetic Zone.
Risk Owner	SOL Data Scientist (generative model design); LC-05 implementation team.
Affected Components / Interfaces	LC-05 (Synthetic Engine — privacy validation function); IF-08 (training input size is a factor); IF-09 (promotion is blocked on validation failure).
Affected Data Entities	DE-08 (Synthetic Person — quarantined on failure); DE-12 (Generation Metadata — failure documented).
Related Requirements	REQ-F-015; REQ-F-016; REQ-F-017; ADR-007.

Decision or Action Required	No stakeholder decision required at Gate-6. Technical mitigation is a Phase I design task. Privacy validation results must be reported in Phase I technical deliverable.
SDP Origin	TNA Section 23 (RISK-007); PRD Section 26 (RISK-007); SDP-ART-04 (DE-08 data quality rules).

RISK-008 Phase II hosting model not resolved before ATO initiation.

Likelihood: Medium	**Severity:** High	**Origin:** TNA Section 23	**Status:** Open	**Artifact:** SDP-ART-06

Cause	DLA cloud strategy decisions are pending as of July 2026. SOL's non-federal environment is not pre-authorized for IL4. The three hosting options (government-authorized commercial cloud, DLA-furnished environment, CMMC-compliant contractor environment) each have different ATO pathways, timelines, and control inheritance implications.
Impact	Phase II RMF ATO initiation is delayed until the hosting model is resolved. The ATO pathway (control inheritance, Authorizing Official, assessment scope) depends entirely on the hosting model selection. Without this decision, the Phase II ATO timeline cannot be planned.
Mitigation	Escalate hosting model decision as a Phase I Month 1 priority item. Present the three hosting options (TNA Section 19.2) with decision criteria to DLA GTPOC and DLA CIO before end of Phase I Month 2. Begin RMF Prepare and Categorize steps immediately in Phase I regardless of hosting model, since these steps are hosting-model-independent.
Residual Risk	Medium. Dependent on stakeholder decision urgency. The longer the decision is deferred, the more Phase II schedule compresses.
Risk Owner	DLA GTPOC; DLA CIO (hosting model authority); SOL Program Manager (decision facilitation).
Affected Components	All Phase II components — the hosting model determines the deployment environment for the full architecture.
Related Requirements	REQ-NF-009; OQ-004; OQ-005.
Related ADRs	ADR-006 (Phase-Gated Security Posture).
Decision or Action Required	Hosting model decision must be made before Phase I Month 2. DLA GTPOC and DLA CIO decision authority. Present options at Phase I kickoff.
SDP Origin	TNA Section 23 (RISK-008); SDP-ART-03 (deployment section); SDP-ART-05 (INT-06 PKI dependencies on hosting model).

RISK-009 Phase II user adoption failure — Activity Directors do not complete independent scenario runs.

Likelihood: Medium	**Severity:** Medium	**Origin:** TNA Section 23; PRD Section 26	**Status:** Open	**Artifact:** SDP-ART-06

Cause	Field-level supervisors in DLA may perceive ALICE as an evaluation or accountability tool rather than a decision support aid. Alternatively, the tool may require more training than anticipated, or the preset scenario library

	may not map well to the specific operational disruptions Activity Directors in the pilot sub-component actually experience.
Impact	Objective O-5 not met. Phase II adoption rate KPP (>= 80% of licensed users complete at least one independent scenario run per quarter) not achieved. Phase III commercialization and enterprise-wide deployment case weakened.
Mitigation	Involve target Activity Director users in Phase I usability evaluation from the earliest possible point (PRD Section 12.2 requires minimum 3 users in Phase I evaluation). Frame ALICE consistently as planning support and decision preparation, not as an evaluation or reporting mechanism for leadership oversight of individual activities. Design the preset scenario library around the specific operational disruptions most relevant to the pilot sub-component, identified through SME interviews during Phase I ontology construction. Guided onboarding workflow (REQ-UX-006: no more than 30 minutes to complete first-time orientation) reduces the initial adoption barrier.
Residual Risk	Medium. Adoption behavior cannot be fully predicted from architecture design alone; it depends on organizational culture, leadership framing, and field-level experience quality.
Risk Owner	DLA GTPOC (stakeholder framing); SOL UX/design team (interface design).
Affected Components	LC-07 (Decision Support Interface — the user-facing adoption risk component); LC-06 (preset scenario library design).
Related Requirements	REQ-NF-010; Objective O-5; PRD Section 12.2 (usability evaluation).
Decision or Action Required	No immediate stakeholder decision required at Gate-6. DLA GTPOC should plan Phase I usability evaluation participant recruitment in advance.
SDP Origin	TNA Section 23 (RISK-009); PRD Section 26 (RISK-005).

