

Historical Architecture Reference

Current scope amendment applies first

This document preserves an earlier PRD/DFD design, including optional future workflows and legacy Brazil examples. It does not describe live capabilities, signed counterparties or the approved first pilot scope.

The v2.10.1 current scope and control amendment, dated 23 September 2026, supersedes conflicting scope, issuance, commercial timing and jurisdiction statements. English governs this update; the underlying translated reference has not been fully rewritten.

Planned structure: BVI project base. Cayman Islands GO token. UAE buyers and sellers first. Proposed round: SAFE (BVI), 20% discount + token warrant (Cayman Islands). Detailed legal structuring follows funding. No signed pilot or institutional contracts.

GlemO records and distributes third-party-issued RWA tokens; it does not issue those assets. The separate GO token structure is planned in the Cayman Islands. Historical Asset Factory wording describes external RWA offering records.

Initial pilot: B2B intake, external asset records, accountable-origin evidence, permissioned reporting, manual buyer-response tracking and invoicing. Retail allocation, settlement, public chain proof, multi-chain automation and modules remain gated later work.

All prototype counterparties, balances and transaction examples are simulated. Production security, required permissions, data rights and provider acceptance precede the relevant live activity.

Read [GlemO_Current_Scope_and_Control_Amendment_2026-09-23.pdf](#) in the root of the same canonical package before estimating or implementing these designs.

GLEMO PRODUCT REQUIREMENTS

GlemO Platform Product Requirements Specification

MVP1 implementation brief for developers, product, design, compliance and external delivery partners

Field	Value
Version	1.0 developer ready
Date	15 September 2026
Audience	Engineering, product, UX, compliance, AI operations, integrations and delivery partners
Product thesis	Asset class neutral liquidity and distribution rail for tokenized real world assets
First proof market	Real estate credit and adjacent private market assets
Primary package	Token2049 institutional data room V4.7

Implementation conclusion. GlemO should be built first as a controlled operating platform, not as an open exchange. MVP1 should prove discovery, eligibility, seller supply, evidence review, admin release, private transaction records, public proof, enterprise SaaS and revenue operations before expanding into automated liquidity, plugins and a broader dApp ecosystem.

1 Purpose and reader task

This document converts the current GlemO Token2049 data room and product prototype into a developer ready requirements specification. It defines what must be built for MVP1, what can remain manual, what data objects are required, what actors need private environments and what controls protect the product from becoming overbroad or regulatorily misleading.

A development team should be able to use this document to estimate the build, structure epics and services, design the database, create user stories, define APIs, plan integrations and decide what must be production ready before launch.

2 Product thesis and boundaries

GlemO is an asset class neutral liquidity and distribution rail for tokenized real world assets. Real estate credit is the first proof market because it gives the platform an understandable source of assets, collateral, documents and commercial demand. The long term platform should also support receivables, private credit, infrastructure, fund interests and other approved tokenized assets through the same operating model.

The product should not present itself as the issuer, custodian, exchange, broker dealer, investment adviser, bank or market maker unless a regulated partner explicitly owns that function. GlemO coordinates discovery, eligibility, evidence, distribution, monitoring, reporting, transaction declaration, enterprise intelligence and operating controls.

- Build the controlled workflow first, then automate pieces once evidence, roles and partner responsibilities are clear.
- Keep real estate as the entry market, not the final category.
- Use Ethereum and Base as initial EVM aligned rails, with partner rails for custody, payment and reconciliation.
- Make the token supportive to community, builders, dApps and retail engagement; do not make token appreciation the financial model.
- Treat AI as a governed operating layer with human review and audit, not an uncontrolled chatbot.

