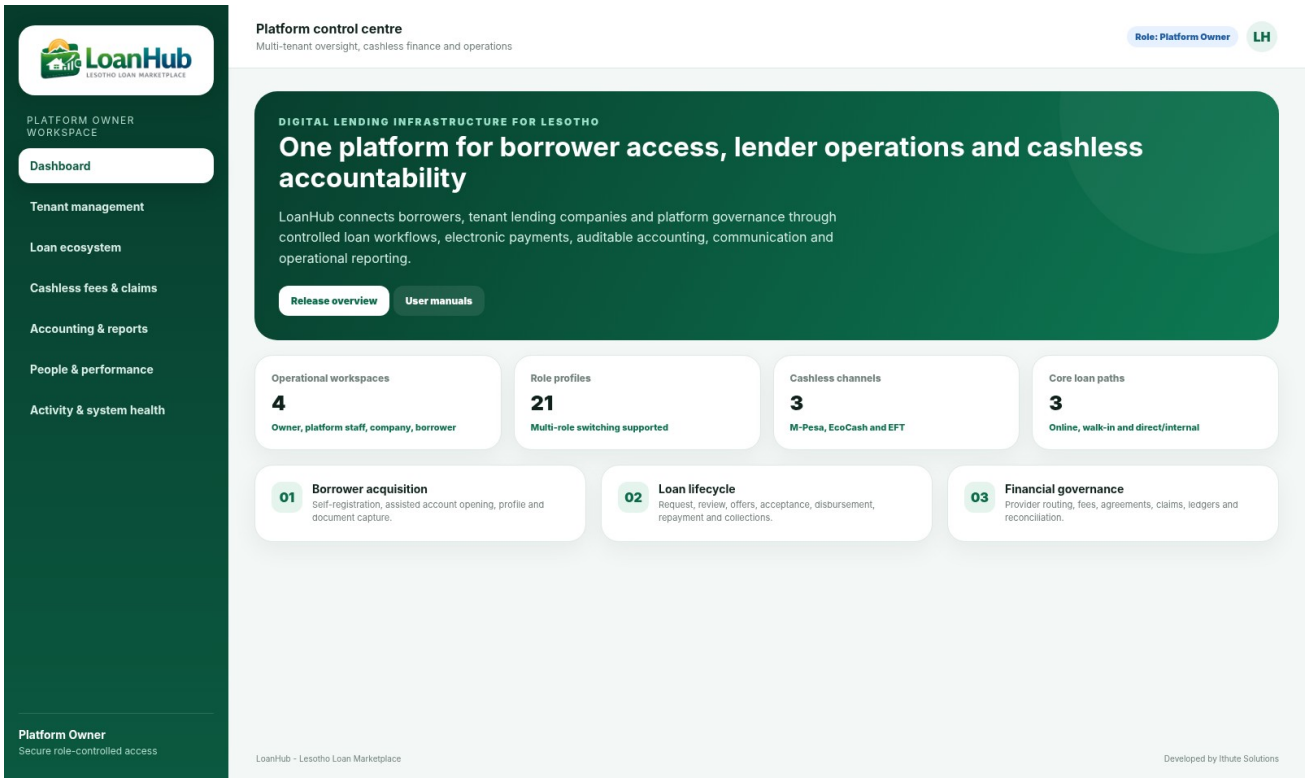
COMMERCIAL PRODUCT DESCRIPTION, RELEASE GUIDE AND COMPLETE USER MANUAL

A sales-ready explanation of what the system does, why it matters, how money moves, how every role works and how the release progresses from Alpha to controlled Beta and production.



Release Candidate 1.0 | Source analysis: frontend(5).zip and backend(4).zip | July 2026

Developed and maintained by Ithute Solutions

DOCUMENT IDENTITY

LoanHub is the product. Ithute Solutions is the developer.

This manual is designed for sales conversations, buyer due diligence, implementation, training, operations, finance, assurance and engineering handover.

Product identity

Always describe the solution as “LoanHub - Lesotho Loan Marketplace”. Ithute Solutions is the software developer and implementation partner.

Release basis

Content is grounded in the current analysed frontend and backend archives. Interface images use LoanHub system branding; provider logos appear only where the applicable provider is being discussed.

Release honesty

The codebase is an engineered release candidate. Live financial operation still requires provider credentials, product approval, external UAT, contracts, compliance review and production sign-off.

> **Use of screenshots** Screens contain neutral labels or placeholders and are intended to explain functionality. They are not evidence of live customer balances or production provider certification.

HOW TO USE THIS MANUAL

One document for selling, implementing and operating LoanHub

Use the first parts for executive and commercial presentations, the middle parts for role training and process execution, and the final parts for engineering, release and assurance.

For sales and investors Start with the product story, buyer value, revenue model, screenshots and demonstration storyline.	**For lending companies** Use the module guide, cash-flow chapters, company role manuals and process instructions.
For borrowers and trainers Use the borrower role manual and online-request, offer, payment and support processes.	**For engineers and auditors** Use architecture, security, API/data inventories, release gates and verification checklists.

Navigation The Word file uses heading styles for the Navigation Pane. The PDF can be searched by chapter title, role or module name.

CONTENTS

Document map

The full manual is intentionally detailed. Each part can also be used as a standalone training or proposal reference.

Item	Description
Part I	Commercial product story and buyer value
Part II	Feature catalogue and module user manual
Part III	Role-by-role operating manual
Part IV	End-to-end process and cash-flow manual
Part V	Engineering, security and operational architecture
Part VI	Alpha-to-Beta release, implementation and sales use
Part VII	Appendices: inventories, glossary and checklists

Recommended sales path Present Part I, selected screenshots from Part II, the cash-flow pages in Part IV and the release roadmap in Part VI. Provide the full document for due diligence.

CONTENTS

Detailed chapter map - commercial and functionality

A structured path through the product, its importance and complete feature set.

- 1. What LoanHub does: LoanHub is a multi-tenant lending marketplace and full loan-management platform. It enables borrowers to apply online, allows lending companies to serve walk-in and existing clients, manages offers and loan accounts, routes money electronically and retains operational evidence.
- 2. The problem it solves: Many lenders rely on paper applications, unstructured spreadsheets, personal messaging, cash handover and isolated branch records. Borrowers repeat the same information and struggle to compare offers. Platform owners cannot easily prove how fees and transactions were calculated.
- 3. Why cashless lending matters: Cash creates opportunities for theft, substitution, delayed posting, false receipts and staff-borrower disputes. Electronic instructions still require verification and reconciliation, but they create references and evidence that cash cannot provide.
- 4. Who buys and uses it: The commercial buyer may be a lending marketplace operator, lending network, microfinance organization, employer-based lender, branch-based lender or technology partner. Daily users include platform staff, tenant owners, branch teams, finance, collections and borrowers.
- 5. Value to the platform owner: The owner can onboard tenants, configure owner payment methods, set borrower service fees, agree transaction charges, issue claims, create platform employees and supervise system health.
- 6. Value to lending companies: A tenant gets client acquisition, online and walk-in lending, loan products, staff roles, branches, electronic payouts and collections, reports, communication and evidence.
- 7. Value to borrowers: A borrower gets one profile, online requests, offer comparison, a private record of loans and payments, service-fee transparency, documents, messages and support.
- 8. Online, walk-in and internal lending: LoanHub supports three acquisition paths: borrower-created marketplace requests; loan-officer-assisted walk-in applications; and internal applications for selected existing clients.
- 9. Commercial revenue model: The owner may configure borrower request fees, assisted account-opening charges, subscriptions and transaction-charge agreements. Each source must be disclosed, configured and settled electronically.
- 10. 0.005% example: When an agreement is configured at 0.005%, the calculation is gross amount × 0.005 ÷ 100. On LSL 10,000, the charge is LSL 0.50.
- 11. Trust through transparency: Authorized owner and company users can review agreement terms, charge-ledger rows, claims, payment references and status.
- 12. Operational control: Branches, role memberships, active role selection, maker-checker, support cases, activity logs and system errors make accountability part of daily work.
- 13. Market differentiation: LoanHub combines marketplace lending, tenant loan management, cashless routing, commercial fee governance, direct lending, embedded communication and platform employee roles.
- 14. Implementation approach: A buyer moves from discovery to configuration, data preparation, sandbox integration, UAT, training, pilot, reconciliation and controlled production.
- 15. What is engineered now: The analysed release contains 66 frontend page routes, 222 backend API routes, 61 mapped database tables and 21 defined roles. Core marketplace, tenant, borrower, cashless, reporting and operational modules are represented in source.
- 16. What remains external: Live M-Pesa, EcoCash and bank operation requires valid merchant accounts, provider-issued credentials, product approval, callback/network configuration and external UAT. Legal, accounting and data-protection reviews remain deployment responsibilities.
- 17. Buyer outcomes: The intended outcomes are shorter and more consistent application processing, less cash handling, better branch visibility, transparent platform charges, stronger evidence and more structured borrower service.

