Organizational Narrative

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC1.2, CC1.3, CC1.4, CC1.5, CC3.1, CC3.2, CC3.3

Table 2: Document history

Date	Comment
Sep 3 2026	Rewritten with actual leadership and governance
Sep 4 2026	Replaced with SOC 2 narrative v1.0

1 Purpose and Scope

This Organizational Narrative describes the organizational structure, governance model, leadership roles and responsibilities, personnel security practices, and regulatory positioning of CredX Tech Inc. in support of CredX's SOC 2 readiness effort.

CredX is a pre-revenue fintech company preparing for a SOC 2 Type I examination as its first milestone, with a Type II examination planned once controls have operated over a review period. **This narrative does not assert that CredX has completed or achieved SOC 2 certification.** It documents the organization as designed and as currently operating, and identifies gaps and target-state items honestly where formal structures — such as a board of directors — are not yet in place.

This narrative focuses on *who* and *how CredX is organized and governed*: leadership, reporting lines, segregation of duties, personnel security, the CredX/Ownest affiliated-entity relationship, and regulatory positioning. Technical control detail is left to the Security Architecture and System Architecture Narratives to avoid duplication and inconsistency across the document set.

Organizational structure and governance are foundational to all three Trust Services Criteria in scope: they establish who is accountable for security decisions, who can authorize access and changes, who owns availability and continuity planning, and who is responsible for protecting confidential information. Gaps in governance formality — most notably the absence of an independent board — are therefore treated as directly relevant to this narrative's scope, not as a peripheral concern.

2 Company Overview

2.1 Legal Entity and Stage

Field	Value
Legal Name	CredX Tech Inc.
Stage	Pre-revenue fintech company
Headquarters	Calgary, Alberta, Canada
Registered Address	Suite 159 #406, 917-85 St SW, Calgary, AB T3H 5Z9
General Contact	connect@credxtech.com
Privacy / Security Contact	privacyteam@credxtech.com

CredX is a pre-revenue company. Consistent with its stage, the organization is intentionally small and its governance and control structures are still maturing. This narrative avoids overstating headcount, formality, or control maturity beyond what is currently documented.

2.2 Business Model

CredX operates an **Embedded Value Platform (EVP)** — a closed-loop set of embedded payments, credit decisioning, and merchant lending infrastructure. CredX is a **non-bank technology provider**: regulated processors, sponsor banks, and licensed lenders handle settlement, custody, lending, underwriting, and AML/KYC obligations. CredX provides the technology, data orchestration, and integration layer connecting merchant POS systems to credit and lending partners.

The EVP is organized around six product pillars: **Cost Reduction**, **BoosT** (Balance Offset & Organic Spending Trigger), **Data as a Product (DaaP)**, **Marketing**, **MarketPlace**, and **Orchestration**. The combined structural outcome is referred to internally as the **"MoaT."** Full detail is in the Products and Services Narrative.

2.3 Geographic Footprint

CredX operates in **Canada first**, with U.S. expansion planned for a later stage. As of this narrative's date, operations are Canada-only — the platform supports **CAD only** and does not yet support multi-currency transactions. All in-scope data processing is currently confined to Canadian infrastructure.

3 Organizational Structure & Governance

3.1 Functional Areas

CredX's work is organized into four functional areas, each with a defined owner. Responsibilities throughout this program — including continuity, incident response, and control ownership — attach to the **function**, so that the program remains valid as the team grows and roles change hands.

- **Leadership** — company strategy, vision, external partner and investor relationships, and risk policy ownership.
- **Sales** — revenue generation, enterprise partnerships, channel expansion, and merchant/lender pipeline.
- **Operations** — merchant and partner onboarding, compliance and regulatory tracking, marketing execution, and internal systems.
- **Technical** — platform administration, security architecture, infrastructure, and vendor technical escalation.

Human Resources and Finance are not currently staffed as distinct functions; their responsibilities sit with Leadership and Operations. Where this program assigns a task to an unstaffed function, the assignment is shown in brackets — for example [**HR**] — so that the obligation stays visible rather than disappearing.

3.2 Leadership Team

Each functional area is currently led by a member of the founding team, supplemented by two external advisors. There is no salaried management layer beneath the leadership team at this time.