RISK-010 Synthetic data classification ambiguity delays Phase II export governance.

Likelihood: Medium	**Severity:** Medium	**Origin:** TNA Section 23	**Status:** Open	**Artifact:** SDP-ART-06

Cause	NIST SP 800-188 (Synthetic Data Guidance) is not yet finalized (as of July 2026). Federal guidance does not formally authorize differential privacy as an automatic mechanism for reducing data sensitivity classification below CUI (RL-23, IAPP November 2024). A formal Privacy Impact Assessment is the required governance mechanism, but PIA initiation in Phase II may be delayed by DLA governance process.
Impact	Synthetic data exports remain under CUI controls pending the PIA determination. Export recipients must be cleared for CUI. Analytical use cases that require non-CUI treatment of synthetic data are blocked until the PIA is complete. Phase III commercialization scenarios that presuppose public-domain synthetic data are also contingent on the PIA outcome.
Mitigation	ADR-007 establishes CUI-by-default as the operational posture — this enables Phase II synthetic data export to proceed under CUI controls without waiting for the PIA determination. Initiate PIA in Phase II Month 1 by engaging DLA CDO and DLA Privacy

	Officer (TNA N-13). Early initiation provides the longest possible runway for the PIA governance process. Monitor NIST CSRC for SP 800-188 finalization (OQ-006). If finalized before Phase II design, incorporate as the formal framework for the PIA classification determination.
Residual Risk	Medium. CUI-by-default treatment provides operational continuity. The residual risk is delay in achieving a potentially less restrictive classification that could expand synthetic data utility.
Risk Owner	DLA CDO (PIA authority); SOL Privacy Officer (PIA initiation and support).
Affected Components / Interfaces	LC-05 (Synthetic Engine — export workflow); IF-15 (Synthetic Data Export Delivery — CUI controls apply pending PIA).
Affected Data Entities	DE-08 (Synthetic Person — classification at issue); DE-10 (Synthetic Data Export — CUI markings on all exports pending PIA).
Related Requirements	ADR-007; OQ-006; REQ-COMP-001; REQ-COMP-004.
Decision or Action Required	PIA initiation in Phase II Month 1 is a required action. DLA CDO must be engaged at Phase II kickoff.
SDP Origin	TNA Section 23 (RISK-010); SDP-ART-01 (RL-23, RL-24); SDP-ART-04 (DE-08 open questions).

RISK-011 Interface contract drift between service components — implementations diverge from documented contracts.

Likelihood: Medium	**Severity:** Medium	**Origin:** SDP-ART-02 (ADR-001 consequence)	**Status:** Open	**Artifact:** SDP-ART-06

Cause	ADR-001 requires that all twelve ALICE service components communicate exclusively through documented interface contracts. If interface contracts are not maintained as versioned, living governance documents — and if implementations are allowed to deviate from contracts without a formal contract update — silent incompatibilities accumulate between components.
Impact	Integration failures during Phase I or Phase II that are difficult to diagnose because the failure mode is an undocumented interface behavior rather than a defect in any single component. Increased integration testing burden. Potential for incorrect data transformation between components.
Mitigation	Define all interface contracts before implementation of any component begins (required by ADR-001 implementation guidance). Maintain interface contracts as version-controlled artifacts in the project repository. Any implementation that deviates from a contract must trigger a formal contract update before the deviation is accepted. Include interface contract compliance as a mandatory integration test criterion. No service component integration test suite should be accepted without negative test cases verifying contract boundary behavior.
Residual Risk	Low to Medium. The risk is controllable through process discipline. The residual risk reflects the reality that process discipline can degrade under schedule pressure.

Risk Owner	SOL Lead Architect (contract governance); LC implementation team leads (contract compliance).
Affected Components	All twelve logical components (LC-01 through LC-12); all 21 interfaces (INT-01 through INT-06; IF-01 through IF-15).
Related Requirements	ADR-001; ADR-003 (LC-03 canonical model specification is an interface contract).
Decision or Action Required	No stakeholder decision required. Process governance task for SOL. Interface contract repository structure should be established in Phase I Month 1.
SDP Origin	SDP-ART-02 (ADR-001 consequences — interface contract drift identified as an inferred risk).

