Vendor due-diligence (TPRM) packet — CAIQ-lite / VSA-style self-assessment

DRAFT — not reviewed by counsel. NOT A CERTIFICATION. NOT LEGAL ADVICE.

What this is. The answers a one-person vendor can give an issuer's third-party-risk team today, assembled only from facts already written in this repository, each with its file path. Where the repository holds no fact the answer says **Not yet answered — ask us at contact@reservebeat.com** rather than a plausible-looking claim. It follows the domain order of the Cloud Security Alliance CAIQ v4 (free self-assessment; STAR Level 1 publication optional) and the Vendor Security Alliance VSA-Core questionnaire (free). It is refreshed at the first enterprise sale and whenever a cited document changes.

Three honest headlines, first:

1. **No SOC 2 report.** `docs/SOC2_HYGIENE.md` opens: "Reserve Ledger has no SOC 2 report and this document is not one." It maps controls to the Trust Services Criteria and names the gaps a single-host deploy cannot close.
2. **No insurance bound.** Tech E&O, cyber, media-liability rider and general liability are DEFERRED, traction-gated. A request for a certificate of insurance is itself a re-open trigger.
3. **One operator.** ReserveBeat LLC (North Carolina, formed 2026-09-30) has a single member and no staff. Organisational controls that assume a second person (segregation of duties across people, HR screening) do not exist; the maker/checker control is enforced in code instead (§3 below).

---

1. Company and contact

Question	Answer	Evidence
Legal entity	ReserveBeat LLC, a North Carolina limited liability company, formed 2026-09-30	Public record: NC Secretary of State
Contact for security and privacy	contact@reservebeat.com; postal line as printed at https://reservebeat.com/contact	`packages/strings/claims.json` `privacy_rights`, `security_report_inbox`
Vulnerability disclosure	`/security` page + `security.txt`; disclose.io core safe-harbor terms adopted; acknowledgement within five business days as a target, not a service level; no bounty	`claims.json` `security_txt_note`, `security_scope_in`, `security_scope_out`
Product description	Reserve and supply figures for stablecoins, reported as stated by issuers and measured on-chain; evidence bundles with hash-chain anchoring; a public read API and a single-tenant issuer workflow	`docs/board/METHODOLOGY.md`
Headcount	1 (the Sole Member)	—
Subprocessors	DigitalOcean (hosting, US), PostHog (analytics, US), Stripe (payments), email relay (Resend), Google (optional sign-in)	`claims.json` `privacy_processors_*`

2. Governance, risk and compliance (CAIQ: GRC, A&A)

Question	Answer	Evidence
Independent audit or certification (SOC 2, ISO 27001)	None. No report exists and none is in progress.	`docs/SOC2_HYGIENE.md` first paragraph
Written security policy	Operating rules exist as runbooks and a hygiene checklist, not as a signed policy document	`docs/SOC2_HYGIENE.md` "Operating rules"; `docs/THREAT-MODEL.md`
Threat model	Published: what is protected, actors, trust boundaries, entry points, threats and answers, egress, untrusted inputs, assumptions, and what it does not claim	`docs/THREAT-MODEL.md` §1–§9
Risk register	Not as a separate artifact; risks are tracked as decisions and held questions (`docs/QUESTIONS-HELD.md`)	—
Customer-facing assurance claims	Every customer-facing sentence about assurance must come from the locked claim library; "if the sentence is not in claims.json, it does not ship"	`docs/SOC2_HYGIENE.md` operating rule 5; `packages/strings/claims.json`
Insurance	None bound (see headline 2)	—