Function	Name	Title / Role	SOC 2-Relevant Responsibilities
Leadership	Kendall Raessler	Founder & Chief Executive Officer	Company vision, strategic direction, 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, channel expansion. Partner Continuity lead under the DR/BCP
Operations	Audrey Wilson	Co-Founder & VP, Marketing & Operations	Internal structure, operational systems, marketing execution, compliance and regulatory tracking. Operations & Compliance Lead under the DR/BCP
Technical	Ray Yip	Chief Technology Officer	Platform administration, security architecture, infrastructure. **Also CTO of Ownest Inc.** Technology & Infrastructure Lead under the DR/BCP

The Sales, Operations, and Technical function owners each report directly to the CEO, who sits at the top of the reporting line.

3.3 Advisors

Two external advisors sit **outside** the functional structure. They provide guidance to the CEO and leadership team but hold **no management authority, no fiduciary oversight role, and no continuity or incident-response responsibility**.

Name	Advisory Role	Contribution
Neal Oswald, ICD.D	Advisor, Digital Transformation Specialist	Advisory support on fintech and financial-institution digital transformation. Not an employee or officer
Carrie Forbes	Advisor & Fintech Liaison (Founder, Rockstar Advisory)	Advisory support and fintech industry liaison. Not an employee or officer

Contact details for incident purposes are held in the Disaster Recovery Policy, Appendix A.

3.4 Reporting Lines

CredX does not yet maintain a graphical organizational chart as a controlled document; the structure is described here in text form:

- Kendall Raessler (CEO) sits at the top of the internal reporting line. All three VP/CTO-level leaders report directly to the CEO.
- Kyle Bunbury, Audrey Wilson, and Ray Yip each lead their respective functional area and, at this stage, **personally perform much of the work in that function** rather than delegating to subordinate staff.
- Neal Oswald and Carrie Forbes sit outside the formal reporting line as external advisors. They provide guidance but hold **no management authority or fiduciary oversight role**.
- **No layer exists above the CEO.** There is no board of directors, board committee, or independent oversight body.

3.5 Governance Gap: No Formal Board or Independent Oversight Body

CredX does not currently have a formal board of directors or an independent oversight body. Strategic and operational decisions are made by the founder-led leadership team, without an external or independent check at the governance level.

CredX's Data Security & Privacy Policy describes an intended governance model in which board-level oversight, with quarterly updates, forms part of enterprise risk management. **That model is target-state** — no formal board exists today, and quarterly board-level risk reporting is not occurring because there is no board to report to.

This is named here as an explicit governance gap and target-state action item, consistent with CredX's policy of flagging gaps rather than omitting or softening them.

Internal audits and compliance reviews are intended to occur at least annually, independent of the board-level gap above. Confirmation of the first such review's completion and scope is an open item.

4 Roles, Responsibilities & Segregation of Duties

4.1 Ownership Mapping

Risk Management Policy Owner Kendall Raessler (CEO) — owns risk policy and serves as Incident Commander under the DR/BCP.

Technology & Security Ownership Ray Yip (CTO) — owns platform administration, security architecture, and infrastructure decisions; Technology & Infrastructure Lead under the DR/BCP.

Compliance & Privacy Ownership Audrey Wilson (VP, Marketing & Operations) — carries day-to-day compliance and regulatory-risk-mitigation responsibilities and is Operations & Compliance Lead under the DR/BCP, with joint accountability alongside the CTO for breach response. CredX's Data Security & Privacy Policy describes a **Chief Compliance Officer (CCO)** role jointly overseeing data protection and security with the CTO; at present this appears to be an aspirational or target-state title rather than a distinct, separately-held office. This title/scope discrepancy is flagged for clarification.

Partner / Vendor Relationship Ownership Kyle Bunbury (VP, Sales) — owns enterprise partnerships and channel expansion, and is Partner Continuity lead under the DR/BCP. **Kendall Raessler** additionally owns external partner relationships at the CEO level, including oversight of the Ownest affiliated-entity relationship together with legal counsel.