3 MVP1 scope

Area	Included in MVP1	Out of MVP1
Marketplace	Public browsing, asset facts, risk labels, official channels, request access	Open unrestricted trading venue
Buyer account	Retail and institutional accounts, wallets, eligibility, transaction history	Fully automated suitability logic in every jurisdiction
Seller workspace	Entity profile, signers, plans, asset drafts, documents, distribution controls	Self service public issuance without admin review
Validation	Validator desk, evidence review, issue status, admin publication gate	Automated legal opinion or automated regulatory approval
Transactions	Private records, standby queue, admin clearance, public sanitized explorer	Instant secondary market or market making
Enterprise SaaS	Free and Enterprise AI plan, request form, billing preference, reports	Complex multi tier pricing
AI	Controlled concierge requests, prompt policy metadata, human QA and delivery log	Unrestricted model access to client confidential data
Rails	Ethereum and Base metadata, partner reconciliation, custody and payment status	Full in house custody or payment processing
Builder ecosystem	Architecture and future portal placeholder	Production plugin marketplace before liquidity loop proof

4 Actor model and permissions

Actor	Description	Core permissions
Visitor	Public user before login	Browse marketplace, see public asset facts, learn risks, request access
Retail buyer	Individual buyer where allowed	Account, profile, wallets, KYC, suitability, asset watchlist, allocation requests, transaction history
Qualified or institutional buyer	Professional investor or institution	Mandates, committee files, larger allocation requests, diligence room, reporting
Seller or originator	Bank, financial institution, originator, asset sponsor or approved publisher	Entity admin, KYB, signers, asset factory, evidence, liquidity rules, distribution analytics
Distribution partner	Approved channel partner or distributor	Available assets, approved copy, lead attribution, transaction leakage and revenue-share rules
Validator	Independent or internal validation role	Evidence triage, document review, opinion, publication recommendation, exception history
Platform admin	GlemO central operations	Publication release, transaction clearance, user controls, billing, reports, audit, platform metrics
AI operations user	Internal AI governance and concierge operator	Request queue, prompt policy, agent output QA, delivery log, data permission review
Rail or custody partner	Partner handling custody, payment or chain rails	Settlement events, reconciliation status, fallback route, evidence hash exchange
Builder or dApp developer	Future ecosystem participant	Plugin registry, sandbox, extension analytics, app submission and review

5 Functional modules

ID	Module	Phase	Screens	Requirement
M01	Public marketplace and asset discovery	MVP1 core	market, assetFactSheet, distributionSaas	Allow public inspection of approved tokenized assets, public risk labels and official distribution channels before account creation.
M02	Buyer onboarding and eligibility	MVP1 core	retailPortal, investorGate, institutionalPortal, investorEducation	Create private buyer accounts with wallet connection, KYC/KYB, suitability, jurisdiction and offering-rule checks.
M03	Seller organization admin	MVP1 core	sellerOrgAdmin, bankOps	Register approved seller entities, manage users, signers, plans, authority evidence and internal approval rules.
M04	Asset factory	MVP1 core	assetFactory	Create pooled offerings or standalone tokenized assets with unit value, supply, rule book, documents, liquidity terms and evidence.
M05	Validator and document review	MVP1 core	validatorDesk, documentReview	Review asset evidence, extract fields, classify issues, request documents and generate validation opinion before publication.
M06	Admin publication and transaction clearance	MVP1 core	adminDashboard, complianceCases, transactionClearance	Control asset release and sensitive transaction approval through standby queues, compliance notes and audit trails.
M07	Transaction declaration layer	MVP1 core	transactionLayer, ledger, reports	Maintain private actor transaction records and public sanitized transaction proof similar to a platform activity explorer.
M08	Asset technical sheet	MVP1 core	assetFactSheet	Expose the complete asset history, tokenization entity, commercializing entities, collateral, documents, performance and liquidity behavior.
M09	Distribution SaaS and partner portal	MVP1 beta	distributionSaas, distributionPartner	Monetize intelligence for sellers and partners through channel map, external availability, leakage, incentives, conversion and partner analytics.
M10	Seller plans and enterprise checkout	MVP1 beta	sellerPlans, enterpriseCheckout	Offer Free and Enterprise AI plan with request form, cart, monthly or annual billing and card or crypto payment preference.
M11	Billing and revenue	MVP1 core	billingRevenue	Track SaaS subscriptions,