3. Identity and access management (CAIQ: IAM)

Question	Answer	Evidence
Authentication	Credentials verified server-side in one place (`POST /auth/login`); scrypt hashes; 12-hour HS256 JWTs signed by an env-bound secret that fails closed when unset; `RESERVE_AUTH_REQUIRED=1` in production	`docs/SOC2_HYGIENE.md` "Access control"
Sign-in abuse controls	Rate-limited, constant-shape sign-in wall; per-user bearer invalidation	`docs/SOC2_HYGIENE.md` gaps table
MFA / SSO for the product	**Not implemented.** Named gap with a named trigger.	`docs/SOC2_HYGIENE.md` gaps row "No MFA / SSO"; `docs/QUESTIONS-HELD.md` §5.1
Authorisation model	Roles in append-only `user_role_history`, checked at the action instant; auditor tokens rejected on non-read methods; mutating endpoints refuse a body `user` that differs from the token identity unless ADMIN	`docs/SOC2_HYGIENE.md` "Authorization", "Identity binding"; `docs/AUTHZ-MATRIX.md`
Segregation of duties	Maker/checker enforced in code for break resolution and bundle approval: the proposer cannot approve their own change	`docs/SOC2_HYGIENE.md` "Change management & auditability"
Least privilege in the database	API runs as `reserve_app` (SELECT-only + row-level security pinned to the tenant); owner role reserved for migrations, seed and pipeline jobs	`docs/SOC2_HYGIENE.md`
MFA on the operator's vendor consoles	**Not yet answered — ask us at contact@reservebeat.com** (GitHub security settings are recorded in `docs/CONSOLE-BATCH.md` §4; DigitalOcean, registrar, Alchemy and Stripe console MFA are not recorded in the repo)	—

Question	Answer	Evidence
Access reviews	One account per person; roles per person (operating rule 2). No periodic review cadence is written.	`docs/SOC2_HYGIENE.md` operating rule 2

4. Data security and privacy (CAIQ: DSP, CEK)

Question	Answer	Evidence
Classification of customer data	Statements (raw bank/custodian files), tokenised counterparties, reconciliation records, evidence artifacts, account records	`docs/THREAT-MODEL.md` §1
PII handling	Counterparty identifiers HMAC-tokenised with an env-bound key; ingestion fails closed without the key; the key cannot be rotated in place	`docs/SOC2_HYGIENE.md`; `docs/RUNBOOK-KEY-ROTATION.md` §5.1
Raw-file retention	Raw bank files purged at 90 days	`docs/SOC2_HYGIENE.md`
Evidence retention	7 years (`retention_years`)	`docs/SOC2_HYGIENE.md`
Email addresses in records	Audit records written since 27 July 2026 carry a one-way hash, never the address; a prod check on 2026-10-10 found 0 of 37,220 audit records holding an `@`	`claims.json` `privacy_rights_self_close`
Encryption in transit	TLS at the Caddy edge for reservebeat.com; HSTS `max-age=31536000; includeSubDomains`, `nosniff`, `referrer-policy`, `x-frame-options: DENY` measured on prod 2026-10-12 and 2026-10-14; inside the compose stack traffic is plaintext past the host (named gap)	`docs/CONSOLE-BATCH.md` §14.2 row 1; `docs/SOC2_HYGIENE.md` gaps row "No TLS in the stack itself"
Encryption at rest	**Not yet answered — ask us at contact@reservebeat.com** (DigitalOcean volume encryption and database-level encryption are not stated in the repo)	—
Secrets management	Environment variables only; never in config tables or `.sql`; `deploy/.env.prod` mode 0600, gitignored; a secrets inventory and per-key rotation procedure exist; cadence annually or on exposure	`docs/SOC2_HYGIENE.md` "Secrets (F27)"; `docs/RUNBOOK-KEY-ROTATION.md` §2–§7
Data residency	United States (hosting subprocessor DigitalOcean; analytics PostHog US)	`claims.json` `privacy_processors_hosting`, `privacy_processors_analytics`
Data export	Evidence bundles in a documented format readable by an Apache-2.0 verifier the customer may run and modify	`verifier/FORMAT.md`; `LICENSE`
Deletion on account close	Closing an API account revokes every key and webhook endpoint and removes the address from the account record; audit and usage records are append-only and survive	`claims.json` `privacy_rights_self_close`

