Verdant Benefits — Enterprise Readiness Slice

Preliminary Requirements and System Specification

Document Type: Pre-Pipeline Functional Specification (M0 Deliverable) **Version:** 0.1 (Initial intake synthesis) **Date:** 2026-07-06 **Prepared For:** AI-Native Software Delivery Pipeline (VH M0–M7) — Epic/Feature Decomposition **Classification:** Published Demonstration Artifact

> **Demonstration notice.** Verdant Benefits and its personnel are fictional; the scenario is a composite. The requirements, specification structure, provenance discipline, and all build artifacts generated from this document are real and independently verifiable. No fictional entity herein is intended to resemble any actual company.

Provenance legend (per-requirement tags):

- **[E]** Extracted — derived from artifacts (the enterprise customer's vendor security questionnaire, the existing application's schema and route inventory, IdP metadata samples, payroll-provider API docs)
- **[S]** SME-stated — stated in stakeholder interviews (role attributed)
- **[I]** Inferred — synthesized by the audit; **flagged for confirmation before build**

Provenance note for this segment: unlike a greenfield venture, a funded startup's audit can extract from a living codebase — [E — codebase review] appears throughout, and carries the highest evidentiary weight in this document.

---

1. System Overview

1.1 What Is the Enterprise Readiness Slice?

Verdant Benefits is an eight-person, seed-funded ($2M) benefits-administration SaaS: ~40 SMB customers manage employee benefit elections, enrollment windows, and payroll deduction sync through Verdant's web application. **[S — CTO/co-founder, Interview 1; E — customer list]** Verdant has signed its first enterprise customer — a 5,000-employee logistics company — contingent on passing a vendor security review. **[E — the customer's 212-question security questionnaire; S — CEO]** This build delivers the **enterprise readiness slice**: single sign-on, role-based access control, SOC 2-shaped audit logging and evidence export, and data-governance controls — **retrofitted onto the existing application without rewriting it**

(Constraint C-3), and explicitly delivering the compliance *surface*, not the compliance *program* (§8).

1.2 Problem Statement

[E — questionnaire sections 3, 5, 7, 9; S — CTO] The security review fails today on four grounds: password-only authentication with no customer-IdP federation; a flat two-role permission model (admin/user) that cannot express the customer's HR-vs-benefits-broker-vs-employee access requirements; no queryable audit trail of sensitive actions; and no articulable data-retention or deletion capability. The deal's close date gives the readiness work a contractual clock **[S — CEO]**; the engineering team is the CTO plus two — the build cannot consume the product roadmap (C-3's origin).

1.3 Operating Environment

- **Existing stack:** single-tenant-schema multi-tenant web app (Node/Postgres), ~140 authenticated routes, session-cookie auth, 2 roles. **[E — codebase and route-inventory review]**
- **Scale:** ~40 SMB tenants (~6,200 total employees) today; the enterprise tenant adds ~5,000 employees and its own IdP (Entra ID). **[E — questionnaire; S — CTO]**
- **Money in flight:** per-employee deduction/contribution amounts sync to one payroll provider per tenant (2 providers live). **[E — payroll sync module review]**

1.4 Key Technical Approach

Three new pure-software systems (Identity & Access, Audit & Evidence, Data Governance) integrating with the **existing application as an internal seam** (X1): the slice attaches at defined boundaries — an authentication front-door, an authorization middleware interposition, an event-emission hook layer, and schema-adjacent governance tables — leaving existing behavior intact behind a regression boundary (C-3, AT-2).

2. Stakeholders and System Roles

Role	Person (fictional)	Interest	Interview provenance
CTO / co-founder	P. Anand	Retrofit without rewrite; team velocity preserved; honest scoping	Interviews 1–3 **[S]**; codebase review **[E]**
CEO / co-founder	N. Osei	The enterprise close date; questionnaire pass; investor optics	Interview 2 **[S]**

Role	Person (fictional)	Interest	Interview provenance
Enterprise customer IT (counterparty)	—	Entra SSO, role separation, audit evidence, DSR handling	Questionnaire + requirements addendum **[E]**
Existing SMB customers	—	Nothing breaks; no forced SSO	Support-ticket themes **[E]**

3. Architecture & Decomposition Model

System A — Identity & Access: SSO federation (SAML 2.0 + OIDC), session management, and the RBAC engine replacing the flat model. **System L — Audit & Evidence:** append-only sensitive-action event log; auditor/customer evidence export. **System D — Data Governance:** retention policies, data-subject export/deletion, PII classification registry. **System X — Seams:** X1 the existing Verdant application (internal seam); X2 customer IdPs (Entra/Okta metadata); X3 payroll-provider APIs (existing, hardened at the boundary).

