Risk Assessment and Management Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.1

Table 2: Document history

Date	Comment
Sep 11 2023	Updated approach
Sep 3 2026	Adopted 5x5 methodology and scored risk register

1 Purpose and Scope

The purpose of this policy is to define the methodology for assessing and treating risks related to information security and business continuity at CredX. This policy establishes a structured approach to identifying, analyzing, mitigating, and monitoring risks that may impact the confidentiality, integrity, and availability of CredX's data and systems.

This policy applies to:

a. All employees, contractors, and stakeholders involved in risk assessment and risk treatment.

b. All company assets, including electronic documents, databases, IT infrastructure, applications, and outsourced services.

c. Risks associated with operations, security, regulatory compliance, business continuity, and third-party relationships.

2 References

a. Risk Assessment Report Template

3 Risk Management Approach

CredX follows a systematic approach to risk management that consists of the following key steps:

1. **Risk Identification** – Identify company assets and the associated threats and vulnerabilities.
2. **Risk Assessment** – Evaluate the likelihood and impact of risks using the 5×5 methodology below.
3. **Risk Treatment** – Determine and implement appropriate mitigation measures.
4. **Risk Monitoring & Reporting** – Continuously assess and report risks to leadership.

4 Risk Governance Structure

- **Policy Owner**: Kendall Raessler, Founder & CEO.
- **Independent oversight**: **CredX does not yet have a formal board of directors or independent oversight body.** Establishing formal board or advisory oversight as CredX scales is a tracked action item. Until then, risk governance rests entirely with the CEO, and this policy should not be read as describing independent challenge.

- **Risk appetite approval**: CEO, with input from the full leadership team (Ray Yip, Kyle Bunbury, Audrey Wilson).
- **Policy review cycle**: annual, or immediately after any material change in business model, funding stage, or regulatory environment.

5 Risk Categories

This policy applies company-wide across **seven risk categories**:

Strategic; Financial; Operational; Compliance/Regulatory; Technology/Cyber; Third-Party/Vendor; and Reputational.

Risk identification focuses on **people, processes, and technology** that could impact CredX's operations or information security. Within the categories above, key sources of risk include:

i. Compliance risks related to regulatory obligations and contractual commitments.

ii. Information security risks such as data breaches, unauthorized access, and insider threats.

iii. Business continuity risks affecting system availability and operational resilience.

iv. Vendor and third-party risks associated with external service providers, including licensed and hosted platforms on which CredX's core product depends.

v. **Fraud risks**, including misappropriation of assets, unauthorized system access, financial fraud, and manipulation of financial reporting. Fraud risk must be explicitly assessed as part of the annual risk assessment.

vi. Risks arising from automated credit decisioning, including model error, disparate impact, and inability to explain an adverse decision. See the Artificial Intelligence Governance Policy.

Each identified risk is assigned a **Risk Owner** responsible for managing and mitigating the risk.

6 Roles and Responsibilities

Role	Risk Responsibility
Leadership — Kendall Raessler (Founder & CEO)	Overall risk accountability; approves risk appetite and this Policy; owns strategic and reputational risk

Role	Risk Responsibility
Technical — Ray Yip (CTO)	Owns technology/cyber risk and third-party technology vendor risk
Sales — Kyle Bunbury (Co-Founder & VP, Sales)	Owns commercial and partner-relationship risk
Operations — Audrey Wilson (Co-Founder & VP, Marketing & Operations)	Owns operational and compliance/regulatory risk
All staff and contractors	Duty to report identified risks or incidents promptly per the Security Incident Response Policy

7 Risk Appetite

CredX has **low risk tolerance** for events affecting regulated personal or financial data, the integrity of credit decisioning, or trust with banking and lending partners. These categories warrant immediate mitigation investment regardless of cost.

CredX has **moderate risk tolerance** for isolated, single-vendor disruptions (for example, one POS integration down) with contained, non-regulatory impact, where monitoring and a documented response are sufficient without dedicated redundancy spend at this stage.

