Control Environment Narrative

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC2.1, CC2.2, CC2.3, CC4.1, CC4.2, CC5.1, CC5.2, CC5.3

Table 2: Document history

Date	Comment
Sep 3 2026	Rewritten with NIST CSF 2.0 maturity scoring
Sep 4 2026	Replaced with SOC 2 narrative v1.0
Sep 4 2026	Recover function re-scored after CTO validation

1 Purpose and Scope

This narrative describes CredX Tech Inc.'s control environment in support of its SOC 2 readiness effort, structured against the AICPA Common Criteria **CC1 through CC9**. It describes controls as designed and, where noted, as implemented in production, and **flags gaps explicitly rather than omitting them**.

CC Reference	Topic Addressed in This Narrative
CC1.1–CC1.5	Control Environment — tone at the top, integrity and ethics, board/oversight, structure, competence, accountability
CC2	Communication and Information
CC3	Risk Assessment
CC4	Monitoring Activities
CC5	Control Activities (policy-to-practice translation)
CC6	Logical and Physical Access Controls
CC7	System Operations
CC8	Change Management
CC9	Risk Mitigation (including vendor/third-party risk)

2 CC1 — Control Environment

2.1 Tone at the Top and Commitment to Integrity

CredX's leadership team has established written expectations for ethical conduct through the **CredX and Ownest Contractor Handbook (v1.1)**, which applies to employees and contractors and sets baseline expectations for conduct, security practices, and business continuity responsibilities. Leadership communicates these expectations directly given the company's small, concentrated team structure, rather than through a large-organization compliance training program.

2.2 Board and Oversight Structure

GAP: CredX does not yet have a formal board of directors or an independent oversight body. In the current target-state governance model described in CredX's Data Security & Privacy Policy, the CEO is designated as the Policy Owner for risk management, with input and review from the full leadership team. Board-level oversight with quarterly updates is an **intended future-state control** as CredX scales. This absence of independent oversight is also reflected in CredX's NIST CSF 2.0 self-assessment, where the "Govern" function is rated low.

2.3 Organizational Structure and Reporting Lines

Full detail is in the Organizational Narrative. In summary, the current leadership team consists of:

- **Leadership** — Kendall Raessler, Founder & CEO. Company vision, strategic direction, and external partner relationships; Policy Owner for Risk Management; Incident Commander under the DR/BCP.
- **Sales** — Kyle Bunbury, Co-Founder & VP, Sales. Revenue generation, enterprise partnerships, and channel expansion; Partner Continuity lead under the DR/BCP.
- **Operations** — Audrey Wilson, Co-Founder & VP, Marketing & Operations. Internal structure, operational systems, marketing execution, and compliance/risk mitigation; Operations & Compliance Lead under the DR/BCP.
- **Technical** — Ray Yip, Chief Technology Officer (also CTO of affiliated company Ownest Inc.). Platform administration, security architecture, and infrastructure; Technology & Infrastructure Lead under the DR/BCP.

Human Resources and Finance are not separately staffed; their responsibilities sit with Leadership and Operations, and are marked [**HR**] where this program assigns work to them.

GAP: The Chief Compliance Officer role described in policy is not confirmed as formally established. CredX's Data Security & Privacy Policy describes a governance model in which the CTO and a CCO jointly oversee data protection and security. A dedicated CCO role has not been confirmed; compliance responsibilities are currently carried by Audrey Wilson under her VP, Marketing & Operations title. This should be clarified with leadership before Type I fieldwork.

2.4 Competence

Leadership brings substantial relevant domain experience:

- **Kendall Raessler** — 25+ years in Canadian financing and lending.
- **Kyle Bunbury** — 20+ years of executive leadership in digital transformation and enterprise systems, including prior board director experience.
- **Audrey Wilson** — 18+ years in the Canadian financial industry across operations, marketing, and regulatory compliance.
- **Ray Yip** — 25+ years building and scaling enterprise and SaaS platforms across e-commerce, payments, and financial services; B.Sc. Honours in Computer Science, University of Manitoba.

CredX additionally draws on two advisors — **Neal Oswald, ICD.D** (30+ years in retail/wholesale financial services digital transformation) and **Carrie Forbes** (Founder, Rockstar Advisory; 2024 International Woman of the Year, Open Banking Expo) — for fintech and digital-transformation guidance.

2.5 Accountability

Accountability for unresolved issues follows a defined escalation pattern: **matters unresolved after five business days escalate to the CEO**. This provides a time-bound accountability mechanism appropriate to CredX's current size, in lieu of a multi-layered management hierarchy.