	operations			setup fees, servicing, bank/institution fees, transaction fees, invoices and collection status.
M12	AI operations and concierge	MVP1 beta	aiOps, conciergeDesk	Turn enterprise requests into governed prompt chains, agent runs, human QA, private scenario reports and delivery logs.
M13	Risk and token reference engine	MVP1 beta	riskEngine	Calculate reference value, risk score, LTV, liquidity status, concentration and disclosure flags without speculative pricing claims.
M14	Rails, custody, payment and reconciliation	MVP1 beta	railPartner, ledger	Use Ethereum and Base as initial EVM-aligned rails while integrating partner custody, payment, settlement and reconciliation events.
M15	Liquidity desk and replacement process	MVP1 beta	liquidityDesk, replacementQueue	Support pooled offering reserves, redemption queues, LMO checks, contract replacement and recomposition events where applicable.
M16	Access control and audit	MVP1 core	accessControl, ledger	Enforce role-based access, MFA policy, sensitive action approvals, immutable audit trail and exportable evidence history.
M17	Readiness register and downloads	MVP1 core	operatingReadiness, downloads	Track artifact status, open evidence, owners, release gaps and downloadable diligence documentation.
M18	Builder and dApp ecosystem	Phase two	ecosystemBuilder	Enable plugins, extensions and dApps after the first liquidity and distribution loop is proven.

6 Critical user journeys

ID	Journey	Flow	Acceptance logic
W01 Public discovery to buyer account	Visitor browses marketplace, opens asset fact sheet, reviews risk language, creates account, verifies email/MFA, connects wallet and starts eligibility flow.	Visitor can see public information, but allocation buttons require account, KYC and offering eligibility.	
W02 Buyer eligibility and allocation request	Buyer completes KYC/KYB, suitability and jurisdiction checks. Platform evaluates offering rules. Eligible buyer can request allocation or join standby.	No allocation request can progress without explicit eligibility status and current disclosure acceptance.	
W03 Seller onboarding	Seller submits organization profile, KYB, signers, authority	Seller cannot publish assets before organization is approved	

	documents, billing plan and internal approval rule.	and at least one authorized signer is verified.	
W04 Asset creation and evidence package	Seller creates Offering, selects Pool or Standalone Asset, defines unit value, supply, rule book, liquidity terms, documents and distribution channels.	Offering remains Draft or Review until required evidence is complete.	
W05 Validator review and publication gate	Validator reviews documents, extracted fields, hash evidence, legal/risk notes and issues opinion. Admin releases or blocks publication.	Validator opinion is necessary but final publication is controlled by GlemO admin in MVP1.	
W06 Transaction standby and clearance	Buyer or seller initiates transaction. Sensitive transactions enter standby. Seller can pre-check evidence. Admin clears, rejects or requests more data.	MVP1 favors controlled review over instant automated execution.	
W07 Private and public transaction declaration	Full transaction details remain private per actor. Sanitized public event declares activity, amount band, proof hash and chain route status.	Public explorer must not expose personal data, wallet identity beyond approved public data, or restricted offering details.	
W08 Enterprise SaaS request and activation	Seller selects Enterprise AI, submits request, chooses monthly or annual billing and card or crypto. GlemO approves scope and activates AI services.	Payment and AI activation require seller approval, scope confirmation and data permission boundary.	
W09 AI concierge delivery	Customer request becomes structured prompt within GlemO master policy. Agent runs analysis. Human QA approves report. Output is delivered and logged.	Raw prompts are not exposed to clients; value is governed workflow and auditable output.	
W10 Rails reconciliation	Platform receives custody, payment, on-chain and settlement events from partners. Ledger reconciles expected vs actual status and flags exceptions.	Ethereum and Base are initial EVM rails; partner rails remain necessary for custody and payments.	