7.1 Risk Appetite by Category

Category	Appetite	Rationale
Strategic	Low	Missteps affect CredX's ability to secure banking and lending partners at a critical early stage
Financial	Low	Pre-revenue runway leaves little room for unplanned cost exposure
Operational	Moderate	Some single-vendor/process risk is acceptable while the team and stack are still small
Compliance / Regulatory	Low	Non-compliance jeopardizes partner trust and licensing eligibility
Technology / Cyber	Low	CredX handles regulated financial and personal data

Category	Appetite	Rationale
Third-Party / Vendor	Moderate	Reliance on Ownest (underwriting), its Base44-hosted decisioning environment, and two POS partners is inherent to the business model; managed through the vendor risk process in the Vendor Management Policy
Reputational	Low	Trust is the core asset of a lending/credit platform

8 Risk Scoring and Assessment

CredX scores each risk, in any of the seven categories above, using a standard **5×5 likelihood × impact matrix**. This methodology is the company-wide standard, not a disaster-recovery-only tool.

- **Likelihood (1–5)**: 1 = Rare, 2 = Unlikely, 3 = Possible, 4 = Likely, 5 = Almost Certain
- **Impact (1–5)**: 1 = Negligible, 2 = Minor, 3 = Moderate, 4 = Major, 5 = Severe
- **Risk Score = Likelihood × Impact** (range 1–25)

8.1 Risk Tiers

Tier	Score	Treatment
Low	1–4	May be accepted with monitoring; must be documented in the Risk Register
Medium	5–9	Monitor and document a response; mitigation where cost-effective
High	10–14	Must be actively mitigated with a named owner and next action
Critical	15–25	Immediate mitigation investment; reported to the CEO within two business days of identification

Acceptance of a High or Critical risk requires documented approval from the CEO, along with a documented rationale and compensating controls.

9 Risk Register

The register below is CredX's current assessed risk position. Scores are **initial estimates for the Incident Response Team to validate and adjust** — they are judgment calls appropriate to CredX's current pre-revenue, pre-infrastructure-finalization stage, not measured historical frequencies. Validating them with the full leadership team is a tracked action item.

ID	Risk	L	I	Score	Tier	Owner
1	Cloud/hosting infrastructure outage	2	5	10	High	Ray Yip
2	Ownest / Base44 decisioning environment outage	2	5	10	High	Ray Yip
3	Data breach, ransomware, or unauthorized access	3	5	**15**	**Critical**	Audrey Wilson / Ray Yip
4	Credit bureau data partner outage or suspension	2	4	8	Medium	Ray Yip
5	POS integration partner outage	4	2	8	Medium	Ray Yip
6	Sponsor bank or lending partner system outage	2	4	8	Medium	Kendall Raessler
7	Loss of, or dispute with, Ownest	2	5	10	High	Kendall Raessler
8	Day.ai / CRM data loss or extended outage	3	3	9	Medium	Kyle Bunbury / Audrey Wilson
9	Functional unavailability (single-person functions)	3	4	12	High	Kendall Raessler
10	Office/workspace disruption	2	1	2	Low	Audrey Wilson
11	Regional/natural disaster affecting Calgary staff	2	4	8	Medium	Ray Yip
12	Absent liability allocation in partner agreements	4	4	**16**	**Critical**	Kendall Raessler / Legal
13	Uncoordinated breach notification across the chain	3	5	**15**	**Critical**	Audrey Wilson

9.0.1 Mitigations and Next Actions

1 — Cloud/hosting infrastructure outage or provider-level failure
Confirmed: the backend is hosted on Heroku Private Spaces (Canadian region), the backup policy is in force, and recovery objectives are documented. *Remaining gap:* confirm multi-region and failover redundancy within Heroku, and perform the first restore test.

2 — Ownest / Base44 hosted decisioning environment outage
Obtain written SLA, backup, uptime, and restore-process documentation

from Ownest for the Base44-hosted decisioning environment, and establish a documented escalation contact for platform-level incidents. **Currently unconfirmed in writing.**

3 — Data breach, ransomware, or unauthorized access Implement the breach notification protocol in the Security Incident Response Policy, and complete the security control review referenced in the Contractor Handbook. Note this risk is scored Critical while the Detect function is scored 0 — CredX currently has limited ability to know a breach has occurred.

4 — Credit bureau data partner outage or access suspension Confirm a fallback or queuing process for decisioning during bureau downtime.

5 — POS integration partner outage Monitor partner status pages and document per-platform merchant concentration, since concentration can promote a single integration to Tier 1 in practice.

6 — Sponsor bank or lending partner system outage Negotiate an incident-coordination clause into partner agreements **before execution**.