RISK-012 **LC-12 secrets management credential rotation causes service outage during Phase II.**				
Likelihood: Low	**Severity:** High	**Origin:** SDP-ART-02 (ADR-004); SDP-ART-03 (LC-12)	**Status:** Open	**Artifact:** SDP-ART-06

Cause	REQ-SEC-008 requires annual rotation of encryption keys and service credentials. If any ALICE service component does not gracefully handle credential rotation — for example, caching a credential that expires without automatic refresh — the service will fail when the rotated credential is presented by LC-12. At enterprise Phase II scale, a credential rotation failure during operational hours could affect multiple services simultaneously.
Impact	Service outage affecting one or more ALICE components during operational hours. Depending on which service account is rotated, the impact ranges from data ingestion failure (LC-02 credentials) to complete user access failure (LC-01/LC-08 signing material) to audit log interruption (LC-09 write credentials). All are severity incidents for a CUI system.
Mitigation	Design all ALICE service components to retrieve credentials from LC-12 on each use, not to cache credentials beyond a short TTL. Test credential rotation in the Phase I development environment before Phase II deployment. Rotation test must confirm that all services continue to operate without interruption during a rotation event. Schedule Phase II credential rotation events outside DLA operational hours (06:00-22:00 Eastern per REQ-NF-004). LC-12 must support zero-downtime rotation: both the prior credential and the new credential must be valid simultaneously during the rotation window.
Residual Risk	Low. Rotation testing before Phase II deployment and zero-downtime rotation design substantially reduce the risk. The residual risk is operational error during the rotation event.
Risk Owner	SOL Security Lead (LC-12 design); LC implementation team (credential refresh design in each service).
Affected Components	LC-12 (Secrets Management — primary); all services that consume credentials from LC-12 (all twelve components).
Related Requirements	REQ-SEC-008; ADR-004.

Decision or Action Required	Credential rotation testing must be included in the Phase II deployment acceptance criteria. A rotation test plan must be produced before Phase II deployment.
SDP Origin	SDP-ART-02 (ADR-004 consequence: credential management complexity); SDP-ART-03 (LC-12 security considerations).

RISK-013 Activity scope not precisely encoded in session tokens — Activity Directors access out-of-scope organizational data.				
Likelihood: Low	**Severity:** High	**Origin:** SDP-ART-02 (ADR-004); SDP-ART-03 (LC-01, LC-08)	**Status:** Open	**Artifact:** SDP-ART-06

Cause	The ALICE role-based access control model requires that Activity Directors are restricted to workforce data within their assigned activity scope (REQ-SEC-004). If the session token issued by LC-08 does not precisely encode the user's activity scope, or if LC-04 does not validate the scope claim at query time, an Activity Director could potentially query readiness data for activities outside their authorization.
Impact	Privacy Act-adjacent data exposure: an Activity Director receiving workforce data for an organizational unit outside their authority could trigger a Privacy Act disclosure issue, depending on the data's identifiability. It would also represent a RBAC control failure under NIST SP 800-53 AC-4 (Information Flow Enforcement).
Mitigation	Define the token format specification (identity claims, role claim, activity scope claim, expiration) as a formal Phase I design artifact before LC-01 and LC-08 integration testing begins (identified as an inferred design task in SDP-ART-03). Include explicit negative test cases in LC-04 integration tests: confirm that a token claiming Activity A scope is rejected when querying Activity B data. Activity scope enforcement must occur at the LC-04 query layer, not at LC-07 rendering — this is an architectural requirement documented in the TNA and confirmed in SDP-ART-03.
Residual Risk	Low. Correct token specification and enforced negative testing substantially eliminate this risk. The residual is implementation error.
Risk Owner	SOL Lead Architect (token format specification); LC-08 and LC-04 implementation teams.
Affected Components / Interfaces	LC-01 (token issuance); LC-08 (IAM — scope assignment); LC-04 (scope enforcement at query); IF-12 (scope-restricted readiness data delivery).
Related Requirements	REQ-SEC-003; REQ-SEC-004; NIST SP 800-53 AC-4.
Decision or Action Required	Token format specification must be produced as a Phase I design artifact before integration testing. No stakeholder decision required.
SDP Origin	SDP-ART-02 (ADR-004 consequence: token scope creep identified as an inferred risk); SDP-ART-03 (LC-01 and LC-08 open questions).

