

90-Day Pilot Pre-Flight Checklist.

Two parallel lanes, customer-side configuration and Sparcle-side preparation, that must complete in the two-week deployment window before the eight-week use window begins. Maps directly to the Bolt and Aeira threat models.

1 Pre-pilot · Two parallel lanes

☐ Customer-owned ☐ Sparcle-owned

Customer (your security + platform team)

- ☐ **IdP wiring.** Configure Okta / Entra / OneLogin / Auth0 / Google / Zoho, or any compliant OIDC provider (OIDC on web and desktop; SAML 2.0 sign-in on the web, desktop next), with required claims: `tenant_id · user_id · region · office · role_band · employment_type · country · is_admin`. Backs Aeira §01 B4.
- ☐ **Per-tenant CMK provisioned** in Vault, AWS KMS, or the local file-backed KMS. PKCS#11 HSM and Azure Key Vault are on the roadmap. Backs Aeira §01 B5 + §03.
- ☐ **LLM endpoint chosen + contracted.** OpenAI Enterprise / Azure OpenAI / Bedrock / on-prem Llama / Mistral / Aleph Alpha. Confirm endpoint logging + replay policy with vendor.
- ☐ **Egress / network rules.** Allow-list Aeira API, LLM endpoint, and source-system endpoints; deny everything else. Confirm your self-hosted tier has zero outbound to Sparcle.
- ☐ **Postgres hardened** per your DBA standard: at-rest encryption, restricted DB role, query logging if required. Aeira does not enforce Postgres-side controls.
- ☐ **Endpoint controls on user devices.** FileVault / BitLocker, MDM enrollment, code-signing enforcement. Threat model out-of-scopes physical compromise.
- ☐ **Bridge consent mode chosen.** Default vs. require-every-action — set tenant-wide. Backs Bolt §02.
- ☐ **Top-10 sources identified** for late-bind backfill priority (see Sparcle lane). Provide list of source ACL primitives Aeira must respect.
- ☐ **Pilot users defined** (up to 30). Include at least one of each persona: executive, engineer, finance, HR, regional rep, to exercise the 8-axis ACL.
- ☐ **Security review window booked.** CISO / SecArch review before kickoff; threat-model walkthrough in week 2.
- ☐ **Procurement docs requested.** DPA template, MSA template, BAA (if PHI could reach Sparcle).
- ☐ **Pen-test summary shared** when Sparcle's external test is done. An external firm is testing Bolt in October 2026, no report yet; this pilot can fund an accelerated scope.

Sparcle (you'll see these completed)

- ☐ **Trial sidecar delivered** (signed binary, embedded Postgres, Contoso 2,573-row demo corpus). Customer can run before any infra work.
- ☐ **Helm chart / docker-compose tuned** for customer's VPC sizing. Production deployment artifacts in customer's internal registry.
- ☐ **Connector backfill** — `check_permissions()` implementations for the top-10 sources you identified. Today: 6 of 103 sources have it; 4-10 more land during pilot's week 1-2.
- ☐ **Per-tenant CMK rotation runbook** + your KMS adapter pre-configured.
- ☐ **End-to-end ingest saga wired** for the chosen connectors (~1-2 days from green-light).
- ☐ **Audit-verifier binary delivered** + walkthrough scheduled with your CISO team.
- ☐ **Threat-model documents** (Aeira + Bolt) reviewed with your SecArch in week 1-2.
- ☐ **Security evidence pack** delivered in week 1-2: internal hardening run (completed 2026-05-13), SBOM, and the standalone audit verifier your team runs offline against your own deployment. An external firm is testing Bolt in October 2026, no report yet; an accelerated third-party test scoped to this pilot is available as a contract trigger.
- ☐ **Pre-filled SIG Lite + CAIQ** handed over to your procurement at kickoff.
- ☐ **Tenant onboarding:** first pilot user accounts (up to 30) provisioned + persona assignments validated against ACL.
- ☐ **Compliance handbook + IR plan** handed over.

Tier scope: This checklist applies to every self-hosted Bolt tier — **Authorize**, **Backbone**, and **Certify** (customer-hosted; recommended for regulated workloads). All Bolt tiers are self-hosted inside your own perimeter with your own LLM; there is no Sparcle-managed hosting tier. See the compliance handbook §4.1 sub-processor table.

Timeline + Acceptance.

90-day pilot: two weeks deploy, eight weeks use, two weeks review and decide, with the remaining days as buffer. Use cannot begin until Phase B sign-off; sign-off requires every deployment row complete.

