Business Continuity Plan

CredX Tech Inc

September 2026

Contents

Table 1: Document history

Date	Comment
Sep 3 2026	Rewritten from DR/BCP v1.4
Sep 4 2026	Replaced with SOC 2 narrative v1.0
Sep 4 2026	Recovery objectives validated; backup policy confirmed

1 Executive Summary

CredX Tech Inc. is a pre-revenue fintech company headquartered in Calgary, Alberta, providing embedded payments, credit decisioning, and merchant lending technology to merchant partners. As CredX pursues a SOC 2 examination — Type I first, then Type II — this narrative summarizes how CredX approaches business continuity and disaster recovery.

The **source of truth** for this topic is CredX's internal *Disaster Recovery & Business Continuity Plan*, version 1.4 (48 pages, last updated 2026-08-17). That document is comprehensive and operational; this narrative distills its structure, key commitments, and known open items into a form suited to an auditor's system description review.

Two things should be clear from the outset:

First, CredX has done real design work. It has named an Incident Response Team, defined criticality tiers for its systems and dependencies, documented an incident response lifecycle and severity model, and described its intended communication and notification pathways.

Second — and equally important for an accurate audit record — parts of that design remain untested in practice. The recovery objectives are documented and the backup policy is in force. What remains is demonstration rather than design: CredX has **not yet performed a restore test** against the validated targets, and has **not yet conducted a tabletop exercise**. This narrative names those gaps directly rather than glossing over them.

2 Purpose and Scope

This narrative addresses the **Availability** Trust Services Criterion primarily, with supporting relevance to **Security** (incident response, breach notification) and **Confidentiality** (data handling during a disruption).

This document is a condensed narrative, not a replacement for the full 48-page internal plan. The full internal plan remains the authoritative source of record and is available as audit evidence on request.

2.1 What This Narrative Governs

The scope of CredX's business continuity approach extends across four dimensions:

- **Technology systems and data** — both CredX-owned systems (the Heroku-hosted backend, mobile applications) and vendor/licensed systems CredX depends on (Ownest/UnderwriteFlow, Day.ai, POS integrations).
- **Third-party and partner dependencies** — POS processors, prospective sponsor bank/lender partners, and other sub-service organizations.

- **People, roles, and communication** — the Incident Response Team, escalation paths, and internal/external communication channels.
- **Regulatory and contractual obligations triggered by a disruption** — privacy law notification duties and, where applicable, partner-driven contractual obligations.

The internal plan complements the **Contractor Handbook (v1.1)**, which contains its own Business Continuity & Incident Response section applicable to contractors, and CredX's data protection and privacy policies. Where CredX's continuity approach intersects with a regulated partner's own incident response obligations, this plan **complements rather than replaces** the partner's independent program — CredX does not attempt to direct or control a bank or lender's internal incident response.

3 Governance and Incident Response Team

CredX is a small, pre-revenue fintech company. Rather than maintaining a separate business continuity function, **CredX's existing leadership team doubles as its Incident Response Team**. This keeps accountability clear but concentrates continuity knowledge in a small number of people.

Function	Continuity Role	Responsibility	Currently Held By
Leadership	Incident Commander	Overall incident authority, external partner relationships, sole public/media spokesperson (or explicit delegate)	Kendall Raessler, Founder & CEO
Technical	Technology & Infrastructure Lead	Platform administration, security architecture, and infrastructure recovery decisions	Ray Yip, CTO (also CTO of affiliated company Ownest)
Sales	Partner Continuity Lead	Continuity of enterprise and channel partner relationships during a disruption	Kyle Bunbury, Co-Founder & VP, Sales
Operations	Operations & Compliance Lead	Drafts partner/merchant incident communications; joint accountability with Technical for breach response	Audrey Wilson, Co-Founder & VP, Marketing & Operations

Function	Continuity Role	Responsibility	Currently Held By
[**HR**]	Personnel Safety & Communication	Employee safety confirmation and internal welfare communication during a physical or environmental event	Not separately staffed — carried by Operations

Continuity responsibilities attach to the **function**, not the individual. The "Currently Held By" column records who fills each function today and is expected to change; the rest of this Plan remains valid when it does.