- 18. Buyer due diligence: Prospective customers should evaluate product fit, security controls, provider coverage, integration responsibilities, data governance, support, migration, recovery and total implementation effort.
- 19. Demonstration storyline: A strong demonstration follows one borrower from registration to request fee, lender offer, acceptance, electronic disbursement, repayment, charge-ledger entry and report. It then shows an internal walk-in case and a support/audit trace.
- 20. Commercial proposal positioning: Position LoanHub as digital lending infrastructure and managed operational transformation. The proposal should distinguish platform licensing/services, provider costs, tenant commercial charges and implementation work.
- 21. Importance to Lesotho: A locally positioned loan marketplace can improve access, digitize lender operations and support electronic financial accountability. Local payment and regulatory realities must guide activation.
- 22. Product promise: LoanHub aims to make lending accessible, operationally controlled, electronically traceable and commercially transparent for borrowers, companies and the platform owner.

CONTENTS

Detailed chapter map - modules and roles

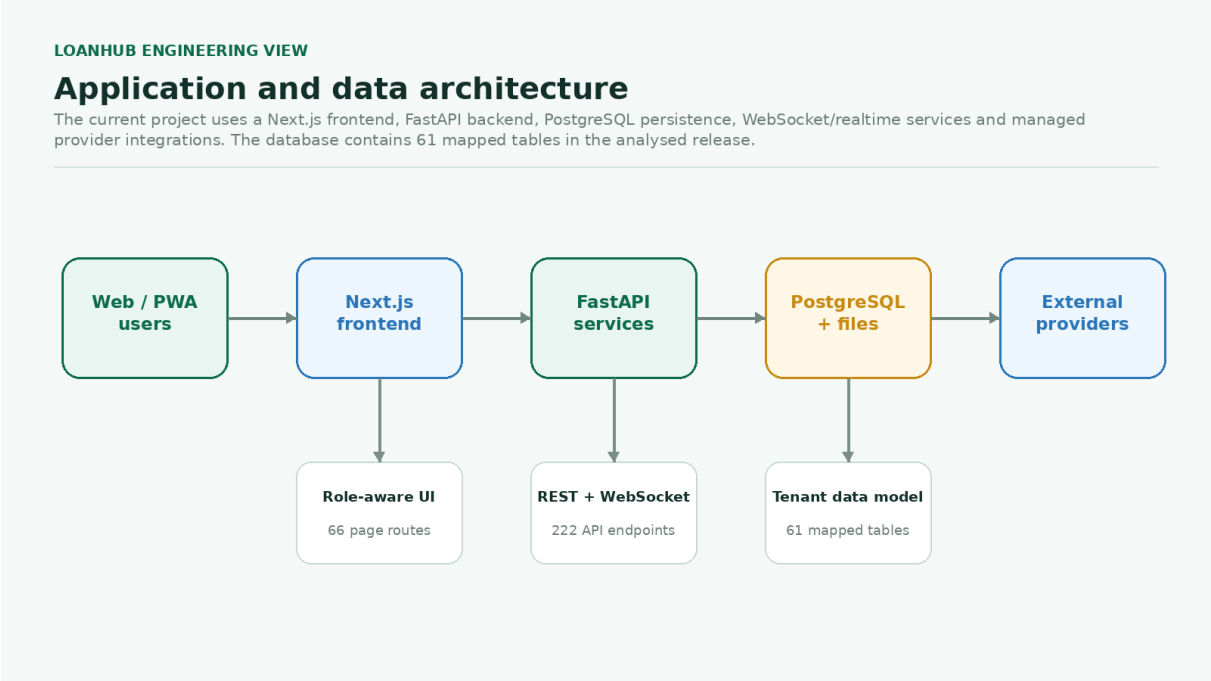
Module chapters explain purpose, value, workflow, configuration, permissions, records and controls. Role chapters explain daily work, restrictions, reports and escalation.

- 28 module chapters, each with a product page and an operating page.
- 21 role manuals covering platform owner, platform staff, tenant roles and borrower.
- 14 end-to-end process chapters covering lending, cashless money movement, charges and corrections.
- 30 engineering and operational chapters.
- Release, sales, implementation and appendix sections.

RELEASE SNAPSHOT

Current analysed source footprint

Counts are derived from the current frontend(5).zip and backend(4).zip supplied for this documentation.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

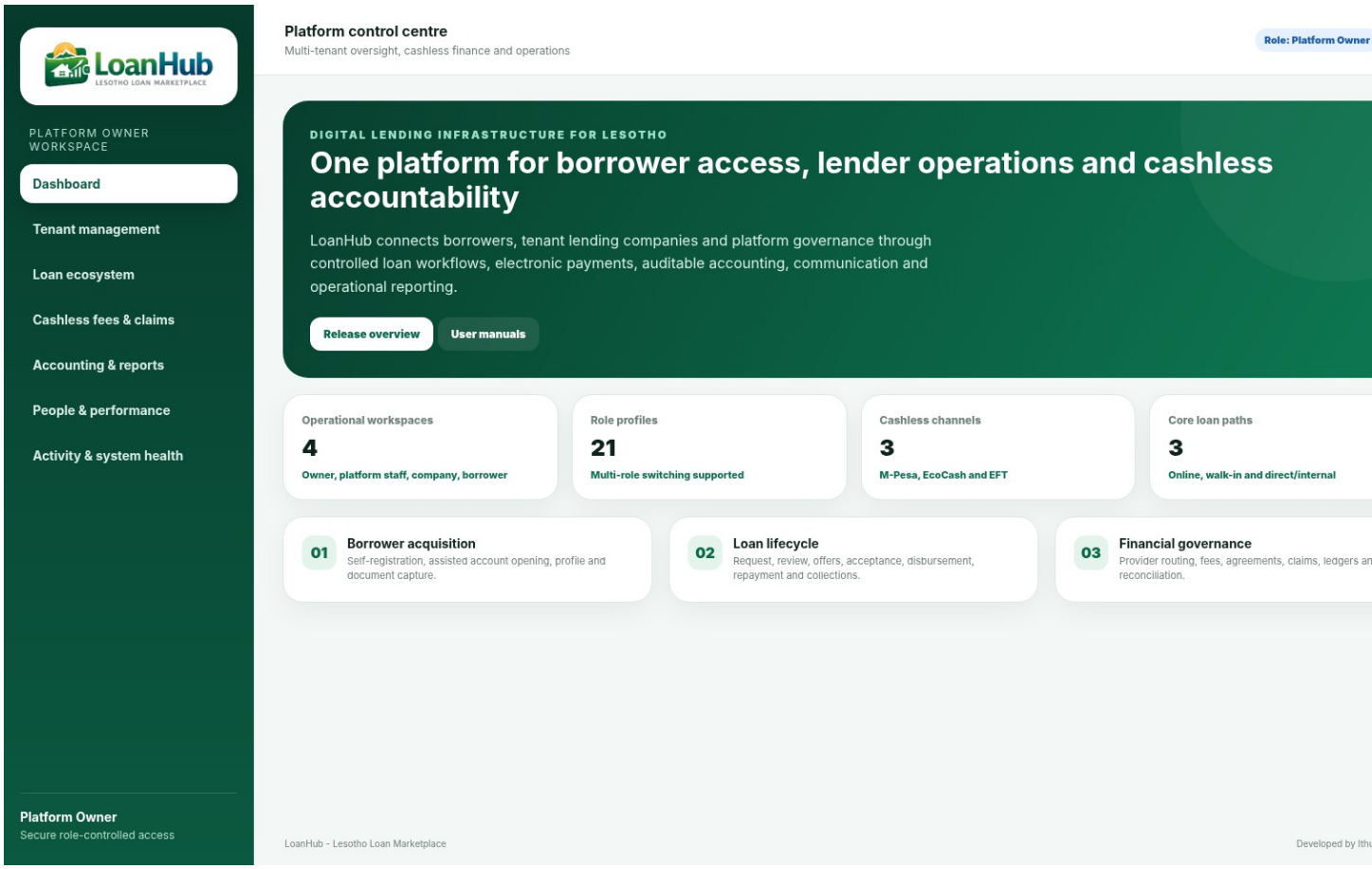
Item	Description
Frontend page routes	66
Backend API route decorators	222
Mapped SQLAlchemy tables	61
Defined user roles	21

Interpretation These figures show engineering breadth. They do not replace functional UAT, security review or provider certification.