② Phase A · Discovery + sign-on · Days -7 → 0

DISCOVERY	-7 → -3	Sparcle: deliver trial sidecar + demo screencast. Customer: stand up trial in dev VM, see Contoso ACL personas filter live. Joint: review the 10-artifact sales portfolio (leave-behind, CISO brief, TCO, architecture, compliance handbook, threat models, vertical brief).
SCOPE LOCK	-3 → -1	Joint: sign pilot MSA + DPA (plus BAA if PHI in scope, SCC if EU). Lock the connector list (top-10 + extended), pilot-user list, success criteria.
KICKOFF	Day 0	Joint kickoff call. Hand off the pre-filled SIG Lite / CAIQ. Schedule weekly Sparcle-side check-ins.

③ Phase B · Deployment · Days 1 → 14

INFRA	1 → 5	Customer: Helm chart or docker-compose deployed in VPC; per-tenant CMK provisioned; egress allow-list applied. Sparcle: tune sizing, complete top-10 connector backfills.
IDP + AUTH	3 → 7	Customer: IdP configured with the 9-claim contract. Joint: first SSO login test; verify JWT validation rejects malformed tokens with 401 + emits no audit event.
CONNECTORS	5 → 12	Joint: wire the chosen connectors (typically: SharePoint / Confluence / Slack / Jira / Salesforce / Workday / Snowflake / ServiceNow / GitHub / GDrive, depending on customer's primary data). Verify each connector's ACL semantics with a test document tagged for restriction.
AUDIT CHAIN	8 → 10	Customer security: run <code>aeira-audit-verify</code> binary on an audit-chain export. Confirm Ed25519 signatures validate against your KMS public key. Modify a byte, confirm verifier reports the break.
THREAT-MODEL WALKTHROUGH	8 → 12	Joint: CISO / SecArch reviews Bolt + Aeira threat models against the deployed system. Document any custom mitigations.
SECURITY EVIDENCE	10 → 13	Sparcle: deliver the evidence pack (internal hardening run, SBOM, offline audit verifier); scope an accelerated third-party pen-test if the pilot funds one. Customer: review with your security team.
PHASE B GATE	14	Joint sign-off: all Phase B rows complete. Sign the deployment-acceptance form on p.3. Use cannot begin until this signs.

Validation + Sign-Off.

The eight-week use window starts only after Phase B sign-off. Acceptance criteria define what "successful pilot" means.

④ Phase C · Use, then review · Days 15 → 90

USER ONBOARDING	15 → 21	Up to 30 pilot users on Bolt desktop + browser extension + PWA. Each onboarded against their assigned persona; ACL behavior validated per user.
WORKFLOW CAPTURE	22 → 63	Users run real cross-source workflows. Each user logs at least 5 multi-source workflows. Sparcle tunes connectors from the weekly check-ins and the issues your team reports. Usage data stays in your deployment.
MEASUREMENT	56 → 70	Measure against acceptance criteria below. Time-on-task, query latency, ACL-correctness checks, audit-chain integrity samples.
REVIEW + DECISION	71 → 84	Joint: review acceptance criteria and sign the one-page outcomes memo. Decision: convert, expand the scope, or end with no further obligation. Reference-case slide drafted only if you agree.
BUFFER	85 → 90	Held for delays. The decision is due by day 90.

Acceptance criteria — what "successful pilot" means

- ACL correctness.** Zero recorded incidents of a user retrieving a document outside their 8-axis ACL scope. Validated by structured test set + observed user activity.
- Audit-chain integrity.** Customer's verifier runs at weeks 4, 7 and 10: all three sample runs return chain-valid + signature-valid. Customer holds the chain export, not Sparcle.
- Latency.** p95 search latency under customer-defined SLA (typical: 250-500ms on 100K-doc corpus; benchmark published before pilot end).
- Connector reliability.** Each connector polls within its declared cadence; zero connector-side credential leaks; conformance harness green throughout.
- User adoption.** ≥70% of pilot users active in the last 2 weeks of use (weeks 9 and 10). ≥5 multi-source workflows logged per active user.
- No new sub-processors introduced.** Per your self-hosted Bolt commitments. Validated in compliance handbook §4.1 review.
- Threat-model walkthrough sign-off.** CISO / SecArch confirms in writing that the deployed system matches the documented threat model + no critical residual risks remain unfunded.

Phase B (Deployment) acceptance: sign at Day 14

Customer security lead · printed name + role

Customer platform lead · printed name

Sparcle deployment lead · printed name + role

Date (YYYY-MM-DD)