Incident Response Team Composition Current leadership — Kendall Raessler, Ray Yip, Kyle Bunbury, and Audrey Wilson — constitutes the Incident Response Team under the DR/BCP. **No dedicated security or compliance staff sit outside the leadership team today.**

4.2 Segregation of Duties Across Functions

Each of the four functional areas is currently staffed by one person. Functions that a larger organization would segregate across several people — Sales leadership, Operations and compliance oversight, and Technical and security ownership — are each carried by a single functional owner, supported by contractors rather than dedicated deputies.

The consequence for segregation of duties is specific and worth naming: **within the Technical function, administration and review are not separated.** The same function that administers production infrastructure also owns security

architecture decisions, with no independent technical reviewer. This is a design limitation of a four-function organization, not an oversight.

Continuity arrangement. Continuity is maintained at the level of the function, not the individual. Each function has a designated covering function that assumes its responsibilities during an absence:

Function	Covering Function
Leadership	Operations
Sales	Operations
Operations	Technical
Technical	Operations

Operations is the default covering function for Leadership and Sales, and Technical covers Operations. The CEO confirms cover at the point of an incident and may designate a contractor where a function's work requires specialist skills.

As CredX scales, the priority segregation improvement is **separating security administration from security review and approval within the Technical function** — through an independent reviewer, an external advisor, or a contracted security review. Clarifying the CCO/compliance question in the Operations function is the second.

5 Human Resources & Personnel Security

5.1 Governing Document

CredX's onboarding, offboarding, security training, role-based access review, and incident-reporting obligations for personnel and contractors are governed by the **CredX and Ownest Contractor Handbook, v1.1**. Because CredX's current workforce is composed substantially of contractor-model arrangements rather than a large traditional employee base, this handbook is the primary source of record for personnel security practices.

5.2 Onboarding & Offboarding

Per the Contractor Handbook v1.1, onboarding and offboarding procedures — including provisioning and deprovisioning of system access — are documented obligations. This narrative does not assert a specific automated deprovisioning tool or SLA beyond what the handbook specifies; confirmation of current turnaround times and whether deprovisioning is fully executed versus partially manual is [**TBD**].

5.3 Background Checks

Status unconfirmed. The facts reviewed for this narrative do not confirm a specific, formal background-check program — criminal record checks, credit checks, or reference verification — as currently implemented for CredX personnel or contractors. [**TBD**]. This should be confirmed against the Contractor Handbook v1.1 and formalized in writing prior to SOC 2 Type I fieldwork if not already documented.

5.4 Security & AML Training

Security training obligations are addressed in the Contractor Handbook v1.1. **AML training is not a direct CredX obligation** in the same sense it would be for a regulated financial institution, because CredX is not a bank, sponsor bank, or FINTRAC-registered Money Services Business and does not independently conduct KYC/KYB. Those obligations sit with CredX's regulated partners. CredX's own role in an AML-adjacent context is limited to maintaining consent records, audit trails, and secure-transmission logs supporting partner AML/KYC processes.

Confirmation that security awareness training has actually been delivered and tracked — frequency, completion records, role-based content — is [**TBD**].

5.5 Role-Based Access Review

Periodic review of role-based access is an obligation in the Contractor Handbook v1.1. Given CredX's small team size, access review is currently expected to be an **informal, leadership-driven process** rather than a tooling-supported access-recertification workflow. Formal cadence, evidence of completed reviews, and a named reviewer independent of the account holder are [**TBD**].

5.6 Incident Reporting Obligations for Personnel

Personnel and contractor incident-reporting obligations are set out in the Contractor Handbook v1.1, complemented by the DR/BCP v1.4, which defines the Incident Response Team, severity levels (P1–P4), and the four-phase incident-response lifecycle. The two documents are **complementary, not duplicative** — the Contractor Handbook governs personnel-level obligations, while the DR/BCP governs the organization-wide response. Neither replaces the incident response obligations of CredX's regulated partners for their own systems.

5.7 Contractor Arrangements

CredX's workforce model relies on **contractor arrangements** for a meaningful portion of its operating capacity across all four functions, consistent with its pre-revenue stage. Contractors extend a function's capacity but do not currently provide documented cover for it — a contractor engaged by the Technical

function, for example, is not a designated deputy for that function's continuity responsibilities. The degree to which every contractor engagement has been formally onboarded under the handbook is [**TBD**].