PART I

Commercial product story

What LoanHub does, the problems it solves, why it matters and how it creates value for buyers, lenders, borrowers and the platform owner.

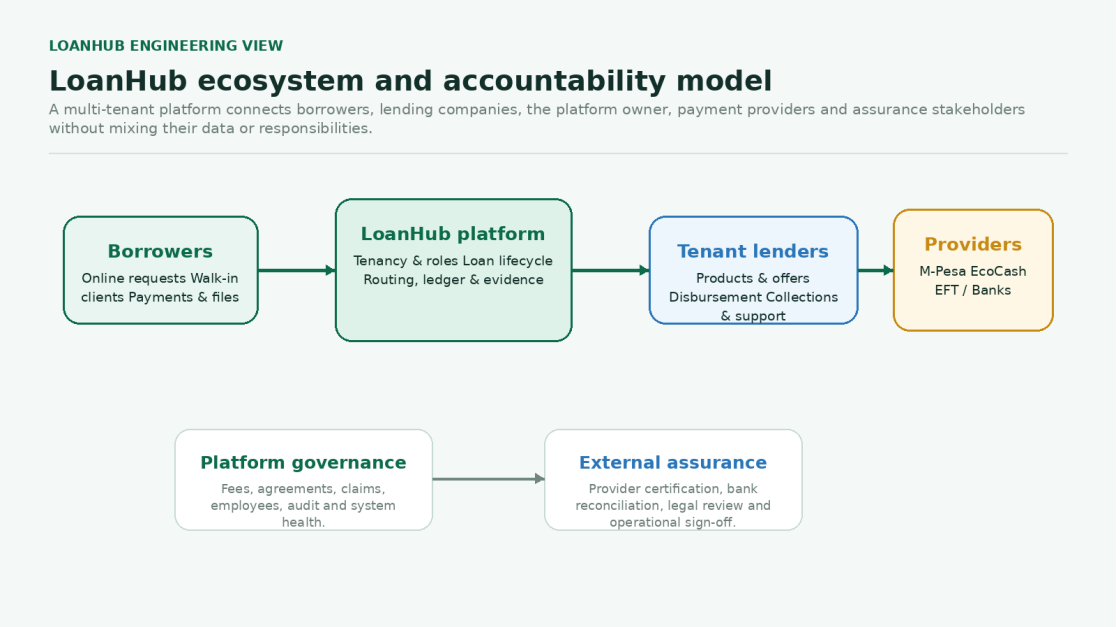


Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

PART I · COMMERCIAL PRODUCT STORY

What LoanHub does

LoanHub is a multi-tenant lending marketplace and full loan-management platform. It enables borrowers to apply online, allows lending companies to serve walk-in and existing clients, manages offers and loan accounts, routes money electronically and retains operational evidence.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why this matters

It is not merely a loan calculator, payment page or customer list. It is a connected operating system for digital lending.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how what loanhub does becomes a governed record inside LoanHub.

Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

The problem it solves

Many lenders rely on paper applications, unstructured spreadsheets, personal messaging, cash handover and isolated branch records. Borrowers repeat the same information and struggle to compare offers. Platform owners cannot easily prove how fees and transactions were calculated.

Why this matters

LoanHub replaces fragmentation with a governed workflow and shared source of truth.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how the problem it solves becomes a governed record inside LoanHub.

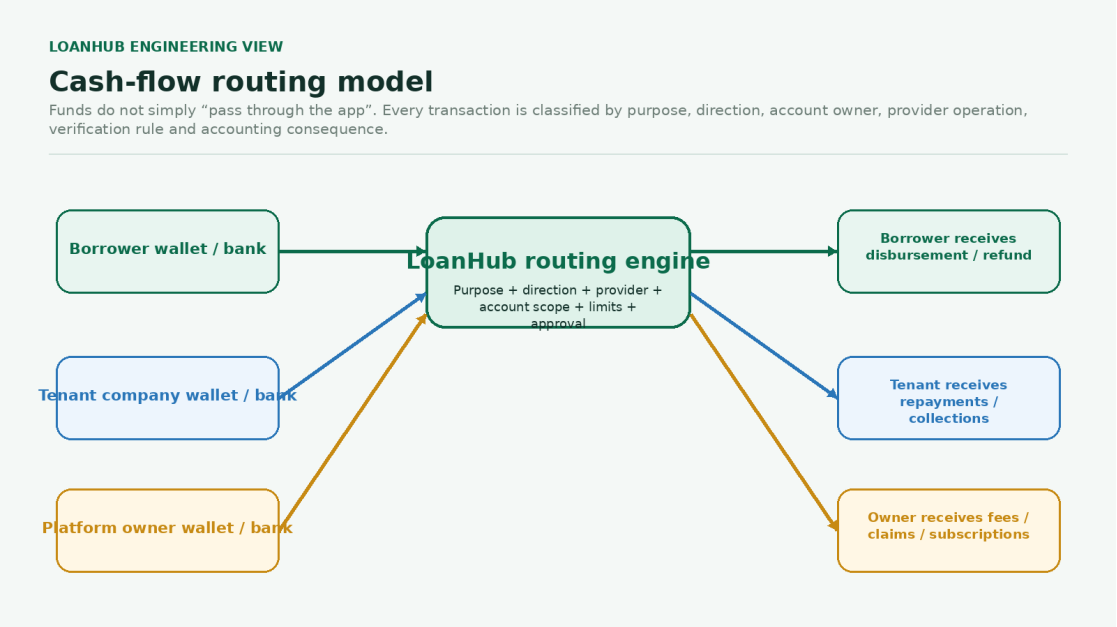
Business value Creates a consistent, explainable operating model that can be demonstrated to management and users.	**Control value** Makes responsibilities, status and evidence visible to authorized people.
Commercial value Supports a service that can be configured, trained, supported and improved over time.	**Buyer question** What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Why cashless lending matters

Cash creates opportunities for theft, substitution, delayed posting, false receipts and staff-borrower disputes. Electronic instructions still require verification and reconciliation, but they create references and evidence that cash cannot provide.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why this matters

LoanHub is designed to reduce cash-in-hand exposure, not to pretend digital payments eliminate all fraud.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how why cashless lending matters becomes a governed record inside LoanHub.

Business value Creates a consistent, explainable operating model that can be demonstrated to management and users.	**Control value** Makes responsibilities, status and evidence visible to authorized people.
Commercial value Supports a service that can be configured, trained, supported and improved over time.	**Buyer question** What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Who buys and uses it

The commercial buyer may be a lending marketplace operator, lending network, microfinance organization, employer-based lender, branch-based lender or technology partner. Daily users include platform staff, tenant owners, branch teams, finance, collections and borrowers.

Why this matters

The value is strongest where multiple companies or branches need common controls without sharing tenant data.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how who buys and uses it becomes a governed record inside LoanHub.

Business value Creates a consistent, explainable operating model that can be demonstrated to management and users.	**Control value** Makes responsibilities, status and evidence visible to authorized people.
Commercial value Supports a service that can be configured, trained, supported and improved over time.	**Buyer question** What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Value to the platform owner

The owner can onboard tenants, configure owner payment methods, set borrower service fees, agree transaction charges, issue claims, create platform employees and supervise system health.

Why this matters

This turns the platform into a governed commercial service rather than an unmanaged website.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how value to the platform owner becomes a governed record inside LoanHub.

Business value Creates a consistent, explainable operating model that can be demonstrated to management and users.	**Control value** Makes responsibilities, status and evidence visible to authorized people.
Commercial value Supports a service that can be configured, trained, supported and improved over time.	**Buyer question** What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Value to lending companies

A tenant gets client acquisition, online and walk-in lending, loan products, staff roles, branches, electronic payouts and collections, reports, communication and evidence.

Why this matters

The company retains its own payment accounts and internal responsibilities.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how value to lending companies becomes a governed record inside LoanHub.

Business value Creates a consistent, explainable operating model that can be demonstrated to management and users.	**Control value** Makes responsibilities, status and evidence visible to authorized people.
Commercial value Supports a service that can be configured, trained, supported and improved over time.	**Buyer question** What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Value to borrowers

A borrower gets one profile, online requests, offer comparison, a private record of loans and payments, service-fee transparency, documents, messages and support.

Why this matters

The borrower chooses an offer and can verify references rather than relying only on verbal promises.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how value to borrowers becomes a governed record inside LoanHub.

