

SECURITY & TRUST OVERVIEW

How Bancabl protects bank data, by design.

Bancabl is the operating system banks use to plan, execute, and report on community investment activity. This document summarizes our control posture and the maturity of our governance program, written for vendor-risk and information-security teams. We describe what is implemented today, what is in progress, and what is planned. We do not claim certifications we have not earned.

1. Security principles

Tenant isolation by default. Every customer's data lives behind a per-tenant boundary enforced at the application, database, and key layers.

Least privilege everywhere. Roles, scopes, and service identities only carry the permissions they need to do their job.

Auditability is a product feature. Writes and exports are captured, attributed, and exportable as exam-ready evidence.

Honest disclosure. Where we are pre-certification or in progress, we say so plainly.

2. Access & permissions

Control	Description	Status
Role-based access (RBAC)	Bank Admin, CRA / Community Development, Executive Viewer, and Internal Admin roles, scoped per tenant.	Live
MFA & SSO	MFA available on all accounts; SAML 2.0 / OIDC SSO with Okta, Entra ID, and Google Workspace.	Live
SCIM provisioning	Automated user lifecycle from your IdP on enterprise plans; deprovisioning is event-driven.	Live
Quarterly access reviews	Automated reminders and exportable user-permission snapshots stored in the audit log.	Live
IP allowlisting	Per-tenant IP restrictions for admin actions and exam-workpaper exports.	Planned

3. Logging & monitoring

Control	Description	Status
Write & export logging	100% of create/update/delete and export actions are logged with actor, timestamp, IP, and resource ID.	Live
Read-event logging (sensitive)	View events on snapshots, reports, and partner records are recorded.	Live
Tamper-evident retention	Append-only log storage with cryptographic integrity checks. Default retention: 7 years.	Live
Exportable workpapers	Audit log exports in CSV and signed PDF, scoped by date range, user, or resource.	Live
SIEM streaming	Webhook and S3 push to Splunk, Datadog, or Sumo Logic for centralized monitoring.	In progress

SECURITY & TRUST OVERVIEW

Data architecture, vendors, and compliance roadmap.

4. Tenant-aware data design

Per-tenant boundary. Row-level security, per-customer encryption keys, and identity-scoped service roles. There are no cross-tenant query paths.

Encryption. AES-256 at rest, TLS 1.2+ in transit, mTLS service-to-service inside the production VPC.

Backups & recovery. Encrypted, point-in-time backups with documented RPO ≤ 1 hour and RTO ≤ 4 hours for the production tier.

Data residency. U.S.-only data residency by default; regional options on request.

5. Vendor oversight

We keep the subprocessor list short and intentional. Each vendor is reviewed annually and selected for posture, scope minimization, and incident transparency.

Subprocessor	Purpose	Region	Attestation
Cloud infrastructure	Compute, storage, networking	U.S.	SOC 2 Type II, ISO 27001
Identity provider	SSO / MFA / SCIM	U.S.	SOC 2 Type II
Email delivery	Transactional notifications only	U.S.	SOC 2 Type II
Error monitoring	Application telemetry (PII-redacted)	U.S.	SOC 2 Type II

6. Incident response readiness

Documented IR runbooks with severity tiers, named on-call owners, and a 72-hour customer notification commitment for confirmed security incidents affecting customer data. Tabletop exercises run on a quarterly cadence.

7. Secure development & release discipline

- Code review and CI on every change; production deploys require dual approval.
- Automated dependency scanning, secret scanning, and SAST on every pull request.
- Production access is time-boxed, MFA-protected, and logged.
- Annual third-party penetration test; remediation tracked in the public summary report (NDA on request).

8. Compliance roadmap

SOC 2 Type II: audit currently in progress with a recognized firm. Type I report targeted next quarter; Type II observation period to follow. We will publish the report when it is issued — not before.

Our control framework is built to support GLBA Safeguards Rule alignment, FFIEC-aligned vendor due-diligence questions, and the typical bank vendor-risk intake. Mapping artifacts are available on request.

Contact. security@bancabl.com · Vendor-risk packets, subprocessor list, and the current SOC 2 status letter are sent on request to verified bank, investor, and partner contacts.