7 Data model baseline

The first production schema should support the following domain objects. Field names are indicative, not final database names. The important design principle is to keep Offering as the umbrella object so that a seller can create either a pooled structure or a standalone tokenized asset without forcing all products into a pool model.

Entity	Indicative fields	Used by
User	id, name, email, role, organizationId, jurisdiction, MFA status, status	All authenticated actors
Organization	id, legalName, type, jurisdiction, KYB status, plan, billing profile	Seller, buyer institution, partner, validator, rail partner
Wallet	id, userId, chain, address, verification status, risk flags	Buyer and treasury wallet controls
Offering	id, structure type, asset class, status, jurisdiction, sellerId, validatorId, adminReleaseStatus	Umbrella object for pools and standalone assets
Asset	id, offeringId, name, collateral type, documents, tokenization party, commercializing entities	Individual tokenized asset or asset inside pool

Pool	id, offeringId, contracts, NAV reference, LMO, replacement rules, reserve status	Optional structure for pooled offerings
TokenReference	offeringId, chain, contract address, standard, supply, unit value, reference methodology	Token layer metadata
EvidenceDocument	id, offeringId, document type, owner, hash, version, review status, expiry date	Validation and audit evidence
ValidationCase	id, offeringId, validator, issues, opinion, status, timestamps	Validator workflow
ComplianceCase	id, actor, transactionId, risk category, notes, decision, attachments	Admin and compliance workflow
Transaction	id, buyerId, sellerId, offeringId, amount, currency, status, payment method, chain event	Private transaction record
PublicTransactionEvent	id, sanitized amount band, asset reference, chain route, proof hash, timestamp	Public explorer event
DistributionChannel	id, offeringId, channel entity, availability, official status, link, terms	Where an asset can be acquired
Lead	id, source, partnerId, assetId, attribution, conversion status, leakage flag	Distribution SaaS analytics
Invoice	id, customer, fee type, billing period, amount, payment method, collection status	Revenue operations
AIRequest	id, customer, scenario, data scope, prompt chain version, agent, QA status, output	Enterprise AI concierge
AuditEvent	id, actor, action, object type, object id, before/after, timestamp, IP/device	Platform-wide audit ledger

8 Service and API architecture

A modular service architecture is recommended even if MVP1 is delivered as a monolith. The service boundaries below should guide routes, repositories, permissions and future extraction into independent services.

Service	Indicative API areas	Responsibility
Identity and Access Service	/auth, /users, /roles, /mfa, /sessions	Authentication, RBAC, MFA, invite flows, audit-ready session state
Organization Service	/organizations, /signers, /kyb	Seller, partner, institutional buyer and validator organization records
Marketplace Service	/offerings, /assets, /public-assets, /asset-facts	Public discovery, asset fact sheet, filters and approved copy
Eligibility Service	/kyc, /suitability, /jurisdiction, /offering-rules/check	Buyer qualification and offering-rule gating
Asset Factory Service	/offerings/drafts, /documents, /rule-books, /publication-requests	Seller asset creation and evidence collection
Validation Service	/validation-cases, /document-reviews, /opinions	Validator workflow and admin publication evidence
Compliance Service	/compliance-cases, /transaction-clearance, /watchlist-events	Standby, approvals, rejection reasons and case management
Transaction Service	/transactions, /public-events, /proof-hashes	Private transaction records and public sanitized explorer
Billing Service	/plans, /checkout-requests, /invoices, /payments	Enterprise SaaS, setup, servicing and transaction fee billing
AI Concierge Service	/ai-requests, /agent-runs, /reports, /qa-reviews	Governed AI request lifecycle and report delivery
Rails Service	/rails, /chain-events, /settlements,	EVM rail events, custody partner events

	/reconciliation	and fallback tracking
Reporting Service	/reports, /exports, /metrics, /dashboards	Management, actor and diligence exports

9 Blockchain and rails requirements

MVP1 should document Ethereum and Base as the initial EVM aligned architecture. Ethereum gives institutional credibility and settlement reference. Base gives lower cost, ecosystem access and developer/community distribution. The product should keep rail abstractions chain agnostic enough to support additional networks later.