Constraint C-1 — Monetary representation (hard constraint, scoped)

All monetary amounts crossing the payroll seam (deduction/contribution payloads) are integer cents (`cents: i64`); floats prohibited. The slice does not create new monetary computation, but every payload it logs, exports, or retains preserves the cents representation exactly (AT-1). *Pipeline note: enforced by deterministic validation.*

Constraint C-2 — Seam idempotency

IdP metadata refresh, SCIM-adjacent operations (if enabled per OQ-6), and payroll-boundary event capture are idempotent under replay, keyed by source identity.

Constraint C-3 — Additive retrofit; regression boundary

The slice shall not require modification of existing route handlers beyond middleware interposition and hook emission; all existing SMB-tenant behavior (password auth for non-SSO tenants, current workflows) is preserved and regression-tested as a boundary condition (AT-2). **[S — CTO: "if this rewrites my app, we've failed"]**

Constraint C-4 — Evidence immutability

Audit events and evidence exports are append-only, tamper-evident (hash-chained per tenant-day), and never editable through any application path.

4. System A — Identity & Access

A1 — SSO Federation

- REQ-A1.1 **[E — questionnaire §3]** The system shall support per-tenant SAML 2.0 and OIDC federation: tenant-admin-configurable IdP metadata (X2), signed assertions/tokens validated per spec, with Entra ID and Okta as the certified reference IdPs.
- REQ-A1.2 The system shall support just-in-time user provisioning on first SSO assertion, mapping IdP attributes to Verdant identity (email as join key; attribute map per tenant). (Directory-sync SCIM: OQ-6.)
- REQ-A1.3 **[E — support themes; S — CTO]** SSO shall be per-tenant opt-in: non-SSO tenants retain password authentication unchanged (C-3); SSO-enabled tenants may set `SSO_REQUIRED`, disabling password login for that tenant (break-glass: OQ-3).
- REQ-A1.4 Session management shall be centralized in the slice: configurable per-tenant session lifetime and idle timeout **[E — questionnaire §3.4: 8h max / 30m idle for the enterprise tenant]**, revocation on deprovisioning signal, concurrent-session policy per tenant.

A2 — Role-Based Access Control

- REQ-A2.1 **[E — questionnaire §5; S — CTO]** The system shall replace the flat model with tenant-scoped roles: `TENANT_ADMIN, HR_ADMIN, BENEFITS_BROKER, PAYROLL_OPERATOR, EMPLOYEE, AUDITOR_READONLY` (full coverage in all authorization consumers), each mapped to a permission set over the existing route inventory. **[E — the 140-route inventory is the mapping's authoritative domain]**
- REQ-A2.2 Authorization shall interpose as middleware over existing routes (C-3): every authenticated request evaluates tenant + role + permission; denials return uniformly (`ERR_FORBIDDEN`) and emit audit events (L1).
- REQ-A2.3 **[E — questionnaire §5.2]** `AUDITOR_READONLY` and `EMPLOYEE` shall hold no mutation permissions by construction (AT-12-class exhaustive check); broker roles are scoped to assigned employer groups only.
- REQ-A2.4 Role assignments are tenant-admin-managed, dual-logged (assignment + first use), and exportable as an access review report **[E — questionnaire §5.6 quarterly access review requirement]**.

5. System L — Audit & Evidence

L1 — Sensitive-Action Event Log

- REQ-L1.1 **[E — questionnaire §7; codebase review]** The system shall emit append-only audit events, via the X1 hook layer, for the sensitive-action catalog:

authentication events (success/failure/SSO/logout/revocation); authorization denials; role and permission changes; benefit-election creation and modification; payroll-sync payload dispatch and acknowledgment (with cents-exact amounts, C-1); PII record access by non-employee roles; data-governance actions (D1/D2); configuration changes.

