SYSTEMS & PRODUCT DESIGN SPECIFICATION

The institutional operating *system* of TSCF.

TradeAxis is the multi-tenant, role-segregated, financial-grade orchestration platform that operates the TSCF programme through five canonical infrastructure modules — TradePoint verification hubs, TrackGuard logistics monitoring, TradeVault escrow and atomic settlement, TradeAxis origination and reporting, and FarmerIQ farmer intelligence — built around the architectural commitment that the bank sees everything, every counterparty sees exactly what their role requires, and every operational concern has its own institutional home.

Joel NtiAmoah Marfo, Founder & CEO

CONTENTS

The *thirteen* sections.

EXECUTIVE SUMMARY

The brief, in *one page*.

For the bank CTO, DFI investment officer, or institutional auditor who needs the architecture in five minutes before reading the detail.

What it is. TradeAxis is the platform that operationalises the TSCF programme. It is not a marketing surface and not a bank-side reporting tool alone — it is the institutional operating system that runs verification, escrow, atomic settlement, logistics protection, and reporting across every TSCF trade against every facility deployed by every bank in the syndicate.

What it commits to. Three architectural commitments anchor the platform. First, *the bank sees everything* — 100% real-time visibility into every stage of every trade against every facility, structurally enforced from the data model upward. Second, *every counterparty sees exactly what their role requires* — segregated workspaces, role-calibrated portals, and engagement workflows for those counterparties whose pattern doesn't justify a portal. Third, *every operational concern has its own institutional home* — quality, treasury, logistics, compliance, and analytics are separately architected modules, not conflated sub-features.

How it is built. The platform delivers its institutional commitments through *five canonical modules* — **TradePoint** (the verification layer; six weighbridge hubs across Northern Ghana, three-point weight verification, field-officer supervised loading), **TrackGuard** (the logistics layer; GPS monitoring with geofencing alerts from hub to buyer warehouse), **TradeVault** (the settlement layer; ringfenced escrow and atomic waterfall engine that makes "bank principal first" structurally enforceable), **TradeAxis** (the origination layer; trade origination, validation scoring, Finance Partner Portal), and **FarmerIQ** (the intelligence layer; 10,000+ registered farmer profiles, the data asset supporting SDG impact reporting and EUDR compliance). Underneath these five canonical modules sits a fourteen-module architectural decomposition across four functional layers, seven portal surfaces, four integration surfaces, and three security perimeters at financial-grade discipline.

How visibility works. The Finance Partner Portal is the bank's institutional showpiece — six dashboard groupings (Facility Overview, Active Trades, Live Logistics, Settlement & Reconciliation, Risk & Exceptions, Counterparty & Compliance) that together deliver the 100% visibility commitment. The Internal Operations Console is Miziba's own cockpit — eight super admin groupings providing cross-facility intelligence that no individual bank sees, including access-restricted Platform Financial Position with related-party governance state visible.

How it gets built. Three phases over eighteen months. **Phase I · MVP** (months 1–5, USD 250K–380K): TSCF—D variant only, all three source patterns live, basic TrackGuard, Finance Partner Portal Groupings 1–4, full security and audit posture, related-party governance enforced in code. **Phase II · Multi-Bank Stack** (months 6–10, USD 400K–580K incremental): TSCF—X export workflow, full Insurance & Guarantee Orchestration, multi-bank tenant isolation, advanced analytics. **Phase III · Institutional Hardening** (months 11–18, USD 200K–350K incremental): regulator interface, SOC 2 Type II, full disaster recovery. Total 18-month investment: *USD 850K–1.31M*.

What this means strategically. The brief is the institutional artefact that converts every successful first meeting into a credible technical due-diligence conversation. It sits in the documentation library at miziba.com/documents alongside the Operations Manual, Bank Engagement Playbook, Capital Strategy, Corporate Governance Manual, and Visual System — completing the institutional documentation pack on the systems-and-platform layer.

SECTION I · PLATFORM THESIS

The platform *thesis*.

What TradeAxis exists to solve. The architectural commitments that anchor every design decision. The institutional principles that distinguish it from the operational tooling of conventional commodity finance.

The *diagnosis*.

African commodity finance has a verification problem, not a credit problem. Bank credit committees do not refuse to deploy capital into smallholder commodity flows because the trades are structurally unbankable — they refuse because the verification infrastructure required to underwrite the trades to institutional standard does not exist. The trader cannot prove the commodity exists. The aggregator cannot prove the source attestation chain. The buyer cannot prove the offtake commitment. The bank cannot reconcile its facility against an audit trail it can defend internally. In the absence of that infrastructure, capital flows around the problem — into corporate receivables, into export-financing programmes for established counterparties, into anywhere that has an existing verification stack — while the commodity flows that need the capital most are systematically excluded.

TradeAxis exists to *build that verification infrastructure* to institutional standard. It is the platform that gives the bank the same auditability over a TSCF trade that it has over a corporate receivable, the same operational visibility that it has over a syndicated facility, and the same security and compliance posture that it expects from any Tier 1 financial system in its operating environment.

The *three architectural commitments*.

Three commitments anchor every design decision in the platform. They are non-negotiable. They are the difference between an institutional operating system and a software product that describes itself as institutional.

I · THE THREE ARCHITECTURAL COMMITMENTS

Three commitments. *Non-negotiable*.

i

The bank sees *everything*.

One hundred percent real-time visibility into every stage of every trade against every facility. Not "comprehensive reporting." Not "real-time dashboards." **Every action, every artefact, every state change, every settlement event, structurally enforced from the data model upward, with the audit-grade evidence chain accessible at any time**. The bank's institutional position as senior secured capital partner determines whether the programme exists at all; the platform is built around protecting that position.

ii

Every counterparty sees *exactly what their role requires*.

Segregated workspaces, role-calibrated portals, structured engagement workflows for counterparties whose pattern doesn't justify a portal. The trader does not see the bank's internal scoring. The buyer does not see the trader's equity record. The DFI does not see the bank's individual trade approvals. **Each counterparty operates within the institutional surface calibrated to their accountability, with no information leakage between roles**. This is what makes the platform multi-tenant in the institutional sense, not just the technical sense.

iii

Every operational concern has its *own institutional home*.

Quality verification is not a sub-feature of hub operations. Treasury management is not a tab inside escrow. Compliance reporting is not a panel inside analytics. Logistics is not a stage in a trade. **Each operational concern is a distinct module with its own data model, its own audit trail, its own permissions matrix, and its own integration surface**. This separation is what makes the platform Fortune 500-grade rather than well-marketed — it ensures every operational accountability has a clear architectural home, and every external audit can find what it needs without archaeology.

> *A platform that conflates operational concerns is a platform that conflates accountability. Institutional credibility lives or dies at the architectural separation layer.*

I · THE INSTITUTIONAL VOCABULARY FAMILY

Seven proper nouns. *One institution*.

The platform anchors to a discipline of proper-noun vocabulary that extends across every layer of the institutional architecture. Two institutional names (Miziba, TSCF), one platform name (TradeAxis), and four canonical infrastructure modules (TradePoint, TrackGuard, TradeVault, FarmerIQ) that together operate the platform.

NAME 01 · THE INSTITUTION — CANONICAL

Miziba

Miziba Infrastructure Ltd. The Ghana-incorporated company that owns the verification, escrow, and atomic settlement infrastructure. Founded 2025 by Joel NtiAmoah Marfo. Distinct from JNI AGRI Ltd, the anchor aggregator co-founded by the same founder — the structural separation between the two entities is governed by five explicit controls.

NAME 02 · THE PROGRAMME — CANONICAL

TSCF

TradeAxis Secured Commodity Finance. The institutional programme that connects independent commodity traders with bank capital under a Master Facility Agreement, secured by the seven-layer protection cascade and settled through the atomic five-tier waterfall. Three product variants: **TSCF—D** (domestic, GHS-denominated, 22–30 day tenor), **TSCF—P** (buyer pre-fund), **TSCF—X** (export, USD/GHS, 37 day tenor).

NAME 03 · THE PLATFORM — CANONICAL

TradeAxis

The multi-tenant, role-segregated, financial-grade orchestration platform that operates the TSCF programme through five canonical infrastructure modules. The subject of this brief. The institutional operating system — not a marketing surface, not a bank reporting tool, but the system of record for every TSCF trade across every facility deployed by every bank. **At the module level**, TradeAxis is also the canonical name for the origination layer (trade origination, validation scoring, Finance Partner Portal) — the same proper-noun vocabulary operates at both the platform and module levels.

NAME 04 · THE VERIFICATION LAYER — CANONICAL MODULE

TradePoint

The physical hub network across Northern Ghana — **six weighbridge-equipped TradePoint hubs** at Tamale, Bolgatanga, Wa, Damongo, Techiman, Wenchi — and the field-side software portal (TradePoint Portal) used by Miziba and JNI AGRI Ltd field officers. The physical layer where commodity is verified before any bank capital deploys, with three-point weight verification (hub scale, weighbridge, destination reconciliation), quality grading, and field officer-supervised loading. *This is where the verification chain begins*.

I · VOCABULARY FAMILY (CONTINUED)

The three remaining *canonical modules*.

NAME 05 · THE LOGISTICS LAYER — CANONICAL MODULE

TrackGuard

The logistics protection capability and portal. **GPS logistics monitoring with geofencing alerts** from loading hub to buyer warehouse, with full route history retained and deviation alerts that trigger automatically to all parties including the finance partner. The institutional system that protects every TSCF consignment from hub-gate dispatch through last-mile delivery — transporter onboarding, GPS-tagged transit, parametric weather monitoring (Phase II), customs clearance on TSCF—X (Phase II), bank-consigned bill-of-lading control (Phase II), and exception pathway routing. Operated by Miziba's logistics team; transporters and freight forwarders participate through structured workflows rather than dedicated portals.

NAME 06 · THE SETTLEMENT LAYER — CANONICAL MODULE

TradeVault

The institutional commitment that makes *bank principal first* structurally true rather than rhetorically true. **The ringfenced escrow and atomic waterfall settlement engine**, held at designated commercial banks under tripartite Escrow Agreement. Receives buyer payments into ringfenced TSCF Escrow Accounts, executes the five-tier waterfall (bank principal → bank fee → Miziba structuring → Miziba monitoring → trader margin) atomically and irreversibly, produces settlement certificates, and reconciles automatically against the bank's own treasury statement. *It is impossible to pay the trader before the bank is fully repaid — not as policy, but as architecture*. Manual fallback documented in Clause 8.2 of the Master Facility Agreement.

NAME 07 · THE INTELLIGENCE LAYER — CANONICAL MODULE

FarmerIQ

The data asset that makes development outcomes auditable. **Intelligence profiles for 10,000+ registered smallholder farmers** across Northern Ghana — payment history, commodity volumes, village location, gender data, mobile money records, and traceability evidence. The data asset that supports SDG impact reporting (SDGs 1, 2, 5, 8, 9), EUDR compliance for European-corridor TSCF—X exports, and DFI investment-committee evidence requirements. Maintained by Miziba and JNI AGRI Ltd field officers operating the TradePoint hub network. *Every farmer payment timestamped and traceable*.

SECTION II · THE FIVE CANONICAL MODULES & FOURTEEN BUILDING BLOCKS

Five *canonical modules*. Fourteen *building blocks*.

The platform organises around two complementary structures. ***Five canonical Miziba modules*** *— TradePoint, TrackGuard, TradeVault, TradeAxis, FarmerIQ — constitute the institutional vocabulary that bank, DFI, and trader counterparties interact with.* ***Fourteen architectural building blocks across four functional layers*** *are how the engineering team decomposes the implementation. Every building block delivers a capability of one or more canonical modules; every canonical module is delivered by multiple building blocks.*

The *four architectural layers*.

Layer A · Counterparty Identity & Onboarding. The people layer. Modules 1–2 handle the verification of every counterparty class and every supply source that participates in the platform.

Layer B · Trade Operations. The deal layer. Modules 3–8 handle the full lifecycle of a TSCF trade from origination through atomic settlement, with logistics, quality, and treasury as distinct architectural homes.

Layer C · Risk, Recovery & Compliance. The protection layer. Modules 9–11 handle insurance and guarantee orchestration, exception and recovery workflows, and the continuous regulatory and compliance operation that institutional finance requires.

Layer D · Platform Infrastructure. The system layer. Modules 12–14 handle reporting, audit and analytics; document vault and lifecycle archive; and the integration hub and notification services that connect every module to every external system.

The next page maps each of the five canonical modules to its architectural building blocks. The pages that follow specify each of the fourteen building blocks in detail.

II · FROM FIVE CANONICAL MODULES TO FOURTEEN BUILDING BLOCKS

How the *five* deliver the *fourteen*.

The five canonical Miziba modules are the institutional vocabulary that bank, DFI, and trader counterparties interact with. The fourteen architectural building blocks are how the engineering team decomposes the implementation. Every building block delivers a capability of one or more canonical modules.

CANONICAL 01 · **TRADEPOINT** — VERIFICATION LAYER

Six weighbridge hubs across Northern Ghana · field officer-supervised loading · three-point weight verification (hub scale, weighbridge, destination reconciliation) · quality grading at the source. **Architectural building blocks:** Module 1 (Onboarding for field officers) · Module 2 (Source Verification at hubs) · Module 5 (Quality Verification & Certification).

CANONICAL 02 · **TRACKGUARD** — LOGISTICS LAYER

GPS monitoring with geofencing alerts from loading hub to buyer warehouse · transporter and freight-forwarder onboarding · bank-consigned BL control (Phase II) · logistics exception pathway routing. **Architectural building blocks:** Module 1 (Transporter onboarding) · Module 6 (Logistics & Movement Control) · Module 9 (transit insurance orchestration).

CANONICAL 03 · **TRADEVAULT** — SETTLEMENT LAYER

Ringfenced TSCF Escrow Accounts held at designated commercial banks · atomic five-tier waterfall engine · settlement certificate generation · bank-statement reconciliation · *bank principal first as architecture, not policy*. **Architectural building blocks:** Module 7 (Escrow & Atomic Settlement) · Module 8 (Treasury, Cash & Currency Management) · Module 13 (settlement certificate archive).

CANONICAL 04 · **TRADEAXIS** — ORIGINATION LAYER

Trade origination workflow with five-item validation scoring · credit decisioning and bank workflow · the Finance Partner Portal · reporting and analytics. **Architectural building blocks:** Module 3 (Trade Origination) · Module 4 (Credit Decisioning & Bank Workflow) · Module 12 (Reporting, Audit & Analytics).

CANONICAL 05 · **FARMERIQ** — INTELLIGENCE LAYER

10,000+ registered farmer profiles · payment history and commodity volumes · village location, gender data, mobile money records · the data asset for SDG impact reporting and EUDR compliance. **Architectural building blocks:** Module 2 (Source Registry · direct farmer pattern) · Module 11 (EUDR documentation pack assembly) · Module 12 (impact reporting layer).

CROSS-CUTTING INFRASTRUCTURE

Modules 10, 13, 14 are cross-cutting infrastructure — the platform substrate.

Module 10 (Exception & Recovery Workflow), Module 13 (Document Vault & Lifecycle Archive), and Module 14 (Integration Hub & Notification Services) operate across all five canonical modules. They do not belong to a single canonical module; they are the institutional substrate that makes all five canonical modules deliverable at financial-grade discipline.

