SecureControl

Banking Controls Platform

Proof of Concept

Business Overview & Capabilities Document

Version 1.0 | February 2026

Prepared for: Project Stakeholders & Management

Classification: Confidential

Contents

1. Executive Summary

SecureControl is a proof-of-concept banking controls platform built to demonstrate how "dual authorisation" -- commonly called the maker-checker principle -- can be digitised, automated, and made auditable end-to-end. The platform is designed for banking and financial institutions that need to enforce the four-eyes principle on every financial transaction.

In traditional banking operations, transaction creation and approval are handled by two separate individuals to prevent fraud, errors, and unauthorised activity. SecureControl replicates this control digitally, adds automated compliance checks that run in real time, and maintains a tamper-evident audit trail of every action.

> *Key value proposition: Reduce manual compliance effort, catch policy violations instantly, and give management a transparent audit trail -- all in one platform.*

At a Glance

- Four distinct user roles -- Maker, Checker, Admin, SuperAdmin -- with strict separation of duties
- Every new transaction is automatically scored against configurable compliance rules
- Transactions that breach policy thresholds are flagged before they reach a human reviewer
- A full Know Your Customer (KYC) onboarding pipeline gates user access until identity is verified
- Complete audit history: who did what, when, and to which record
- Role-specific dashboards with real-time statistics and actionable insights
- Modern, responsive interface accessible from desktop and mobile browsers

2. Problem Statement & Business Need

The Challenge

Financial institutions face stringent regulatory requirements around transaction authorisation, customer identity verification, and activity audit trails. Manual processes are error-prone, slow, and difficult to scale. When compliance checks are handled informally or through spreadsheets, institutions risk:

- Regulatory penalties due to missing or incomplete audit trails
- Fraud exposure when one person can both create and approve transactions
- Delayed detection of suspicious or policy-violating transactions
- Inconsistent enforcement of risk thresholds across teams and branches
- Customer onboarding bottlenecks when KYC verification is paper-based
- Difficulty demonstrating compliance posture to auditors and regulators

What the Business Needs

A digital dual-authorisation system that:

- Enforces separation of duties between the person who creates a transaction and the person who approves it
- Automatically evaluates every transaction against a set of configurable compliance rules before it reaches a reviewer
- Maintains a complete, timestamped audit trail of every action -- from user login to transaction approval
- Streamlines customer onboarding with structured KYC collection, validation, and checker-based approval
- Provides management dashboards for oversight of team activity, compliance posture, and operational metrics
- Can be deployed quickly and iterated upon as regulations and business rules evolve

3. Solution Overview

SecureControl addresses every requirement above through an integrated web-based platform. Below is a simplified view of how data flows through the system:

```
+-------------------+        +---------------------+        +------------------+
| MAKER             |        | SYSTEM              |        | CHECKER          |
| Creates a new     |------->| Runs compliance     |------->| Reviews pending  |
| transaction       |        | checks; flags       |        | transactions;    |
|                   |        | violations; scores  |        | approves/rejects |
+-------------------+        +---------------------+        +------------------+
                                      |
                                      v
                             +---------------------+
                             | AUDIT LOG           |
                             | Every action        |
                             | recorded with       |
                             | timestamp & user    |
                             +---------------------+
                                      |
                                      v
                             +---------------------+
                             | MANAGEMENT          |
                             | DASHBOARDS          |
                             | Real-time stats,    |
                             | audit explorer,     |
                             | user oversight      |
                             +---------------------+
```

How It Works -- In Plain Language

1. **A Maker logs in** and creates a transaction (e.g., a fund transfer of $50,000). The system saves it as "pending".
2. **The Policy Engine kicks in** automatically checking the transaction against compliance rules -- amount thresholds, duplicate detection, blacklisted accounts, and business-hours restrictions.
3. **Violations are recorded** and if the total risk score exceeds a threshold, the transaction is flagged for heightened scrutiny.
4. **A Checker opens their dashboard** and sees the pending transaction along with any policy violation warnings. They review, add notes, and approve or reject.
5. **Everything is logged** -- creation, analysis results, checker decision, timestamps, and user identifiers go into the audit trail.
6. **Management views dashboards** showing real-time counts of pending, approved, rejected, and flagged transactions, plus a searchable audit log.