RISK-014 Audit log event volume at enterprise scale causes LC-09 storage or throughput degradation.				
Likelihood: Low	**Severity:** Medium	**Origin:** SDP-ART-02 (ADR-005); SDP-ART-03 (LC-09)	**Status:** Open	**Artifact:** SDP-ART-06

Cause	At full enterprise scale — 30,000 positions, 20+ concurrent users, daily ingestion cycles, weekly simulation sessions, and continuous audit event generation — the event volume delivered to LC-09 may be substantially higher than Phase I estimates. Seven-year retention without deletion multiplies the storage burden.
Impact	LC-09 throughput saturation could cause audit events to queue or be dropped, creating audit coverage gaps. This would be a NIST SP 800-53 AU compliance failure. Storage exhaustion could cause LC-09 to fail entirely, which would propagate as a service failure to all components that depend on LC-09 for write confirmation.
Mitigation	Estimate Phase II enterprise-scale event volume during Phase I technical design. The calculation requires: events per ingestion cycle × daily frequency + events per scenario run × expected daily scenarios + baseline user action events per operational hour × operational hours per day. Design LC-09 with asynchronous event ingestion and a durable event queue that decouples audit event receipt from log store write latency. Provision storage for 7-year retention based on estimated enterprise-scale volume with a 50% headroom margin. Implement storage monitoring in LC-11 with alerts at 70% and 90% capacity thresholds.
Residual Risk	Low. Volume estimation and asynchronous design substantially reduce the risk. Storage provisioning with headroom eliminates exhaustion risk if correctly planned.
Risk Owner	SOL Lead Architect (LC-09 throughput design); SOL infrastructure team (storage provisioning).
Affected Components	LC-09 (Audit Logging — primary risk component); LC-11 (Observability — monitors LC-09 storage health).
Related Requirements	REQ-NF-012; REQ-SEC-009; NIST SP 800-53 AU-11.
Decision or Action Required	Enterprise-scale audit event volume estimate must be produced during Phase I technical design. Storage provisioning for Phase II deployment must be based on this estimate. This is a Phase I design task, not a stakeholder decision.
SDP Origin	SDP-ART-02 (ADR-005 consequence: event volume at enterprise scale); SDP-ART-03 (LC-09 open questions).

RISK-015 DPMAP aggregate-only extract schema not formally defined — individual performance records delivered in INT-03.				
Likelihood: Low	**Severity:** High	**Origin:** SDP-ART-04 (DE-03); SDP-ART-05 (INT-03)	**Status:** Open	**Artifact:** SDP-ART-06

Cause	The DoDI 1400.25, Vol. 431 constraint requires that only aggregate performance tier distributions (by occupational series and grade band) may be ingested from DPMAP — no individual performance ratings. If the data use agreement or extract specification does not formally define the aggregate-only schema and enforce it technically, the DPMAP extract could include individual records. An individual-record DPMAP extract delivered to ALICE would constitute a Privacy Act violation.
Impact	Receipt of individual DPMAP performance records would be a Privacy Act compliance failure (5 U.S.C. § 552a; DoDI 1400.25 Vol. 431). LC-02 PII detection would flag the records and abort ingestion, preventing them from entering the Processed Zone — but the delivery itself would represent a governance failure requiring formal incident response.
Mitigation	Define the DPMAP aggregate-only extract schema formally in the data use agreement, with explicit exclusion of individual-record fields. Require DLA HRMS or the DPMAP system owner to confirm in writing that the extract mechanism is technically incapable of including individual ratings in the defined schema. Implement a data structure validation check in LC-02 specifically for INT-03 receipts: confirm that no individual-record fields are present before any processing occurs. Include DPMAP schema compliance testing in the Phase I integration acceptance criteria for INT-03.
Residual Risk	Low. DUA schema definition and technical validation create a two-layer defense. The LC-02 PII detection scan is the backstop if both other controls fail.
Risk Owner	DLA HRMS / DPMAP system owner (extract schema definition); SOL Privacy Officer (DUA schema review); LC-02 implementation team (data structure validation).
Affected Components / Interfaces	INT-03 (DPMAP Ingestion — the delivery channel for this risk); LC-02 (ingestion validation backstop).
Affected Data Entities	DE-03 (Person-Position Link — performance tier attribute derived from DPMAP aggregate).
Related Requirements	REQ-COMP-002; REQ-INT-003; DoDI 1400.25, Vol. 431.
Decision or Action Required	DPMAP DUA schema specification must be negotiated with DLA HRMS and DPMAP system owner before INT-03 is activated. This is a pre-Phase I data governance task.
SDP Origin	SDP-ART-04 (DE-03 data quality rules and open questions); SDP-ART-05 (INT-03 inferred risk in open questions).