LAYER A

Counterparty identity & onboarding

MODULE 01 — FULL AT MVP

Counterparty Onboarding & *KYC/KYB*

The entry point for traders, aggregators, buyers, insurance partners, and DFI partners — counterparty classes whose participation depends on identity and credit verification. Module 1 owns the unified Counterparty Registry as system of record, with operational profiles written by other modules (notably TrackGuard for transporters and freight forwarders).

SUB-COMPONENTS	Trader onboarding flow · aggregator onboarding flow · buyer onboarding flow · insurance partner onboarding · DFI partner onboarding · bank onboarding (technical integration) · Counterparty Registry as system of record
VERIFICATION	Regulator-grade identity verification · beneficial ownership tracing · sanctions screening · document collection · structured approval workflow
BANK VISIBILITY	Every onboarded counterparty visible in Finance Partner Portal Grouping 6 (Counterparty & Compliance) with full audit access
PORTAL TOUCHPOINTS	Trader Portal · Aggregator Portal · Buyer Portal · Internal Operations Console (counterparty management)
INTEGRATIONS	Sanctions screening providers · identity verification services · tax authority lookup (GRA TIN verification)

MODULE 02 · CANONICAL: **FARMERIQ** + TRADEPOINT — FULL AT MVP · ALL THREE PATTERNS

Source Registry & *Origin Verification*

The supply-source verification layer. **The direct farmer pattern is operationalised through FarmerIQ** — the canonical Miziba module that maintains intelligence profiles for 10,000+ registered smallholder farmers across Northern Ghana, with payment history, commodity volumes, village location, gender data, and mobile money records. Three distinct verification patterns: **direct farmer delivery** (FarmerIQ), **cooperative or village-group bulk delivery**, and **Tier-2 aggregator bulk delivery**. Each pattern produces the same downstream artefact — a verified source declaration that flows into the trade audit trail and ultimately into the bank's Finance Partner Portal. EUDR-compliance traceability runs through all three patterns for European-corridor exports, drawing on FarmerIQ's geolocation and gender data.

FARMERIQ REGISTRY	10,000+ registered smallholder farmers · biometric/QR ID · mobile money linkage · payment history · commodity-cycle history · quality reputation · women-cooperative grouping · gender data · village geolocation · EUDR-ready
COOPERATIVE REGISTRY	Village groups, women's cooperatives, farmer associations · KYB pack · internal governance documentation · aggregation manifest format · member-attestation discipline
TIER-2 REGISTRY	Intermediate aggregators · KYB pack · source-chain attestation · quality certification standards · audit history
BULK VERIFICATION	Structured workflow calibrated separately for cooperative and aggregator-bulk patterns · warranties signed by appropriate counterparty
EUDR COMPLIANCE	FarmerIQ geolocation and deforestation-free attestation chain through all three patterns · for European-corridor TSCF—X trades
BANK VISIBILITY	Source declaration visible on every trade in Active Trades panel · verification pattern labelled (direct/cooperative/Tier-2) · FarmerIQ profile accessible by drill-down on direct farmer pattern

LAYER B

Trade operations · the deal layer

MODULE 03 · CANONICAL: TRADEAXIS (ORIGINATION) TSCF—D AT MVP · X & P PHASE II

Trade *Origination*

The independent trader's workspace for structuring new TSCF deals. **This is TradeAxis at the module level** — the canonical Miziba origination module that runs the five-item validation scoring (offtake contract, equity confirmation, source attestation, quality certification, buyer reasonableness) and produces a structured trade memo for bank credit-committee review. Buyer offtake contract upload, aggregator selection, commodity specification, source-pattern selection (direct farmer / cooperative / Tier-2), facility request, equity confirmation, quality certification reference. Outputs a structured trade memo that flows directly to Module 4 (Credit Decisioning) for bank credit-committee review.

VARIANT SUPPORT	TSCF—D origination at MVP · **TSCF—P and TSCF—X added in Phase II**
TRADEAXIS SCORING	Five-item validation: offtake contract validation · equity confirmation · source attestation · quality certification · buyer price reasonableness
OUTPUTS	Structured trade memo · equity-confirmation receipt · offtake-contract artefact · quality-certification reference
BANK VISIBILITY	Every trade memo visible at origination in Finance Partner Portal Grouping 2 (Active Trades), stage marked ORIGINATION
PORTAL	Trader Portal (web + mobile responsive)

MODULE 04 · CANONICAL: TRADEAXIS (BANK WORKFLOW) FULL AT MVP · SINGLE BANK

Credit Decisioning & *Bank Workflow*

The bank-side workspace where credit officers review trade memos, run their own internal risk scoring, request additional information, approve or reject facilities, and execute drawdown instructions. **The bank-facing surface of the TradeAxis canonical module** — with the TradeAxis origination workflow (Module 3) producing the trade memo and the TradeAxis bank workflow (this module) routing it through credit committee. Maintains complete audit trail of every decision, every information request, and every approval signature.

WORKFLOW	Trade memo review · internal risk scoring · information request routing back to trader · approval/rejection with reasoning · drawdown instruction · facility-state tracking
AT MVP	Single pilot bank workflow · **multi-bank tenant isolation in Phase II**
BANK VISIBILITY	Native to bank — every action by credit officer audit-logged in Grouping 2 (Active Trades) drill-down for that trade
PORTAL	Finance Partner Portal (institutional-grade)
INTEGRATIONS	Bank's internal credit scoring system · bank's facility ledger · bank's treasury system

MODULE 05 · CANONICAL: TRADEPOINT (QUALITY) BASIC AT MVP · FULL PHASE II

Quality Verification & *Certification*

The quality lifecycle is its own architectural domain — **operationalised through TradePoint**, the canonical Miziba verification module. Pre-shipment certification, hub-side grading at the six TradePoint hubs, dispute resolution with the buyer, Layer 4 retention pool reconciliation, and EUDR-compliance traceability for export trades. Quality verification is not a sub-feature of hub operations; it is a distinct module with its own audit trail, with TradePoint as its physical and software substrate.

AT MVP	Basic grading absorbed into TradePoint Portal field-officer workflow · **standalone module Phase II** with full pre-shipment certification, dispute-resolution workflow, retention-pool reconciliation
SUB-COMPONENTS (PHASE II)	Pre-shipment certification workflow · structured quality grading per commodity · quality-dispute resolution with buyer · Layer 4 retention pool reconciliation · EUDR documentation pack assembly
BANK VISIBILITY	Quality state on every trade in Active Trades drill-down · quality-dispute exceptions in Grouping 5 (Risk & Exceptions)

LAYER B

Trade operations continued

MODULE 06 · CANONICAL: **TRACKGUARD** — BASIC AT MVP · FULL PHASE II

Logistics & *Movement Control*

This is TrackGuard — the canonical Miziba logistics module. GPS logistics monitoring with geofencing alerts from loading hub to buyer warehouse, full route history retained, deviations triggering automatic alerts to all parties including the finance partner. The logistics protection layer that runs from hub-gate dispatch through last-mile delivery. Transporters and freight forwarders are managed by Miziba's logistics team via TrackGuard — counterparties do not log into a dedicated portal of their own. TrackGuard absorbs operational onboarding for both classes (KYB, vehicle/route certification, GPS-device registration, BL-issuance authority where applicable).

AT MVP	Domestic transit only · transporter onboarding · GPS-tagged dispatch · real-time monitoring · route-deviation and dwell-time alerts
PHASE II ADDITIONS	**Parametric weather layer** · **customs and clearance workflow** · **bank-consigned bill-of-lading control** · **port-side handover documentation** · **freight-forwarder operational onboarding**
SUB-COMPONENTS	Transporter onboarding · freight-forwarder onboarding (Phase II) · dispatch workspace · transit monitoring · weather layer (Phase II) · customs workflow (Phase II) · BL control (Phase II) · port-side handover (Phase II) · last-mile delivery · logistics exception pathway
BANK VISIBILITY	Live consignment map and table in Finance Partner Portal Grouping 3 (Live Logistics) with GPS, route, ETA, weather, BL state · aggregated across all active facilities

MODULE 07 · CANONICAL: **TRADEVAULT** — FULL AT MVP · NON-NEGOTIABLE

Escrow & *Atomic Settlement*

The institutional commitment that makes "bank principal first" structurally true rather than rhetorically true. **This is TradeVault** — the canonical Miziba settlement module. Receives buyer payments into ringfenced TSCF Escrow Accounts (held at designated commercial banks under tripartite Escrow Agreement), executes the five-tier waterfall (bank principal → bank fee → Miziba structuring → Miziba monitoring → trader margin) atomically and irreversibly, produces settlement certificates, and reconciles automatically against the bank's own treasury statement. **This module cannot be MVP'd at less than full institutional standard** — either the waterfall executes atomically with bank principal returned first, or the bank's senior-secured position is not enforceable. *It is impossible to pay the trader before the bank is fully repaid — not as policy, but as architecture*. Manual fallback documented in Clause 8.2 of the Master Facility Agreement.

AT MVP	Full at MVP standard · GHS settlement only · **USD multi-currency in Phase II**
TRADEVAULT ENGINE	Ringfenced TSCF Escrow Account management · atomic five-tier waterfall in code · settlement certificate generation · bank-statement reconciliation · cryptographically sealed waterfall execution log
BANK VISIBILITY	Every TradeVault waterfall execution shown in real time in Grouping 4 · principal/fee state · reconciliation status
LEGAL ANCHOR	Tripartite Escrow Agreement · Waterfall Agreement signed by all parties before escrow funded · MFA Clause 8.2 (manual fallback)

MODULE 08 — BASIC AT MVP · FULL PHASE II

Treasury, Cash & *Currency Management*

The treasury workflow that operates alongside escrow. Facility utilisation forecasting, drawdown timing optimisation, currency exposure management on TSCF—X (USD/GHS), interest accrual computation, fee recognition timing. A bank's treasury team operates differently from its credit team and needs its own workspace.

AT MVP	Basic cash-position visibility within Module 7 · **standalone treasury workflow Phase II**
PHASE II SUB-COMPONENTS	Facility utilisation forecasting · drawdown timing optimisation · FX exposure management · interest accrual · fee recognition

LAYER C

Risk, recovery & compliance

MODULE 09 — TRANSIT INSURANCE AT MVP

Insurance & *Guarantee Orchestration*

Workflow for activating Layer 6 insurance policies (buyer credit, transit, parametric weather, key-person) and Layer 7 DFI guarantees on a per-trade basis. Tracks coverage in real time, routes claim instructions on stress events, manages policy renewal cycles, and reconciles claim payouts back into the settlement engine.

AT MVP	Per-trade transit insurance activation · **full four-policy stack and DFI guarantee orchestration in Phase II**
LAYER 6 (PHASE II)	Buyer credit insurance · transit insurance · parametric weather insurance · key-person insurance
LAYER 7 (PHASE II)	DFI guarantee capacity activation · quarterly portfolio reporting to DFI partners · claim-instruction routing
BANK VISIBILITY	Insurance state on every trade in Active Trades drill-down · DFI guarantee status in Grouping 6 (Counterparty & Compliance)

MODULE 10 — BASIC AT MVP · FULL PHASE II

Exception & *Recovery Workflow*

The structured workflow for handling stress events — quality dispute, payment delay, transit anomaly, weather event, transporter failure, buyer default, force majeure. Each exception class has a pre-defined recovery sequence that routes through Layers 4–7 of the protection cascade in order.

AT MVP	Basic exception flagging in Finance Partner Portal Risk & Exceptions panel · manual escalation by Miziba operations team · **structured recovery-pathway viewer in Phase II**
PHASE II SUB-COMPONENTS	Active exceptions queue with classification · recovery pathway viewer (Layer 4→5→6→7 sequence) · claim instruction workflow · stress-test panel for scenario modelling · historical recovery patterns
BANK VISIBILITY	Every exception flagged in real time in Grouping 5 (Risk & Exceptions) with severity, age, classification, and proposed mitigation pathway

MODULE 11 — BASIC AT MVP

Regulatory & *Compliance Operations*

Continuous regulatory and compliance workflow — sanctions re-screening, Bank of Ghana reporting, Ghana Revenue Authority tax position, EUDR documentation, IFRS-compliant fee recognition, AML transaction monitoring, suspicious activity reporting.

AT MVP	Bank of Ghana basic reporting · GRA tax position · AML transaction monitoring · sanctions re-screening
PHASE II ADDITIONS	EUDR documentation pack assembly · SEC reporting · **SARB pre-positioning** for export-corridor expansion
PHASE III ADDITIONS	Full regulator API surface · SOC 2 Type II audit cycle · advanced AML pattern detection
BANK VISIBILITY	Regulatory submission calendar in Grouping 6 · compliance pack accessible at trade and portfolio level

LAYER D

Platform infrastructure · the system layer

MODULE 12 · CANONICAL: TRADEAXIS + FARMERIQ — REPORTING/AUDIT FULL AT MVP

Reporting, Audit & *Analytics*

The data layer that powers every stakeholder's view of trade state. **The reporting and analytics surface of TradeAxis** (the origination canonical module) feeding the Finance Partner Portal — and **the impact reporting surface of FarmerIQ** generating SDG impact dashboards, EUDR documentation packs, and DFI portfolio reports. Single source of truth across the Finance Partner Portal, the DFI guarantee dashboard, the counterparty self-service portals, the regulator interface, and the internal Miziba operations console. Every report is derived from the same underlying data; every view is consistent with every other view.

AT MVP	Full reporting and audit at institutional standard · **analytics dimension Phase II**
PHASE II ANALYTICS	Cycle-time forecasting · exception-pattern recognition · transporter-reliability scoring · buyer-payment-behaviour modelling · weather-risk prediction · default-probability scoring
SCOPE	Single source of truth across all stakeholder views · consistency guaranteed by data-model architecture

MODULE 13 — FULL AT MVP · NON-NEGOTIABLE

Document Vault & *Lifecycle Archive*

Version-controlled, cryptographically sealed repository for every artefact in every trade. Contracts, certificates, KYC packs, escrow instructions, settlement confirmations, audit reports, regulator submissions. Tamper-evident, retention-policy enforced, auditable to the day for the regulatory retention period (7 years minimum, longer where local law requires).

AT MVP	Full at MVP standard · non-negotiable
SUB-COMPONENTS	Cryptographically sealed artefact storage · version control with full history · content-hashing · retention-policy enforcement · audit-access workflow · lifecycle archival of closed trades
BANK VISIBILITY	Every artefact in every trade downloadable from Active Trades drill-down · full audit trail accessible at any time
RETENTION	7 years minimum · longer where local law or counterparty contract requires

MODULE 14 — 3 INTEGRATIONS AT MVP

Integration Hub & *Notification Services*

The messaging and integration backbone. Adapters, message queue, retry logic, dead-letter handling, integration-health monitoring. Notification dispatch via mobile money SMS to farmers, email to bank credit officers, portal push to traders, dashboard alerts to DFI partners.