4. User Roles & Responsibilities

SecureControl implements strict role-based access. Each role has a defined set of permissions and a dedicated dashboard tailored to its responsibilities.

Role Matrix

Role	Created By	What They Can Do
Maker	Self-signup	Create transactions, complete KYC onboarding, view own transaction history
Checker	SuperAdmin	Review and approve/reject transactions, review KYC applications, view all data
Admin	SuperAdmin	Same as Checker plus visibility into policy rules configuration
SuperAdmin	System seed	Full system oversight: create users, view all dashboards, manage the platform

> *Separation of duties: A Maker can NEVER approve their own transaction. Only a Checker (or Admin) can approve or reject transactions created by a Maker.*

Role-Based Dashboards

Maker Dashboard

- See personal transaction history and status at a glance
- Create new transactions (fund transfers, payments, account changes, loan approvals)
- Track which transactions are pending, approved, rejected, or flagged

Checker Dashboard

- Queue of pending transactions ordered oldest-first (FIFO) for fair processing
- Policy violation details shown alongside each transaction for informed decisions
- Approve or reject with mandatory notes for audit purposes
- KYC application review queue with approve / reject / request-more-info actions

SuperAdmin Dashboard

- User Overview: total users by role, recent sign-ups
- Transaction Overview: pending, approved, rejected, flagged counts
- KYC Overview: applications pending review, total processed
- Audit Overview: recent system events, today's audit count
- User Management: create new Checker or Admin accounts with automated credential delivery

5. Key Business Workflows

5.1 Transaction Lifecycle

The transaction lifecycle is the core workflow. It ensures no single individual can both originate and approve a financial action.

#	Stage	Actor	What Happens
1	Create	Maker	Enters transaction type, amount, source/destination accounts, notes
2	Analyse	System	Policy engine evaluates 4 rule types; scores risk 0-100
3	Flag (if needed)	System	Risk score >= 40 changes status to 'flagged' automatically
4	Review	Checker	Views transaction + violations; adds notes; approves or rejects
5	Record	System	Audit log entry created for every state change

5.2 Transaction Types Supported

Transaction Type	Business Purpose
Fund Transfer	Movement of funds between accounts with full source/destination tracking
Payment Approval	Authorisation of scheduled or one-time payment requests
Account Change	Modifications to account parameters, beneficiaries, or settings
Loan Approval	Processing and authorisation of loan disbursement or restructuring

5.3 User Onboarding Workflow

New users go through a controlled onboarding pipeline:

- Step 1: User registers with name, email, and password
- Step 2: System sends a one-time password (OTP) to the email for verification
- Step 3: On successful OTP verification, the account is created with Maker role
- Step 4: User is directed to a 5-step KYC identity verification wizard
- Step 5: Submitted KYC application enters a review queue for Checkers
- Step 6: User cannot access the transaction dashboard until KYC is approved
- Step 7: If KYC is rejected, the user is informed of the reason and can re-apply

Business benefit: No user can create transactions without verified identity, ensuring regulatory compliance from the very first interaction.

6. Compliance & Risk Controls

Every new transaction is automatically evaluated by the built-in Policy Engine before it reaches a human reviewer. This dramatically reduces the risk of non-compliant transactions slipping through and ensures checkers are armed with the right information.

6.1 Automated Policy Checks

The engine currently supports four types of configurable compliance rules:

Amount Threshold

Flags transactions whose amount exceeds a defined limit. Severity scales automatically based on how far the amount exceeds the threshold -- from Low (just over) to Critical (10x or more over the limit).

Duplicate Detection

Identifies potential duplicate transactions by looking for matching amounts sent to the same destination account within a rolling 24-hour window. Multiple matches raise the severity level.