- Create Chain, TokenContract, Wallet, ChainEvent and ReconciliationEvent objects even if MVP1 uses simulated or partner supplied events.
- Do not custody client assets directly unless a regulated custody path is defined.
- Separate commercial transaction status from on chain event status. A transaction can be approved, pending payment, pending settlement, reconciled, failed or reversed.
- Record transaction proof hash and public event reference without exposing private buyer or seller data.
- Support stablecoin payment instructions as a payment method state, not as an assumed payment license.

10 Compliance and operating controls

- Every asset publication requires seller approval, evidence package, validator review and admin release.
- Sensitive transactions enter standby until admin clearance in MVP1.
- Seller pre check can prepare evidence but does not replace central platform clearance.
- Compliance cases must include actor, object, issue category, decision, owner, timestamp and attachments.
- Public disclosures must identify responsible regulated partners where applicable.
- Financial promotion, suitability and jurisdiction status must be visible before allocation actions.
- Manual review is acceptable in MVP1 when each step has owner, status, SLA and audit event.

11 AI requirements

The AI layer should be treated as an enterprise operating service. The client submits a business request; GlemO converts it into a structured internal prompt governed by policy, data permissions and human review. Raw prompts should not be exposed to clients as the product value.

Capability	MVP1 behavior	Control requirement
Concierge request intake	Capture customer, scenario, target assets, desired output and urgency	Validate account plan and data permission before processing
Prompt policy layer	Attach prompt chain version, allowed data sources and restricted terms	Version all prompt policies and retain audit evidence
Agent run	Generate market x ray, benchmark, scenario or distribution report	Flag unsupported claims and require human QA
Human QA	Approve, return for revision or reject report	Reviewer, notes and decision are retained
Delivery	Deliver approved output to customer workspace	Log delivery, report version and recipient permissions

12 Non functional requirements

Category	Requirement
Security	MFA for sensitive users, RBAC by actor, least privilege, encrypted data at rest and in transit, secure wallet connection, session expiry and

	admin impersonation controls.
Privacy	Public explorer uses sanitized events only. Personal data, investor identity, wallet identity and restricted documents stay private by role and jurisdiction.
Auditability	Every sensitive event must write an audit event: login, role change, asset submission, evidence update, validator opinion, admin release, transaction clearance, invoice, AI report delivery.
Compliance posture	The product is infrastructure. It should not claim to be issuer, custodian, exchange, broker dealer, investment adviser or market maker unless a regulated entity is explicitly responsible.
Reliability	Core dashboards and records should remain available during partner rail delays. External chain or payment failure must degrade into pending or exception states, not silent failure.
Internationalization	Core investor/data-room pages support EN, ES, FR and AR. Platform prototype supports EN, PT, ES, FR and AR. Production should use a translation key system with review workflow.
Observability	Operations needs logs, metrics, uptime, failed jobs, payment failures, KYC exceptions, wallet errors, chain event mismatch and AI report SLA dashboards.
Performance	Marketplace and dashboards should load quickly on mobile. Tables must support pagination/filtering before production data volume grows.
Data retention	Define retention by object type, jurisdiction and contract. Audit, transaction and compliance records require controlled retention and export.
Accessibility	Responsive layouts, readable contrast, keyboard navigation, semantic labels and screen-reader friendly state changes are required for production.