AT MVP	3 integrations · pilot bank GHS settlement (file-based) · MTN Mobile Money · SMS gateway
PHASE II ADDITIONS	Vodafone Cash · AirtelTigo Money · pilot bank API integration · insurance partner integrations · **EUDR data feed** · customs system integration (TSCF—X)
PHASE III ADDITIONS	Regulator API surface · multi-bank API integration · international SWIFT messaging

II · THE COUNTERPARTY ARCHITECTURE

Four parties. *One trade*.

The architectural separation that the fourteen modules enforce. Trader at the centre as borrower under the Master Facility Agreement. Bank as senior secured capital partner. Buyer as institutional offtaker. Miziba as the verification and settlement infrastructure layer.

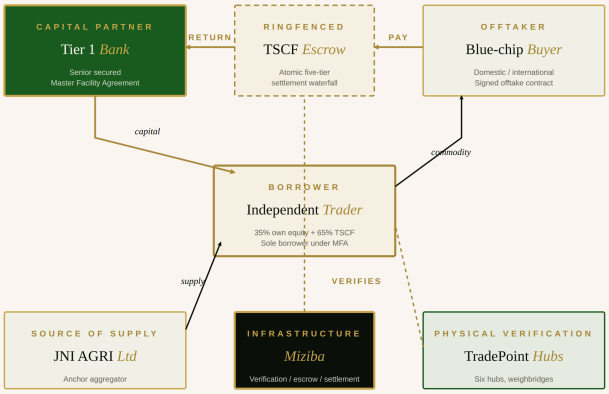
M I Z I B A

COUNTERPARTY ARCHITECTURE
Asset 07 · Trade Relationship Map

FOUR PARTIES · ONE TRADE

The counterparty *architecture*.

Trader at the centre of every trade. Bank as senior secured capital partner. Buyer as institutional offtaker. Miziba as the verification and settlement layer between them. The architecture is structurally separated — no party can act for another.



CAPITAL	COMMERCE	DEMAND	STRUCTURE
Bank	Trader	Buyer	Miziba
Tier 1 institutional bank. Senior secured under Master Facility Agreement.	Independent commodity trader. 35% own equity. Sole borrower under MFA.	Blue-chip offtaker. Domestic on TSCF—D, international on TSCF —X.	Verification, escrow, settlement layer. Not a counterparty to the trade.

MIZIBA · COUNTERPARTY ARCHITECTURE V1.0 — *Trader is sole borrower · Miziba is infrastructure* — ASSET 07 / 09

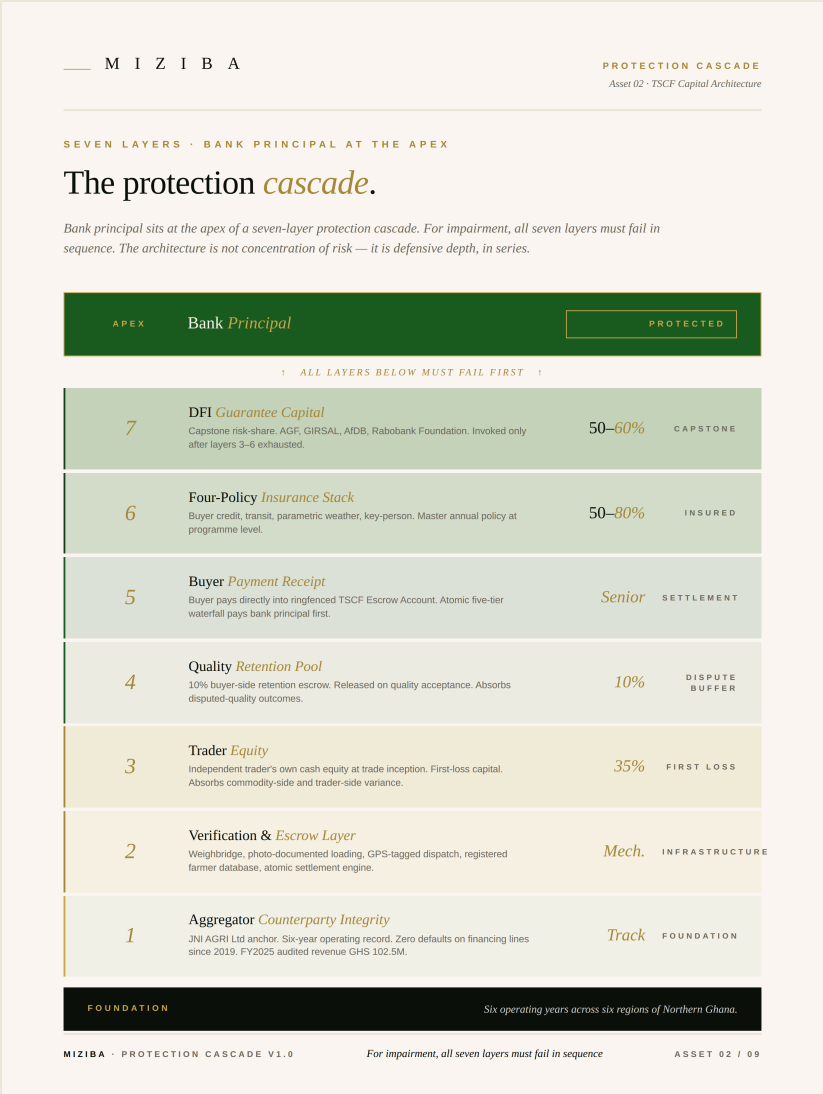
VISUAL REFERENCE · ASSET 07

The structural diagram of every TSCF trade. Capital flows from bank to trader, commodity flows from aggregator/source through trader to buyer, payment flows from buyer through ringfenced escrow back to bank. Miziba sits as infrastructure across all three flows. The architecture is structurally separated — no party can act for another, the institutional commitment is enforceable from the data model upward.

II · THE SEVEN-LAYER PROTECTION CASCADE

Bank principal at the *apex*.

The structural commitment that the platform's modules enforce. For impairment of bank principal, all seven layers must fail in sequence. The architecture is not concentration of risk — it is defensive depth, in series, structurally enforced through the platform's modules and the atomic settlement engine.



VISUAL REFERENCE · ASSET 02

Bank principal sits at the apex. Layer 7 (DFI guarantee) is the capstone risk-share, invoked only after all commercial layers fail. Layer 6 (four-policy insurance) covers the operational risk classes. Layer 5 (buyer payment receipt to ringfenced escrow) is the senior settlement instrument. Layer 4 (10% buyer-side retention pool) absorbs quality-dispute outcomes. Layer 3 (35% trader equity) is first-loss capital. Layer 2 (verification & escrow infrastructure) is the platform itself. Layer 1 (JNI AGRI Ltd counterparty integrity) is the operational foundation.

II · THE SIX-STAGE TRADE LIFECYCLE

Six stages. *Audit-grade evidence* at each.

The TSCF—D trade lifecycle that the platform's modules operate together. Each stage produces an independent audit artefact that flows in real time to the bank's Finance Partner Portal. The cycle is short (22–30 days), the exposure is bounded, the recovery path is documented in advance.

M I Z I B A

TRADE LIFECYCLE
Asset 05 · TSCF—D Six-Stage Cycle

DAYS 1 — 30 · SELF-LIQUIDATING PER TRADE

The trade *lifecycle*.

Six stages from contract to settlement on a shared verification stack. Each stage produces an independent audit artefact visible to the bank in real time.

i
DAY 1 · ORIGINATION
Trade contract & *buyer commitment*
Independent trader signs binding offtake contract with blue-chip buyer. Buyer commits to ringfenced TSCF Escrow Account for settlement. Aggregator signs Quality Certification.
VERIFICATION — Signed contract on file. Buyer KYC complete. Quality cert lodged.
BANK SIDE — Origination memo received. Buyer commitment verified.
ESCROW — Account opened, beneficiary nomination filed.

ii
DAY 3 · CAPITAL RELEASE
Trader *equity in*, bank facility funded
Trader contributes 35% own equity into trade account. Bank disburses 65% TSCF facility against signed offtake and verified inventory. All capital ringfenced.
VERIFICATION — Equity receipt confirmed. 35% threshold validated.
BANK SIDE — Facility drawn. Drawdown notice issued.
CAPITAL STATE — 100% capital deployed against verified loading queue.

iii
DAYS 4–10 · LOADING
Hub-side *verified loading*
Sacks weighed on calibrated weighbridge at TradePoint hub. Photo-documented loading event with timestamp and GPS metadata. Field officer signs loading manifest. Farmer signatures collected.
VERIFICATION — Weighbridge data, loading photos, GPS metadata captured.
BANK SIDE — Real-time loading evidence in Finance Partner Portal.
FARMER PAY — Same-day mobile money settlement, 98.5% SLA.

iv
DAYS 10–14 · DISPATCH
GPS-tagged *transit* to buyer
Loaded transport dispatched with GPS tracking. Transit insurance active. Bank-side reporting portal shows live position. Delivery confirmation triggers buyer-side quality assessment window.
VERIFICATION — GPS log archived. Insurance policy active. ETA confirmed.
BANK SIDE — Live transit visibility. Exception flags for delays.
INSURANCE — Transit cover live. Parametric weather monitor.

v
DAYS 14–20 · QUALITY
Buyer *quality acceptance*
Buyer takes delivery, performs quality grading. 10% retention pool covers any quality dispute. On acceptance, full payment instruction issued to buyer treasury for direct deposit into TSCF Escrow Account.
VERIFICATION — Quality cert from buyer. Retention pool released or held.
BANK SIDE — Buyer payment instruction visible in portal.
DISPUTE — If dispute: 10% retention covers, normal cycle continues.

vi
DAYS 22–30 · SETTLEMENT
Atomic *five-tier waterfall*
Buyer payment lands in escrow. Atomic five-tier waterfall executes in code: bank principal first, bank fee, Miziba fees, trader margin last. Trade closed.
VERIFICATION — Escrow receipt, waterfall execution log, trade close certificate.
BANK SIDE — Principal returned + fee received. Facility undrawn for next trade.
CYCLE — Self-liquidating. Same facility re-deploys for next trade.

MIZIBA · TRADE LIFECYCLE V1.0 — *22–30 day TSCF—D cycle · bank principal senior throughout* — ASSET 05 / 09

VISUAL REFERENCE · ASSET 05

Six stages from contract to settlement. Day 1 origination · Day 3 capital release with trader equity in and bank facility funded · Days 4–10 hub-side verified loading at TradePoint · Days 10–14 GPS-tagged transit via TrackGuard · Days 14–20 buyer quality acceptance · Days 22–30 atomic five-tier waterfall execution.

II · THE THREE TSCF VARIANTS

One structure. *Three operating modes*.

The platform's variant architecture. The protection cascade and waterfall logic remain constant; only the trade lifecycle, currency, and tenor change between variants. TSCF—D launches at MVP; TSCF—P and TSCF—X arrive in Phase II.

M I Z I B A

VARIANT COMPARISON
Asset 06 · TSCF Product Architecture

ONE STRUCTURE · THREE OPERATING MODES

TSCF—D · TSCF—P · *TSCF—X*.

The TSCF architecture supports three product variants, each calibrated for different trade flows and counterparty arrangements. The protection cascade and waterfall logic remain constant; only the trade lifecycle, currency, and tenor change.

DOMESTIC

TSCF—*D*

GHS-denominated, domestic blue-chip offtaker.

TENOR	*22–30* days
CURRENCY	GHS
FACILITY	65% TSCF / 35% trader equity
COMMODITIES	Sorghum, soya, sesame
BUYER	Domestic feedmill, brewery, processor
PILOT TICKET	GHS *300–500K*
USE CASE	Default product. Pilot trades. Proof of mechanics.

PRE-FUND

TSCF—*P*

Buyer pre-funded against verified loading.

TENOR	*14–22* days
CURRENCY	GHS / USD
FACILITY	Bridge to buyer pre-fund release
COMMODITIES	Cashew, shea, sesame
BUYER	Buyer with treasury capacity, pre-pays escrow
PILOT TICKET	GHS *500K–1M*
USE CASE	Reduced tenor risk. Highest-trust buyers.

EXPORT

TSCF—*X*

Bank-consigned bills of lading on export trade.

TENOR	*37* days
CURRENCY	USD / GHS
FACILITY	65% TSCF / 35% trader equity, BL-consigned
COMMODITIES	Cashew, shea, sesame (export grade)
BUYER	International handlers, EU/Asia/MENA corridors
PILOT TICKET	USD *50–150K*
USE CASE	Foreign exchange earner. EUDR-compliant traceability.

SHARED ARCHITECTURE

*All three variants share the **seven-layer protection cascade**, the **atomic five-tier settlement waterfall**, the same **independent verification stack**, and the same **bank-side reporting portal**. Only the trade lifecycle, currency, and tenor change between variants.*

MIZIBA · VARIANT COMPARISON V1.0 — *One structure. Three operating modes.* — ASSET 06 / 09

VISUAL REFERENCE · ASSET 06

TSCF—D

(Domestic, GHS-denominated, 22–30 day tenor, GHS 300–500K pilot ticket).

TSCF—P

(Buyer pre-fund, GHS or USD, 14–22 day tenor, GHS 500K–1M ticket).

TSCF—X

(Export, USD/GHS, 37 day tenor, USD 50–150K ticket, EUDR-compliant traceability for European corridor). All three share the seven-layer protection cascade, the atomic five-tier settlement waterfall, the same independent verification stack, and the same bank-side reporting portal.

SECTION III · THE SEVEN PORTAL SURFACES

Seven *portals*. Seven roles.

Every portal calibrated to actual operational engagement — not architectural symmetry. Counterparties whose engagement is continuous get a portal. Counterparties whose engagement is event-driven get structured workflows. The discipline distinguishes Fortune 500 institutional platforms from products that over-engineer for the appearance of comprehensiveness.

The portal *necessity test*.

A counterparty needs a dedicated portal when their engagement pattern with the platform is continuous — logging in regularly, taking actions, monitoring state. They do not need a portal when their engagement is event-driven — receiving notifications, responding to specific triggers, consuming curated reports. By that test, seven counterparty classes justify portals; three classes (transporters, freight forwarders, insurance/DFI partners) are served through structured workflows operated by Miziba staff via the Internal Operations Console and TrackGuard.

Visibility is a data commitment; a portal is a software product. Counterparties without portals still have full visibility into the data they need — delivered via SMS, WhatsApp, email, secure file transfer, or curated reports generated by Module 12 and dispatched by Module 14. They do not log in; they participate.

The *seven portals*.

Each portal has its own form factor (mobile-first, web, or web+mobile responsive), its own primary user, its own permissions matrix, and its own deployment phasing. The following pages specify each portal in turn.

III · PORTALS 01 & 02

The field side. *The borrower*.

PORTAL 01 · FIELD SIDE

TradePoint Portal

Mobile-first, native iOS/Android, offline-first, glove-compatible touch targets. Tablet-optimised version for hub supervisors.

Primary user. Miziba and JNI AGRI Ltd field officers operating at the six TradePoint hubs across Northern Ghana — Tamale, Bolgatanga, Wa, Damongo, Techiman, Wenchi.