3.1 Contact Information

Name	Mobile	Email
Kendall Raessler	403.200.9001	kendall@credxtech.com
Ray Yip	403.605.7012	ray@credxtech.com
Kyle Bunbury	403.464.9465	kyle@credxtech.com
Audrey Wilson	403.200.2244	audrey@credxtech.com

Incident roles are as listed in the Incident Response Team table above. **Audrey Wilson is the designated backup for all three other members; Ray Yip is Audrey Wilson's backup.**

All four addresses above are CredX addresses on a single mail domain, replacing the personal and affiliate-company addresses previously recorded. This introduces a dependency the Plan should name: **an incident affecting CredX's mail domain or Google Workspace tenancy degrades the primary contact path for the whole Incident Response Team simultaneously** — the same circular dependency already noted for Slack and Google Workspace as coordination channels.

The **mobile numbers are therefore the authoritative fallback**, consistent with the phone/SMS tree designated as the backup channel in the Communication Plan. Audrey Wilson should additionally maintain one out-of-band personal address per team member in the secure contact sheet held outside CredX systems.

A current copy of this table must be held **outside** systems that could themselves be affected by an incident — in particular, not solely in Google Drive. Audrey Wilson owns keeping it current, and distribution of this Plan should be controlled accordingly.

3.2 Functional Continuity Risk

Each of CredX's four functions is currently staffed by one person, with contractors extending capacity rather than providing documented cover. The loss or unavailability of any function's owner therefore removes that function's incident-response capacity until cover is established.

Mitigation — cross-function cover. Each function has a designated covering function that assumes its continuity responsibilities during an absence:

Function Unavailable	Covering Function	Effect on Incident Response
Leadership	Operations	Operations assumes incident declaration and approval authority, including partner and public communication sign-off
Technical	Operations, with contracted technical support	Restoration decisions escalate to the CEO; a contracted engineer is engaged for hands-on recovery
Sales	Operations	Partner and merchant relationship communication consolidates into Operations
Operations	Technical	Breach notification tracking and partner communication drafting move to Technical, with CEO approval unchanged

The CEO confirms cover at the point of an incident. **Technical is the function with the thinnest cover** — Operations can coordinate a technical incident but cannot perform platform restoration, so a contracted engineer is the real dependency there. Identifying and retaining that contractor in advance is a tracked action item.

This arrangement is documented but **has not been tested**; the tabletop exercise below is the mechanism for testing it.

3.3 Broader Governance Context

GAP: CredX does not yet have a formal board of directors or independent oversight body; board-level oversight of business continuity is a target-state item as the company scales.

CredX's Data Security & Privacy Policy describes an intended governance model in which the CTO and a Chief Compliance Officer jointly oversee data protection and security, supported by internal audits or compliance reviews at least annually and board-level oversight with quarterly updates.

GAP: The Chief Compliance Officer title referenced in policy may be aspirational or target-state. Audrey Wilson currently carries compliance responsibilities under her VP, Operations title rather than a distinct CCO title, and no independent board yet exists to receive the quarterly updates described in policy.

CredX's advisory bench includes **Neal Oswald, ICD.D** and **Carrie Forbes** (founder, Rockstar Advisory). Neither currently holds a formal continuity or incident-response role; their involvement is advisory rather than operational, and neither is a substitute for the succession mitigation described above.

4 Business Impact Analysis Summary

The internal plan applies a **three-tier criticality model**. This tiering drives prioritization of recovery effort during an incident.

Tier	Definition	Examples
Tier 1 — Critical	Customer- or partner-facing; disruption directly impacts revenue or compliance obligations	Core transaction processing, credit decisioning integration, POS partner integrations, sponsor bank/lender relationships
Tier 2 — Important	Internal operational systems; service degrades materially if unavailable for more than approximately 24 hours	Internal collaboration tools, CRM/pipeline systems, internal reporting
Tier 3 — Low	Non-essential or back-office systems with minimal immediate impact if unavailable	Non-critical administrative tools, archival systems

4.1 Key Tier 1 Dependencies

UnderwriteFlow decisioning platform CredX's core credit decisioning application, built on a licensed technology stack from affiliated company **Ownest Inc.** and hosted on the Ownest/Base44 environment. See the Ownest Relationship Continuity section for the specific continuity gap.

Day.ai CRM The system of record for sales pipeline, contacts, and onboarding status. **Recommended weekly export** to a CredX-controlled store to reduce reliance on the vendor for continuity.

POS partner integrations (Clover, Square) The point-of-sale connections through which merchant transactions originate. Both are treated as critical due to their role in the core transaction lifecycle.

Prospective sponsor bank / lender relationships Peoples Trust Company and **Innovation Federal Credit Union** — named as Tier 1 dependencies for planning purposes even though **neither relationship is an executed contract**; both remain prospective/pilot-stage.