7 — Loss of, or dispute with, Ownest (source code / technology access) Establish a source-code escrow or continuity agreement. **Currently unmitigated.**

8 — Day.ai / CRM data loss or extended outage Set up a recurring CRM data export, and tighten workspace-visibility and sharing settings — shared data is not retroactively unshared.

9 — Functional unavailability (illness, departure, incapacitation) Each of the four functions — Leadership, Sales, Operations, Technical — is staffed by one person. A documented cross-function cover arrangement exists (Operations covers Leadership and Sales; Technical covers Operations; Operations plus a contracted engineer covers Technical) but has **not been tested**. Next actions: retain a pre-identified contract engineer for Technical cover, and exercise the arrangement in the first tabletop.

10 — Office/workspace disruption No action required; the team is remote-capable.

11 — Regional/natural disaster affecting Calgary-based staff Confirm cloud region redundancy once hosting is finalized. Linked to Risk 1.

12 — Ambiguous or absent liability allocation in banking/lending partner and merchant agreen No sponsor bank, lender, or merchant agreement currently executed contains data-breach liability, indemnification, or notification-sequencing terms. **Must be resolved before any of these agreements are signed.**

13 — Delayed or uncoordinated breach notification across the partner chain (banking partner → CredX → merchant). No notification-chain protocol exists today. Adopt the procedure in the Security Incident Response Policy and build matching SLAs into partner and merchant agreements.

9.1 5×5 Risk Heat Map

Likelihood ↓ / Impact →	1 – Negligible	2 – Minor	3 – Moderate	4 – Major	5 – Severe
5 – Almost Certain	5	10	15	20	25
4 – Likely	4	**#5 (8)**	12	**#12 (16)**	20
3 – Possible	3	6	**#8 (9)**	**#9 (12)**	**#3, #13 (15)**
2 – Unlikely	**#10 (2)**	4	6	**#4, #6, #11 (8)**	**#1, #2, #7 (10)**
1 – Rare	1	2	3	4	5

Risks 3, 7, 12, and 13 are rated Critical and share a common root cause: **CredX's technology architecture and partner contracts are both still in formation.** Closing the open action items tracked in the Business Continuity Plan directly reduces these scores.

10 Risk Treatment and Mitigation

For risks requiring treatment, the following mitigation strategies may be applied:

1. **Implement security controls**: Strengthening security measures such as encryption, access controls, and monitoring systems.
2. **Transfer risk**: Through insurance or third-party agreements. Note that indemnification clauses shift financial responsibility between parties after the fact; **they do not shift regulatory findings**.
3. **Avoid the risk**: By discontinuing high-risk activities.
4. **Accept the risk**: Only if mitigation costs exceed the impact of the risk. This must be documented and approved by the CEO.

Residual risks after mitigation must be documented in the Risk Register.

11 Risk Monitoring and Reporting

- **Register review**: The full Risk Register is reviewed at each six-month program review, and immediately after any risk event materializes or any tracked open action item is resolved.
- **Critical risk escalation**: Any risk scored Critical is reported to the CEO within **two business days** of identification.
- **Annual risk assessments** must be conducted at a minimum.
- The **Risk Register** is updated whenever new risks are identified.
- Any **significant organizational, technological, or regulatory changes** trigger an immediate risk review.
- **Leadership Reporting:** Risk treatment plans and risk assessment results must be reported to the leadership team, including new risks identified, changes to existing risk scores, treatment status, and any accepted risks.
- **Board Reporting:** **[TBD]** As CredX grows, establish a quarterly risk report to the Board or investors. No such body currently exists, so this control is not yet operating.
- A **Risk Assessment Report** is maintained as part of SOC 2 audit readiness.
- **Fraud Risk Assessment:** An explicit fraud risk assessment must be conducted as part of the annual risk assessment, covering at minimum: misappropriation of assets, unauthorized system access, financial fraud, and integrity of financial reporting. Findings must be documented in the Risk Register.

12 Policy Review & Version Control

This policy is reviewed annually, or immediately after any material change in business model, funding stage, or regulatory environment.

13 Continuous Improvement

The risk assessment process is continuously improved through:

- Regular internal audits and testing.
- Incident analysis and lessons learned.
- Enhancing controls based on emerging threats and business needs.

This policy ensures CredX's commitment to strong risk management practices, supporting compliance with relevant industry and regulatory standards.