CORE WORKFLOWS

- **Shift authentication** · biometric plus PIN, session segregation per officer, device-health check
- **Inbound load receipt** · farmer or aggregator delivery, ID lookup against Source Registry
- **Weighbridge capture** · Bluetooth-integrated, no manual data entry, cryptographically signed
- **Quality grading** · structured per-commodity workflow, photo evidence at each checkpoint
- **Farmer settlement** · mobile money push at hub-gate, SMS confirmation, signature capture
- **Loading-event documentation** · vehicle, GPS device, seal numbers, dispatch manifest
- **Dispatch handoff** · clean handover to TrackGuard, GPS tracking activates
- **End-of-shift reconciliation** · daily summary, supervisor counter-sign, sync to platform

PORTAL 02 · THE BORROWER

Trader *Portal*

Web + mobile responsive. Optimised for desktop trade origination workflow with mobile companion for status monitoring.

Primary user. Independent commodity traders — the borrowers under TSCF facilities. Each trader operates against their own segregated workspace; no information leakage across traders.

CORE WORKFLOWS

- **Trade origination** · buyer contract upload, aggregator selection, commodity and source-pattern specification
- **Facility request** · equity confirmation, structured trade memo generation, submission to credit decisioning
- **Status monitoring** · live state of every active trade across the six lifecycle stages
- **Document management** · access to every artefact produced in the trader's own trades
- **Settlement view** · trader margin tracking, payment confirmations, fee reconciliation
- **Performance dashboard** · cycle-time history, margin performance, exception history
- **Notification preferences** · channel selection (email, SMS, in-app push), event filtering

III · PORTALS 03 & 04

Source side. *Demand side*.

PORTAL 03 · SOURCE OF SUPPLY

Aggregator *Portal*

Web. Optimised for the operational rhythm of an aggregator managing supply across multiple TSCF trades and multiple commodity flows.

Primary user. JNI AGRI Ltd as anchor aggregator at MVP; Tier-2 aggregators added in Phase II. Each aggregator operates against their own segregated workspace.

CORE WORKFLOWS

- **Quality certification** · per-trade quality cert lodgement, performance history
- **Source-attestation management** · all three patterns (direct farmer, cooperative, Tier-2)
- **Hub coordination** · cross-hub supply allocation, loading-window scheduling
- **Farmer-base management** · visibility into registered farmers in the aggregator's network
- **Trade participation history** · every trade the aggregator has supplied into
- **Settlement view** · payments received, retention pool state, dispute resolution
- **Audit trail** · access to every artefact in trades the aggregator participates in

PORTAL 04 · THE OFFTAKER

Buyer *Portal*

Web. Calibrated for institutional buyers managing offtake commitments and quality acceptance across multiple TSCF trades.

Primary user. Domestic blue-chip offtakers on TSCF—D and TSCF—P; international export buyers on TSCF—X. Each buyer operates against their own segregated workspace.

CORE WORKFLOWS

- **Offtake contract management** · per-trade contract execution, pricing benchmarks, performance history
- **Quality acceptance** · structured grading workflow at delivery, retention-pool reconciliation
- **Payment instruction** · direct deposit to ringfenced TSCF Escrow Account, payment-direction notice
- **Trade pipeline view** · upcoming deliveries, ETA, quality expectations
- **Dispute resolution** · structured workflow for quality disputes, retention pool engagement
- **Document access** · offtake contracts, quality certificates, delivery receipts, payment confirmations
- **EUDR documentation** · pre-shipment compliance pack for TSCF—X European corridor (Phase II)

III · PORTALS 05 & 06

Logistics protection. *Bank visibility*.

PORTAL 05 · LOGISTICS PROTECTION

TrackGuard

Web. Operated internally by Miziba's logistics team. Transporters and freight forwarders participate through structured workflows rather than dedicated portals.

Primary user. Miziba's logistics operations team. Manages every transporter, every freight forwarder, every active consignment, every customs clearance, every bank-consigned BL across the platform.

CORE WORKFLOWS

- **Transporter onboarding** · KYB pack, vehicle/route certification, GPS-device registration, insurance verification
- **Freight forwarder onboarding** (Phase II) · bonded-warehouse certification, BL-issuance authority
- **Dispatch workspace** · vehicle assignment, GPS pairing, seal numbers, dispatch manifest
- **Real-time transit monitoring** · GPS tracking, route-deviation alerts, dwell-time alerts, ETA calculation
- **Parametric weather** (Phase II) · weather threshold monitoring, Layer 6 insurance trigger
- **Customs & clearance** (Phase II) · export documentation, certificate-of-origin, EUDR pack
- **Bill-of-lading control** (Phase II) · bank-consigned BL, electronic original custody, release instruction
- **Logistics exception pathway** · route deviation, transit delay, weather event, transporter failure

PORTAL 06 · INSTITUTIONAL SHOWPIECE

Finance *Partner* Portal

Web, institutional-grade dark-surface register. The 100% visibility commitment lives here. See Section IV for full architecture.

Primary user. Bank stakeholders — credit officers, treasury operators, compliance officers, risk officers, audit. Each role has its own permission profile within the portal; the architectural commitment is that the bank as institution sees everything.

SIX DASHBOARD GROUPINGS

- **Grouping 1** · Facility Overview (top strip, always visible)
- **Grouping 2** · Active Trades (centre-left, primary working surface)
- **Grouping 3** · Live Logistics (centre-right, TrackGuard integration)
- **Grouping 4** · Settlement & Reconciliation (lower-left)
- **Grouping 5** · Risk & Exceptions (lower-right, Phase II full)
- **Grouping 6** · Counterparty & Compliance (left navigation drill-down)

III · PORTAL 07

Miziba's view of *Miziba*.

PORTAL 07 · THE INTERNAL COCKPIT

Internal *Operations* Console

Web, role-segregated within itself. The super admin dashboard is the executive view. See Section V for full architecture.

Primary user. Miziba internal staff — verification officers, settlement engineers, compliance officers, customer support, and the executive layer (Joel, Daniel, CFO equivalent) who access the super admin dashboard.

EIGHT SUPER ADMIN GROUPINGS

- **Grouping 1** · Programme State Ribbon (cross-bank summary)
- **Grouping 2** · Facility Estate (every bank, every facility)
- **Grouping 3** · Active Trades Heatmap (cross-facility intelligence)
- **Grouping 4** · TrackGuard Logistics Estate (full live picture)
- **Grouping 5** · Counterparty Estate (every class, every counterparty)
- **Grouping 6** · Platform Financial Position (access-restricted)
- **Grouping 7** · Platform Health & Integration State
- **Grouping 8** · Compliance, Governance & Strategic Signals

Counterparties served by *structured workflows*.

Five counterparty classes are served through structured engagement workflows rather than dedicated portals: **transporters** (onboarded via TrackGuard, dispatched via SMS/WhatsApp, settled via Miziba accounts payable), **freight forwarders** (managed identically through TrackGuard with secure file transfer for BL workflows), **insurance partners** (per-trade policy activation by email, monthly premium reconciliation reports, claim instructions via secure file transfer), **DFI partners** (quarterly portfolio reports, annual impact and risk reports, document-share access for institutional documentation), and **farmers** (registered in the Source Registry, mobile money settlements with SMS confirmation at hub-gate, annual statement via SMS link).

None of these classes log into a dedicated portal. All of them get full visibility into the data their role requires — delivered via the channel calibrated to their actual operational behaviour.

III · THE PORTAL DISCIPLINE

Seven portals. *Not nine*.

The architectural error to avoid is treating "stakeholder visibility" as synonymous with "stakeholder portal." Visibility is a data commitment; a portal is a software product. The discipline of building only the portals that justify their operational engagement distinguishes Fortune 500 institutional platforms from products that over-engineer for the appearance of comprehensiveness.

PORTAL JUSTIFIED

Continuous *operational engagement*

Field officer logs in every shift to capture weighbridge readings, photo loadings, farmer settlements. Continuous engagement justifies a dedicated mobile-first portal.

Trader logs in regularly to originate trades, monitor state, manage documents. Continuous engagement justifies a portal.

Aggregator manages quality certifications, source attestations, hub coordination across multiple trades. Continuous engagement justifies a portal.

Buyer manages offtake contracts, quality acceptance, payment instructions across multiple trades. Continuous engagement justifies a portal.

Bank monitors facility state daily, drills into trades, reviews exceptions. Continuous institutional oversight justifies the institutional showpiece.

STRUCTURED WORKFLOW SUFFICIENT

Event-driven *engagement pattern*

Transporter receives per-consignment dispatch instructions via SMS or WhatsApp. GPS device on the vehicle reports directly to the platform. Settlement comes through Miziba's accounts payable. No login required.

Freight forwarder participates per-shipment via secure file transfer and structured email. Existing institutional channels they already use with every shipper. No login required.

Insurance partner receives per-trade activation confirmations and monthly reconciliation reports. Claim instructions via secure file transfer. Engagement is event-driven on stress events. No login required.

DFI partner receives quarterly portfolio reports and annual impact and risk reports. Investment-committee cycle is quarterly anyway. No login required.

Farmer receives mobile money settlement at hub-gate with SMS confirmation. Annual statement via SMS link. No login required.

THE INSTITUTIONAL COMMITMENT

Counterparties without portals still have full visibility into the data their role requires.

The structured workflow is not a degraded form of portal access. It is the appropriate engagement pattern for the counterparty's actual operational behaviour. Every report, every notification, every audit access that a portal would deliver is delivered through the structured workflow — calibrated to the channel that the counterparty already uses, with the audit trail flowing back into the platform's reporting layer (Module 12) for institutional consistency.

SECTION IV · THE FINANCE PARTNER PORTAL

The bank's *100% visibility*.

The architectural showpiece of the platform. Six dashboard groupings that together deliver the institutional commitment of complete real-time visibility into every stage of every trade against every facility — structurally enforced from the data model upward, audit-grade at every level of drill-down.

What "100% visibility" actually *means*.

The phrase is rhetorical unless it is structurally defined. In this platform it means seven specific things, each of which the portal architecture enforces:

Facility-level. Real-time deployment, available headroom, YTD turnover, average cycle time, exception flag count, default record, recovery history.

Trade-level. Every active trade visible by ID, commodity, trader, current stage, day in cycle, hub, facility amount, exception flag status. Click-through into any trade reveals the complete audit trail.

Stage-level. For every trade stage (origination, capital release, loading, dispatch, quality, settlement), the bank sees the verification artefacts (signed contracts, weighbridge data, loading photos, GPS logs, quality certificates), the actor who produced them, the timestamp, and the cryptographic hash that proves immutability.

Settlement-level. Every waterfall execution shown in real time with bank principal received, bank fee credited, Miziba fees subordinated, trader margin released. Reconciliation to the bank's own treasury statement is automatic.

Exception-level. Every flag (delayed loading, transit anomaly, quality dispute, payment delay, stress scenario) routed to the bank in real time with proposed mitigation pathway and recovery instruction template.

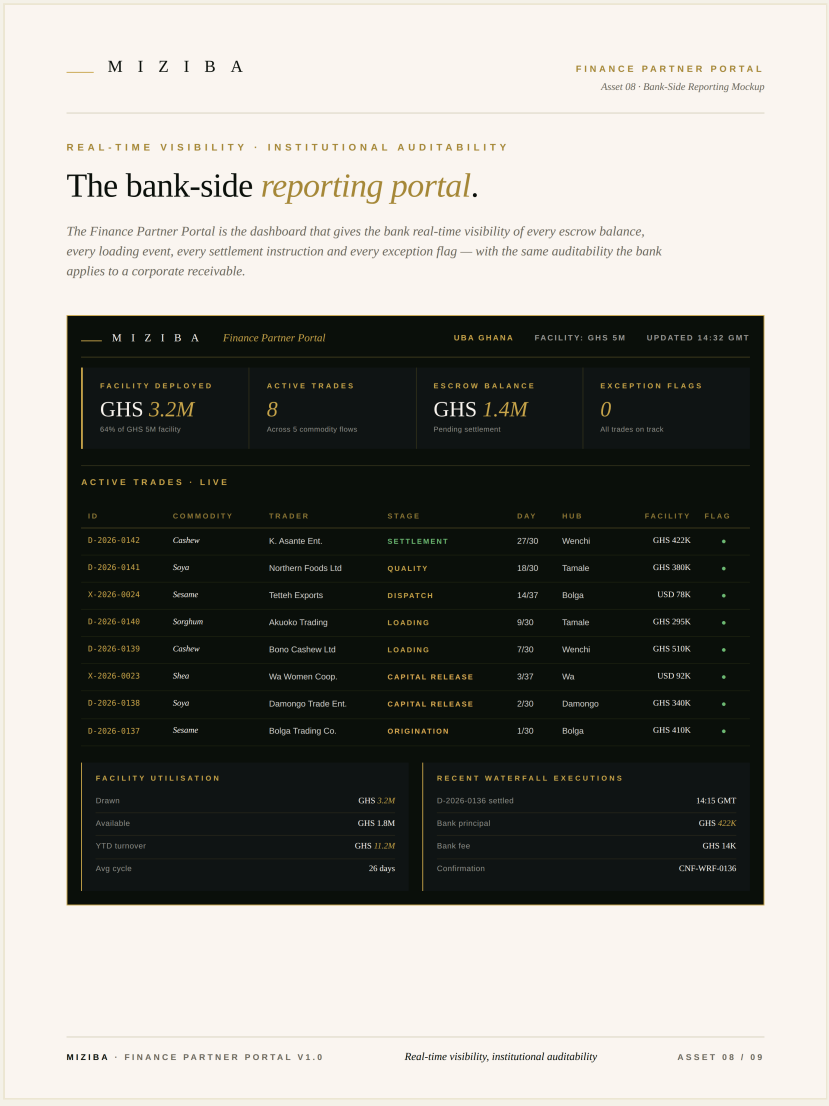
Audit-level. Every artefact in the trade is downloadable, every action is logged, every change is versioned, every access is recorded. The bank's internal audit and external regulators can reconstruct any trade end-to-end at any time.

Counterparty-level. Every trader, aggregator, buyer, transporter, freight forwarder, insurance partner, and DFI partner registered against the facility — with their KYC/KYB pack, performance metrics, current exposure, and audit history.

IV · THE PORTAL VISUALISED

The portal, *visualised*.

The bank-side institutional surface in production register. Dark institutional dashboard, single-page facility overview with drill-down into every trade, integrated logistics view, real-time waterfall execution log.



M I Z I B A

FINANCE PARTNER PORTAL
Asset 08 · Bank-Side Reporting Mockup

REAL-TIME VISIBILITY · INSTITUTIONAL AUDITABILITY

The bank-side *reporting portal*.

The Finance Partner Portal is the dashboard that gives the bank real-time visibility of every escrow balance, every loading event, every settlement instruction and every exception flag — with the same auditability the bank applies to a corporate receivable.