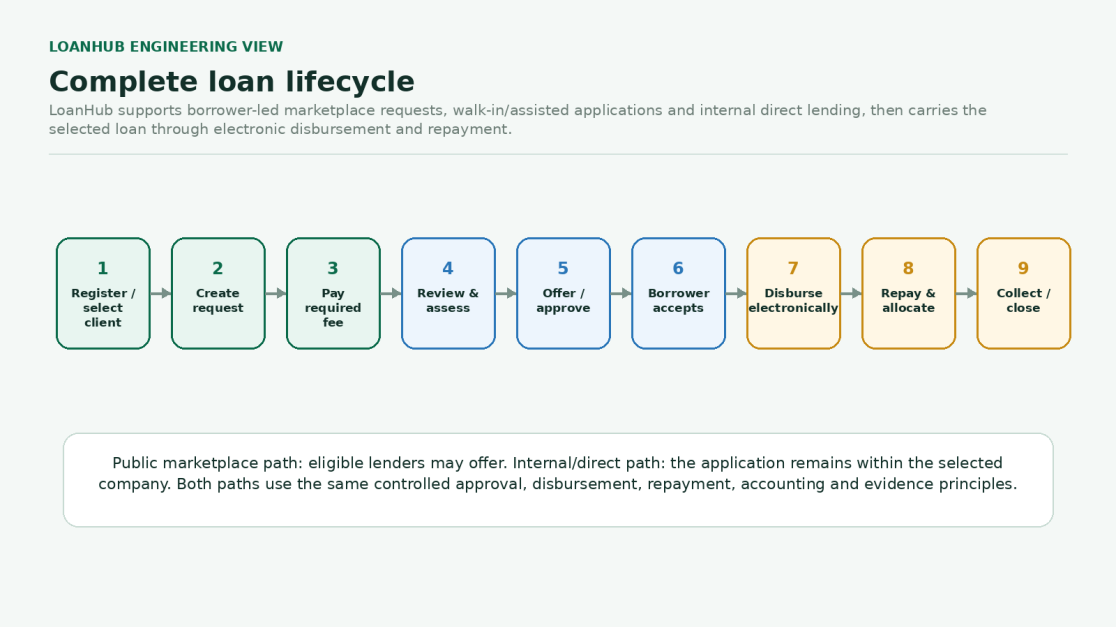
Business value Creates a consistent, explainable operating model that can be demonstrated to management and users.	**Control value** Makes responsibilities, status and evidence visible to authorized people.
Commercial value Supports a service that can be configured, trained, supported and improved over time.	**Buyer question** What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Online, walk-in and internal lending

LoanHub supports three acquisition paths: borrower-created marketplace requests; loan-officer-assisted walk-in applications; and internal applications for selected existing clients.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why this matters

This means digital transformation does not exclude customers who arrive at a branch or need assistance.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how online, walk-in and internal lending becomes a governed record inside LoanHub.

Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Commercial revenue model

The owner may configure borrower request fees, assisted account-opening charges, subscriptions and transaction-charge agreements. Each source must be disclosed, configured and settled electronically.

Why this matters

The model supports platform sustainability while keeping charges visible and auditable.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how commercial revenue model becomes a governed record inside LoanHub.

Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

0.005% example

When an agreement is configured at 0.005%, the calculation is gross amount × 0.005 ÷ 100. On LSL 10,000, the charge is LSL 0.50.

Why this matters

The interface and documentation must not confuse a percentage with the decimal multiplier 0.005.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how 0.005% example becomes a governed record inside LoanHub.

Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Trust through transparency

Authorized owner and company users can review agreement terms, charge-ledger rows, claims, payment references and status.

Why this matters

Trust comes from shared evidence and defined dispute paths, not from hiding calculations.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how trust through transparency becomes a governed record inside LoanHub.

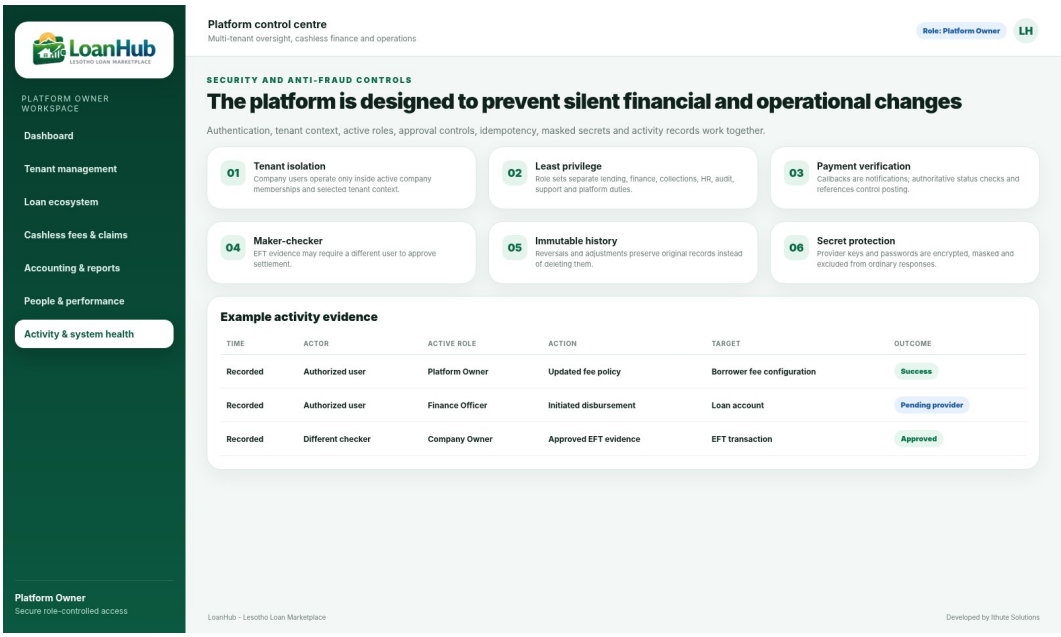
Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Operational control

Branches, role memberships, active role selection, maker-checker, support cases, activity logs and system errors make accountability part of daily work.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why this matters

A complete lending system must manage people and exceptions, not only the happy-path loan.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how operational control becomes a governed record inside LoanHub.

Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Market differentiation

LoanHub combines marketplace lending, tenant loan management, cashless routing, commercial fee governance, direct lending, embedded communication and platform employee roles.

Why this matters

The combination is more valuable than each feature in isolation because records remain connected.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how market differentiation becomes a governed record inside LoanHub.

Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Implementation approach

A buyer moves from discovery to configuration, data preparation, sandbox integration, UAT, training, pilot, reconciliation and controlled production.

Why this matters

The implementation method is part of the product because financial software must be adopted safely.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how implementation approach becomes a governed record inside LoanHub.

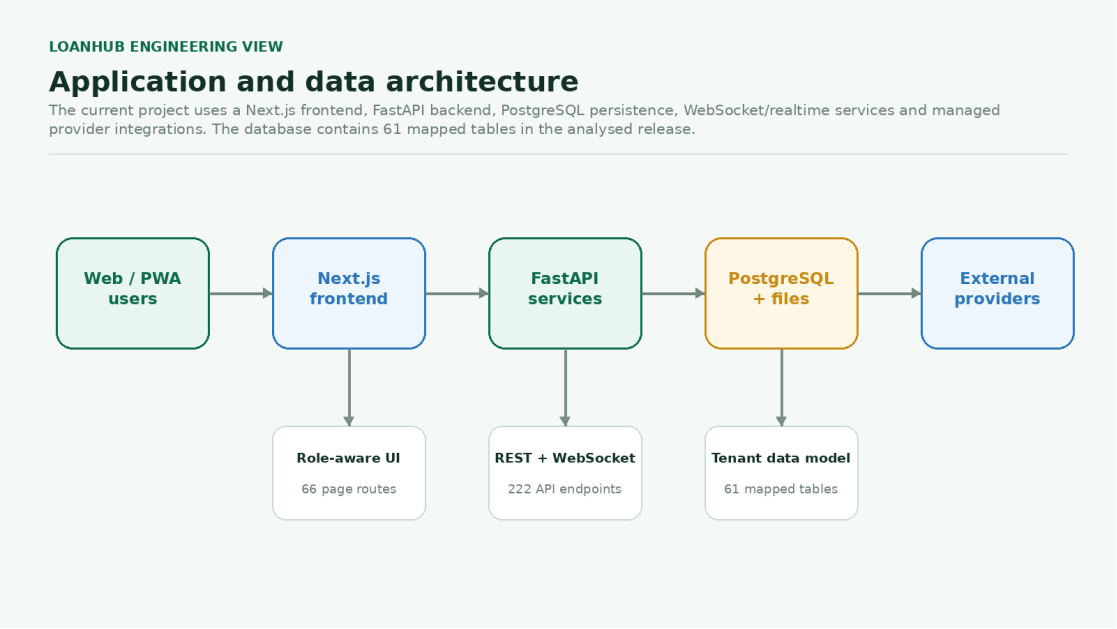
Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

What is engineered now

The analysed release contains 66 frontend page routes, 222 backend API routes, 61 mapped database tables and 21 defined roles. Core marketplace, tenant, borrower, cashless, reporting and operational modules are represented in source.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why this matters

These counts describe the analysed codebase, not provider certification or production usage.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how what is engineered now becomes a governed record inside LoanHub.

Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

What remains external

Live M-Pesa, EcoCash and bank operation requires valid merchant accounts, provider-issued credentials, product approval, callback/network configuration and external UAT. Legal, accounting and data-protection reviews remain deployment responsibilities.

Why this matters

The sales process should be honest about this boundary.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how what remains external becomes a governed record inside LoanHub.

Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Buyer outcomes

The intended outcomes are shorter and more consistent application processing, less cash handling, better branch visibility, transparent platform charges, stronger evidence and more structured borrower service.

Why this matters

Outcome measurement should be agreed during implementation rather than invented in the brochure.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how buyer outcomes becomes a governed record inside LoanHub.

Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Buyer due diligence

Prospective customers should evaluate product fit, security controls, provider coverage, integration responsibilities, data governance, support, migration, recovery and total implementation effort.

Why this matters

The manual is designed to answer those questions clearly.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how buyer due diligence becomes a governed record inside LoanHub.

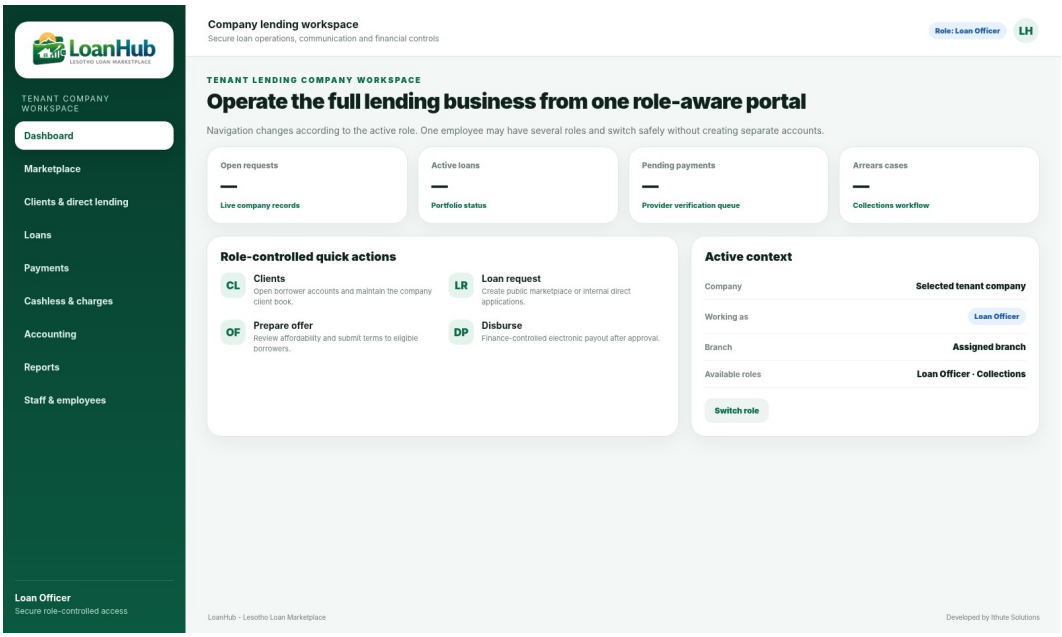
Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Demonstration storyline

A strong demonstration follows one borrower from registration to request fee, lender offer, acceptance, electronic disbursement, repayment, charge-ledger entry and report. It then shows an internal walk-in case and a support/audit trace.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why this matters

This tells a business story rather than clicking unrelated menus.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how demonstration storyline becomes a governed record inside LoanHub.

Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Commercial proposal positioning

Position LoanHub as digital lending infrastructure and managed operational transformation. The proposal should distinguish platform licensing/services, provider costs, tenant commercial charges and implementation work.

Why this matters

Do not present external provider fees as LoanHub revenue.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how commercial proposal positioning becomes a governed record inside LoanHub.

Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Importance to Lesotho

A locally positioned loan marketplace can improve access, digitize lender operations and support electronic financial accountability. Local payment and regulatory realities must guide activation.

Why this matters

The product name and interface identify LoanHub as the Lesotho Loan Marketplace.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how importance to lesotho becomes a governed record inside LoanHub.

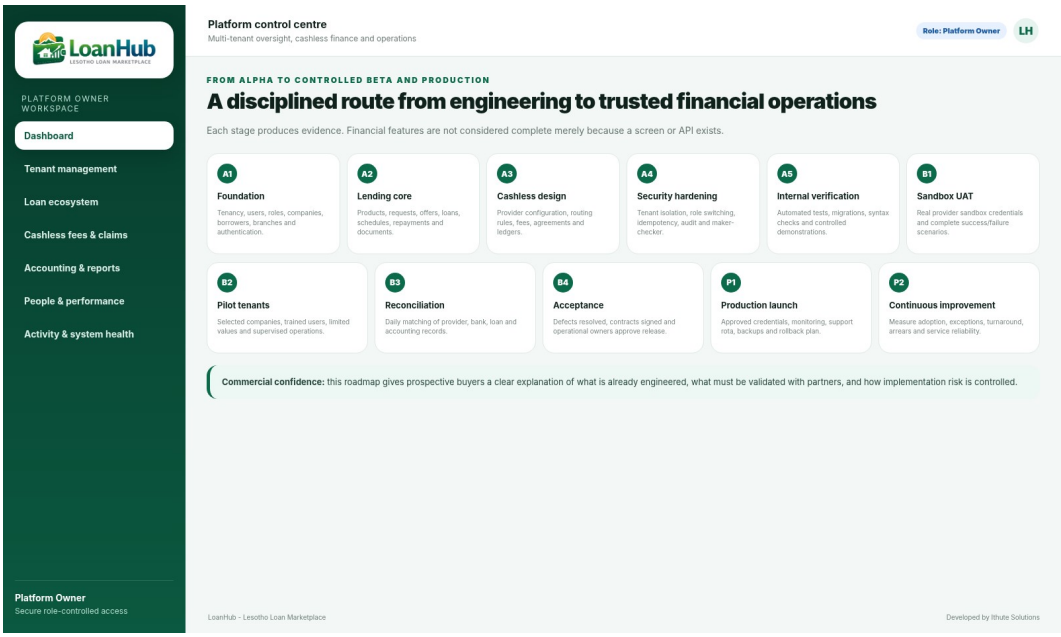
Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART I · COMMERCIAL PRODUCT STORY

Product promise

LoanHub aims to make lending accessible, operationally controlled, electronically traceable and commercially transparent for borrowers, companies and the platform owner.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why this matters

Every release decision should be tested against that promise.

How to sell this point

Connect this capability to the buyer's current process. Ask where information, approvals, money references and customer communication are currently lost. Then show how product promise becomes a governed record inside LoanHub.