- REQ-L1.2 Events carry actor, tenant, timestamp (UTC), acted-on entity, before/after where applicable, and request correlation id; the per-tenant-day hash chain (C-4) renders tampering evident.
- REQ-L1.3 **[E — questionnaire §7.3]** The log shall be queryable by tenant admins (their tenant only) across actor, entity, action, and time range, with results exportable (CSV/JSON).

L2 — Evidence Export

- REQ-L2.1 **[S — CEO; E — questionnaire cover letter]** The system shall generate the **security-review evidence pack** on demand: SSO configuration attestation, role/permission matrix as deployed, access-review report, audit-log coverage statement mapped to the sensitive-action catalog, retention-policy configuration, and DSR capability demonstration record — rendered to PDF with generation timestamp and hash manifest.
- REQ-L2.2 Evidence artifacts are immutable snapshots (C-4), retained per D1 policy, and reproducible: the same period regenerates identically (AT-7-class).
- REQ-L2.3 SIEM forwarding (Splunk HEC) is deferred: OQ-5.

6. System D — Data Governance

D1 — Retention Policies

- REQ-D1.1 **[E — questionnaire §9; I — defaults flagged]** The system shall enforce per-category retention: benefit-election records (plan year + 7 years, default **[I — flagged; broker/counsel to confirm ERISA-driven value]**), audit events (400 days hot, archival beyond), terminated-employee PII (grace period then D2 pipeline), session/telemetry (90 days) — all tenant-visible as configuration and enforced by scheduled, logged jobs.

D2 — Data-Subject Export & Deletion

- REQ-D2.1 **[E — questionnaire §9.4]** The system shall produce a per-employee data export (all PII and election records, machine-readable) on tenant-admin request, logged as a sensitive action.
- REQ-D2.2 The system shall execute deletion requests via a two-stage pipeline (soft-mark with reversal window → hard anonymization), preserving referential integrity of payroll history through anonymization rather than row deletion **[S — CTO; E —**

schema review: payroll rows FK employees], with completion evidence logged (L1) and retention-policy conflicts surfaced, never silently overridden.

D3 — PII Classification Registry

- REQ-D3.1 **[E — schema review]** The system shall maintain the PII classification registry (table.column → category: `IDENTITY, CONTACT, FINANCIAL, HEALTH_ADJACENT, EMPLOYMENT`) — initialized from the audit's schema review, CTO-confirmed — driving D1/D2 scope and the questionnaire's data-inventory answer. Registry changes are versioned and audited.

7. System X — Seams

Contracted boundaries: typed payloads, versioned interfaces, idempotent operations; counterparty behavior — including the existing application's — specified at the boundary with provenance.

X1 — The Existing Verdant Application (internal seam)

- REQ-X1.1 **[E — codebase review]** Integration attaches at four defined points only: (a) the authentication front door (session issuance delegated to A1); (b) authorization middleware interposition (A2.2); (c) the event-emission hook layer (L1 catalog); (d) governance-adjacent tables (D1–D3). No other modification of existing handlers is in scope (C-3).
- REQ-X1.2 **[I — flagged]** The route inventory (140 routes as extracted) is assumed complete; routes added during the build must register in the permission map before deploy (`ERR_UNMAPPED_ROUTE` fails closed, not open).

X2 — Customer IdPs

- REQ-X2.1 Tenant IdP metadata (Entra/Okta reference set **[E — metadata samples from the enterprise customer]**) is imported, validated, refresh-scheduled, and versioned; signature-validation failures fail closed with tenant-admin notification.

X3 — Payroll Provider Boundary (existing, hardened)

- REQ-X3.1 The slice shall wrap the two existing payroll dispatch paths with boundary capture: payload logging (C-1 cents-exact), acknowledgment correlation, and idempotent retry keyed by dispatch id — without altering provider-facing formats (C-3). **[E — payroll module review]**

8. Constraints and Exclusions

8.1 Scope Boundary (published coverage map)

In scope: the readiness slice of §§4–7. **Explicitly out of scope, v0.1: the compliance program itself** — SOC 2 is an organizational audit of policies, personnel practices, vendor management, and change control; this build delivers the *technical-controls surface and its evidence*, not certification, policy authorship, or the audit engagement (**the load-bearing exclusion — S — CTO and CEO aligned, Interview 2**); rewriting or re-architecting the existing application (C-3); SCIM directory sync (OQ-6); SIEM forwarding (OQ-5); customer-facing trust portal (OQ-7, deferred); penetration testing and remediation of pre-existing application vulnerabilities beyond the slice's boundaries (tracked separately **[S — CTO]**); multi-region data residency (OQ-4).