M I Z I B A *Finance Partner Portal* — UBA GHANA · FACILITY: GHS 5M · UPDATED 14:32 GMT

FACILITY DEPLOYED	ACTIVE TRADES	ESCROW BALANCE	EXCEPTION FLAGS
GHS *3.2M*	*8*	GHS *1.4M*	*0*
64% of GHS 5M facility	Across 5 commodity flows	Pending settlement	All trades on track

ACTIVE TRADES · LIVE

ID	COMMODITY	TRADER	STAGE	DAY	HUB	FACILITY	FLAG
D-2026-0142	*Cashew*	K. Asante Ent.	SETTLEMENT	27/30	Wenchi	GHS 422K	•
D-2026-0141	*Soya*	Northern Foods Ltd	QUALITY	18/30	Tamale	GHS 380K	•
X-2026-0024	*Sesame*	Tetteh Exports	DISPATCH	14/37	Bolga	USD 78K	•
D-2026-0140	*Sorghum*	Akuoko Trading	LOADING	9/30	Tamale	GHS 295K	•
D-2026-0139	*Cashew*	Bono Cashew Ltd	LOADING	7/30	Wenchi	GHS 510K	•
X-2026-0023	*Shea*	Wa Women Coop.	CAPITAL RELEASE	3/37	Wa	USD 92K	•
D-2026-0138	*Soya*	Damongo Trade Ent.	CAPITAL RELEASE	2/30	Damongo	GHS 340K	•
D-2026-0137	*Sesame*	Bolga Trading Co.	ORIGINATION	1/30	Bolga	GHS 410K	•

FACILITY UTILISATION

Drawn	GHS *3.2M*
Available	GHS 1.8M
YTD turnover	GHS *11.2M*
Avg cycle	26 days

RECENT WATERFALL EXECUTIONS

D-2026-0136 settled	14:15 GMT
Bank principal	GHS *422K*
Bank fee	GHS 14K
Confirmation	CNF-WRF-0136

MIZIBA · FINANCE PARTNER PORTAL V1.0 — *Real-time visibility, institutional auditability* — ASSET 08 / 09

VISUAL REFERENCE · ASSET 08

The Finance Partner Portal in production form. Top stat ribbon shows facility deployed, active trades, escrow balance, exception flag count. Live trades table with stage colour-coding (origination, capital release, loading, dispatch, quality, settlement) and exception status. Bottom strips show facility utilisation and recent waterfall executions with bank principal, bank fee, Miziba fees, trader margin individually traced.

IV · THE SIX DASHBOARD GROUPINGS

Six groupings. *One screen*.

i Facility *Overview*

TOP STRIP · ALWAYS VISIBLE

The single-row stat ribbon that answers "what is the state of my facility right now." Read-only at-a-glance information; the institutional pulse-check.

SUB-FEATURES

Facility deployed (currency, % of headroom) · Available headroom · Active trade count · YTD turnover · Average cycle time (last 30 days) · Exception flag count (colour-coded by severity) · Default record (always reads "Zero") · Critical alert indicator

ii Active *Trades*

CENTRE-LEFT · PRIMARY WORKSPACE

The central working surface. The table of every trade currently drawing on the facility, with sortable filterable views, stage indicators, day-in-cycle progress, and full drill-down into every trade's audit trail.

SUB-FEATURES

Live table view (sortable, filterable by stage/hub/commodity/trader/exception) · Stage column (colour-coded: origination, capital release, loading, dispatch, transit, quality, settlement) · Day-in-cycle counter with progress bar · Trade-card drill-down (timeline, artefacts, actors, exception history) · Exception filter (single-click) · Stage-progression filter · Saved views per officer · CSV/PDF export for committee circulation

iii Live *Logistics*

CENTRE-RIGHT · TRACKGUARD INTEGRATION

The map-and-table view of every consignment currently in motion. The grouping that gives the bank what no traditional commodity finance facility provides — real-time visibility into the physical commodity itself, in motion.

SUB-FEATURES

Live map of Northern Ghana operating zone with active consignments as moving markers · Consignment table (origin hub, destination, transporter, GPS status, ETA, exception flags) · Route view (planned vs. actual with deviation alerts) · Weather overlay across active corridors (Phase II) · Transporter performance (on-time rate, exception rate) · TSCF—X export panel (Phase II): port-of-loading, BL state, customs clearance, vessel ETA · Layer 6 insurance state per consignment

iv Settlement & *Reconciliation*

LOWER-LEFT · FINANCIAL CONTROL

The financial-control workspace. Where the bank's treasury and credit office reconcile against the platform's settlement engine. Every waterfall execution traceable; every drawdown auditable; every fee accrual reconcilable.

SUB-FEATURES

Recent waterfall executions (chronological list with bank principal, bank fee, Miziba fees, trader margin individually traced) · Pending settlements (Stage v–vi trades with expected receipt date) · Escrow balance summary (total across ringfenced accounts) · Bank-statement reconciliation (automated match, exceptions flagged) · Drawdown history (origination memo, approval, instruction reference) · Fee accrual (running total) · Recovery records archive

v Risk & *Exceptions*

LOWER-RIGHT · EXCEPTION MANAGEMENT

The exception-management workspace. Where the bank reviews flagged trades, makes recovery decisions, and routes claim instructions through the protection cascade layers in sequence.

SUB-FEATURES

Active exceptions queue (sorted by severity and age) · Exception classification (quality dispute, payment delay, transit anomaly, weather event, transporter failure, buyer default, force majeure) · Recovery pathway viewer (Layer 4 retention → Layer 5 buyer recourse → Layer 6 insurance → Layer 7 DFI guarantee) · Claim instruction workflow · Stress-test panel (Phase II) · Historical recovery patterns

vi Counterparty & *Compliance*

LEFT NAV · INSTITUTIONAL DISCIPLINE

The institutional-discipline workspace. Where the bank monitors who is operating against its facility. What a bank's audit-and-compliance team looks at on a quarterly basis. What an external regulator examines on demand.

SUB-FEATURES

Trader registry (KYC pack, equity history, performance, current exposure) · Aggregator confirmations (JNI AGRI Ltd quality cert, Tier-2 audits) · Buyer registry (offtake performance, payment history) · Transporter registry (KYB, performance, certifications) · Insurance partner status (Layer 6 policies, renewal, claim history) · DFI guarantee status (Layer 7 capacity, claim history) · Compliance pack (KYC refresh schedule, sanctions logs, regulatory submissions) ·

RELATED-PARTY DISCLOSURES

(Joel-JNI AGRI Ltd, five structural controls visualised)

THE FINANCE PARTNER PORTAL COMMITMENT

Six groupings — together they constitute the bank's complete operating view of the TSCF facility.

The bank does not operate Miziba's platform; the bank operates *its own facility*, hosted by Miziba, with the same auditability the bank applies to any internal system in its operating environment.

IV · ROLE SEGREGATION WITHIN THE PORTAL

One portal. *Four bank roles*.

The bank as institution sees everything. But within the bank, four distinct roles operate against the portal with calibrated permissions — each seeing the groupings most relevant to their accountability, with read-only access to the rest for institutional consistency.

The four *bank-side roles*.

ROLE 01 · CREDIT — CORE WORKING ROLE

Bank Credit *Officer*

Reviews trade memos, makes credit decisions, monitors deployed facilities. **Full access** to Grouping 2 (Active Trades) for working with new and active trades. Read-only access to Groupings 1, 3, 4, 5, 6 for institutional context.

ROLE 02 · TREASURY — FINANCIAL CONTROL

Bank *Treasury Operator*

Manages facility funding, drawdown execution, settlement reconciliation. **Full access** to Grouping 4 (Settlement & Reconciliation). Read-only access to Groupings 1, 2 for trade context. Limited access to Grouping 5 for exception state.

ROLE 03 · RISK — EXCEPTION MANAGEMENT

Bank Risk & *Recovery Officer*

Full access to Grouping 5 (Risk & Exceptions) including stress-test panel and claim instruction workflow. Read-only access to Groupings 1, 2, 3, 4 for full context on exception scenarios.

ROLE 04 · COMPLIANCE — INSTITUTIONAL DISCIPLINE

Bank Compliance & *Audit Officer*

Full access to Grouping 6 (Counterparty & Compliance) including all KYC/KYB packs, sanctions logs, regulatory submissions, related-party disclosures. Read-only access to all other groupings with audit-access annotations — every read by this role is itself logged for institutional audit chain integrity.

SECTION V · INTERNAL OPERATIONS CONSOLE

The super admin *cockpit*.

Miziba's operational nerve centre. The surface where Joel, Daniel, and senior internal staff see the entire TradeAxis estate at a glance and can act on it. Eight groupings deliver cross-facility intelligence that no individual bank sees, including access-restricted Platform Financial Position with related-party governance state.

What this console *is*.

The Internal Operations Console is qualitatively different from every other portal in the platform. It is not "the bank's view of their facility" or "the field officer's view of their hub." It is *Miziba's view of Miziba* — aggregating every bank facility, every active trade, every counterparty, every consignment in motion, every regulatory submission, every strategic stakeholder engagement, and every dimension of the platform's own financial position.

The institutional reference points are Bloomberg Terminal's enterprise admin view, Stripe's internal operations dashboard, and the executive cockpits in Tier 1 core banking systems like Temenos T24 or Mambu. Information-dense, action-oriented, role-segregated within itself, audit-logged at every interaction.

The eight *groupings*.

The dashboard organises around eight groupings, structured as a single-screen executive view with progressive drill-down on every element. The next page presents the dashboard in production form; the page after that specifies the eight groupings.

V · THE DASHBOARD VISUALISED

The cockpit, *visualised*.

The Internal Operations Console super admin dashboard in production register. Eight groupings on a single screen with persistent navigation, role-switch capability, and access-restricted Platform Financial Position drawer.

M I Z I B A

SUPER ADMIN DASHBOARD
Asset 10 · TradeAxis Internal Operations

EIGHT GROUPINGS · WHOLE-PLATFORM VISIBILITY

The super admin *dashboard*.

Miziba's view of Miziba. The internal operations cockpit aggregating the entire TradeAxis estate — every bank facility, every active trade, every counterparty, every consignment in motion.

MIZIBA · SUPER ADMIN DASHBOARD V1.0 — *Whole-platform visibility. Eight groupings. Cross-facility intelligence.* — ASSET 10 / 10

VISUAL REFERENCE · ASSET 10

The super admin dashboard. Top stat ribbon with eight programme-level metrics. Left navigation across all modules and counterparty classes. Centre panels: Facility Estate (five-bank syndicate), TrackGuard Live Logistics (map plus consignment table), Trades Heatmap (cross-facility), Counterparty Estate (every class). Right rail: catalytic performance, pipeline this week, regulatory submissions, exceptions 24h, Platform Financial (restricted), document library. Bottom: system health strip across all integrations. Footer with incident escalation panic button.

V · THE EIGHT SUPER ADMIN GROUPINGS

Eight groupings. *Whole-platform visibility*.

i Programme *State Ribbon*

TOP STRIP · PULSE-CHECK

Programme-level health at the institutional summary layer. What Joel sees in the first three seconds when he opens the dashboard each morning.

SUB-FEATURES

Total facility deployed across all banks (USD-normalised) · Total facility headroom · Active trades count (all facilities, all variants) · YTD turnover · Total farmer payments YTD · Default record (always "Zero") · Active hub count (6/6) · Critical exception flag (single colour-coded indicator)

ii Facility *Estate Map*

CENTRE-LEFT · BANK SYNDICATE

Visual representation of every bank facility in the platform. Tiled view sorted by deployment percentage descending; banks at risk of headroom exhaustion float to the top.

SUB-FEATURES

Bank brand mark · facility size, currency, deployment % (gauge) · active trade count · days since first deployment / days remaining on facility tenor · exception flag count specific to facility · last drawdown date and amount · bank credit officer contact · Pipeline tile (banks in MFA negotiation)

iii Active Trades *Heatmap*

CENTRE-LEFT BOTTOM · CROSS-FACILITY

Cross-facility trade visibility that no individual bank sees. The analytical view that reveals patterns the bank-by-bank view cannot.

SUB-FEATURES

Volume heatmap by hub · volume heatmap by commodity · volume heatmap by variant (TSCF—D / P / X mix) · stage distribution across the six lifecycle stages · exception cluster detection (when multiple trades flag the same exception class)

iv TrackGuard *Logistics Estate*

CENTRE-RIGHT · FULL LIVE PICTURE

The full live logistics picture across the platform. The surface Miziba's logistics operations lead uses to manage the entire estate; the super admin view aggregates the operational view.

SUB-FEATURES

Live consignment map (all hubs, all corridors) · active corridor performance · transporter fleet utilisation · freight forwarder state (Phase II) · parametric weather alert panel (Phase II) · TrackGuard exception queue

v Counterparty *Estate*

CENTRE-RIGHT BOTTOM · FULL REGISTRY

The complete counterparty registry with operational state across every class. Each cohort clickable for drill-down; search bar across the top for any counterparty by name.

SUB-FEATURES

Trader cohort (active, by facility, by commodity, by exposure) · Aggregator cohort (JNI AGRI Ltd anchor + Tier-2) · Buyer cohort (domestic + international) · Transporter cohort (with TrackGuard onboarding pipeline) · Freight forwarder cohort (Phase II) · Source Registry summary (10,189+ direct farmers, cooperatives, Tier-2 chains) · Insurance partner state · DFI partner state

vi Platform *Financial Position*

RESTRICTED · CFO & CEO ONLY

No bank sees this. **Miziba's own financial state**. Access-restricted to Joel, Daniel, the CFO equivalent, and the auditor. Other senior internal staff see the rest of the dashboard but this grouping is segregated.

SUB-FEATURES

Revenue YTD (structuring fees, monitoring fees, by facility and class) · Fee accrual pipeline (committed, expected dates) · Operating cost trajectory (against budget) · Cash position and runway calculation · Capital strategy state (equity raised, remaining, partner relationships) · **RELATED-PARTY ARRANGEMENTS**

(JNI AGRI Ltd state, five structural controls visualised)

vii Platform *Health & Integration*

BOTTOM STRIP · TECHNICAL OPS

The technical operational view used by the platform engineering lead and the security officer. System uptime per portal, integration health matrix, performance metrics, security posture.

SUB-FEATURES

System uptime per portal and per critical module · Integration health matrix (every active integration) · Performance metrics (response times, throughput, error rates) · Security posture (last pen test, last audit, active incidents, anomalies) · Change-management queue (with bank-approval gate) · Document vault state (storage, retention, integrity)

viii Compliance & *Strategic Signals*

RIGHT RAIL · INSTITUTIONAL DISCIPLINE

The institutional discipline view. What Joel uses for board reporting, capital partner updates, strategic decision-making.

SUB-FEATURES

Regulatory submission calendar · Audit calendar (internal, external, SOC 2 cycle) · Programme KPI panel (farmer payments, women paid, villages reached, catalytic equation actuals vs target) · Strategic stakeholder calendar (bank meetings, DFI engagements, board, conferences) · Brand artefact deployment state · Newsroom and PR signal

SECTION VI · FOUR INTEGRATION SURFACES

Four *integrations*. Each contracted.

The platform is not a closed system. It connects to four external surfaces, each with its own integration contract, its own security perimeter, its own change-management discipline, and its own deployment phasing.

SURFACE 01 · BANK CORE BANKING — FILE-BASED AT MVP, API PHASE II

Bank Core Banking *Integration*

Secure connection to the bank's facility ledger, treasury system, and statement reconciliation infrastructure. Each bank's integration is configured during the technical onboarding phase of the MFA negotiation. Three integration patterns supported, selected per bank based on bank's existing capability.