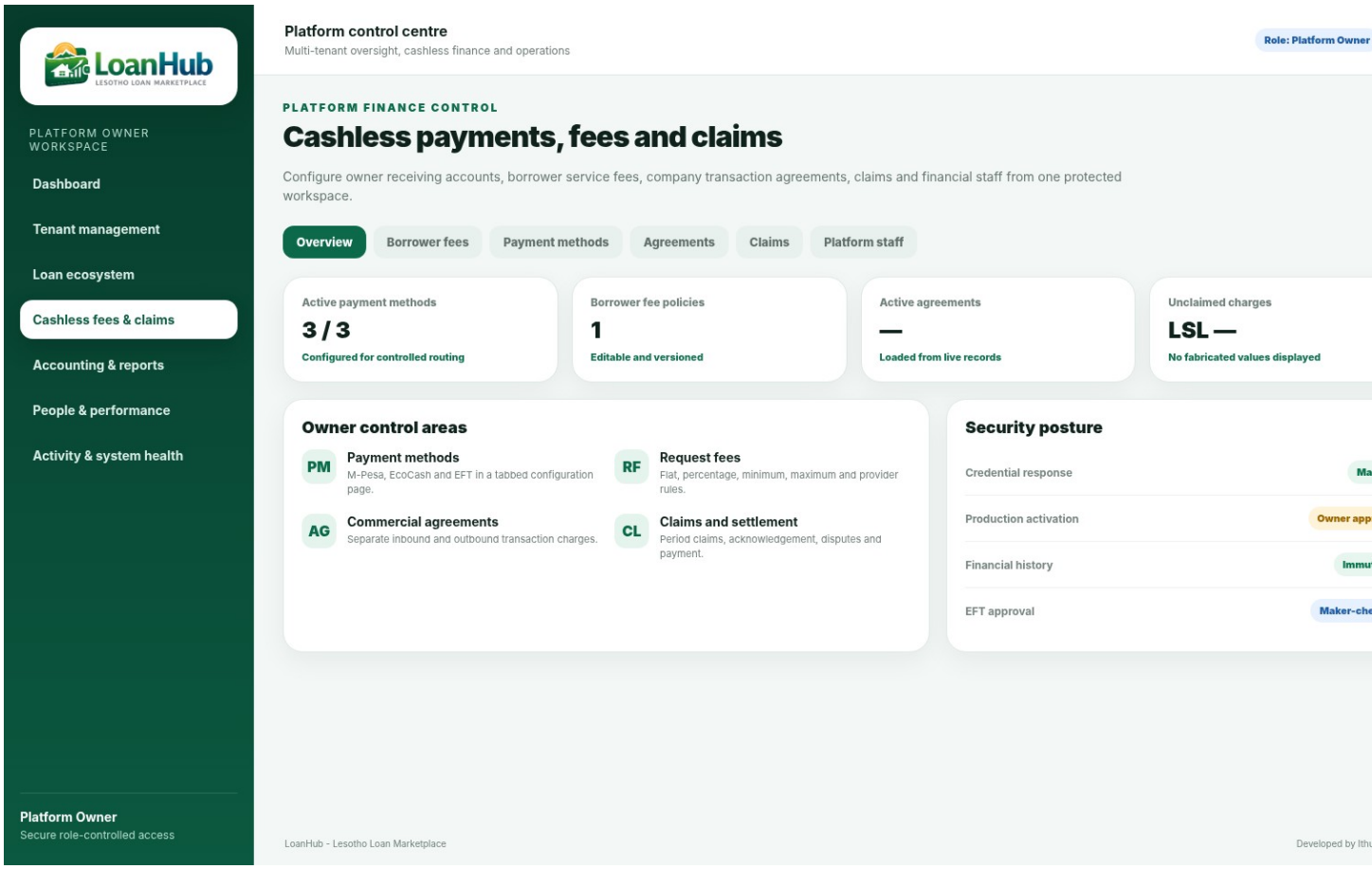
Business value	Control value
Creates a consistent, explainable operating model that can be demonstrated to management and users.	Makes responsibilities, status and evidence visible to authorized people.
Commercial value	**Buyer question**
Supports a service that can be configured, trained, supported and improved over time.	What operational cost, risk or customer frustration will this capability replace?

Sales discipline Do not promise measured savings or provider coverage until the buyer's baseline and external approvals have been confirmed.

PART II

Feature catalogue and module user manual

Every major module is explained from both the product/value perspective and the operating/user perspective.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

PART II · MODULE 01

Public landing and account choice

Introduces LoanHub, separates borrower and company registration paths, and directs existing users to secure authentication.

Why the module is important

Prospects understand the product before entering regulated workflows.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Clear product identity and Ithute Solutions developer branding
- Account-type selection
- Responsive visitor pages
- No operational data exposed publicly

How to use: Public landing and account choice

This page is the operational checklist for users and trainers working with public landing and account choice.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for public landing and account choice, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant public landing and account choice record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 02

Authentication and password recovery

Provides login, token refresh, session control, active-account enforcement and password-recovery entry points.

Why the module is important

A controlled identity layer protects every borrower, tenant and platform workspace.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Authenticated API access
- Inactive-account rejection
- Refresh-token lifecycle
- Role-aware post-login routing

How to use: Authentication and password recovery

This page is the operational checklist for users and trainers working with authentication and password recovery.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for authentication and password recovery, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant authentication and password recovery record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 03

Company registration and onboarding

Captures company identity, operations and owner information, then creates a pending tenant request for platform review.

Why the module is important

A consistent onboarding record replaces informal tenant creation and supports due diligence.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Multi-step registration
- Validation and review step
- Pending/approved/rejected/suspended status
- Company owner account creation

How to use: Company registration and onboarding

This page is the operational checklist for users and trainers working with company registration and onboarding.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for company registration and onboarding, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant company registration and onboarding record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 04

Borrower registration and profile

Supports self-registration plus personal, contact, identity, address and employment information.

Why the module is important

Lenders receive structured borrower data and borrowers maintain one reusable profile.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Borrower account
- Person profile
- Employment and address
- Identity references and documents

How to use: Borrower registration and profile

This page is the operational checklist for users and trainers working with borrower registration and profile.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for borrower registration and profile, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant borrower registration and profile record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 05

Tenant approval and subscription

Lets platform users review companies and control access according to company status and subscription.

Why the module is important

Commercial and operational access can be gated without deleting tenant history.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Company status gate
- Subscription plans
- Billing records
- Workspace availability

How to use: Tenant approval and subscription

This page is the operational checklist for users and trainers working with tenant approval and subscription.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for tenant approval and subscription, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant tenant approval and subscription record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 06

Branch management

Creates company branches and links operational users, loans and reporting to branch context.

Why the module is important

Multi-branch lenders gain centralized oversight with local accountability.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Branch creation and status
- Branch assignment
- Branch analytics
- Branch-scoped operations

How to use: Branch management

This page is the operational checklist for users and trainers working with branch management.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for branch management, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant branch management record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 07

Company staff and role memberships

Creates company memberships, assigns roles, branches, primary status and active/inactive access.

Why the module is important

One person can support several duties while authorization remains explicit.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Multiple memberships per user
- Primary role
- Branch assignment
- Disable without deleting history

PART II · MODULE 07 OPERATIONS

How to use: Company staff and role memberships

This page is the operational checklist for users and trainers working with company staff and role memberships.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for company staff and role memberships, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant company staff and role memberships record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 08

Platform employee management

Allows the platform owner to create support, finance, administration, audit, operations and compliance employees.

Why the module is important

The owner can delegate work without sharing the superadmin account.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Platform staff profile
- Role-specific workspace
- Activation/deactivation
- Department and job title

How to use: Platform employee management

This page is the operational checklist for users and trainers working with platform employee management.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for platform employee management, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

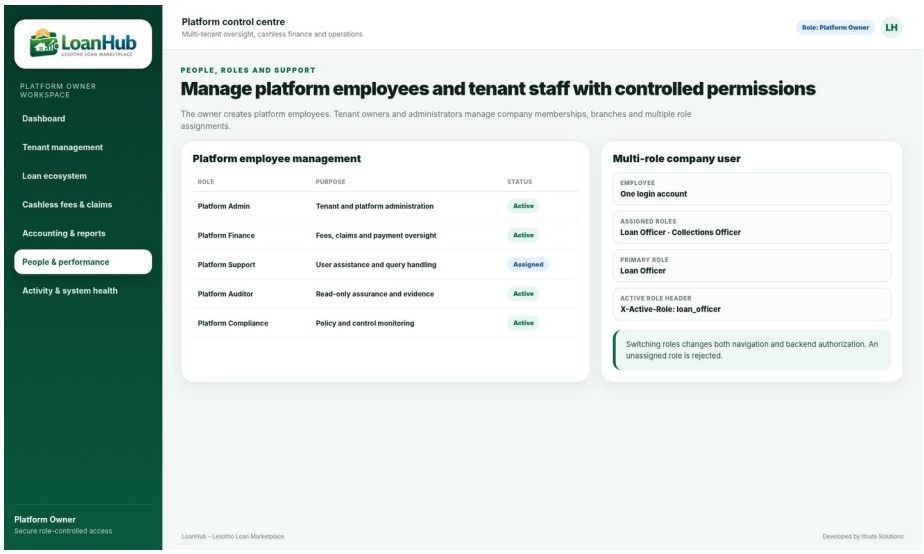
- Open the authorized workspace and confirm the active company and role.
- Select the relevant platform employee management record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 09

Active role and company switching

Lets multi-role or multi-company users select the context in which they are working.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

The same login remains usable without merging permissions or creating duplicate accounts.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- X-Company-ID context
- X-Active-Role context
- Role-aware navigation
- Server-side membership validation