GAP: Because the Peoples Trust Company and Innovation Federal Credit Union relationships are not yet executed, CredX cannot yet rely on contractual continuity or notification commitments from these prospective partners.

4.2 Risk Context Behind the Tiering

CredX maintains a risk register using a **5×5 likelihood-by-impact methodology**, with tiers of Low (1–4), Medium (5–9), High (10–14), and Critical (15–25). CredX has stated a **low risk appetite** for events affecting regulated personal or financial data, credit decisioning integrity, or bank/lending partner trust, and a **moderate tolerance** for isolated, single-vendor disruptions with contained, non-regulatory impact.

The register's highest-rated risks trace to two root causes mapping directly onto the Tier 1 dependencies above: (1) **the technology architecture is still finalizing** — hosting is now confirmed as Heroku Private Spaces, but production verification of several controls remains incomplete — and (2) **sponsor bank, lender, and merchant contracts are not yet executed**.

Notably, the **cloud/hosting outage risk was downgraded from Critical (score 15) to High (score 10)** once Heroku Private Spaces hosting was confirmed, illustrating how resolving infrastructure uncertainty directly reduces continuity risk.

5 Recovery Objectives (RTO/RPO)

CredX's Recovery Time and Recovery Point Objectives are documented below and have been reviewed against the confirmed Heroku Private Spaces (Canadian region) environment. They are the objectives against which recovery is measured.

Tier	Example Systems	Target RTO	Target RPO
Tier 1 — Critical	Core transaction processing, Ownest decisioning integration, POS partner integrations, payment/transaction data	4 hours weekdays / 12 hours weekends	24 hours

Tier	Example Systems	Target RTO	Target RPO
Tier 2 — Important	CRM/pipeline data, onboarding systems, internal communications	8 hours	24 hours
Tier 3 — Low	Marketing site, development environment, non-essential internal tools	48 hours	48 hours

These bands follow the recovery model used by comparable platforms of similar size and architecture, with a weekday/weekend split on the Tier 1 RTO reflecting reduced out-of-hours staffing across four single-person functions.

The Tier 1 RPO warrants specific attention. A 24-hour RPO means accepting up to a full day of lost data in a recovery event, and for CredX that data includes **orders, payments, loan draw-downs, and ledger entries** — records with financial and contractual consequence for merchants, consumers, and lending partners, which cannot be reconstructed from the POS side alone once lost. This window is accepted at CredX's current pre-revenue transaction volume. It should be **re-examined before production launch and again as merchant volume grows**, since the cost of a day's lost ledger data scales directly with throughput.

This validation work is now unblocked in one respect: CredX's hosting environment has been confirmed as **Heroku Private Spaces, Canadian region**. With hosting confirmed, the internal plan calls for the CTO to validate concrete, infrastructure-specific RTO/RPO targets against this environment; **that validation itself has not yet occurred.**

GAP: the targets are validated but not yet tested. Validation confirms the objectives are appropriate and achievable by design — sufficient for a SOC 2 Type I examination, which assesses control design at a point in time. A **Type II** examination assesses operating effectiveness over a review period and requires **real, measured recovery data**: an actual failover or restore timed against these targets. CredX does not yet have that. Completing the first restore test is the remaining step, and CredX should expect it to be a primary area of auditor follow-up between Type I and Type II.

5.1 Why This Sequencing Makes Sense

CredX's overall cyber security readiness, assessed against the NIST CSF 2.0 six functions, sits at **approximately 1.5 out of 4** ("Developing," leaning toward "Ad Hoc") — a level the internal plan considers appropriate for a pre-revenue-stage company but not yet production-verified across the board.

Setting the targets was deliberately sequenced *after* hosting confirmation: CredX avoided fixing a recovery target against infrastructure that was not yet finalized.

With Heroku Private Spaces confirmed, the targets were reviewed and the backup policy settled. The **Recover** function is accordingly **documented but untested** — a design-maturity position that does not by itself raise the operating-effectiveness picture, since no restore has been performed.

For context, the **Detect** function scores **0 out of 4** — there is no live monitoring or SIEM capability today. That gap bears directly on recovery measurement: **without reliable detection, the clock on an actual recovery event is harder to start accurately**, so the eventual restore test should record how detection latency was accounted for in the measured time.

6 Backup and Recovery Procedures

The following backup standards are the **in-force policy**, no longer recommended minimums:

- Daily automated backups.
- Backups encrypted at rest.
- Minimum 90-day retention.
- Restore testing performed at least twice yearly.