6 Affiliated Entity Relationship

6.1 The Ownest Inc. Relationship

Ownest Inc. is an affiliated company with a structural and technical relationship to CredX that is **material to organizational independence and objectivity** in a SOC 2 context.

Attribute	Description
Relationship Type	Software licensing arrangement — CredX's core software, including the UnderwriteFlow decisioning application, is built on a licensed technology stack from Ownest Inc.
Shared Leadership	**Ray Yip serves as Chief Technology Officer of both CredX and Ownest concurrently**
Functional Role	Ownest handles credit underwriting on CredX's behalf: a customer completes a credit questionnaire hosted by Ownest (client-side, directly with Ownest — not routed through CredX's backend); Ownest returns the completed application via webhook; CredX requests loan proposals from Ownest; an accepted proposal becomes the loan terms
Data Boundary	**CredX does not post applicant financial data to Ownest via API.** Only a correlation/loan ID is exchanged over the API integration
Hosting Note	UnderwriteFlow has been referenced elsewhere as hosted on a platform called "Base44." Base44/Ownest should be treated as the hosted decisioning environment; written backup/redundancy guarantees for that environment are not yet confirmed

6.2 Why This Matters for Organizational Independence & Objectivity

Ray Yip's dual role as CTO of both CredX and Ownest means the **same individual holds technology and security decision-making authority over both organizations**, at exactly the seam where CredX's platform depends on Ownest's licensed technology stack for a core function. This is a legitimate consideration for a SOC 2 auditor and for CredX's own risk assessment: it concentrates knowledge and control in one person across an entity boundary, and it means CredX's internal technical oversight of the Ownest dependency is **not fully independent of Ownest itself**.

This is not presented as a disqualifying issue — dual-role technology leadership across closely affiliated companies is a common structure for early-stage related organizations. It is presented honestly as a factor that CredX's eventual board or advisory oversight body should specifically consider.

6.3 Open Item: No Formalized Technology Continuity / Escrow Arrangement

The Ownest relationship is classified as a **Tier 1 (Critical) continuity dependency** in the DR/BCP, because CredX's core lending/underwriting functionality would not operate without it.

No source-code or technology escrow arrangement, documented handover/transition plan, or contractual continuity/support-SLA with Ownest has been confirmed as formalized at this time.

This is a named, tracked governance action item, owned jointly by Kendall Raessler and legal counsel, and should be resolved — or at minimum have a documented remediation timeline — prior to SOC 2 Type II fieldwork given its Tier 1 criticality rating.

7 Regulatory & Compliance Positioning

7.1 Non-Bank Technology Provider Role

CredX is **not a bank, not a sponsor bank, and not a FINTRAC-registered Money Services Business**. CredX does not independently conduct KYC or KYB checks. These obligations belong to CredX's regulated partners — sponsor bank(s) and licensed lender(s) — who handle settlement, custody, lending, underwriting, and AML/KYC compliance. CredX's role is limited to technology, data orchestration, and the integration layer, and its incident-response role with respect to regulated activity is limited to maintaining consent records, audit trails, and secure-transmission logs.

7.2 Sponsor Bank & Lending Partner Relationships

Partner contracts are prospective, not yet executed. CredX has prospective/pilot-stage relationships with **Peoples Trust Company** and **Innovation Federal Credit Union**. As of the DR/BCP v1.4, these relationships are prospective and pilot-stage — **not yet executed contracts**.

Innovation Federal Credit Union has converted to federal charter status and is likely to be regulated by OSFI going forward.

This narrative does not describe these partnerships as active, contracted relationships. Execution status should be re-confirmed at each narrative review cycle.

7.3 Applicable Privacy Law

CredX's primary privacy law obligation is the **Alberta Personal Information Protection Act (PIPA)**, a provincial statute recognized by the federal government as "substantially similar" to, and therefore displacing, **PIPEDA** for Alberta operations. PIPEDA continues to apply to interprovincial or international personal-information handling. CredX is expected to meet both frameworks in practice.

For future U.S. expansion, CredX's policy also references CCPA/CPRA, the Virginia Consumer Data Protection Act, the Gramm-Leach-Bliley Act, and applicable FTC guidance — **though these are not yet operative** given CredX's current Canada-only footprint.