Question	Answer	Evidence
Use of customer data for model training	Not done; no sentence anywhere in the claim library offers it	`packages/strings/claims.json` (absence)

5. Change management and secure development (CAIQ: CCC, AIS)

Question	Answer	Evidence
Source control and review	Every change lands as a commit; main is protected; changes land through a pull request that must pass the `ci-gate` check	`docs/SOC2_HYGIENE.md` "Source control"; `scripts/lane/land-pr.sh` header
Static analysis	SAST gate: semgrep (vendored rules), ruff, eslint security plugin, actionlint; floors enforced in CI	`docs/SAST.md`
Dynamic testing	DAST gate: OWASP ZAP against a throwaway stack, one scanner per principal, floors enforced in CI	`docs/DAST.md`
Secret scanning	gitleaks in CI; dev-box secret-guard hooks. GitHub's own push protection is N/A on a personal-account private repo	`docs/SOC2_HYGIENE.md` gaps row (read 2026-10-14); `.github/workflows/ci.yml`
Dependency management	Dependabot, monthly cadence; majors review dated 2027-01	`docs/CONSOLE-BATCH.md` §16
Migrations	Numbered and forward-only	`docs/SOC2_HYGIENE.md`; `docs/MIGRATIONS.md`
Rollback	Documented rollback runbook; the prod deploy record names its rollback deploy	`docs/RUNBOOK-ROLLBACK.md`
Third-party penetration test	None. DAST is self-run.	`docs/DAST.md` (no external tester named)

6. Logging, monitoring and incident response (CAIQ: LOG, SEF)

Question	Answer	Evidence
Audit logging	`audit_log` rows for logins (including failures), role grants/revokes, ingestion, reconciliation, break and bundle lifecycle	`docs/SOC2_HYGIENE.md` "Audit trail"
Log integrity / off-host shipping	**Gap:** no off-host log shipping; a host compromise can edit local logs	`docs/SOC2_HYGIENE.md` gaps row
Edge access logs	Every request header logged at the edge with Cookie/Authorization redacted; rolled file, 30 days	`deploy/Caddyfile`
Monitoring and alerting	Dead-man checks that page a human (ntfy) for prod health, stale off-box dumps and the public surface; a watcher of the watcher	`docs/RUNBOOK-backup-restore.md` "Dead-man that reaches a human"; `deploy/rb-ops/README.md`

Question	Answer	Evidence
Incident response procedure	Severity table; detect, contain (levers strongest first), preserve evidence, notify, post-mortem template	`docs/RUNBOOK-INCIDENT-RESPONSE.md` §0–§5
Customer breach notification	72 hours from awareness (DPA Cover Page default; confirm at signature)	`docs/legal/drafts/C3-dpa-common-paper-v1.1.md`
Status page	**Not yet answered — ask us at contact@reservebeat.com** (none is named in the repo)	—

7. Business continuity and resilience (CAIQ: BCR) — BCP = the runbooks + the drills

Question	Answer	Evidence
Backups	Nightly `pg_dump`; off-droplet pull to a second machine; empty or stale dumps page the dead-man	`docs/RUNBOOK-backup-restore.md` ("Prod — nightly automated backup + off-droplet pull"; "Dead-man")
Restore drill	Restore from the off-droplet copy drilled 2026-07-19 (PASSED); 2026-10-05 drill RTO 228 s; Drill 4 and Drill 7 in the drills log	`docs/RUNBOOK-backup-restore.md`; `docs/DRILLS.md` Drill 4, Drill 7
Failure drills	Ingestion failure, bridge-timing expiry, anchor verification from a tombstoned artifact, restore, redeploy loss, nightly leg failure, off-box copy	`docs/DRILLS.md` Drills 1–7 with run log
Standby	A second recorder on an independent machine (NUC) since 2026-09-09, hourly watched	`docs/RUNBOOK-STANDBY-NUC.md`; `deploy/rb-ops/README.md` `standby_status`
Single host, no failover	**Gap, stated:** documented recovery beats redundancy at this stage; backups are off-host but the primary is one droplet	`docs/SOC2_HYGIENE.md` gaps table
Recovery objectives (RPO/RTO)	RPO ≈ 24 h (nightly dump); RTO measured 228 s for the database restore step (2026-10-05); full-stack RTO from bare metal is "one `provision.sh` run" and is not timed in the repo	`docs/RUNBOOK-backup-restore.md`; `docs/SOC2_HYGIENE.md`
"What if the one-person vendor disappears"	(a) The verifier and the bundle format are Apache-2.0: any examiner, auditor or customer may run, modify and redistribute them without asking (`LICENSE`); (b) customer data is exportable in that format; (c) a single-tenant customer's instance can be rebuilt from `provision.sh` by a successor operator; (d) code escrow is **not** in place — a request for it is a deal point	`LICENSE`; `verifier/FORMAT.md`; `docs/SOC2_HYGIENE.md` "Availability & recovery"