RISK-016 De-identification specification not completed before DCPDS data delivery — Privacy Act records ingested without validated controls.

Likelihood: Medium	**Severity:** High	**Origin:** SDP-ART-04 (DE-03, DE-05)	**Status:** Open	**Artifact:** SDP-ART-06

Cause	The de-identification specification document — defining the precise field removal list, tokenization method, and aggregation approach for DCPDS and DLA TMS records — is a required pre-ingestion governance artifact

	(identified as an inferred design task in SDP-ART-04). If DLA delivers a DCPDS extract before this specification is jointly approved by the DLA Privacy Officer and SOL Privacy Officer, LC-02 may lack the precise field definitions required to guarantee complete de-identification.
Impact	Ingestion of records with incompletely specified de-identification creates a risk of residual PII fields entering the Processed Zone. If any Privacy Act-protected individual information reaches the Processed Zone, it constitutes a Privacy Act violation (5 U.S.C. § 552a), an architecture invariant breach (AP-1), and an ADR-002 zone boundary failure requiring immediate incident response.
Mitigation	Produce the de-identification specification document as a Phase I Month 1 deliverable, before any DLA data is received. The specification must be reviewed and approved by both the DLA Privacy Officer and the SOL Privacy Officer before any DLA data flows to the ALICE environment. Gate the INT-01 and INT-02 data use agreement execution on completion and approval of the de-identification specification. LC-02 PII detection scan is the technical backstop but must not be relied upon as the primary control; the specification must be the first line of defense.
Residual Risk	Medium. The PII detection scan in LC-02 provides technical backstop protection. The residual risk is that the detection scan configuration is based on the same (potentially incomplete) field definitions as the specification.
Risk Owner	SOL Privacy Officer (specification authorship); DLA Privacy Officer (approval authority).
Affected Components / Interfaces	LC-02 (Data Ingestion — de-identification implementation); INT-01 (DCPDS/DCHRMS); INT-02 (DLA TMS).
Affected Data Entities	DE-03 (Person-Position Link); DE-05 (Certification Currency Record) — both require de-identification from Privacy Act source records.
Related Requirements	5 U.S.C. § 552a; AP-1 (Privacy as Architectural Invariant); ADR-002; REQ-NF-008; REQ-COMP-001.
Decision or Action Required	De-identification specification must be approved before any DLA data is delivered to the ALICE environment. This is a Phase I Month 1 critical-path task. DLA Privacy Officer engagement must be established at contract award.
SDP Origin	SDP-ART-04 (DE-03 and DE-05 open questions and inferred design tasks — identified during Data Catalog construction).

RISK-017 OPM FWD proxy data format schema not mapped to ALICE canonical model before the DLA data decision point — Phase I ingestion blocked.

Likelihood: Low	**Severity:** Medium	**Origin:** SDP-ART-05 (INT-05)	**Status:** Open	**Artifact:** SDP-ART-06

Cause	INT-05 (OPM FWD) is the Phase I proxy fallback when DLA-specific data is unavailable. If the LC-03 schema mapping for the OPM FWD data format is not developed before the DLA data access decision point (approximately

	Phase I Month 2, when the DUA status becomes clear), Phase I ingestion will be blocked even via the proxy path.
Impact	Both INT-01 (DLA data pending DUA) and INT-05 (proxy path schema not ready) are unavailable simultaneously. Phase I ontology construction and synthetic generation are blocked. Phase I timeline is jeopardized.
Mitigation	Develop the LC-03 OPM FWD schema mapping in Phase I Month 1, in parallel with DCPDS schema mapping development — not as a later contingency. The OPM FWD data format documentation is publicly available; schema mapping development does not require DLA access or approvals. Test INT-05 ingestion in the Phase I development environment before the DUA decision point. The proxy path should be operational before the primary path is confirmed.
Residual Risk	Low. The OPM FWD data format is public and schema mapping development can proceed immediately at contract award without any DLA coordination dependencies.
Risk Owner	SOL Lead Architect (LC-03 schema mapping); LC-03 implementation team.
Affected Components / Interfaces	LC-03 (Schema Abstraction — OPM FWD mapping scope); INT-05 (OPM FWD — the interface that would be blocked).
Related Requirements	REQ-F-005; ASM-002.
Decision or Action Required	No stakeholder decision required. Phase I Month 1 technical task for the LC-03 implementation team.
SDP Origin	SDP-ART-05 (INT-05 open questions — identified during Interface Catalog construction).