Blacklist Check

Cross-references both the source and destination account against a maintained blacklist of flagged entities. Any match is treated as Critical severity.

Business Hours Check

Flags transactions created outside standard business hours (Monday-Friday, 9 AM - 6 PM). This is an informational check -- low severity -- but provides visibility into unusual activity patterns.

6.2 Risk Scoring

Each violated rule adds to a composite risk score (range: 0-100). If the total score reaches 40 or above, the transaction is automatically flagged for heightened review.

Severity	Points	Business Meaning
Critical	40	Immediate attention -- blacklist match or extreme amount breach
High	25	Escalation to senior management recommended
Medium	15	Enhanced checker review required
Low	5	Informational -- after-hours or minor threshold breach

6.3 Automated Recommendations

The engine generates plain-language recommendations alongside violations:

- "Review transaction details carefully" -- on any violation
- "Escalate to senior management" -- when critical or high severity detected
- "Verify beneficiary identity" -- when a blacklist match is found

Business impact: Compliance checks that previously required manual review of every transaction are now automated. Checkers focus their attention where it matters most.

7. Customer Onboarding (KYC)

The platform includes a full digital Know Your Customer (KYC) pipeline. This ensures that every user's identity is verified against Indian regulatory standards before they can transact.

7.1 The 5-Step KYC Wizard

Step	Section	Information Collected
1	Personal Info	Full name, date of birth, PAN number, Aadhaar number
2	Contact Details	Mobile number, email, current address, permanent address
3	Employment	Account type (savings/current/salary), occupation, annual income, PEP status
4	Nominee	Nominee name, relationship, date of birth (optional, can be skipped)
5	Review	Summary of all data with section-level edit before final submission

7.2 Validation Standards

- PAN: Validated against standard format (ABCDE1234F)
- Aadhaar: Validated as exactly 12 digits
- Mobile: Validated as exactly 10 digits
- Duplicate applications are prevented at the system level

7.3 Review & Approval Process

- Submitted applications appear in the Checker's KYC review queue
- Checker can approve, reject (with reason), or mark as 'under review'
- On approval, the user's dashboard access is unlocked automatically
- On rejection, the user sees the reason and can re-submit
- Each application gets a unique tracking ID (format: KYC-2026-000001)
- The KYC status page auto-refreshes every 30 seconds for real-time updates

Business benefit: End-to-end digital KYC -- from identity capture to checker approval -- eliminates paper-based delays and creates an audit trail for every application.

8. Audit & Transparency

Regulators and internal auditors require a clear record of who did what, when, and to which entity. SecureControl automatically logs every meaningful action without requiring manual record-keeping.

8.1 What Gets Logged

Event	When It Fires
Transaction Created	A Maker submits a new transaction
Transaction Approved	A Checker approves a pending transaction
Transaction Rejected	A Checker rejects a pending transaction
Blacklist Entry Added	An admin adds an account to the blacklist
Blacklist Entry Removed	An admin deactivates a blacklist entry
Policy Rule Updated	An admin modifies a compliance rule
User Login	Any user successfully authenticates
User Created	SuperAdmin creates a new Checker or Admin user
User Role Updated	SuperAdmin changes a user's role
User Deactivated	SuperAdmin deactivates a user account

8.2 Audit Record Detail

Every audit entry captures:

- Who performed the action (user identity)
- What action was taken (standardised action code)
- Which entity was affected (with entity type and ID)
- Before and after snapshots (previous state vs. new state)
- When the action occurred (server timestamp)
- Client IP address (where available)

8.3 Audit Explorer

Management and auditors can access a dedicated Audit Log page that displays a paginated, searchable list of the most recent events. Each entry shows the user, action, affected entity, and timestamp -- providing a single source of truth for compliance reviews.

> *Audit readiness: When regulators request evidence of who approved a transaction and when, the answer is available instantly from the audit explorer.*

9. Dashboard & Reporting

Each role sees a tailored dashboard designed for their daily responsibilities. Information is displayed through real-time statistics cards, transaction tables, and status indicators.