PATTERN A · SWIFT	SWIFT MT-series messages where bank operates SWIFT for facility communications
PATTERN B · REST API	Real-time API where bank exposes facility ledger and treasury endpoints
PATTERN C · FILE-BASED	Daily reconciliation file exchange via secure file transfer where neither SWIFT nor API is available — the MVP default
AT MVP	Pattern C with pilot bank · Pattern B added in Phase II as banks expose APIs
SECURITY	TLS 1.3 minimum, mutual authentication, encrypted at rest, content-hashed, audit-logged at every exchange

SURFACE 02 · MOBILE MONEY — MTN AT MVP, FULL COVERAGE PHASE II

Mobile Money *Integration*

Direct integration with Ghana's three mobile money providers for same-day farmer settlement at hub-gate. Push payment with immediate confirmation receipt back to the verification module — the institutional discipline that makes 98.5% same-day farmer settlement SLA enforceable.

AT MVP	MTN Mobile Money (largest by market share) · Vodafone Cash and AirtelTigo Money handled manually for the small farmer subset that prefers them
PHASE II	Full coverage across all three providers · programmatic provider selection per farmer's registered preference
SLA TARGET	98.5% same-day settlement · confirmation receipt logged in audit trail

SURFACES 3 & 4 *Insurance & guarantee · regulator*

SURFACE 03 · INSURANCE & DFI — FILE-BASED PHASE II

Insurance & *Guarantee Provider Integration*

API or file-based integration with each Layer 6 insurance carrier and each Layer 7 DFI guarantee provider. Configured per partner. Used for policy activation per trade, claim instruction routing, coverage tracking, and premium reconciliation.

AT MVP	Single transit insurance carrier · basic file-based exchange for policy activation
PHASE II	Full Layer 6 stack (buyer credit, transit, parametric weather, key-person) plus Layer 7 DFI guarantee partners (AGF, GIRSAL, AfDB, Rabobank Foundation, DBG)
STRUCTURED ENGAGEMENT	DFI partners receive quarterly portfolio reports and annual impact and risk reports rather than dedicated portal access

SURFACE 04 · REGULATOR — MANUAL AT MVP, API PHASE III

Regulator *Reporting Surface*

Read-only access for the Bank of Ghana, Ghana Revenue Authority, and the Securities & Exchange Commission to access programme-level reporting on demand. Pre-positioned for SARB and EU EUDR as the export corridor expands.

AT MVP	Manual report submission to Bank of Ghana and GRA on existing schedules
PHASE II	EUDR documentation pack for European-corridor TSCF—X · SARB pre-positioning
PHASE III	Full read-only API surface for regulators to pull programme-level reporting on demand

VI · INTEGRATION ARCHITECTURE PRINCIPLES

Five principles. *Engineered for resilience*.

i

Every integration is *versioned* and contracted.

No integration runs against a moving target. Every integration has a versioned contract (API spec, file format, message schema) lodged in the Document Vault, with change-management discipline that requires partner notification before any change is deployed.

ii

Every exchange is *audit-logged*.

Every message sent, every file received, every API call made or received is logged with timestamp, source, destination, payload hash, and outcome. The bank's audit team can reconstruct any integration exchange from the audit log alone.

iii

Every failure has a *recovery path*.

Retry logic on transient failures. Dead-letter handling on persistent failures. Operational alerting on integration health degradation. No integration failure leaves a trade in an inconsistent state — the platform's data model maintains consistency even when external systems are temporarily unavailable.

iv

Every integration *respects the security perimeter*.

TLS 1.3 minimum, mutual authentication where supported, encrypted at rest, no integration grants access beyond what the integration contract specifies. Integration credentials rotated quarterly. Penetration testing covers every integration surface.

v

Every change requires the *bank-approval gate*.

Modifications to integrations that affect the settlement engine, the bank's facility data, or the audit trail require explicit bank approval before deployment. The change-management workflow is built into Module 14 (Integration Hub); no engineer can deploy unilaterally.

VI · THE INTEGRATION DATA FLOWS

Where the data *actually moves*.

Three illustrative data flows that traverse the integration surfaces in the course of normal trade operation.

Flow A · *Capital release*.

Trader confirms equity in Trader Portal → Module 7 (Escrow) records equity receipt → Module 4 (Credit Decisioning) routes drawdown instruction to bank → **Surface 01 (Bank Core Banking)** exchanges drawdown instruction → Bank treasury executes facility deployment → Surface 01 returns confirmation → Module 7 records facility funding → Trade state updates to "capital released" → Finance Partner Portal reflects new state → **Module 10 (Notification)** dispatches confirmations to trader, bank credit officer, aggregator. *Total elapsed time: minutes*.

Flow B · *Farmer settlement at hub-gate*.

Field officer captures weighbridge reading in TradePoint Portal → Module 4 (Verification) records loading event → Mobile money push triggered → **Surface 02 (Mobile Money)** exchanges push instruction with MTN MoMo → MoMo confirms settlement → Surface 02 returns confirmation → Module 14 generates SMS confirmation to farmer → **Surface 02 (SMS gateway)** dispatches farmer SMS → Field officer captures farmer signature in TradePoint Portal → Audit trail sealed in Module 13 (Document Vault). *Total elapsed time: seconds*.

Flow C · *Atomic settlement at trade close*.

Buyer payment lands in ringfenced TSCF Escrow Account → **Surface 01 (Bank Core Banking)** notifies platform of escrow receipt → Module 7 (Atomic Settlement) executes five-tier waterfall in code → Surface 01 receives bank principal return instruction → Surface 01 receives bank fee credit instruction → Module 7 issues Miziba structuring fee, monitoring fee, trader margin disbursements → Module 13 generates settlement certificate → Finance Partner Portal Grouping 4 updates with waterfall execution log → Module 10 dispatches settlement confirmations to all stakeholders. *Total elapsed time: minutes from buyer payment receipt to atomic completion*.

Each flow demonstrates the same architectural discipline: every action audit-logged, every integration versioned and contracted, every counterparty notified through their calibrated channel, every state change visible in the Finance Partner Portal in real time. **The integration surfaces are not bolted onto the platform — they are part of how the platform's institutional commitments are structurally enforced.**

SECTION VII · THREE SECURITY PERIMETERS

Three perimeters. *Engineered from the foundation*.

The platform is engineered to bank-grade security standards from the architectural foundation, not retrofitted. Three perimeters operate together — identity, data, operational — with no compromise at MVP. Security is the one architectural domain that cannot be MVP'd in financial-grade software.

Why security *cannot be compressed*.

Every other architectural domain in this brief has an MVP scope and a Phase II expansion. Security does not. A bank credit committee will not approve a facility against a platform whose security posture is "MVP at launch, full standard in Phase II" — because security failures are catastrophic at any point in the lifecycle, not just at scale. **Day one of operation is when the platform is most vulnerable to attack**, because attackers target new systems before defensive practices have hardened. Compressing security at MVP is the architectural decision that sinks the institutional positioning before the first trade clears.

Accordingly, all three security perimeters operate at full institutional standard from MVP launch day, with quarterly penetration testing and annual SOC 2 Type II audit cycle established from the start.

VII · PERIMETER SPECIFICATIONS

Identity. Data. *Operational*.

PERIMETER 01 · IDENTITY — FULL AT MVP

Identity *Perimeter*

Multi-factor authentication for every user role with hardware-token support for bank and DFI roles, biometric mobile authentication for field officer and trader roles. Single sign-on integration with bank identity providers where required. Session segregation by role with continuous session validation.

BANK USERS	MFA with hardware token + password + biometric · SSO with bank's identity provider · session timeout 30 minutes idle
FIELD OFFICERS	Biometric (fingerprint/face) + PIN · device-bound credentials · offline-capable authentication
TRADERS & BUYERS	MFA via SMS or authenticator app + password · session timeout 60 minutes idle
INTERNAL STAFF	MFA with hardware token + SSO · super admin access requires additional approval gate
AUDIT	Every authentication event audit-logged with IP, device, location, role assumed

PERIMETER 02 · DATA — FULL AT MVP

Data *Perimeter*

Encryption at rest and in transit. PII tokenisation. Hard tenant isolation. Content-hashed and tamper-evident artefacts. Immutable logs. Retention policy enforcement.

ENCRYPTION	AES-256 at rest · TLS 1.3 in transit · field-level encryption for sensitive PII (BVN, TIN, account numbers)
TENANT ISOLATION	Hard segregation between counterparty tenants · multi-bank tenant isolation in Phase II prevents any cross-bank data leakage
ARTEFACT INTEGRITY	SHA-256 content hash on every artefact · tamper-evident chain · integrity-check workflow in Module 13
LOG IMMUTABILITY	Append-only audit logs · cryptographically chained · 7-year retention minimum
BACKUP	Encrypted backup · geographically redundant · quarterly recovery testing

PERIMETER 03 · OPERATIONAL — FULL AT MVP

Operational *Perimeter*

Production access strictly role-gated. All deployments through change-management workflow with bank-approval gate for any modification to the settlement engine. Quarterly penetration testing, annual SOC 2 Type II audit cycle, incident response runbook with 24-hour partner notification SLA.

PRODUCTION ACCESS	Role-gated · just-in-time elevation with approval gate · all production access audit-logged · no shared credentials
CHANGE MANAGEMENT	Every deployment through review and approval workflow · bank-approval gate for settlement engine changes · rollback discipline tested before deployment
TESTING	Quarterly penetration testing · continuous vulnerability scanning · security-focused code review on every change
AUDIT	SOC 2 Type II audit cycle from Phase III · ISO 27001 alignment from MVP · PCI DSS where card-payment integration applies
INCIDENT RESPONSE	24-hour partner notification SLA · documented runbook · quarterly incident response drill

VII · THE SECURITY COMMITMENTS

What banks can *audit*.

The security posture is not a marketing claim — it is a set of auditable commitments that any bank's information-security team can examine and verify before facility execution. The following is what Miziba commits to deliver and to evidence.

SECURITY COMMITMENT 01

Every bank's data is hard-isolated from every other bank's data.

Multi-bank tenant isolation is enforced at the database level, not at the application level. No SQL query, no API call, no internal staff role has the technical capability to traverse the tenant boundary. The bank's security team can audit the isolation architecture as part of the technical due-diligence pack — the architecture is not "promised to be secure," it is structurally incapable of cross-bank leakage.

SECURITY COMMITMENT 02

Every audit artefact is cryptographically tamper-evident.

Every weighbridge reading, every loading photo, every settlement instruction, every signed contract carries a cryptographic content hash recorded in the immutable audit log. Any subsequent modification to an artefact is detectable at the hash level. The bank's audit team can verify artefact integrity at any time without depending on Miziba's assurance.

SECURITY COMMITMENT 03

Every change to the settlement engine requires bank-side approval.

Modifications to the atomic five-tier waterfall logic, the escrow account configuration, the fee calculation engine, or any code path that affects bank principal recovery are gated behind explicit bank approval. The bank's risk officer is structurally part of the platform's deployment workflow — no Miziba engineer can deploy a settlement-engine change unilaterally.

SECURITY COMMITMENT 04

Every security incident is disclosed within 24 hours.

Confirmed security incidents are disclosed to all affected partners (banks, DFIs, insurance providers) within 24 hours of identification, with documented incident response runbook and post-incident review process. The bank's information-security team can review the incident response procedure as part of due diligence.

SECTION VIII · ONBOARDING DISCIPLINE

Every counterparty. *Calibrated entry*.

Each stakeholder class enters the platform through a structured flow calibrated to their role and risk profile. Some classes enter through dedicated portals; others through structured engagement workflows operated by Miziba staff. The discipline ensures every counterparty arrives ready to operate at institutional standard from their first interaction.

Bank *onboarding*.

Technical integration phase (4-6 weeks) begins after MFA negotiation reaches indicative term sheet. Six work-streams: integration contract specification (file format, API spec, or SWIFT message schema), credential provisioning and rotation discipline, security perimeter alignment, audit access provisioning, credit-officer training, and drawdown rehearsal trade. Concludes with a supervised pilot trade that exercises every integration touchpoint end-to-end.

Trader *onboarding*.

Identity-and-credit verification under Module 1 (KYC/KYB pack, beneficial ownership tracing, sanctions screening). Equity confirmation against trader's existing balance sheet. Master Facility Agreement counterparty designation. Trader Portal access credentialed. Training session on trade origination workflow. First trade as a supervised pilot with Miziba operations team observation.

Aggregator *onboarding*.

JNI AGRI Ltd as anchor aggregator was onboarded under structured agreement with Miziba; the relationship is documented in the related-party governance pack and operates under the five structural controls visualised in Asset 09 of the Visual System. Tier-2 aggregator onboarding (Phase II) follows the same KYB pack discipline plus quality certification audit, farmer-base verification, hub-network confirmation, and anchor-partner agreement.

Buyer *onboarding*.

KYB pack for institutional buyers. Offtake-contract template execution (institutional buyers; pre-negotiated terms). Payment-direction notice acknowledgement (Master Facility Agreement supplement). Escrow-account familiarisation. Quality-acceptance protocol training. First-trade supervision by Miziba operations team.

Field officer *onboarding*.

Internal Miziba and JNI AGRI Ltd staff onboarding. Mobile-platform training. Weighbridge-protocol certification. Photo-evidence discipline training. Supervised first loading event. Quarterly recertification cycle.

VIII · STRUCTURED ENGAGEMENT WORKFLOWS

Counterparties without *portals*.

Five counterparty classes are served through structured engagement workflows rather than dedicated portals. Each workflow is itself operated by Miziba staff via TrackGuard or the Internal Operations Console, with every interaction audit-logged into the platform's reporting layer.

Transporter *onboarding through TrackGuard*.

Operational onboarding by Miziba's logistics team. KYB pack collected via document upload (vehicle registrations, driver licences, insurance certificates, GPS-device serial numbers). Master Transport Agreement executed offline, scanned and lodged in Document Vault. Per-consignment dispatch instructions sent via SMS or WhatsApp to the driver's registered number. GPS device on the vehicle reports directly to Module 6. Settlement via Miziba accounts payable. Performance metrics tracked in TrackGuard; the transporter receives a monthly performance summary by SMS.

Freight forwarder *onboarding through TrackGuard* (Phase II).

Same operational pattern as transporter onboarding, with additional certifications for bonded-warehouse status, customs-clearance accreditation, BL-issuance authority, port relationships, and EUDR-compliance capability for European-corridor exports. Per-shipment booking confirmations and BL workflows handled via secure file transfer.

Insurance partner *engagement* (Phase II expansion).

Master annual policy executed offline. Per-trade policy activation confirmations auto-generated by Module 9 and dispatched to carrier via email. Monthly premium reconciliation reports auto-generated and dispatched. Policy renewal alerts on the master annual policy. Claim instructions routed to the carrier's claims system via secure file transfer when stress events trigger Layer 6.

DFI partner *engagement* (Phase II expansion).

Quarterly portfolio-level reports auto-generated by Module 12 and dispatched. Annual impact-and-risk reports auto-generated. Real-time notification only when claim instruction is being routed (rare-to-never event in well-functioning programme). Document-share access to institutional documentation pack.

Farmer *engagement*.

Registered in Source Registry by JNI AGRI Ltd field officers. Mobile money settlements with SMS confirmation at hub-gate. Physical receipt with field officer signature. Annual statement of trade history dispatched via SMS link to read-only summary page. **The farmer is not asked to interact with software they don't already use** — the platform meets them in the channel they already operate in.