RISK-018 Phase I acceptance standard for proxy-based synthetic validation not confirmed — DLA GTPOC rejects Phase I deliverable.

Likelihood: Medium	**Severity:** High	**Origin:** SDP-ART-05 (INT-05 open questions; OQ-010)	**Status:** Open	**Artifact:** SDP-ART-06

Cause	Phase I deliverable acceptance depends on whether DLA GTPOC will accept fidelity and accuracy validation results derived from OPM FWD proxy data as evidence of ALICE architecture viability when DLA-specific DCPDS data is not available during Phase I. The PRD identifies this as OQ-010 (open question), and the acceptance standard has not been confirmed in any source document.
Impact	If the GTPOC requires DLA-specific data fidelity validation for Phase I acceptance and DLA data is not available during Phase I, the deliverable acceptance criterion cannot be met. Phase II funding recommendation would be withheld. This is the highest consequence outcome for the Phase I program.
Mitigation	Confirm the Phase I acceptance standard with DLA GTPOC at Phase I kickoff — this is the first agenda item for the kickoff meeting, not a question to defer. Document the accepted evidence standard in the Phase I performance plan

	or a kickoff meeting decision memorandum signed by the GTPOC. Design the Phase I technical deliverable to provide the maximum possible DLA-specific validation evidence, even if partial, to supplement proxy-based validation. If the GTPOC requires DLA-specific data validation, escalate DUA execution as the critical path item — the GTPOC's acceptance standard drives the urgency of RISK-001 mitigation.
Residual Risk	Medium. The residual risk after confirmation is low if the GTPOC accepts proxy-based validation; it remains High if DLA-specific data validation is required and DLA data is not available within the Phase I period. The interaction with RISK-001 (DUA execution) makes this a compound risk.
Risk Owner	DLA GTPOC (acceptance standard authority); SOL Program Manager (confirmation and documentation).
Affected Components	Phase I deliverable scope and acceptance criteria — affects all Phase I components.
Related Requirements	OQ-010; PRD Section 12.2 (MVP success criteria); REQ-F-005 (OPM FWD proxy acceptance).
Decision or Action Required	GTPOC must confirm the Phase I acceptance standard at Phase I kickoff. This is a non-negotiable early program action. The answer directly affects RISK-001 urgency and the Phase I performance plan structure.
SDP Origin	SDP-ART-05 (INT-05 open questions, OQ-010 — identified during Interface Catalog construction).

4. Risk Interaction Analysis

Several risks in the register interact such that the materialization of one risk elevates the likelihood or impact of others. The following table documents the primary risk interactions to support integrated risk management.

Primary Risk	Interacting Risk(s)	Interaction Description	Combined Effect if Both Materialize
RISK-001 (DUA not executed)	RISK-003 (fidelity below threshold); RISK-018 (acceptance standard)	If DUA is not executed, Phase I relies entirely on OPM FWD proxy data. If fidelity is also below threshold with proxy data, Phase I has no compliant synthetic validation evidence. If the acceptance standard also requires DLA-specific validation, the Phase I deliverable cannot be accepted.	High — compound failure of Phase I deliverable acceptance.
RISK-003 (fidelity below threshold)	RISK-007 (membership inference attack)	Small population sizes that drive fidelity failures also drive higher membership inference attack risk. Both are caused by insufficient training corpus.	High — combined failure means synthetic population cannot be promoted (fails both fidelity and privacy validation simultaneously).
RISK-004 (CAC	RISK-013 (activity scope	If CAC is unavailable in Phase I and an alternative MFA is	Medium — creates Phase II redesign scope