13 MVP delivery backlog

Phase	Objective	Primary deliverables
Sprint 0	Technical foundation	Repository, design system, auth skeleton, route map, database schema, environment strategy, CI/CD, staging deployment
Sprint 1	Public marketplace and asset sheet	Public marketplace, asset detail, channel disclosure, risk labels, responsive layout, static seed data
Sprint 2	Identity and buyer onboarding	Login, profiles, wallets, KYC/suitability placeholders, retail and institutional portals
Sprint 3	Seller admin and asset factory	Organization admin, signers, plan, asset draft, evidence upload, offering structure support
Sprint 4	Validator and admin gates	Validator desk, document review, publication status, admin dashboard and compliance cases
Sprint 5	Transaction layer	Private transaction records, standby clearance queue, public explorer and audit ledger
Sprint 6	Revenue and enterprise SaaS	Seller plans, enterprise checkout request, invoices, payment method state and billing dashboard
Sprint 7	AI concierge and reports	AI request workflow, prompt policy metadata, report delivery, management exports
Sprint 8	Rails and reconciliation	Ethereum/Base event placeholders, partner rail integration model, reconciliation

		statuses
Sprint 9	Hardening and readiness	Permissions, mobile QA, translation QA, audit export, security review, launch checklist

14 Acceptance criteria

ID	Acceptance criterion
A01	A visitor can inspect an approved asset public page without login and see risk labels, responsible entities and available official channels.
A02	A retail buyer can create account, connect wallet, complete KYC/suitability placeholders and see only eligible actions.
A03	An institutional buyer can maintain mandate profile, diligence files, committee workflow and allocation requests.
A04	A seller can submit organization profile, signers, plan, billing preference and asset draft.
A05	A seller can create either pooled offering or standalone asset without forcing pool structure.
A06	A validator can review evidence, flag issues, request documents and submit an opinion.
A07	Admin can approve, reject or hold publication and transaction events with reason and audit history.
A08	Private transaction details are visible only to allowed actors; public explorer shows sanitized event data.
A09	Enterprise SaaS request captures company, scope, billing cycle, card or crypto payment preference and approval status.
A10	Billing dashboard shows SaaS, setup, servicing, transaction fees, invoices and payment collection state.
A11	AI request lifecycle captures input scope, prompt policy version, agent run, human QA and delivered output.
A12	Rails dashboard records Ethereum/Base route, partner custody/payment status and reconciliation exceptions.
A13	Every sensitive mutation writes an immutable audit event and can be exported by admin.
A14	Mobile navigation supports forward/back movement across role environments without trapping users.
A15	The platform can produce a readiness report showing missing documents, open risks and owners before launch.

15 Open decisions before production build

ID	Decision	Why it matters
D01	Jurisdiction launch perimeter	Define where retail access is allowed, where qualified/institutional only is required and which disclosures differ by jurisdiction.
D02	Regulated partner allocation	Decide which partner handles custody, tokenization, payments, KYC/KYB and legal issuance for MVP1.
D03	Wallet custody model	Confirm whether MVP1 is non-custodial wallet connect only, partner custody only, or mixed.
D04	Transaction fee basis	Define exact basis points, minimum fee,

		who pays, refund logic and treatment of external transactions.
D05	Token role	Separate product utility, ecosystem incentives and governance from investor revenue model.
D06	AI data boundary	Define what client data can be used in AI agents, retention rules and human review obligations.
D07	Public transaction explorer granularity	Choose whether public volume is exact, banded, delayed or fully aggregated by asset class.
D08	Secondary liquidity policy	Confirm what MVP1 can say and do without implying exchange or market maker activity.

16 Suggested production architecture

The initial build can be delivered as a modular web application with clear service boundaries. A practical architecture is a TypeScript frontend, API layer, relational database, object storage for documents, queue for async review jobs, audit ledger table, external KYC/KYB provider, payment provider, wallet connection and partner rail adapters. The exact framework can be chosen by the delivery team, but the boundaries should remain stable.