CredX operates through four functional areas — Leadership, Sales, Operations, and Technical — each currently staffed by one person, with contractors extending capacity. **Functional continuity is explicitly named as a risk** in the DR/BCP, mitigated by a documented cross-function cover arrangement: each function has a designated covering function, confirmed by the CEO at the point of an incident.

3 CC2 — Communication and Information

3.1 Internal Communication

CredX's primary internal communication channel for security and operational incidents is a **dedicated Slack channel**, with a **phone/SMS call tree as backup** if Slack is unavailable. Audrey Wilson drafts partner and merchant incident communications, which Kendall Raessler approves before release; coordination with regulated partners routes through each partner's designated incident contact; and **only the CEO, or an explicit delegate, speaks publicly or to the media**.

3.2 External Communication Commitments

CredX's Data Security & Privacy Policy commits to specific consumer rights and communication channels for privacy-related requests, consistent with Alberta PIPA and PIPEDA:

- **Access** — consumers may request access to their personal information held by CredX.
- **Correction** — consumers may request correction of inaccurate personal information.
- **Deletion** — consumers may request deletion, subject to applicable retention law.
- **Portability** — consumers may request their data in a portable format.
- **Opt-out** — consumers may opt out of specified data uses.

Requests are directed to **privacyteam@credxtech.com** or via CredX's web contact form. These commitments are grounded in Ann Cavoukian's seven Foundational Privacy by Design principles. One open item: **Principle 7 (user-facing consent/access mechanisms) is not yet confirmed as fully implemented.**

3.3 Information Quality and Relevance

Operational information supporting control decisions flows through a small number of channels appropriate to CredX's size: application logs, the transaction/ledger data model, and direct leadership communication in Slack.

CredX notes known limitations in information completeness relevant to decision quality — **integration events such as token refresh failures and rejected webhooks are not currently captured in the audit log** (only in shorter-retention application logs), which constrains the granularity of information available for control monitoring.

4 CC3 — Risk Assessment

4.1 Risk Management Policy Scope

CredX's Risk Management Policy establishes a structured risk assessment process across **seven risk categories**: Strategic; Financial; Operational; Compliance/Regulatory; Technology/Cyber; Third-Party/Vendor; and Reputational.

4.2 Risk Scoring Methodology

CredX uses a **5×5 likelihood-by-impact methodology**: Likelihood 1 (Rare) through 5 (Almost Certain), Impact 1 (Negligible) through 5 (Severe). Risk Score = Likelihood × Impact, producing a range of 1–25.

Tier	Score Range	Description
Low	1–4	Minimal likely effect; routine monitoring sufficient
Medium	5–9	Moderate effect; planned mitigation within normal cycles
High	10–14	Significant effect; active mitigation and tracking required
Critical	15–25	Severe effect; immediate mitigation regardless of cost

4.3 Risk Appetite Statement

CredX maintains **low tolerance** for risk events affecting regulated personal or financial data, credit decisioning integrity, or sponsor bank / lending partner trust — such events require immediate mitigation regardless of cost. CredX maintains **moderate tolerance** for isolated, single-vendor disruptions with contained, non-regulatory impact.

4.4 Current Critical-Tier Risk Drivers

As of the most recent risk register review, CredX's highest-rated risks trace to **two root causes**:

- **Technology architecture finalization** — hosting is confirmed as Heroku Private Spaces (Canadian region), but production verification of the technical controls specified in the Security Architecture Narrative remains incomplete.
- **Unexecuted partner contracts** — sponsor bank, lender, and merchant agreements, including with Peoples Trust Company and Innovation Federal Credit Union, are prospective or pilot-stage and not yet executed.

For context on directional risk trend: **cloud/hosting outage risk was downgraded from Critical (score 15) to High (score 10)** once Heroku Private Spaces hosting was confirmed, illustrating that risk scores are actively revisited as facts are verified rather than held static.

5 CC4 — Monitoring Activities

5.1 Ongoing Monitoring Commitments

CredX's Data Security & Privacy Policy commits to **internal audits and compliance reviews at least annually**. Under the DR/BCP, the full continuity plan and the risk register are reviewed on the same **six-month cycle**, with tabletop exercises twice yearly (Q1 and Q3) and backup restore testing at least twice yearly. The backup policy is confirmed in production; **neither the restore test nor the tabletop has yet been conducted.**

5.2 Monitoring Gaps

GAP: Live security monitoring and SIEM capability does not yet exist. CredX's NIST CSF 2.0 self-assessment scores the "Detect" function at **0 out of 4** — the lowest-rated function in the framework. This is explicitly targeted for Phase 2 (Enterprise Security) of the Layered Security Roadmap.

GAP: No independent audit function or board-level oversight body currently exists to provide separate — as opposed to management-led — evaluation of the control environment.