VIII · ONBOARDING TIMELINE BY CLASS

How long. *For each class*.

COUNTERPARTY CLASS	ONBOARDING SURFACE	TYPICAL DURATION
Bank	Technical integration with bank's IT, MFA negotiation, credit-officer training	*4–6 weeks*
DFI partner	Investment-committee cycle, structured engagement workflow, capacity activation	3–6 months
Independent trader	KYC/KYB through Module 1, Trader Portal, supervised first trade	*5–10 working days*
Aggregator (Tier-2)	KYB plus quality cert audit and farmer-base verification	2–4 weeks
Buyer (institutional)	KYB, offtake contract, payment-direction notice, supervised first trade	2–3 weeks
Transporter	TrackGuard operational onboarding, certifications, GPS device pairing	*3–7 working days*
Freight forwarder	TrackGuard onboarding plus BL authority and EUDR capability verification	1–3 weeks
Field officer	Internal training, weighbridge protocol cert, supervised first loading	2 weeks
Insurance partner	Master annual policy execution plus integration test cycle	3–6 weeks
Farmer	Field-officer enrolment at hub-gate or village · biometric/QR ID, MoMo linkage	*15 minutes*

VIII · THE ONBOARDING DISCIPLINE

Every counterparty arrives *ready*.

THE INSTITUTIONAL COMMITMENT

Onboarding is itself a module, not a separate exercise.

Module 1 (Counterparty Onboarding & KYC/KYB) and the structured engagement workflows operated through TrackGuard and the Internal Operations Console together constitute a unified onboarding discipline. Every counterparty enters the platform through a curated experience that mirrors the institutional discipline of the programme itself — not a generic "create account" flow, not a permissive trial period, not a self-service signup.

The bank sees every onboarding event in real time. Every KYC pack lodged, every sanctions screen passed, every Master Agreement executed flows into Grouping 6 (Counterparty & Compliance) of the Finance Partner Portal. The bank's audit team can verify counterparty onboarding integrity at any time without dependency on Miziba's assurance.

Why this matters *strategically*.

The single most common failure mode of platforms that promise institutional discipline is the gap between the onboarding experience and the operational experience. A platform that markets itself as Fortune 500-grade but onboards counterparties through a generic signup flow loses institutional credibility on first interaction. The TradeAxis onboarding discipline closes this gap structurally — every counterparty's first interaction with the platform is consistent with the institutional discipline of every subsequent interaction.

For the bank, this means that every counterparty active against its facility has been verified to institutional standard before they could draw on bank capital. For Miziba, this means that the institutional positioning is reinforced at every entry point, not just at the showpiece surfaces. For the broader programme, this means that operational risk is actively managed at the perimeter rather than absorbed during operation.

SECTION IX · DATA ARCHITECTURE & AUDIT INTEGRITY

How visibility is *structurally enforced*.

The bank's 100% visibility commitment is not a UI promise — it is a property of the platform's data model, audit infrastructure, and integrity discipline. This section specifies how the commitment is enforced from the data layer upward.

The *single source of truth* principle.

Every report, every dashboard, every counterparty view, every regulator submission is derived from the same underlying data. There is no "bank-side data" or "trader-side data" or "internal-only data" — there is platform data, and there are role-segregated permissions that determine which subset of platform data each role sees. **The bank's view and Miziba's view of the same trade are derived from the same database row, with the same audit trail, with the same artefact references.** Consistency between views is enforced by architecture, not by reconciliation.

The *append-only audit log*.

Every action across every module is recorded in an append-only audit log with cryptographic chaining. Every entry carries: timestamp (UTC), actor (user ID + role), module (which module the action originated in), action type (create/read/update/delete with semantic detail), affected entity (trade ID, counterparty ID, artefact ID), payload hash (SHA-256 of action payload), and chain reference (cryptographic link to previous entry).

Tampering with the audit log is detectable at the chain level. The bank's audit team can reconstruct any sequence of platform events from the audit log alone, without depending on Miziba's assurance — and can verify the audit log's own integrity through chain validation.

The *artefact integrity* discipline.

Every artefact stored in Module 13 (Document Vault) carries a content hash recorded at the moment of storage. The hash is logged in the audit log; the audit log is cryptographically chained; the chain is independently verifiable. Subsequent modification to any artefact is structurally detectable — the modified artefact would produce a different hash, breaking the audit trail.

The *permission matrix*.

Every read and write operation against the platform's data model is mediated by a permission matrix that maps roles to operations. The permission matrix is itself audit-logged and version-controlled; changes to permissions are rare, controlled, and traceable. **No engineer, no internal staff member, no operator has the technical capability to bypass the permission matrix.** The matrix is enforced at the data layer, not at the application layer.

IX · TRADE RECONSTRUCTION DISCIPLINE

Reconstruct any trade. *At any time*.

The institutional standard that converts the visibility commitment into an auditable property of the platform. The bank's audit team or external regulators can reconstruct any trade end-to-end at any time, from origination through settlement, with full evidence chain and timeline integrity.

What reconstruction *looks like*.

A bank audit team requests reconstruction of trade D-2026-0142 (a TSCF—D cashew trade closed three weeks ago). The platform produces:

The trade timeline. Origination event (Day 1), capital release (Day 3), six loading events at Wenchi TradePoint hub (Days 4-9), GPS-tagged dispatch (Day 10), transit log with route and weather data (Days 10-13), buyer quality acceptance (Day 18), atomic settlement waterfall (Day 27). Every event with timestamp, actor, location, and outcome.

The artefact chain. Signed offtake contract from buyer. Quality certification from JNI AGRI Ltd. Weighbridge readings from each loading event. Photo evidence of loading bays, vehicles, seals. GPS log of transit. Buyer quality acceptance certificate. Bank drawdown instruction. Buyer payment receipt. Atomic waterfall execution log. Settlement certificate. Mobile money confirmations to farmers. Each artefact with content hash and chain reference.

The audit log slice. Every action against the trade by every actor, in chronological order, with payload hashes and chain links. Every read access to the trade's artefacts (including the audit team's own current request). Every permission elevation or role switch involving the trade. Every integration exchange that touched the trade.

The protection cascade state. For each layer of the seven-layer protection cascade, the state at trade close: trader equity (Layer 3 active and confirmed), retention pool (Layer 4 funded and unused), buyer payment (Layer 5 received in full), insurance (Layer 6 active for transit cover, no claims), DFI guarantee (Layer 7 not invoked).

Why this matters *institutionally*.

A bank's internal audit cycle, an external regulator's investigation, a DFI's portfolio review, or a counterparty's dispute resolution can all proceed against the platform's reconstruction capability without requiring Miziba's narrative or interpretation. The institutional standard is that the platform's data is sufficient evidence, structurally and auditable. **Trade reconstruction is the test that verifies whether the visibility commitment is real or rhetorical**; the platform passes this test by design.

IX · DATA RETENTION & LIFECYCLE

Seven years. *Often longer*.

The retention *standard*.

The platform's default retention policy is **7 years from trade close**, aligned with Bank of Ghana statutory record-keeping requirements, Ghana Revenue Authority tax retention obligations, and AML record-keeping standards. This is the minimum; longer retention applies where local regulation, counterparty contract, or audit cycle requires.

Lifecycle *states*.

Every trade in the platform progresses through three lifecycle states. **Active**: from origination through settlement, 22-37 days for TSCF trades. Full read/write access for involved counterparties. **Recently closed**: from settlement through 90 days post-close. Read-only access remains, dispute window remains open, post-trade audit can be scheduled. **Archived**: after the 90-day post-close window. Read-only access via audit interface; data remains in the Document Vault under retention policy; integrity validated quarterly.

What persists in *archive*.

Every artefact, every audit log entry, every settlement certificate, every counterparty confirmation persists in archive at full integrity. The bank's audit team can request reconstruction of an archived trade with the same fidelity as a recently-closed trade; the only difference is access pattern (audit interface vs. live drill-down in Finance Partner Portal).

What does *not* persist.

The platform is structurally incapable of deleting historical trade data within the retention window. There is no "delete trade" operation accessible to any role. Trades that are voided during origination (before any drawdown) are marked voided and persist with their full void-event audit trail. **Audit chain integrity is non-negotiable** — deletion would break the chain and is therefore architecturally impossible.

Beyond retention *window*.

After the regulatory retention window expires (7 years minimum, longer where applicable), data may be transitioned to deep-archive storage with reduced access frequency but maintained integrity. Permanent deletion of historical trade data requires explicit institutional policy decision and bank-approval gate; no automatic deletion is built into the platform.

SECTION X · THE MVP SCOPE

Compressed-plus. *Discipline at first build*.

The full architecture is fourteen modules, seven portals, four integrations. The MVP is what gets built first — sized for the pilot trade window, the pilot bank's defensibility requirements, and the institutional discipline of shipping fast and proving mechanics before expanding.

The *strategic frame*.

The MVP must do three things, in order of priority: **run the pilot trades end-to-end without operational failure**; **give the bank 100% visibility into those trades at the level required for credit-committee defence**; **operate without exposing Miziba to operational, regulatory, or reputational failure modes the platform cannot yet handle**. Anything that touches bank-side visibility, settlement integrity, or institutional auditability must be built to full standard at MVP. Everything else is a candidate for compression.

What the MVP *does*.

Three to five pilot trades at GHS 300-500K each, totalling GHS 1.0-2.5M. Single anchor aggregator (JNI AGRI Ltd). One or two pilot banks. TSCF—D variant only. All three source patterns live (direct farmer, cooperative bulk, Tier-2 aggregator bulk). Three TradePoint hubs operational. The pilot proves the operational mechanics, generates first-trade evidence with bank-confirmed visibility, and converts a pilot bank into a credible reference for Phase II rollout.

What the MVP *does not do*.

No TSCF—X export trades (Phase II). No multi-bank tenant isolation (Phase II). No advanced analytics layer (Phase II). No EUDR-compliance documentation pack assembly (Phase II). No standalone Quality Verification module (Phase II). No standalone Treasury workflow (Phase II). No dedicated Aggregator or Buyer Portals (Phase II; pilot served through Internal Operations Console and structured email). No DFI guarantee orchestration (Phase II). No regulator API surface (Phase III).

X · MVP MODULE-BY-MODULE SCOPE

Ten modules at MVP. *Four deferred*.

MODULE	NAME	MVP STATUS
01	Counterparty Onboarding & KYC/KYB	*Full at MVP*
02	Source Registry & Origin Verification	*Full at MVP · all 3 patterns*
03	Trade Origination	TSCF—D only at MVP
04	Credit Decisioning & Bank Workflow	Single bank at MVP
05	Quality Verification & Certification	Basic at MVP
06	Logistics & Movement Control (TrackGuard)	Basic at MVP · domestic only
07	Escrow & Atomic Settlement	*Full at MVP · non-negotiable*
08	Treasury, Cash & Currency Management	Basic at MVP
09	Insurance & Guarantee Orchestration	Transit insurance only at MVP
10	Exception & Recovery Workflow	Basic at MVP
11	Regulatory & Compliance Operations	Basic at MVP
12	Reporting, Audit & Analytics	Reporting/audit full · analytics Phase II
13	Document Vault & Lifecycle Archive	*Full at MVP · non-negotiable*
14	Integration Hub & Notification Services	3 integrations at MVP

THE MVP DISCIPLINE

Two modules cannot be compressed: Module 7 (Atomic Settlement) and Module 13 (Document Vault).

Both deliver on the institutional commitments that make TSCF defensible at all. The atomic five-tier waterfall and the cryptographically sealed audit trail are the architectural commitments to the bank that "bank principal first" and "every artefact auditable" are structurally true rather than rhetorically true. Compromising them at MVP means compromising the entire programme thesis at first launch. Both are built to full Fortune 500 institutional standard from MVP launch day.

X · MVP PORTAL SCOPE

Five portals at MVP. *Two deferred*.

PORTAL	MVP SCOPE	MVP STATUS
TradePoint Portal	Mobile-first, native iOS/Android, offline-first. Eight core workflows operational. Bluetooth weighbridge integration where hubs have calibrated scales	*Full at MVP*
Trader Portal	Web + mobile responsive. Origination workflow, status monitoring, document access. Advanced features deferred	Basic at MVP
Aggregator Portal	JNI AGRI Ltd operated through Internal Operations Console at MVP. Tier-2 aggregators served through structured workflows	Phase II
Buyer Portal	Pilot buyers served through structured email workflows at MVP. Quality acceptance via direct engagement with Miziba operations team	Phase II
TrackGuard	Basic at MVP — transporter onboarding, GPS dispatch, transit monitoring, route deviation alerts. Weather, customs, BL, port-side handover all Phase II	Basic at MVP
Finance Partner Portal	**Groupings 1-4 at full MVP standard**: Facility Overview, Active Trades, Live Logistics, Settlement & Reconciliation. Groupings 5-6 (Risk & Exceptions, Counterparty & Compliance) at Phase II full	*Full at MVP*
Internal Operations Console	Basic at MVP — six of eight super admin groupings live. Grouping 6 (Platform Financial Position) and Grouping 8 (Compliance & Strategic Signals) deferred to Phase II	Basic at MVP

Why the *Aggregator and Buyer Portals are deferred*.

Both portals serve counterparties whose pilot-stage engagement can be handled by Miziba operations staff through the Internal Operations Console without compromising the bank's visibility. JNI AGRI Ltd, as the only aggregator at MVP and the anchor partner under existing institutional arrangement, can operate through direct contact with Miziba's verification officers. The 1-2 pilot buyers can be served through structured email engagement with offtake contracts and quality acceptance handled offline. **Every action these counterparties take during pilot still flows into the platform through Miziba-staff-mediated workflows that are themselves audit-logged** — the bank's visibility commitment is intact.

X · MVP RISK ASSESSMENT

One risk. *Mitigated by structure*.

The honest assessment of what the MVP scope foregoes, and how the pilot programme structure mitigates the residual exposure. The discipline is to be transparent about constraints rather than pretend they don't exist.

Risk · *TSCF—X readiness at end of Phase I*.

By deferring TSCF—X export functionality (export workflow, BL control, customs, freight-forwarder onboarding, EUDR compliance), the platform cannot run an export trade until Phase II completes around month 10. If a DFI partner conditions guarantee capacity on export-trade evidence, Miziba would need to manually run an off-platform export trade for the demonstration, which is operationally credible but institutionally weaker than running it through the platform.

Mitigation through programme structure. DFI engagement runs on quarterly investment-committee cycles regardless of platform timing — AGF, GIRSAL, AfDB, and Rabobank Foundation all make capacity decisions at quarterly cadence. Having TSCF—X live for 4 months versus 6 months versus 10 months is unlikely to be the determining factor in DFI capacity decisions; the determining factor will be whether pilot trades cleared cleanly and the bank facility is performing. **One completed TSCF—D trade is worth ten promised TSCF—X trades** in the institutional credibility calculus.

Risk · *Cooperative source supply*. Addressed by inclusion at MVP.