Primary Risk	Interacting Risk(s)	Interaction Description	Combined Effect if Both Materialize
unavailable in Phase I)	token drift)	implemented, the token format specification may be developed for the interim MFA mechanism rather than for CAC. If CAC token format differs materially, scope encoding may require redesign in Phase II.	for LC-08 and LC-01 if Phase I token format does not carry over to CAC implementation.
RISK-006 (CMMC not completed)	RISK-008 (hosting model unresolved)	If the hosting model is not selected before Phase II begins, the CMMC assessment cannot be scoped correctly (the CMMC boundary depends on which systems process DLA CUI, which depends on the hosting model). The two risks share the same scheduling constraint.	High — both risks on the Phase II critical path compound to delay Phase II operational access.
RISK-015 (DPMAP schema not defined)	RISK-016 (de-identification spec not completed)	Both risks involve inadequate pre-ingestion data governance documentation. Both require DLA Privacy Officer engagement before data ingestion begins. If either is incomplete, the corresponding ingestion pipeline (INT-03 or INT-01/INT-02) cannot be safely activated.	High — both risks materialized simultaneously would mean ALICE has no compliant data source during Phase I.
RISK-016 (de-identification spec incomplete)	RISK-001 (DUA not executed)	If DUA execution is delayed, it reduces the pressure to complete the de-identification specification (since no DLA data can be received without a DUA). This creates a risk that specification development is also deferred, producing a compound delay when the DUA is eventually executed.	Medium — both deferred together may compress the timeline between DUA execution and safe data ingestion.

5. Risk Response Register — Actions by Phase I Timeline

The following table organizes required risk response actions by Phase I execution timeline. Actions are sequenced to address compound risks and critical-path dependencies first.

Action Window	Risk(s) Addressed	Action Required	Owner	Output / Confirmation
At contract award (before Phase I Month 1)	RISK-001, RISK-006, RISK-016, RISK-018	(1) Initiate DUA coordination with DLA GTPOC and DLA CDO. (2) Initiate CMMC Level 2 gap assessment. (3) Begin de-identification specification drafting. (4) Request Phase I acceptance standard	SOL Program Manager; SOL Privacy Officer.	DUA draft initiated; CMMC gap assessment started; de-identification spec outline drafted; GTPOC acceptance

Action Window	Risk(s) Addressed	Action Required	Owner	Output / Confirmation
		confirmation from GTPOC.		standard documented.
Phase I kickoff meeting	RISK-002, RISK-003, RISK-004, RISK-008, RISK-018	(1) Confirm DCHRMS migration schedule for pilot sub-component (OQ-004). (2) Confirm pilot sub-component selection (OQ-001). (3) Confirm CAC integration feasibility (ASM-008). (4) Confirm hosting model decision timeline (OQ-004). (5) Confirm and document GTPOC Phase I acceptance standard.	DLA GTPOC (information and decisions); SOL PM (documentation).	Kickoff meeting decision memorandum with confirmed answers to each item.
Phase I Month 1	RISK-005, RISK-011, RISK-017	(1) Develop OPM FWD proxy schema mapping in LC-03. (2) Establish interface contract repository and first contract drafts. (3) Begin ABM framework license review (ASM-005). (4) Produce token format specification (RISK-013 prevention). (5) Produce role ontology specification (DE-02 inferred task).	SOL Lead Architect; implementation team.	LC-03 OPM FWD mapping validated; interface contract repository established; token format spec approved; ontology specification drafted.
Phase I Month 2	RISK-014, RISK-015	(1) Complete enterprise-scale audit event volume estimate for LC-09 Phase II storage provisioning. (2) Complete DPMAP aggregate-only schema definition and coordinate with DLA HRMS for DUA inclusion (RISK-015). (3) Confirm EBS access authorization status (OQ-007 / RISK — EBS access deferral decision).	SOL Lead Architect; SOL Privacy Officer; DLA GTPOC.	LC-09 Phase II storage estimate documented; DPMAP DUA schema confirmed; EBS access decision made.
Phase I Months 3–5	RISK-003, RISK-007	(1) Execute synthetic generation with Phase I training corpus. (2) Validate fidelity (KS test, chi-squared; target ≤ 5% deviation). (3) Validate privacy (membership inference attack; target ≤ 50%). (4) Document all results in DE-12 Generation Metadata. (5) If fidelity fails: implement augmentation strategy and document.	SOL Data Scientist; LC-05 implementation team.	DE-12 Generation Metadata records with validation results; fidelity and privacy audit reports for Phase I technical deliverable.
Before Phase II deployment	RISK-012	(1) Execute credential rotation test in Phase II pre-deployment environment.	SOL Security Lead; LC-12	Rotation test report; zero-downtime rotation

