SecureControl

Project Status & Roadmap

Banking Maker-Checker Controls | Proof of Concept

Version 1.0 | February 2026

Prepared for: Project Stakeholders & Management

Classification: Confidential

1. What Has Been Delivered

The following capabilities have been fully implemented and are functional in the current proof-of-concept build.

Authentication & Access Control

- Email/password sign-up with 6-digit OTP verification via Resend email (send, resend, verify)
- OTP data stored in encrypted httpOnly cookie with 5-minute expiry and 3-attempt limit
- Email/password sign-in with role-aware redirect (Maker, Checker, Admin, SuperAdmin)
- Middleware-based route protection using Supabase SSR -- unauthenticated users redirected automatically
- KYC-gated access -- Makers cannot reach the dashboard until KYC is approved
- 4-role system: Maker (self-register), Checker (admin-created), Admin (admin-created), SuperAdmin (seeded)

User Management (SuperAdmin)

- Create Checker and Admin users from the admin portal with auto-generated secure passwords
- Credential delivery via branded HTML email through Resend -- user is NOT created if email fails
- Paginated user listing with search and role-based filtering
- SuperAdmin seeder script with optional Resend email notification

KYC (Know Your Customer)

- 5-step KYC onboarding wizard: Personal Info, Contact, Employment/Account, Nominee, Review
- PAN, Aadhaar, and mobile number format validation (regex-based, client + server)
- KYC submission, review (approve/reject/under-review), and update APIs with full audit trail
- Real-time KYC status polling page (30-second interval) with auto-redirect on approval
- Checker KYC review dashboard with stats grid, application table, and detail dialogs
- Maker KYC update page with change tracking and locked identity fields (PAN/Aadhaar)
- Auto-generated KYC Application IDs (KYC-YYYY-NNNNNN format)

Transaction Management (Maker-Checker Workflow)

- Transaction creation: 4 types (fund transfer, payment approval, account change, loan approval), 7 currencies
- Auto-analysis on creation -- all active policy rules are evaluated and violations saved immediately
- Approve/reject workflow with mandatory checker notes and rejection reasons
- Maker transaction list with status and type filters (URL search-param driven)
- Checker pending and flagged transaction review pages with inline policy violation display
- Transaction detail page with account flow visualization, timeline, and violations section
- SWR-based transaction hooks with client-side cache invalidation on mutations

Policy Engine

- Amount threshold check -- flags transactions exceeding configurable limits with scaled severity
- Duplicate transaction detection -- same amount + destination within a 24-hour window
- Blacklist account check -- source and destination matched against active blacklist (CRITICAL severity)
- Business-hours check -- flags transactions created outside 9 AM - 6 PM, Mon - Fri
- Composite risk score (0-100) with auto-flagging at score >= 40
- Contextual recommendation engine (escalation advice, beneficiary verification)
- Policy rules management page with enable/disable toggles and audit logging

Blacklist Management

- Full CRUD: add, toggle active/inactive, and delete blacklist entries
- Checker management interface and admin read-only overview
- 3 pre-seeded blacklist entries for demo purposes

Audit Trail

- Comprehensive audit log on every state change -- transactions, blacklist, policies, KYC, users
- Audit log table with detail dialog showing old/new value JSON diffs
- Last 100 events displayed with Suspense-based loading

Dashboard & UI

- Role-specific dashboards: Maker (4 stats + recent txn), Checker (4 stats + pending), Admin (12 stats + users + audit)
- Role-based sidebar navigation with active state highlighting
- Loading skeletons for every page (10+ skeleton variants)
- Lazy-loaded heavy components via Next.js dynamic imports
- 60+ shadcn/ui components, Tailwind CSS, fully responsive design

Database & Security

- 7 tables: profiles, transactions, policy_rules, policy_violations, blacklist, audit_logs, kyc_applications
- Row Level Security (RLS) on all tables with granular per-role policies
- Auto-create profile trigger on auth user insert, auto-updated_at timestamps
- KYC approval sync trigger -- auto-updates profile.kyc_completed flag
- Database-level CHECK constraints on all enum fields + PAN/Aadhaar/mobile format regex
- Indexes on all frequently queried columns for performance

Email Services

- Resend API integration for OTP verification emails and credential delivery emails
- Branded HTML templates with plain-text fallbacks for both email types
- No dev-mode fallbacks -- all emails go through Resend in every environment

2. What We Will Build Next

The following enhancements are planned to move the PoC toward production readiness and full regulatory compliance.

Near-Term (High Priority)

1. Multi-Factor Authentication (MFA) for privileged roles (Checker, Admin, SuperAdmin)
2. Policy rule approval workflow + versioning -- maker-checker for rule changes with rollback capability
3. Compliance evidence export -- generate PDF/CSV audit bundles for regulators on demand
4. Rate limiting + session management -- enforce session timeouts, concurrent session limits, API rate caps
5. Field-level encryption & PII masking -- encrypt PAN/Aadhaar at rest; mask in UI (last 4 digits only)
6. SLA-based escalation & alerting -- auto-escalate aging transactions with email/Slack notifications

Medium-Term (Strategic)

7. SSO integration (SAML/OIDC) -- enterprise identity providers like Azure AD, Okta, Google Workspace
8. Customer risk-tiering -- classify customers as low/medium/high risk based on profile and transaction patterns
9. Ongoing KYC refresh + AML screening -- periodic re-verification and sanctions list integration
10. Rule simulation / back-testing -- test new policy rules against historical transactions before activation
11. Behavioural & velocity-based risk rules -- detect rapid-fire transactions, amount spikes, geographic anomalies
12. Case management system -- investigation lifecycle tracking with notes, assignments, and resolution workflow
13. End-user dashboards -- customer-facing views for account status, transaction history, and KYC status
14. Core banking & enterprise integrations -- APIs for core banking, general ledger, and payment gateways (optional)

3. Summary

The current PoC delivers a fully functional maker-checker transaction workflow, multi-step KYC onboarding, a configurable policy engine with real-time risk analysis, comprehensive audit logging, role-based access control with RLS, and production-ready email services via Resend. The dashboard provides role-specific views for Makers, Checkers, and SuperAdmins with responsive UI and lazy-loaded components.

The near-term roadmap focuses on security hardening (MFA, PII masking, session management), governance (policy versioning, compliance exports), and operational improvements (SLA escalation). The medium-term roadmap targets enterprise-grade integrations (SSO, core banking), advanced risk detection (behavioural rules, risk-tiering), and operational tooling (case management, back-testing).

End of Document