Originally identified as a deferred-from-MVP capability that would constrain pilot supply chain flexibility. Resolution: **Module 2 (Source Registry & Origin Verification) is built at full three-pattern capability from MVP launch**. Direct farmer, cooperative bulk, and Tier-2 aggregator bulk all operational. The pilot trades have full supply-chain flexibility from launch. EUDR-compliance traceability is pre-positioned in the data model for Phase II export-corridor activation.

Why this scope is *institutionally defensible*.

The MVP delivers everything required for the pilot bank to defend the facility internally: 100% visibility into pilot trades, full audit trail, atomic settlement integrity, related-party governance enforced in code, security posture at full Fortune 500 standard. The deferred capabilities (TSCF—X export, multi-bank tenant isolation, advanced analytics, EUDR documentation, full insurance stack) are valuable at scale but not essential at pilot scale. Compressing them at MVP is the correct discipline; building them prematurely is feature creep dressed up as strategic ambition.

SECTION XI · THREE-PHASE BUILD STRATEGY

Three phases. *Eighteen months*.

MVP, expansion, institutional hardening. Each phase ships operational capability that justifies its own investment; together they deliver the full institutional architecture against operational evidence rather than against promises.

PHASE	SCOPE	INVESTMENT
Phase I *MVP*	MONTHS 1–5 10 modules at MVP standard, 5 portals, 3 integrations, TSCF—D only with all 3 source patterns, single anchor aggregator, 1-2 pilot banks, 3 hubs, full security and audit posture	*USD 250K—380K*
Phase II *Multi-bank stack*	MONTHS 6–10 Full 14-module architecture, all 7 portals, full Finance Partner Portal six groupings, full super admin dashboard eight groupings, TSCF—X export workflow, full Insurance & Guarantee Orchestration with Layer 7 DFI capacity, multi-bank tenant isolation, advanced analytics	USD 400K—580K incremental
Phase III *Institutional hardening*	MONTHS 11–18 Regulator interface (BoG, GRA, SEC, EUDR, SARB pre-positioning), advanced analytics layer, secondary-market preparation, SOC 2 Type II audit, full disaster recovery, ISO 27001	USD 200K—350K incremental
18-month total	The full institutional platform — built incrementally against operational evidence rather than as a single bet	***USD 850K—1.31M***

XI · PHASE I · MVP IN DETAIL

Phase I. *The pilot stack*.

End-of-phase *outcome*.

Three to five pilot TSCF—D trades successfully run through the platform end-to-end. Pilot bank has 100% visibility, defends the facility internally, agrees to expand. First-trade evidence base built. Reference architecture proven. Programme launches into Phase II with institutional credibility.

Build target by *month*.

Month 1. Foundation — data model, security perimeters, identity infrastructure, Document Vault, base audit log, environment setup, core integrations stubbed.

Month 2. Counterparty stack — Module 1 (KYC/KYB), Module 2 (Source Registry, all three patterns), Trader Portal basic, Internal Operations Console basic.

Month 3. Trade operations — Module 3 (Trade Origination, TSCF—D), Module 4 (Credit Decisioning), Module 6 (TrackGuard basic), TradePoint Portal core workflows, MTN Mobile Money integration.

Month 4. Settlement and reporting — Module 7 (Atomic Settlement, full standard, non-negotiable), Module 9 (transit insurance), Module 12 (reporting and audit), Finance Partner Portal Groupings 1-4, pilot bank file-based integration.

Month 5. Hardening and pilot launch — security testing, integration testing, supervised pilot trade execution, bank credit-officer training, drawdown rehearsal trade, programme go-live.

Investment *profile*.

USD 250K-380K across the 5-month build window, depending on engineering team composition and integration complexity. Concentrated in months 1-3 (foundation + core modules); months 4-5 weight more on integration, testing, and operational readiness.

Capital-efficient by discipline. Phase I avoids the foundational categories of MVP cost overrun: scope creep, premature optimisation, premature scaling, and premature multi-tenant architecture. Each of these is a Phase II investment that compounds when made too early.

XI · PHASES II & III IN DETAIL

Expansion. *Then hardening*.

Phase II · *Months 6–10*.

The expansion phase. Builds against operational evidence from Phase I. Introduces TSCF—X export workflow with bank-consigned BL control, customs and clearance integration, EUDR-compliance documentation, and freight-forwarder operational onboarding through TrackGuard. Activates the full Insurance & Guarantee Orchestration stack including Layer 7 DFI capacity. Introduces multi-bank tenant isolation as additional banks come online from the five-bank parallel engagement. Adds Aggregator Portal, Buyer Portal, full Risk & Exceptions panel and Counterparty & Compliance grouping in Finance Partner Portal, full super admin dashboard with Platform Financial Position. Introduces the analytics dimension of Module 12 (cycle-time forecasting, exception-pattern recognition, transporter-reliability scoring, default-probability modelling).

Investment: USD 400K-580K incremental. End-of-phase outcome: full architectural scope operational, multi-bank multi-aggregator deployment running, TSCF—X exports clearing with EUDR compliance, DFI guarantee capacity engaged.

Phase III · *Months 11–18*.

The institutional-hardening phase. Builds against the operational scale of Phase II. Introduces regulator API surface for Bank of Ghana, Ghana Revenue Authority, and Securities & Exchange Commission, with pre-positioning for SARB and EU EUDR. Completes the analytics layer with predictive modelling, behavioural pattern recognition, weather-risk prediction. Prepares the platform for secondary-market participation (e.g. trade receivables securitisation pipeline). Achieves SOC 2 Type II audit certification. Implements full disaster recovery posture with geographic redundancy and quarterly recovery testing. Achieves ISO 27001 alignment and PCI DSS where applicable.

Investment: USD 200K-350K incremental. End-of-phase outcome: platform at full institutional standard, regulator-ready, audit-certified, prepared for cross-border expansion and secondary-market integration.

Why phasing this way is *strategically correct*.

Each phase ships operational capability that justifies its own investment. Phase I generates the first-trade evidence that converts the pilot bank into a credible reference. Phase II expands against that evidence to full multi-bank operation. Phase III hardens against operational scale. **The platform is built incrementally against operational learning rather than as a single bet against architectural ambition** — which is the discipline that distinguishes successful institutional platform builds from those that ship late or never.

SECTION XII · FORTUNE 500 INSTITUTIONAL BENCHMARKS

The reference *points*.

How TradeAxis maps to the institutional platforms that bank stakeholders, DFI investment officers, and external auditors already understand. Not "we are like Bloomberg" — but a structural mapping of where TradeAxis takes its design discipline from each reference, and where it differs by virtue of operating a different problem domain.

Bloomberg *Terminal*.

The Finance Partner Portal takes its institutional discipline from Bloomberg Terminal: information density at scale, role-segregated within the workspace, dark-surface register that financial professionals expect, action-oriented rather than passive-reporting. Where TradeAxis differs: Bloomberg is read-only for most users (consuming market data); TradeAxis is read-write for the bank credit officer (taking actions against the facility). Bloomberg is multi-tenant with thousands of subscribers; TradeAxis is multi-tenant with a small number of institutional banks each with full segregation.

Goldman Sachs *Marquee*.

Marquee is Goldman's client-facing platform that exposes institutional capabilities to corporate and institutional clients. The Trader Portal and Buyer Portal take design discipline from Marquee: institutional surface for sophisticated counterparties, integrated workflow rather than separate tools, single sign-on with role-segregated capabilities. Where TradeAxis differs: Marquee operates inside Goldman's existing institutional infrastructure; TradeAxis is the institutional infrastructure for a new programme being built from foundation.

Stripe *Internal Operations*.

The Internal Operations Console takes design discipline from Stripe's internal admin tooling: super-admin role with cross-tenant intelligence not available to any single customer, layered permissions within the admin workspace itself, role-switch capability for support and oversight, panic-button discipline for incident response. Where TradeAxis differs: Stripe operates at consumer-payment scale (millions of transactions); TradeAxis operates at commodity-finance scale (hundreds of trades, but each with significant institutional weight).

Tier 1 core banking systems · *Temenos T24, Mambu, Finastra*.

Module 7 (Escrow & Atomic Settlement) and Module 13 (Document Vault) take their institutional discipline from Tier 1 core banking systems: financial-grade integrity, change-management with bank-approval gate, audit chain that meets regulator standards, integration patterns calibrated to the operating reality of bank IT. Where TradeAxis differs: core banking systems are general-purpose (handling any bank operation); TradeAxis is purpose-built for TSCF, with deep operational specialisation in the seven-layer protection cascade and atomic five-tier waterfall.

McKinsey-grade *institutional advisory*.

The brief itself, the Operations Manual, the Bank Engagement Playbook, the Capital Strategy, the Corporate Governance Manual, and the Visual System take their institutional discipline from the documentation cadence of top-tier strategy and management consulting work. Source Serif 4 typography, italic gold persuasion fulcrums, eyebrow/headline/lede hierarchy, structured argument with explicit commitments and trade-offs. The institutional reference is not a software product but a documentation standard.

XII · WHERE THE BENCHMARKS END

What TradeAxis *uniquely does*.

The benchmarks help orient the platform's institutional discipline against reference points that bank stakeholders already understand. But TradeAxis operates a problem domain that none of the benchmark platforms operates — and the unique requirements of that domain produce institutional commitments that benchmarks do not have.

Three things *no benchmark platform does*.

One · *Verification at the source*.

No benchmark platform operates a field-side mobile portal that captures weighbridge readings, photo-documents loading events, settles farmers via mobile money at hub-gate, and feeds that evidence chain into the bank's institutional reporting layer. The TradePoint Portal is unique to the TSCF problem domain — building institutional verification infrastructure where smallholder commodity flows originate, in operating conditions that include intermittent connectivity, dust, heat, and shared device usage across shifts.

Two · *The atomic five-tier waterfall*.

No benchmark platform executes a five-tier settlement waterfall in code that allocates buyer payment irreversibly across bank principal, bank fee, structuring fee, monitoring fee, and trader margin in atomic sequence. Module 7 is institutionally distinctive — it is what makes "bank principal first" structurally true rather than rhetorically true, and it is what gives the bank its senior secured position as an enforceable property of the platform's data model.

Three · *The seven-layer protection cascade as architectural discipline*.

No benchmark platform organises its risk architecture around a defensive-depth cascade that runs from JNI AGRI Ltd counterparty integrity through Miziba verification infrastructure, trader equity, retention pool, buyer payment receipt, four-policy insurance, and DFI guarantee in series. The cascade is not a marketing diagram — it is an architectural principle that runs through every module's data model, every portal's permission matrix, every integration's security perimeter, and every audit artefact's retention policy.

What this *means strategically*.

TradeAxis is not "Bloomberg for African commodity finance" or "Goldman Marquee for smallholder supply chains." It is a purpose-built institutional platform for a problem domain that the benchmark platforms do not operate. The benchmarks help orient the discipline; the originality of the domain produces the institutional commitments. **This is the architectural posture that distinguishes a Fortune 500-grade platform from a derivative one** — not "we built a clone of established platforms," but "we built the institutional platform that this problem domain has been missing, with the design discipline that established platforms have established as the institutional standard."

XII · RELATED-PARTY GOVERNANCE

The related-party *structural integrity*.

The platform structurally enforces the five controls that govern the Joel-JNI AGRI Ltd relationship. Not as policy documentation — as code that prevents the related-party arrangement from being abused, and as audit infrastructure that proves the enforcement.

VISUAL REFERENCE · ASSET 09

The structural separation between Miziba Infrastructure Ltd and JNI AGRI Ltd, with Joel NtiAmoah Marfo's 50% holding in JNI AGRI explicitly disclosed. Five structural controls enforced by the platform:

BORROWER INTEGRITY

(independent trader is the borrower; never JNI AGRI Ltd; never Miziba),

PRICING TRANSPARENCY

(TSCF commodity pricing benchmarked to published market rates; no preferential pricing for JNI AGRI),

AGGREGATOR ONBOARDING

(TSCF designed for multiple aggregators; JNI AGRI anchors but doesn't have exclusive access; Tier-2 aggregators participate on equal terms),

INDEPENDENT AUDIT

(both companies maintain separate audited financials; JNI AGRI Ltd FY2025 audit independently filed; Miziba financials separately auditable),

DISCLOSURE DISCIPLINE

(Joel's 50% holding disclosed in writing to every institutional counterparty before facility execution).

SECTION XIII · PLATFORM GOVERNANCE & CHANGE MANAGEMENT

How the platform *is governed*.

The platform itself is an institutional asset that requires institutional governance. This section specifies the governance structure, the change-management discipline, and the bank-approval gate that protects the institutional commitments embedded in the platform's design.

The platform governance *structure*.

Three governance layers operate above the platform's engineering and operations teams. **The Platform Steering Committee** sets architectural direction, approves the multi-year roadmap, ratifies phase transitions, and sits inside Miziba's broader institutional governance reporting to the board. **The Change Advisory Board** reviews and approves operational changes that affect the platform's institutional commitments — including the bank-approval gate for settlement-engine changes, the integration contract change-management discipline, and the security-perimeter modification protocol. **The Incident Response Authority** activates on confirmed security incidents or operational failures, with documented runbooks, partner notification SLA, and post-incident review discipline.

The *bank-approval gate*.

The single most important change-management discipline. Modifications to the atomic five-tier waterfall logic, the escrow account configuration, the fee calculation engine, the protection cascade enforcement, or any code path that affects bank principal recovery are gated behind explicit bank approval before deployment. **The bank's risk officer is structurally part of the platform's deployment workflow** — not as a courtesy, but as an architectural feature. No Miziba engineer can deploy a settlement-engine change unilaterally. The bank's audit team can verify the bank-approval gate as part of technical due-diligence; it is enforced in code, not in policy.

Change *cadence*.

Major releases at quarterly cadence, with bank-approval gate review and partner notification at least 30 days in advance. **Minor releases** at monthly cadence, with audit-logged review but lighter approval discipline (operational improvements that don't touch institutional commitments). **Security patches** deployed as required, with 24-hour partner notification SLA for any patch affecting integrations or audit infrastructure. **Hot fixes** for production incidents deployed under Incident Response Authority with retrospective approval and post-deployment review.

FROM HERE

Build *discipline*. Ship the *MVP*. Earn the *scale*.

The architecture is locked. Five canonical Miziba modules — TradePoint verification, TrackGuard logistics, TradeVault settlement, TradeAxis origination, and FarmerIQ intelligence — deliver the institutional commitments through fourteen architectural building blocks across four functional layers. Seven portals calibrated to operational engagement. Four integrations contracted and audit-logged. Three security perimeters at full standard from MVP launch. Six dashboard groupings deliver the bank's 100% visibility commitment. Eight super admin groupings give Miziba whole-platform visibility.

The MVP is institutionally defensible. USD 250K–380K across five months. TSCF—D variant only with all three source patterns live. One anchor aggregator. One or two pilot banks. Three to five pilot trades that prove the operational mechanics and convert a pilot bank into a credible reference for Phase II rollout. The full institutional architecture follows against operational evidence rather than against architectural ambition. Total 18-month investment: USD 850K–1.31M.

This brief sits in the institutional documentation library at miziba.com/documents alongside the Operations Manual, Bank Engagement Playbook, Capital Strategy, Corporate Governance Manual, and Visual System. It completes the institutional documentation pack on the systems-and-platform layer.

Joel NtiAmoah Marfo, Founder & CEO