How to use: Active role and company switching

This page is the operational checklist for users and trainers working with active role and company switching.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for active role and company switching, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

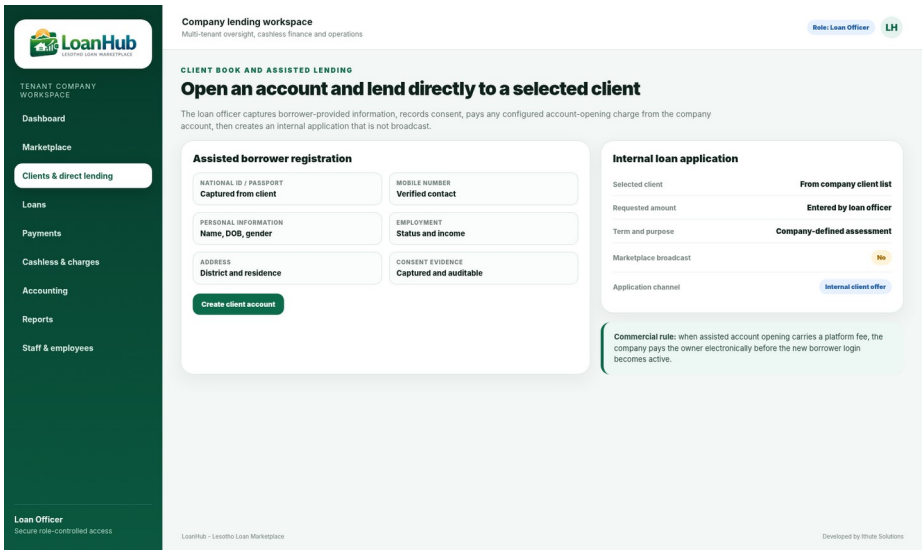
- Open the authorized workspace and confirm the active company and role.
- Select the relevant active role and company switching record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 10

Client book and assisted account opening

Allows authorized company staff to register a borrower using information and consent supplied by the client.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

Walk-in borrowers are included without forcing them to self-register before receiving service.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Client search
- Assisted capture
- Consent evidence
- Optional company-paid opening fee

How to use: Client book and assisted account opening

This page is the operational checklist for users and trainers working with client book and assisted account opening.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for client book and assisted account opening, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant client book and assisted account opening record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 11

Loan product configuration

Defines lender-specific terms and rules used to construct offers and direct loans.

Why the module is important

Companies can standardize pricing and terms across branches and officers.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Product names and limits
- Term and pricing rules
- Activation status
- Offer preparation support

How to use: Loan product configuration

This page is the operational checklist for users and trainers working with loan product configuration.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for loan product configuration, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

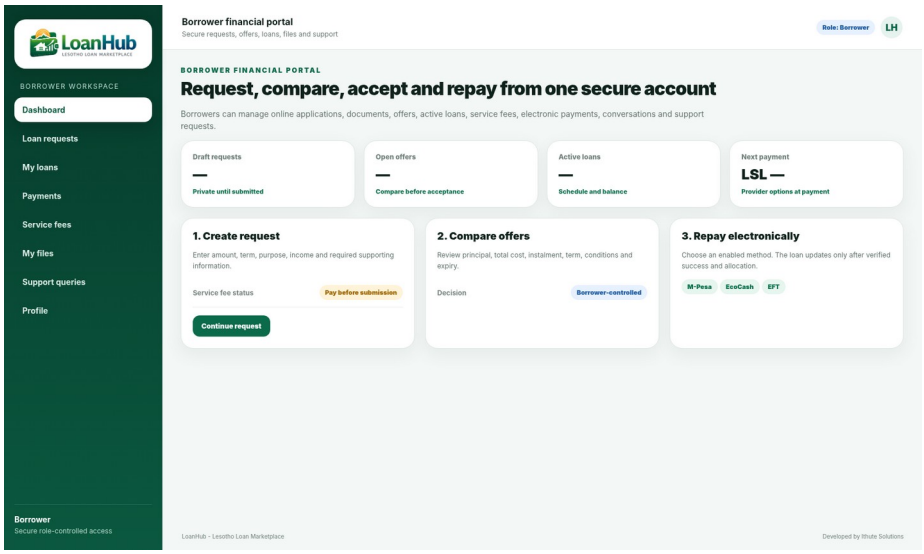
- Open the authorized workspace and confirm the active company and role.
- Select the relevant loan product configuration record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 12

Online loan requests

Enables a borrower to create, save, pay any required service fee and submit a request to the marketplace.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

Borrowers reach several eligible lenders without repeated paper applications.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Private draft
- Fee quote and payment gate
- Submission/open status
- Documents and purpose

How to use: Online loan requests

This page is the operational checklist for users and trainers working with online loan requests.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for online loan requests, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

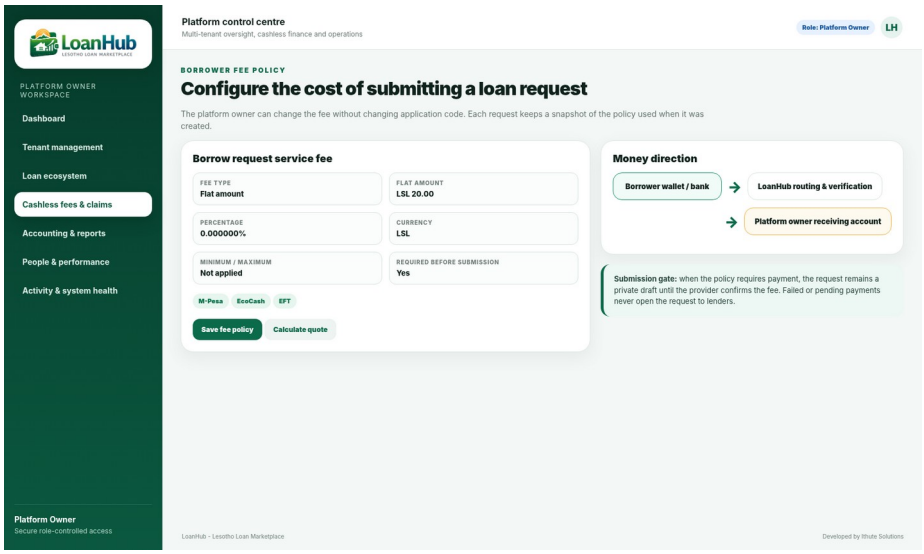
- Open the authorized workspace and confirm the active company and role.
- Select the relevant online loan requests record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 13

Borrower service-fee policy

Lets the platform owner configure flat, percentage or combined fees with limits, provider choices and effective periods.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

Commercial changes are made through configuration rather than code.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Flat and percentage fee
- Minimum/maximum
- Required-before-submission
- Policy snapshot

How to use: Borrower service-fee policy

This page is the operational checklist for users and trainers working with borrower service-fee policy.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for borrower service-fee policy, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

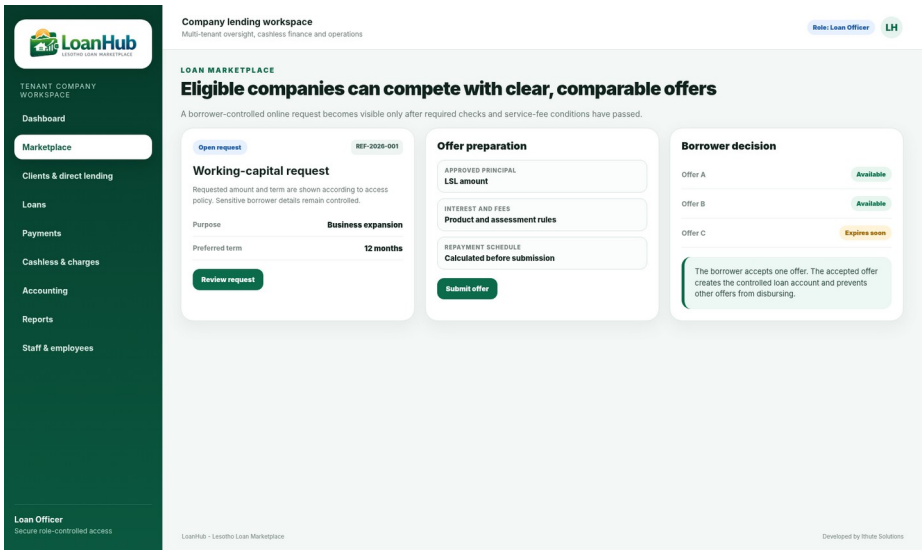
- Open the authorized workspace and confirm the active company and role.
- Select the relevant borrower service-fee policy record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 14

Marketplace access and request visibility

Controls which lenders can see open requests and which borrower data is revealed.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

Competition is enabled while sensitive information remains governed.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Eligible request feed
- Access rules
- Request detail dialog
- Offer entry point

How to use: Marketplace access and request visibility

This page is the operational checklist for users and trainers working with marketplace access and request visibility.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for marketplace access and request visibility, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant marketplace access and request visibility record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 15

Loan offers and borrower acceptance

Supports prepared terms, counter-offers where applicable, borrower comparison and one controlled acceptance.