- Frontend: responsive web app with route guards by role and language key system.
- Backend: API layer with modules for identity, marketplace, organizations, offerings, validation, compliance, transactions, billing, AI and rails.
- Database: PostgreSQL or equivalent relational store for regulated workflow traceability.
- Storage: encrypted document storage with file hash, versioning, owner and retention rules.
- Jobs: asynchronous workers for document parsing, notifications, AI report generation, reconciliation and exports.
- Observability: structured logs, event metrics, queue monitoring, failed integration alerts and admin health dashboard.
- Security: MFA, RBAC, scoped tokens, audit events, encrypted secrets and least privilege infrastructure access.

17 Implementation notes for developers

1. Start with the domain model and role matrix before building screens. The prototype has many screens; the production system must be driven by permissions and object status.
2. Build the Offering lifecycle as the central workflow: Draft, Evidence Pending, Validator Review, Admin Review, Published, Suspended, Closed.
3. Keep transaction lifecycle separate from offering lifecycle: Draft, Standby, Compliance Review, Approved, Payment Pending, Settlement Pending, Reconciled, Failed, Cancelled.
4. Treat all visible dashboard numbers as derived metrics from event and transaction tables. Avoid manually entered KPI values in production.
5. Create a translation workflow early. Investor pages and product screens have different language coverage today.
6. Use feature flags for phase two modules such as builder ecosystem, plugin marketplace and advanced rail automation.
7. Model manual review as first class product functionality. Manual does not mean undocumented; each manual action needs owner, status and audit trail.
8. Avoid making legal or investment advice claims in UI text. Use approved disclosure fields for investor facing copy.
9. Design mobile navigation with role based shortcuts and a persistent back to home route for each actor.
10. Before launch, run a complete scenario from seller creation to public transaction declaration and investor report export.

18 Definition of ready and definition of done

Stage	Required before work starts	Required before release
Feature	Actor, object, permission, status changes, acceptance criteria and dependencies are identified.	Tested route, audit events, empty/error/loading states, translation keys and mobile behavior are complete.
Integration	Provider owner, sandbox credentials, data mapping, failure states and compliance owner are known.	Successful happy path, failed path, retry path, log evidence and admin visibility are complete.
AI workflow	Allowed data scope, prompt version, output format, QA owner and delivery path are defined.	Prompt run, QA decision, report version, delivery log and customer visibility are complete.
Compliance control	Rule owner, decision states, required evidence and escalation path are documented.	Case history, attachments, decision reason, audit event and export are complete.
Investor facing screen	Approved copy, risk language, data source and visibility rules are confirmed.	Responsive layout, contrast, role gating, analytics event and QA review are complete.

19 Appendix current screen map

Code	Screen	Route id
01	Product Home	market
02	Journey Map	platformSitemap
DFD	DFD and Requirements	dataFlowRequirements
03	MVP1 Scope	mvp1Scope
04	Backoffice Map	roleConsole
05	Actor Dashboards	actorDashboards
06	Transaction Layer	transactionLayer
07	Asset Fact Sheet	assetFactSheet
08	Distribution SaaS	distributionSaas
09	Retail Login	retailPortal
10	Wallet and KYC	investorGate
11	Portfolio	investorPortfolio
12	Institutional Portal	institutionalPortal
13	Risk Education	investorEducation
14	Originator Ops	bankOps
15	Seller Admin	sellerOrgAdmin
16	Asset Factory	assetFactory
17	Seller Plans	sellerPlans
18	Distribution Partner	distributionPartner
19	Liquidity Desk	liquidityDesk
20	Replacement	replacementQueue
21	Validator Desk	validatorDesk
22	Document Review	documentReview
23	Executive Admin	adminDashboard
24	Access Control	accessControl
25	Compliance Cases	complianceCases
26	Clearance Queue	transactionClearance
27	Reports	reports
28	Billing and Revenue	billingRevenue

29	AI Ops	aiOps
30	Concierge Desk	conciergeDesk
31	Rails Partner	railPartner
32	Risk and Token	riskEngine
33	Ledger	ledger
34	Builder Portal	ecosystemBuilder
35	Readiness Register	operatingReadiness
36	Downloads	downloads