9.1 Maker View

- Total transactions submitted by the user
- Breakdown: pending, approved today, rejected today
- Recent transactions table with status badges and quick detail links
- One-click 'New Transaction' action

9.2 Checker View

- Pending transaction count (items awaiting action)
- Flagged transaction count (policy-violated items requiring extra scrutiny)
- Personal productivity: approved and rejected counts for the day
- FIFO-ordered pending queue with inline approve/reject actions
- Policy violations displayed alongside each transaction for context

9.3 SuperAdmin View

- User Overview: total count per role, recent user activity
- Transaction Overview: pending, approved, rejected, flagged -- across all users
- KYC Overview: applications pending review vs. completed
- Audit Overview: today's event count, recent audit entries
- User Management: create new Checker/Admin users with auto-emailed credentials
- Links to Audit Log explorer and Policy Rules overview

9.4 Common Features

- Responsive design: works on desktop, tablet, and mobile browsers
- Light and dark theme support
- Loading skeletons for fast perceived performance
- Collapsible sidebar navigation customised per role

10. Security Posture

Security is layered across the entire stack rather than relying on any single mechanism.

Identity & Access

- Email/password authentication with server-side encrypted session cookies
- OTP email verification during registration (5-minute expiry, 3-attempt limit)
- User roles read from database (not from the authentication token) -- preventing token-tampering attacks
- Temporary passwords for admin-created accounts enforce complexity requirements

Authorisation Layers

Every request passes through three independent security checkpoints:

- Layer 1 -- Route Protection: Middleware blocks access to pages the user's role is not permitted to see
- Layer 2 -- API Verification: Every API call re-verifies the caller's identity and role before processing
- Layer 3 -- Database Policies: Row Level Security in the database restricts data visibility and write access per role, even if the upper layers are bypassed

Data Protection

- All database queries enforce Row Level Security; no direct table access is possible
- Sensitive operations like user creation use a privileged server-side key that is never exposed to the browser
- Identity fields (PAN, Aadhaar) are validated on both client and server
- Secrets and API keys are stored in environment variables and never committed to version control

> *Defence in depth: Even if one security layer is compromised, the remaining layers prevent unauthorised data access or privilege escalation.*

11. Technology Choices (Why It Matters)

The technology stack was selected for speed of development, enterprise-grade security, and long-term maintainability. Here is what each layer does for the business:

Layer	Technology	Business Reason
Frontend	Next.js + React	Fast, interactive UI with server-side rendering for security
Styling	Tailwind CSS	Consistent, maintainable design across all pages
Database	Supabase (Postgres)	Enterprise Postgres with built-in auth, RLS, and real-time
Authentication	Supabase Auth	Battle-tested auth with session management included
Email	Resend API	Reliable transactional email for OTPs and notifications
Validation	Zod + Hook Form	Prevents invalid data from reaching the database
Language	TypeScript	Catches bugs at development time, not in production
Analytics	Vercel Analytics	Lightweight usage and performance insights
Deployment	Vercel	Zero-downtime deployments with global CDN

> *All chosen technologies are widely adopted, well-documented, and backed by active communities -- reducing vendor lock-in risk and ensuring access to engineering talent.*

12. Deployment & Availability

Current Deployment Model

- The application is hosted on Vercel with automatic deployments from the code repository
- Database and authentication services are provided by Supabase (managed cloud)
- Both services offer high availability, automatic backups, and regional redundancy

Environment Configuration

The platform is configured through environment variables -- no code changes are needed to move between development, staging, and production environments. Variables include database connection strings, authentication keys, and email API credentials.

Setup for New Environments

- 1. Provision a new Supabase project and enable email authentication
- 2. Run the provided SQL migration scripts to create the database schema
- 3. Seed the SuperAdmin account using the provided CLI script
- 4. Configure environment variables on the hosting provider
- 5. Deploy -- the application is fully operational

> *A new environment (e.g., staging or UAT) can be stood up in under 30 minutes by following the documented setup steps.*

13. What Has Been Delivered (Scope)

Below is a comprehensive summary of everything implemented in this proof-of-concept, organised by functional area.