8. Infrastructure and endpoint security (CAIQ: IVS, UEM)

Question	Answer	Evidence
Hosting	One DigitalOcean droplet running the compose stack behind Caddy; services bound to the host	`docs/SOC2_HYGIENE.md`; `deploy/`

Question	Answer	Evidence
Network exposure	Edge is Caddy with TLS; operations access over Tailscale SSH; a read-only `rbops` ssh user with a forced command for operations reads	`deploy/rb-ops/README.md` (`prod` verb; `droplet/README.md`)
Container restart	Containers restart with the docker daemon; stack is one `provision.sh` run from bare metal	`docs/SOC2_HYGIENE.md`
Patch cadence (OS, images)	Dependencies monthly via Dependabot; image majors dated 2027-01; OS patch cadence on the droplet is **Not yet answered — ask us at contact@reservebeat.com**	`docs/CONSOLE-BATCH.md` §16
Operator endpoint controls (disk encryption, screen lock, EDR)	**Not yet answered — ask us at contact@reservebeat.com**	—
Physical security	Cloud provider's (DigitalOcean) for prod; the standby NUC and the dev box are in the operator's home — **Not yet answered — ask us at contact@reservebeat.com** for any further statement	`docs/RUNBOOK-STANDBY-NUC.md`

9. Supply chain and subprocessors (CAIQ: STA)

Question	Answer	Evidence
Subprocessor list and notice	Named on `/privacy` and in the DPA Annex III; 10 business days' notice of a new one (DPA default; confirm)	`claims.json` `privacy_processors_*`; `docs/legal/drafts/C3-dpa-common-paper-v1.1.md`
Open-source licence register	Audited register of dependencies and their licences	`docs/legal/OSS-LICENSES-2026-09.md`
Provider terms reviewed	Terms of every upstream provider (RPC, timestamping, email, analytics, registrar) read and banked, with gaps named	`docs/legal/PROVIDER-TERMS.md`
Timestamping providers	Used on public terms that promise nothing; neither leg is contracted; absence of an anchor is disclosed	`docs/board/METHODOLOGY.md` §5
Vendor risk management of our own vendors	Informal: PROVIDER-TERMS review plus spend caps (Alchemy cap set by the operator)	`docs/legal/PROVIDER-TERMS.md`

10. Human resources (CAIQ: HRS)

Question	Answer	Evidence
Background checks	N/A — no employees or contractors with data access	—
Security training	N/A — single operator; no training record exists	—
Offboarding	N/A today; per-user bearer invalidation and role revocation exist in the product for when it is needed	`docs/SOC2_HYGIENE.md`

11. Questions the packet cannot answer from the repo

1. Disk encryption, screen lock and patch cadence on the dev box and the standby NUC (§8).
2. MFA on the DigitalOcean, registrar, Alchemy and Stripe consoles (§3).
3. Encryption at rest on the droplet's volume (§4).
4. OS patch cadence on the droplet (§8).
5. Whether a status page will exist (§6).
6. Whether to publish this self-assessment as CSA STAR Level 1 once the first enterprise conversation needs it (free; optional).