8.2 Technical Constraints

C-1 cents-exact monetary payloads at the payroll boundary; C-2 idempotent seam operations; C-3 additive retrofit with regression boundary; C-4 hash-chained evidence immutability; fail-closed authorization for unmapped routes (X1.2); per-tenant isolation in every query path the slice introduces.

9. Open Questions and Assumptions

#	Status	Question / Ambiguity	Assumption / Resolution path
OQ-1	OPEN	Enterprise tenant's exact role-to-IdP-group mapping	Attribute map assumed group-claim-driven **[I]**; customer IT workshop to confirm before UAT
OQ-2	OPEN	Password-auth deprecation timeline for SSO tenants	`SSO_REQUIRED` per-tenant flag suffices v0.1 **[S — CTO]**
OQ-3	OPEN	Break-glass access when a tenant's IdP is down	Assumed: time-boxed, dual-logged emergency admin

#	Status	Question / Ambiguity	Assumption / Resolution path
			path **[I — flagged; questionnaire §3.7 asks]**; CTO to rule
OQ-4	OPEN	Data residency (customer asked about region pinning)	Out of v0.1; single-region attested **[E — questionnaire response draft]**
OQ-5	OPEN	SIEM forwarding (Splunk HEC) requested by customer IT	Deferred; evidence export (L2) satisfies the review per the customer's addendum **[E]**; the L1 event stream is forwarding-ready by construction
OQ-6	**DEFERRED**	**SCIM directory sync.** The enterprise customer's IT requested SCIM provisioning/deprovisioning during the requirements addendum call. **[E/S]** Explicitly deferred from v0.1 — JIT provisioning (A1.2) plus revocation-on-signal (A1.4) satisfies the review; full SCIM is a scope-change candidate post-close.	The identity model (A1.2's attribute mapping) and session revocation path were designed to admit SCIM without structural rework
OQ-7	OPEN	Customer-facing trust/status portal	Deferred; evidence pack (L2.1) is the v0.1 vehicle

#	Status	Question / Ambiguity	Assumption / Resolution path
OQ-8	OPEN	Retention default for election records (7-year assumption)	**[I — flagged]** ERISA-driven; broker/counsel to confirm before D1 defaults ship

10. Acceptance & Performance

10.1 Business Acceptance Tests (selected)

- **AT-1 (property):** every payroll-boundary payload logged, exported, or retained preserves cents-exact amounts equal to the dispatched values, over the full corpus.
- **AT-2 (regression boundary):** the existing SMB regression suite passes unchanged post-retrofit; non-SSO tenant flows are byte-identical at the API level where contracted.
- **AT-3:** SAML/OIDC conformance against the Entra and Okta reference configurations, including signature-failure fail-closed behavior.
- **AT-5:** exhaustive route-permission check — every route in the inventory maps to the matrix; `EMPLOYEE` and `AUDITOR_READONLY` reach zero mutation paths; unmapped-route requests fail closed.
- **AT-7:** evidence-pack regeneration for a fixed period is hash-identical; audit-chain verification detects a seeded tamper.
- **AT-9:** IdP metadata refresh and payroll-boundary retries are replay-safe (zero duplicate effects).
- **AT-11:** DSR pipeline — export completeness against the PII registry; deletion anonymizes without breaking payroll referential integrity; conflicts surface per D2.2.
- **AT-13:** session policy enforcement — enterprise tenant's 8h/30m limits; revocation-on-signal terminates sessions ≤ 60 s.

10.2 Performance Targets

Authorization middleware overhead ≤ 10 ms p95 per request; SSO assertion processing ≤ 500 ms; audit-event emission non-blocking to request path; evidence pack generation ≤ 3 minutes. **[I — sized from §1.3; flagged]**

Appendix A (provenance source register): enterprise customer vendor security questionnaire (212 questions) + requirements addendum; existing-application codebase and 140-route inventory review; schema review (PII registry basis); IdP metadata samples (Entra, Okta);

payroll module review; stakeholder interviews 1–3. Appendix B (acceptance traceability) and the M7-generated build package are published alongside this document on the case-study page.