SecureControl

Gap Analysis & Improvement Roadmap

Banking Maker-Checker Controls | Proof of Concept

Version 1.0 | February 2026

Prepared for: Project Stakeholders & Management

Classification: Confidential

1. Identified Gaps

The following gaps have been identified in the current proof-of-concept against production-readiness and regulatory compliance standards for banking control systems.

Governance & Change Control

- No maker-checker workflow for policy rule changes -- rules can be modified without independent approval
- No rule versioning or rollback mechanism -- no ability to revert to a previous rule configuration
- No approval trail for configuration updates -- changes to system settings are not audited through an approval chain

Regulatory & Compliance Readiness

- No regulatory mapping linking controls to specific requirements and evidence (control -> requirement -> evidence)
- Audit logs are described but lack an immutability or tamper-proof mechanism (e.g., append-only, hash chaining)
- No formal data retention policy defined for KYC records, audit logs, or transaction history
- No regulator-ready export package -- no ability to generate PDF/CSV evidence bundles for audits or inspections

Security & Access Management

- No SSO (SAML/OIDC) integration for enterprise identity providers
- No session timeout or device management controls -- sessions persist without forced re-authentication
- No masking or encryption strategy for sensitive PII (PAN, Aadhaar) displayed in the UI

Customer Risk & KYC Lifecycle

- No customer risk-tier classification (low / medium / high risk) based on profile or behaviour
- No periodic or ongoing KYC refresh workflow -- identity verification is one-time only
- No document upload or verification capability -- only format-level validation of identity numbers

Operations & Monitoring

- No monitoring or alerting framework described for system health, anomalies, or SLA breaches
- No transaction reconciliation process post-approval to confirm settlement accuracy
- No structured escalation process for aging or high-risk transactions requiring management intervention

2. Recommended Improvements

The improvements below are prioritised to address the gaps identified above. They are grouped into near-term (high impact, lower effort) and medium-term (deeper integrations).

Near-Term (High Priority)

1. Enforce Multi-Factor Authentication (MFA) for privileged roles (Checker, Admin, SuperAdmin) to strengthen access security
2. Add policy rule approval workflow + versioning -- all rule changes go through maker-checker with full version history and rollback
3. Add export capability for compliance evidence -- generate PDF/CSV audit bundles on demand for regulators
4. Implement rate limiting + session management standards -- enforce session timeouts, concurrent session limits, and API rate caps
5. Field-level encryption & PII masking -- encrypt PAN/Aadhaar at rest; mask sensitive fields in the UI (show last 4 digits only)
6. SLA-based escalation & alerting workflows -- auto-escalate transactions that exceed review time thresholds with email/Slack notifications

Medium-Term (Strategic)

7. SSO integration (SAML/OIDC) -- enable enterprise single sign-on with identity providers like Azure AD, Okta, or Google Workspace
8. Customer risk-tiering model -- classify customers as low, medium, or high risk based on KYC profile, transaction patterns, and external data
9. Ongoing KYC refresh + AML screening integration -- schedule periodic re-verification and integrate with AML/sanctions screening services
10. Rule simulation / back-testing capability -- test new policy rules against historical transactions before activating them in production
11. Behavioural & velocity-based risk rules -- detect unusual patterns such as rapid-fire transactions, sudden amount spikes, or geographic anomalies
12. Case management system -- track flagged transactions through a formal investigation lifecycle with notes, assignments, and resolution tracking
13. End-user dashboards -- provide customer-facing views of account status, transaction history, and KYC status based on the current design
14. Core banking & enterprise system integrations -- connect to core banking APIs, general ledger, and payment gateways for end-to-end processing (optional)

3. Gap-to-Improvement Mapping

The table below maps each identified gap to the recommended improvement that addresses it.

#	Gap	Recommended Improvement
1	No maker-checker for policy changes	Policy rule approval workflow + versioning
2	No rule versioning / rollback	Policy rule approval workflow + versioning
3	No config change approval trail	Policy rule approval workflow + versioning
4	No regulatory mapping	Export capability for compliance evidence
5	Audit logs not tamper-proof	Field-level encryption & immutable log design
6	No data retention policy	Formal retention rules + automated archival
7	No regulator export package	PDF/CSV evidence bundle export
8	No SSO integration	SAML/OIDC SSO integration
9	No session timeout / device mgmt	Rate limiting + session management
10	No PAN/Aadhaar masking	Field-level encryption & PII masking
11	No customer risk-tiering	Customer risk-tiering model
12	No ongoing KYC refresh	Ongoing KYC refresh + AML screening
13	No document upload / verification	Ongoing KYC refresh + document mgmt
14	No monitoring / alerting	SLA-based escalation & alerting workflows
15	No post-approval reconciliation	Core banking integration + reconciliation
16	No structured escalation	SLA-based escalation & alerting workflows

4. Next Steps

We recommend addressing the near-term items (1-6) in the next development sprint to close the most critical compliance and security gaps. Medium-term items (7-14) should be planned into subsequent phases with formal requirements and architectural design reviews.

- Prioritise MFA, PII masking, and session management for immediate security hardening
- Implement policy rule versioning and approval workflow to close the governance gap
- Deliver export capability to satisfy regulator evidence requirements
- Plan SSO, risk-tiering, and AML integration as Phase 2 strategic initiatives
- Evaluate core banking integration scope based on target deployment environment

End of Document