BuildPaid OS

SOC 2 Pre-Attestation Evidence Package

Control self-assessment mapped to the AICPA Trust Services Criteria

SP Prospective Partners LLC dba BuildPaid · September 11, 2026 · No NDA required to read this document

---

Control self-assessment mapped to the AICPA Trust Services Criteria · Prepared for lender security & compliance review SP Prospective Partners LLC dba BuildPaid · June 23, 2026 · No NDA required to read this document This is not a SOC 2 report. No SOC 2 examination has been performed and no independent service auditor has issued an opinion. This document is a good-faith self-assessment that maps BuildPaid's current and planned controls to the AICPA Trust Services Criteria (TSC), prepared to support vendor due diligence ahead of a formal SOC 2 examination. The status labels — In Place, Partial, Planned — reflect BuildPaid management's own assessment, not an audited conclusion.

How To Read This Document

Status key. In Place — implemented and evidenced today. Partial — partially implemented or operating informally. Planned — intended and on the SOC 2 readiness roadmap. Scope. This assessment covers the Security common criteria (CC1–CC9) plus Availability (A1) and Confidentiality (C1). Processing Integrity and Privacy criteria are not addressed in this version. BuildPaid's assurance today rests primarily on deterministic, provenance-anchored auditability — every capital decision is reproducible and independently verifiable from an append-only event log — which complements, but does not substitute for, a third-party attestation.

Cc1–Cc5 Governance, Risk & Control Activities

Criterion Control Status CC1 Documented governing doctrine, versioned and hash-stamped (current v1.4.0): truth gates In Place money, fail closed, no mutation without a recorded kernel event. The ruleset in force is tied to every verdict. CC1 Formal code of conduct, HR security policies, and independent oversight. Early-stage / Partial founder-led; policies are being formalized. CC2 Security posture and this control assessment published and provided to customers for review. In Place CC3 Fail-closed risk design on the capital path: missing or unevaluable evidence resolves to In Place BLOCKED/HELD, never to a permissive default. CC3 Formal, documented enterprise risk-assessment process and risk register. Planned CC4 Continuous governance sweeper evaluates portfolio invariants on a schedule and emits In Place breach events to the append-only log when a control condition fails. CC4 Formal management control-monitoring program with documented review cadence. Planned CC5 Deterministic governed rules enforced by a single-authority kernel; one governance verdict is In Place the sole decider of capital eligibility and every surface reads it rather than recomputing. CC5 Segregation of duties: BuildPaid governs whether capital may move; the bank signs and In Place moves funds on its own rails. BuildPaid never holds keys and never initiates settlement — a structural separation between governance and settlement.

Cc6–Cc8 Access, Operations & Change

Criterion Control Status CC6 All access over TLS/HTTPS. Token/JWT-gated internal endpoints. Per-organization data In Place isolation. CC6 Physical and environmental controls inherited from subservice organizations (AWS, Vercel), In Place which maintain their own independent security attestations. CC6 Enforced MFA on all administrative access, formal access provisioning/de-provisioning, and Partial periodic access reviews. Provider-level authentication is available; enforcement and review are being formalized. CC6

Encryption at rest for the managed database. Provided by AWS managed Postgres; Partial configuration to be confirmed and evidenced for the audit. CC7 Deploy-time verification gates (syntax/parse checks on every function and inline script before In Place release) and runtime schema validation on emitted payment instructions (ISO 20022 pain.001.001.09 validated against the official XSD with libxml2). CC7 Centralized log aggregation, alerting, vulnerability management, and a documented Planned incident-response plan. CC8 Change integrity: append-only, provenance-hashed (SHA-256) event log; corrections are new In Place chained events, never edits or deletes. Versioned doctrine ties each change to the rules in force. CC8 Formal multi-party change-approval workflow and ticketing. Changes are technically gated; Partial approval workflow is being formalized.

Cc9 / A1 / C1 Risk Mitigation, Availability & Confidentiality

Criterion Control Status CC9 AI is advisory only; the kernel is authoritative. AI cannot move money, override arbitration, In Place bypass a compliance gate, or alter provenance, and every AI signal is hashed to the record before it can influence any action. CC9 Vendor/subservice risk management. Core providers (AWS, Vercel, Stripe) maintain their own Partial attestations; a formal vendor-risk register is being established. A1 Application and data hosted on high-availability managed infrastructure (AWS, Vercel). In Place A1 Automated managed-database backups (AWS RDS). Retention policy and restore testing to Partial be documented and evidenced. A1 Uptime monitoring and a published availability commitment. Planned C1 Per-organization data isolation and a one-way trust model: external systems of record can In Place feed the governed truth layer but cannot mutate it. C1 Demonstration environments use synthetic data; no real borrower PII or financial-account data In Place is present in demos. C1 Confidentiality commitments via MSA and DPA (drafts available for counsel); Partial data-classification policy being formalized.

Subservice Organizations (Inherited Controls)

BuildPaid relies on established providers for infrastructure and runs no payment custody of its own. AWS (infrastructure and managed Postgres), Vercel (application hosting), and Stripe (payment processing) each maintain their own independent security and compliance attestations (e.g., SOC 2, ISO 27001, and PCI-DSS as applicable). A formal SOC 2 examination of BuildPaid would treat these as carved-out subservice organizations. Critically, BuildPaid does not custody, hold, or move funds; settlement occurs on the bank's own rails, so the highest-risk money-movement controls sit with regulated parties, not with BuildPaid.

Roadmap To Attestation

1. Formalize the Partial and Planned controls above into written policies and operating procedures. 2. Adopt a compliance-automation platform (e.g., Vanta, Drata, Secureframe, or Thoropass) to continuously collect control evidence from AWS, Vercel, and the code host. 3. Complete a readiness assessment to close gaps before examination. 4. Engage an independent CPA firm for a SOC 2 Type I examination (controls suitably designed at a point in time). 5. Progress to SOC 2 Type II (controls operating effectively across an observation period, commonly three to twelve months). BuildPaid states its posture plainly: the product is early-stage and pilot-focused, and it is not yet SOC 2 certified. Its assurance story today rests on deterministic, provenance-anchored auditability rather than a third-party attestation, with SOC 2 Type II on the roadmap. A pilot can run under a mutual NDA, MSA, and DPA, and responses to a lender security questionnaire are available on request. We would rather be accurate about what exists than impressive about what does not. SP Prospective Partners LLC dba BuildPaid · buildpaid.ai · app.buildpaid.ai · Sean Pace, Founder · sean@buildpaid.ai This document is a management self-assessment prepared for diligence purposes as of June

23, 2026. It is not a SOC 2 report, an audit, a warranty, or legal advice. Status labels reflect management's own assessment and have not been examined by an independent auditor.