Action Window	Risk(s) Addressed	Action Required	Owner	Output / Confirmation
		Confirm all services continue operating without interruption during rotation. (2) Document rotation test results in Phase II deployment acceptance criteria.	implementation team.	confirmed.
Phase II Month 1	RISK-010	(1) Initiate Privacy Impact Assessment with DLA CDO and DLA Privacy Officer. (2) Provide DE-12 Generation Metadata records from Phase I as PIA technical evidence. (3) Monitor NIST CSRC for SP 800-188 finalization.	SOL Privacy Officer; DLA CDO; DLA Privacy Officer.	PIA initiation documented; PIA scope and timeline agreed with DLA CDO.

6. Gate-6 Summary and Decision Required

What Was Created

Artifact 6 (Risk Register) consolidates 18 risks across six source origins: TNA Section 23 (10 risks), PRD Section 26 (cross-referenced but renumbered in the TNA), and SDP-ART-02 through SDP-ART-05 (8 new risks identified during SDP cross-artifact analysis). Each risk record provides: a risk statement, cause, impact, likelihood and severity ratings, mitigation actions, residual risk, risk owner, affected components and interfaces, related requirements and ADRs, and the decision or action required. The Risk Interaction Analysis in Section 4 documents six compound risk relationships that could produce materially worse outcomes if multiple risks materialize simultaneously. The Risk Response Register in Section 5 organizes required actions by Phase I execution timeline.

New Risks Identified in This Artifact

- **RISK-011:** Interface contract drift between service components. Source: ADR-001 consequence analysis.
- **RISK-012:** LC-12 credential rotation causes service outage. Source: ADR-004 / LC-12 security analysis.
- **RISK-013:** Activity scope not encoded correctly in session tokens. Source: ADR-004 / LC-08 token specification gap.
- **RISK-014:** LC-09 audit log event volume at enterprise scale. Source: ADR-005 / LC-09 storage analysis.
- **RISK-015:** DPMAP aggregate-only schema not formally defined. Source: DE-03 data quality rules / INT-03 interface analysis.
- **RISK-016:** De-identification specification not completed before DCPDS data delivery. Source: DE-03 / DE-05 inferred design tasks.
- **RISK-017:** OPM FWD proxy schema not mapped before DLA data decision point. Source: INT-05 Phase I scheduling analysis.
- **RISK-018:** Phase I acceptance standard not confirmed for proxy-based validation. Source: OQ-010 / INT-05 open questions.

Open Issues Requiring Stakeholder Decision at Gate-6

- **[Critical]** RISK-018: DLA GTPOC must confirm the Phase I acceptance standard for proxy-based synthetic validation at Phase I kickoff. This confirmation must be documented. The answer directly determines whether RISK-001 is a critical-path blocker.
- **[Critical]** RISK-016: De-identification specification must be initiated at contract award and approved by DLA Privacy Officer before any DCPDS or DLA TMS data flows to ALICE. This is a program start condition.
- **[High]** RISK-001: DUA initiation at contract award is a program start condition. DLA GTPOC must confirm DUA initiation authority (OQ-002) before or at kickoff.
- **[High]** RISK-006: CMMC Level 2 gap assessment must begin at contract award. SOL leadership must authorize the budget and resource allocation for C3PAO assessment by Q2 2026.
- **[High]** RISK-008: Hosting model decision is required before Phase I Month 2. DLA GTPOC and DLA CIO must be engaged at Phase I kickoff with the three hosting options (TNA Section 19.2) and decision criteria.
- **[High]** RISK-015: DPMAP DUA schema definition must be negotiated with DLA HRMS system owner before INT-03 is activated. SOL Privacy Officer must initiate this coordination.

Decision Required

Gate-6 Decision: Please approve Artifact 6 (Risk Register) to proceed to Artifact 7 (Traceability Matrix), or provide specific revision instructions. If any risk statement, cause, impact, mitigation, residual risk assessment, or risk owner assignment requires modification, please identify the risk ID (RISK-XXX) and the specific change required. All RISK-XXX IDs established in this artifact will be carried forward through the remaining SDP artifacts.