*Real-time threat detection tools referenced in an earlier, less detailed version of the Data Security & Privacy Policy are **[unconfirmed — to verify with CTO]** as actually deployed, since the more recent and more detailed DR/BCP work independently found the Detect function scored at 0/4. This narrative treats the DR/BCP finding as authoritative.*

6 CC5 — Control Activities

6.1 Access Control Design

CredX's Security Requirements Specification calls for **role-based access control built on least privilege**, with account lockout after repeated failed authentication attempts. Administrative and operational accounts are required to use **MFA**, and production access is restricted, with all admin actions subject to audit logging.

6.2 Employee and Contractor Security

Personnel-level controls are documented in the **CredX and Ownest Contractor Handbook (v1.1)**, which specifies onboarding and offboarding checklists, security and AML training requirements, an annual penetration testing requirement, and vendor audit requirements.

GAP: A quarterly access review is recommended practice for a least-privilege access model but has not yet been scheduled or formalized as a recurring control. Target date: [TBD].

7 CC6 — Logical and Physical Access Controls

7.1 Logical Access Model

CredX applies a role-based, least-privilege access control model across its systems. Administrative and production access additionally requires **MFA**.

7.2 Physical and Environmental Controls

CredX **does not operate its own physical data centers**. The backend platform and PostgreSQL database run on Heroku Private Spaces in the Canadian region, chosen specifically for data residency, with all PII and payment-related workloads confined to the Canadian Private Space. Object storage is AWS S3 in `ca-central-1`, holding merchant logo images only. **Both stores encrypt data at rest at the platform layer.**

Heroku, as the infrastructure provider, manages the underlying physical data center security, environmental controls, and facility access. CredX's physical/environmental control equivalent is therefore **the selection, configuration, and contractual boundary of this managed infrastructure** rather than a self-operated facility.

7.3 Known Access Control Exception — Unauthorized Read Path

GAP: the single-merchant lookup is not role-restricted. It requires only a valid session — no role restriction — unlike every sibling merchant operation, all of which are administrator-only. Session validation confirms an unrevoked session for a non-blocked user but performs **no role check**. The lookup applies no field selection, and the stored POS credential is exposed as a field on the merchant type.

The result is that **any authenticated user of any role can read a merchant's POS access credential through the API**. This is a CC6 logical-access deficiency and an instance of broken function-level authorization (OWASP API Security Top 10), a framework CredX names as an alignment target. *Owner: Technical function. Severity: Critical.*

7.4 Known Access Control Exception — Plaintext Credential Storage

GAP: stored POS integration credentials and the wallet-pass rotating-code secret are held UNENCRYPTED in the production database, inconsistent with CredX's own encryption-at-rest requirement for sensitive data. By contrast, **merchant API keys are properly stored as salted hashes**.

This is a named control deficiency under CC6. *Owner: Technical function. Target remediation date: [TBD].*

This exception is treated as a **top-priority open remediation item** for SOC 2 readiness and **must not be omitted from any narrative or walkthrough**, since an auditor performing code-level review would identify it regardless.

8 CC7 — System Operations

8.1 Incident Detection and Response

CredX's DR/BCP documents a **four-phase incident response lifecycle**: (1) Preparation, (2) Detection & Analysis, (3) Containment, Eradication & Recovery, and (4) Post-Incident Activity. Incidents are classified using severity levels **P1 through P4**, each with a defined response window.

The Incident Response Plan has not yet been exercised via a tabletop test.

8.2 Vulnerability Management

CredX's Security Requirements Specification calls for SAST, DAST, mobile application penetration testing, API security testing/fuzzing, and third-party penetration testing.

GAP: Quarterly independent penetration testing is stated as a target in the Data Security & Privacy Policy; whether this cadence is actually being executed on a recurring basis has not been confirmed and is flagged as unconfirmed pending verification with the CTO.

8.3 Capacity and Availability Management

Specified availability controls include rate limiting and throttling, DDoS protections, health checks with automated restarts, and regular, tested backups.

9 CC8 — Change Management

CredX's primary documented change-control safeguard today is **environment isolation**: development, staging, and production environments are separated via distinct Heroku Private Spaces or strict network segmentation. This isolation reduces the risk that unapproved or untested changes reach production.

GAP: A formal, documented change-management policy — covering code review requirements, deployment approval gates, and rollback procedures — has not yet been confirmed as existing beyond environment isolation. Formalizing and documenting this policy is recommended before SOC 2 Type II fieldwork, since Type II specifically tests operating effectiveness of controls over a period of time. Target date: [TBD].