Authentication & User Management

- Email/password registration with OTP email verification
- Login with role-based routing to appropriate dashboard
- Sign-out with secure session cleanup
- SuperAdmin user creation flow (Checkers and Admins) with automated credential emails
- Role-based route protection (middleware-enforced)

KYC Onboarding

- 5-step digital KYC wizard with Indian identity validation (PAN, Aadhaar)
- Auto-generated KYC application IDs for tracking
- Checker review queue with approve/reject/under-review workflows
- Dashboard access gating until KYC is approved
- Real-time status polling with auto-redirect on approval
- Re-application flow for rejected applications

Transaction Management

- 4 transaction types: Fund Transfer, Payment Approval, Account Change, Loan Approval
- Multi-currency support (INR, USD, EUR, GBP, JPY, CAD, AUD)
- Full maker-checker lifecycle: create -> analyse -> review -> approve/reject
- Transaction detail view with account flow, timestamps, and checker notes
- Status-based filtering and search across transaction history

Policy Engine & Compliance

- 4 automated rule types: amount threshold, duplicate detection, blacklist check, business hours
- Composite risk scoring (0-100) with automatic flagging at score >= 40
- Severity-based colour coding: critical, high, medium, low
- Contextual recommendations for checkers
- Policy violations displayed alongside transactions in the review queue

Blacklist Management

- Maintain a list of flagged account numbers with entity name and reason
- Toggle active/inactive without deleting records
- Automatic cross-referencing during policy analysis

Audit Trail

- 10 distinct audited event types covering all critical actions
- Before/after state snapshots for change tracking
- Paginated audit log explorer accessible to authorised roles

Dashboards

- 3 role-specific dashboards (Maker, Checker, SuperAdmin) with real-time statistics
- Responsive layout with collapsible sidebar and theme switcher
- Loading skeletons and progressive data display

Component Library

- 50+ reusable, accessible UI components (buttons, forms, tables, dialogs, etc.)
- Dark/light theme support across all components
- Responsive across desktop, tablet, and mobile viewports

14. Future Roadmap & Business Opportunities

The proof of concept establishes a solid foundation. Below are the planned enhancements that would add significant business value in subsequent phases.

Phase 2 -- Enhanced Workflows

- Multi-level approval chains: configurable escalation paths (e.g., manager -> compliance officer -> head of department)
- SLA tracking: monitor and alert on aging pending transactions to prevent processing delays
- Maker/checker workload balancing: assign transactions based on domain expertise and availability
- Automated notifications: email, Slack, and Teams alerts on critical violations or SLA breaches

Phase 3 -- Document Processing

- Cheque ingestion pipeline: upload cheque images/PDFs, run OCR, and auto-extract transaction details
- Automated authenticity scoring: AI-based checks on uploaded documents
- Document attachment support on transactions for supporting evidence

Phase 4 -- Analytics & Reporting

- Risk trend dashboards: visualise compliance posture over time
- Export capabilities: generate CSV and PDF reports for regulators and auditors
- Historical analytics: transaction volume, approval rates, average processing time
- Anomaly detection: identify unusual patterns in transaction activity

Phase 5 -- Enterprise Integration

- Core banking integration: connect to existing banking systems via APIs or ETL pipelines
- AML screening: integrate with anti-money laundering services for enhanced compliance
- Event streaming: publish transaction events to enterprise message queues for downstream systems
- Advanced observability: Sentry, Datadog, and Grafana dashboards for operational monitoring

> *Each phase builds on the existing architecture without requiring a rewrite. The modular design ensures new capabilities can be added incrementally as business needs evolve.*

End of Document

SecureControl -- Banking Controls Platform -- Proof of Concept

Generated: February 25, 2026