Confirmed. The policy above is implemented and operating in production. **The one element not yet demonstrated is the restore testing requirement itself** — the twice-yearly drill is policy, but no drill has been run. Confirming a backup policy establishes that backups are being taken as specified; only a restore demonstrates that they can actually be recovered from, which is what a SOC 2 Type II examination of the Availability criterion tests.

Separately, the **backup and redundancy guarantees provided by the Ownest/Base44 hosted decisioning environment have not yet been confirmed in writing.**

Recommendation on vendor lock-in: the internal plan recommends CredX maintain its own export or backup of critical decisioning and merchant data **outside the Ownest environment**, so that CredX is not solely dependent on Ownest's own backup and availability posture for data it needs to operate or recover its business. The same logic applies to Day.ai and to Google Workspace records.

7 Ownest Relationship Continuity

CredX's core software — including the UnderwriteFlow decisioning application — is built on a licensed technology stack from **Ownest Inc.**, an affiliated company (**Ray Yip serves as CTO of both CredX and Ownest**). This makes Ownest one of CredX's most significant continuity dependencies, and the internal plan flags it as a **Tier 1 governance action item rather than a resolved control**.

None of the following are yet formalized between CredX and Ownest:

- A source-code or technology escrow arrangement.
- A documented handover or transition plan in the event Ownest is unable to continue providing the licensed platform.
- A contractual continuity commitment or support SLA covering availability, incident response, or recovery timeframes.

GAP: No source-code/technology escrow, documented handover plan, or contractual continuity/support-SLA is yet formalized with Ownest, despite CredX's core software being built on Ownest's licensed technology stack. Owned jointly by Kendall Raessler and legal counsel; treated as a Tier 1 governance action item.

7.1 Why This Matters for Availability

UnderwriteFlow performs the credit questionnaire and decisioning steps of CredX's core transaction lifecycle: a customer's credit application is completed directly on Ownest's hosted questionnaire, Ownest returns the completed application via webhook, CredX requests loan proposals, and an accepted proposal becomes the loan terms drawn down at the point of sale.

If the Ownest/Base44 hosted environment were to become unavailable, CredX would have no independently-operated fallback for this step today — which is precisely why the escrow, handover-plan, and support-SLA gaps are rated Tier 1.

From a data-handling perspective, **CredX does not transmit applicant financial data to Ownest over its own API integration** — only a correlation or loan identifier passes between the two systems, with applicant details flowing client-side directly to Ownest's questionnaire. This limits, but does not eliminate, CredX's data-confidentiality exposure in an Ownest outage scenario; **the primary exposure in that scenario is to Availability** — CredX's ability to continue originating and servicing loans — rather than to Confidentiality of data already at rest.

8 Incident Response Process Summary

Phase	Summary
1. Preparation	Roles, tools, and communication channels defined in advance
2. Detection & Analysis	Identification and initial assessment of a potential incident, including severity classification
3. Containment, Eradication & Recovery	Limiting impact, removing the root cause, and restoring affected systems or processes

Phase	Summary
4. Post-Incident Activity	Root-cause review, lessons learned, and updates to the plan or controls as needed

8.1 Severity Levels

Incidents are classified **P1 (highest) through P4 (lowest)**, each with a defined response window in the internal plan. Auditors should consult the internal plan directly for the specific response-time thresholds.

Severity	General Description
P1	Highest severity — significant customer, partner, or compliance impact; fastest defined response window
P2	High severity — meaningful impact to a Tier 1 or Tier 2 system or dependency
P3	Moderate severity — limited or contained impact, typically to a Tier 2 or Tier 3 system
P4	Low severity — minimal impact; handled through standard operational channels

Severity classification is performed during the Detection & Analysis phase and determines which Incident Response Team members are engaged, how quickly partner/merchant communication is triggered, and whether the regulatory notification track is activated.

9 Data Breach Notification Summary

For incidents involving personal information tied to a lending transaction, the notification chain is:

1. Banking / lending partner identifies or is notified of a potential issue.
2. CredX is notified and assesses its role, given that CredX itself does not perform KYC/KYB or hold custody of funds.
3. CredX notifies the affected merchant.
4. The merchant, in turn, is responsible for notifying its own customers and insurer as applicable.