10 CC9 — Risk Mitigation (Vendor / Third-Party Risk)

CredX depends on a defined set of external systems and sub-service organizations across POS integration, payment/wallet instruments, communications, and credit underwriting. The complete sub-service organization list is documented in full in the System Description.

10.1 Due Diligence on Prospective Regulated Partners

CredX's relationships with sponsor bank and lending partners — **Peoples Trust Company, Innovation Federal Credit Union, and credit-bureau data partner Equifax Canada** — are **prospective or pilot-stage** as of this narrative's date, and formal agreements are not yet executed.

Before executing these agreements, CredX should complete **security and privacy due-diligence questionnaires** with each counterparty to confirm data-handling, security, and regulatory posture, including OSFI-related expectations given Innovation Federal Credit Union's conversion to federal charter status. This due-diligence step is recommended and **not yet formalized as a required pre-contract gate**.

Note: Equifax Canada appears here as a prospective credit-bureau data partner but does not appear among the eleven sub-service organizations in the System Description. Confirm whether a bureau integration exists within the current system boundary. Owner: Ray Yip.

10.2 Ongoing Vendor Oversight

GAP: An annual security review cadence for existing vendors — Clover, Square, Twilio, SendGrid, Ownest — **is recommended as a standard third-party risk mitigation control but has not yet been formalized** as a recurring, scheduled process.

CredX's relationship with **Ownest Inc.** is a named **Tier 1 continuity dependency**; no source-code or technology escrow arrangement has been confirmed as in place. This is tracked as a governance action item owned by Kendall Raessler and legal counsel.

11 Control Gaps Summary

The table below consolidates every control gap named across CC1–CC9 into a single tracking view, to drive remediation planning ahead of SOC 2 Type I readiness and, subsequently, Type II fieldwork.

Gap Description	CC	Owner	Priority
Single-merchant lookup lacks a role restriction, exposing the stored POS credential to any authenticated user of any role	CC6	Technical function	**Critical**
POS integration credentials and the wallet-pass secret stored unencrypted (contrast: API keys are salted-hashed)	CC6	Technical function	**Critical**
Undocumented POS device application outside every system boundary description	CC9	Technical function	High
No live security monitoring / SIEM capability; NIST CSF "Detect" scored 0/4	CC4 / CC7	Ray Yip / Engineering (Phase 2 Roadmap)	**Critical**
Sponsor bank, lender, and merchant contracts (incl. Peoples Trust Company, Innovation Federal Credit Union) not yet executed	CC3 / CC9	Kendall Raessler	**Critical**

Gap Description	CC	Owner	Priority
No formal board of directors or independent oversight body; CEO is Policy Owner for risk with leadership-team input in the interim	CC1	Leadership Team	High
No independent audit function or board-level oversight of the control environment	CC4	Leadership Team	High
Quarterly independent penetration testing cadence stated as a target but not confirmed as actually occurring	CC7	Ray Yip / Engineering	High
Formal, documented change-management / code-review / deployment-approval policy not confirmed beyond environment isolation	CC8	Ray Yip / Engineering	High (before Type II)
Ownest Inc. technology dependency lacks confirmed source-code/technology escrow or transition-plan arrangement	CC9	Kendall Raessler / Legal Counsel	High
Chief Compliance Officer role referenced in policy not confirmed as formally established; compliance duties currently held by VP Ops	CC1	Kendall Raessler / Leadership	Medium
Quarterly access review recommended but not yet scheduled as a recurring control	CC5	Ray Yip / Engineering	Medium
Vendor security/privacy due-diligence questionnaire process for new and existing vendors not yet formalized	CC9	Audrey Wilson / Compliance	Medium
Annual security review cadence for existing vendors not yet formalized as a recurring process	CC9	Audrey Wilson / Compliance	Medium

Target dates are [**TBD**]. CredX leadership is committed to tracking these items to closure and updating this narrative as remediation progresses. This document will be reviewed and reissued at least every six months, or sooner following any material change to governance, infrastructure, or partner contract status.

12 References

- COSO, *Internal Control – Integrated Framework*

- AICPA, *Trust Services Criteria* (SOC 2), Common Criteria CC1–CC9
- NIST Cybersecurity Framework (CSF) 2.0 — https://www.nist.gov/cyberframework
- Ann Cavoukian, *7 Foundational Principles of Privacy by Design* — https://www.privacybydesign.ca
- Government of Alberta, *Personal Information Protection Act* (PIPA)
- Government of Canada, *Personal Information Protection and Electronic Documents Act* (PIPEDA)
- CredX internal source documents: Data Security & Privacy Policy; Risk Management Policy; Security Requirements Specification; CredX and Ownest Contractor Handbook v1.1; Disaster Recovery & Business Continuity Plan v1.4; CredX Partner Data Map