7.4 Breach Notification Standard

Breach notification under both PIPA and PIPEDA is governed by the **"real risk of significant harm" (RROSH)** standard, requiring notification without unreasonable delay, or as soon as feasible, once RROSH is determined.

OSFI's 24-hour reporting requirement applies directly to federally regulated bank and lending partners, not to CredX itself, but it informs and drives the internal escalation SLA design in the DR/BCP so that CredX can support partner reporting timelines. CredX maintains a **24-month breach record log** regardless of RROSH outcome on any individual incident.

7.5 Current SOC 2 Status

CredX is NOT YET SOC 2 certified. CredX is pursuing SOC 2 readiness with a Type I examination targeted first, followed by Type II once controls have operated over a review period.

This narrative and its companions represent the system description and control environment **as designed and as currently in progress** — not a completed or attested certification.

Note: earlier CredX marketing material stated "SOC 2 Compliance – Infrastructure and processes independently audited and certified." **That statement was inaccurate and is not repeated or endorsed here or in any companion narrative.**

7.6 Compliance Framework Alignment Targets

Framework	Applicability
PIPA / PIPEDA	**Direct** — primary Canadian privacy law obligations

Framework	Applicability
PCI DSS	Indirect — applies to payment data via processors, not CredX directly holding card data
SOC 2 Trust Services Criteria	**Direct** — subject of this narrative set; Security, Availability, Confidentiality in scope
OSFI	Indirect — via regulated sponsor bank/lending partners
FINTRAC	Indirect — via regulated partners; CredX does not register directly
ISO 27001	Aspirational alignment — security management principles, not certified
OWASP Mobile Top 10 / API Security Top 10	Aspirational alignment — referenced in the Security Architecture Narrative

8 Open Governance Action Items

Named Gap	Recommended Owner	Priority
No formal board of directors or independent oversight body	Kendall Raessler, with input from Neal Oswald and Carrie Forbes	High
CCO title/role undefined relative to VP Operations title	Kendall Raessler and Audrey Wilson	Medium
No quarterly board-level risk reporting cadence exists	Kendall Raessler; recipient body pending item 1	Medium
No confirmed formal background-check program	Operations (Audrey Wilson) / [**HR**]	Medium
Role-based access review cadence and evidence not confirmed	Technical (Ray Yip)	High
Ownest technology continuity / escrow not formalized (Tier 1 dependency)	Kendall Raessler + legal counsel	**Critical**
Sponsor bank / lending partner contracts not yet executed	Kendall Raessler, Kyle Bunbury	High
Single-person functions with untested cross-function cover	Leadership (Kendall Raessler)	Medium
Within Technical, security administration and review are not separated	Technical (Ray Yip) / future oversight body	Medium

Target dates are [**TBD**] as of this version; leadership should assign specific target dates at the next review cycle.

Technical and control-level exceptions — the plaintext credential storage gap and the Detect/monitoring gap among them — are tracked separately in the Control Environment and Security Architecture Narratives.

9 Appendix — Internal Document References

- **CredX and Ownest Contractor Handbook, v1.1** — onboarding/offboarding, security training, role-based access review, and incident-reporting obligations.
- **CredX Disaster Recovery & Business Continuity Plan (DR/BCP), v1.4** — 48 pages; Incident Response Team roles, criticality tiers, RTO/RPO discussion, Ownest continuity dependency, testing/maintenance cadence.
- **CredX Data Security & Privacy Policy** — governance model, PII classification, Privacy by Design principles.
- **CredX Partner Data Map and Security Requirements Specification** — referenced in the Security Architecture and System Architecture Narratives.

External frameworks and legal references:

- AICPA Trust Services Criteria (Security, Availability, Confidentiality)
- Personal Information Protection Act (Alberta) — https://www.qp.alberta.ca/documents/Acts/P06P5.pdf
- PIPEDA — https://laws-lois.justice.gc.ca/eng/acts/p-8.6/
- Office of the Superintendent of Financial Institutions — https://www.osfi-bsif.gc.ca/
- FINTRAC — https://fintrac-canafe.canada.ca/