9.1 Regulatory Track

Two regulatory tracks apply in parallel, reflecting CredX's Alberta base and its handling of data that may cross provincial or federal lines:

- **Alberta Office of the Information and Privacy Commissioner (OIPC)** — primary regulator under Alberta PIPA, the "substantially similar" provincial law that displaces PIPEDA for Alberta operations.
- **Office of the Privacy Commissioner of Canada (OPC)** — applies where data handling is interprovincial or otherwise falls under federal PIPEDA.
- **Office of the Superintendent of Financial Institutions (OSFI)** — escalation path relevant to federally regulated banking/lending partners. **OSFI's own 24-hour reporting obligation applies to those partners directly, not to CredX**, but it informs CredX's internal escalation timelines.

Both privacy statutes apply the **"real risk of significant harm" (RROSH)** standard, and both call for notification without unreasonable delay once that threshold is met. Regardless of whether RROSH is met for a given event, CredX maintains a **breach record log covering a 24-month period**.

GAP: This notification chain is not yet contractually formalized with CredX's prospective sponsor bank/lender partners, since those partnership agreements are not yet executed. Until they are, the chain reflects **CredX's intended approach rather than a binding, agreed process**.

9.2 Relationship to Privacy by Design

CredX's privacy program is grounded in Ann Cavoukian's **seven Foundational Principles of Privacy by Design**. One open gap is directly relevant to continuity planning: **Principle 7 (user-facing consent and access mechanisms) is not yet confirmed as implemented.**

10 Communication Plan Summary

Audience	Approach
Internal	Slack (primary, via a dedicated incident channel) with a phone/SMS tree as backup if Slack is unavailable
Partner / Merchant	Audrey Wilson drafts communications; Kendall Raessler approves before they are sent. Coordination with regulated partners routes through each partner's designated incident contact
Public / Media	Only the CEO (Kendall Raessler) or an explicitly named delegate speaks publicly or to media; no other team member is authorized to do so during an incident

This structure keeps a **single approval point** for anything reaching a partner, merchant, or the public — appropriate for a company of CredX's size. Where

the Leadership function is itself unavailable, **Operations assumes approval authority for partner and public communications** under the cross-function cover arrangement above, so the approval gate does not simply lapse.

Records-retention continuity: Google Workspace (Drive, Docs, Sheets) versioning and retention settings serve as the **de facto backup mechanism** for day-to-day records today. The internal plan recommends periodic export of critical legal and financial documents to a secondary secure store; **this recommendation has not yet been confirmed as implemented.**

11 Testing and Maintenance Commitments

Activity	Commitment	Status
Tabletop exercise	At least twice yearly; Q1 and Q3 recommended	**Not yet conducted**
Backup restore test	At least twice yearly	**Not yet conducted** — backup policy now confirmed, so this is unblocked
Full plan review	Every 6 months, or after a major change, incident, or leadership change	Recurring commitment per internal plan
Risk register review	Same 6-month cycle as the full plan review	Recurring commitment per internal plan

GAP: No tabletop exercise has yet been conducted. This should not be understated: **a documented plan with untested procedures represents a design that has not yet been exercised**, which is a meaningful distinction for an auditor evaluating readiness for a Type II examination.

12 Relationship to This Narrative Set

Two of the three items previously flagged here are now closed:

- **Recovery Objectives — Closed.** Reviewed against the confirmed Heroku Private Spaces environment; targets confirmed unchanged.
- **Backup Procedures — Closed for CredX's own environment.** The backup policy is confirmed in production. **Written confirmation of the Ownest/Base44 environment's backup guarantees remains outstanding** — that dependency is a third party's, not CredX's, and cannot be closed unilaterally.

The remaining items an auditor should expect to see closed — or clearly in progress — **before a SOC 2 Type II examination period begins**:

- **Restore test** — at least one actual restore performed and timed against the validated RTO/RPO targets. This is the single most consequential open item for the Availability criterion: everything else about recovery is now documented, and only this demonstrates it works.
- **Tabletop exercise** — at least one conducted and documented exercise demonstrating the Incident Response Team can execute the plan, including the cross-function cover arrangement.

This distinction matters because a **Type I** examination assesses whether controls are suitably designed as of a point in time, while a **Type II** examination assesses whether those controls **operated effectively over a review period**. Design-stage documentation can support a Type I examination. Evidence of operation over time — tested recovery objectives, confirmed backups, and at least one completed tabletop exercise — will be necessary before CredX is ready for Type II fieldwork.

Readers should treat this narrative as **a summary and index into the full internal plan, not a substitute for it**. Where this narrative and the internal plan differ in level of detail, the internal plan governs.