Why the module is important

The selected contract path is clear and other offers cannot disburse after acceptance.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Offer status
- Term and instalment information
- Expiry
- Single accepted offer

How to use: Loan offers and borrower acceptance

This page is the operational checklist for users and trainers working with loan offers and borrower acceptance.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for loan offers and borrower acceptance, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

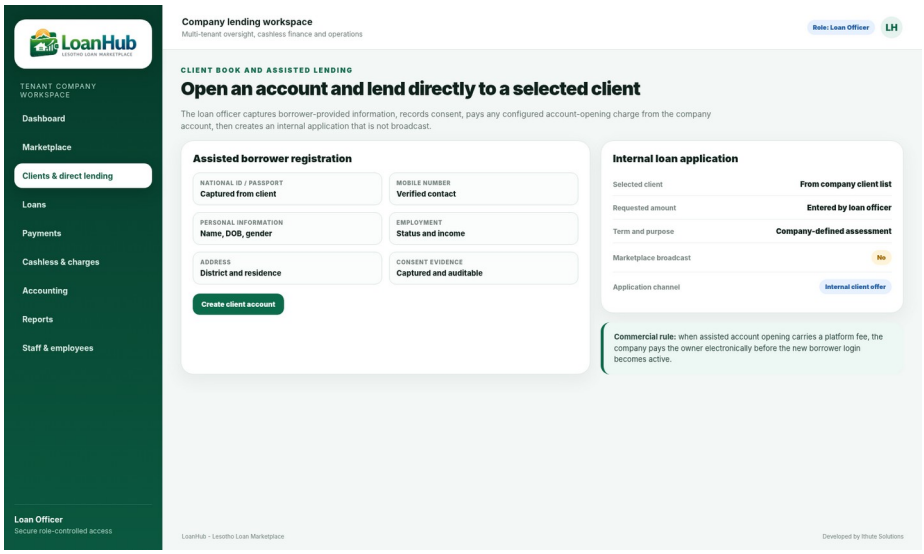
- Open the authorized workspace and confirm the active company and role.
- Select the relevant loan offers and borrower acceptance record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 16

Direct and internal lending

Creates a company-specific application for a selected client without broadcasting it to other lenders.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

Existing clients and walk-in cases can be served privately inside the same lifecycle controls.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Internal-client-offer channel
- Selected borrower
- Company-only visibility
- Controlled loan conversion

How to use: Direct and internal lending

This page is the operational checklist for users and trainers working with direct and internal lending.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for direct and internal lending, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant direct and internal lending record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 17

Loan account and repayment schedule

Creates the loan account from accepted/approved terms and establishes balances and installments.

Why the module is important

The commercial agreement becomes an operational schedule that finance and collections can manage.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Principal and terms
- Status lifecycle
- Installment schedule
- Balance tracking

How to use: Loan account and repayment schedule

This page is the operational checklist for users and trainers working with loan account and repayment schedule.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for loan account and repayment schedule, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant loan account and repayment schedule record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 18

Electronic disbursement

Initiates outbound money from the tenant company to the borrower after approval and provider validation.

Why the module is important

Cash handover risk is reduced and every payout has a provider and system reference.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- M-Pesa B2C
- EcoCash supported payout/refund path
- EFT payout
- Pending/success/failure states

How to use: Electronic disbursement

This page is the operational checklist for users and trainers working with electronic disbursement.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for electronic disbursement, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant electronic disbursement record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 19

Repayments and allocation

Receives electronic borrower payments and allocates verified money to the correct loan and schedule.

Why the module is important

Loan balances change only when money is confirmed and assigned.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Payment purpose
- Provider verification
- Payment allocation
- Receipt evidence

How to use: Repayments and allocation

This page is the operational checklist for users and trainers working with repayments and allocation.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for repayments and allocation, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

- Open the authorized workspace and confirm the active company and role.
- Select the relevant repayments and allocation record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 20

Collections and arrears

Identifies overdue obligations and records contact, promises, actions and escalation.

Why the module is important

A structured collections record replaces informal notes and untraceable cash collection.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Arrears view
- Collection notes
- Promise-to-pay
- No cash-in-hand rule

How to use: Collections and arrears

This page is the operational checklist for users and trainers working with collections and arrears.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for collections and arrears, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

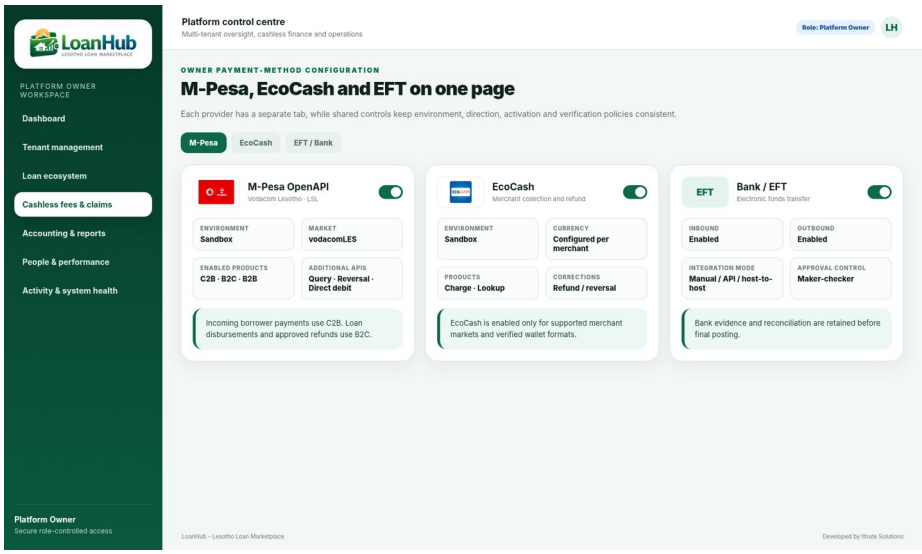
- Open the authorized workspace and confirm the active company and role.
- Select the relevant collections and arrears record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 21

M-Pesa OpenAPI integration

Uses the Lesotho market session model and enabled C2B, B2C, B2B, reversal, query and direct-debit products.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

M-Pesa supports local wallet collections and payouts under provider-approved credentials.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Encrypted application key flow
- Session key
- C2B/B2C/B2B
- Status, reversal and mandate operations

How to use: M-Pesa OpenAPI integration

This page is the operational checklist for users and trainers working with m-pesa openapi integration.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for m-pesa openapi integration, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

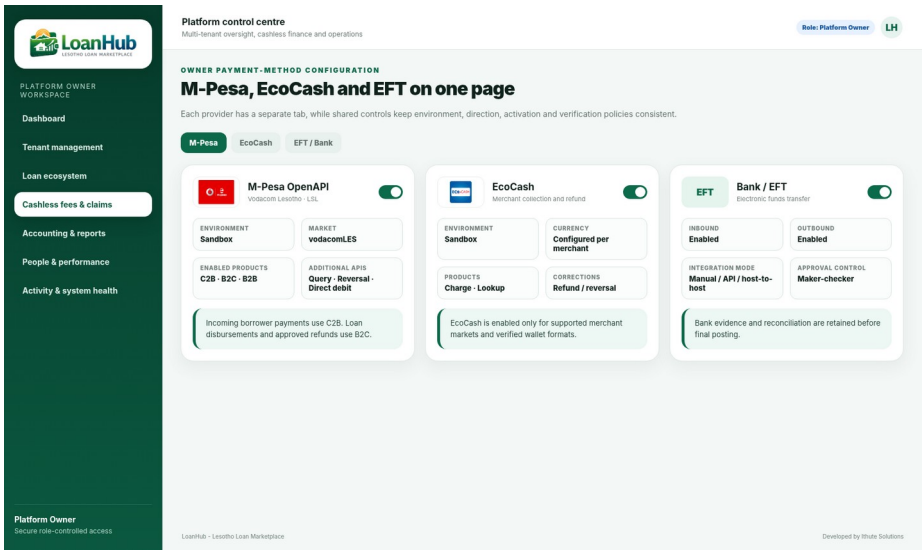
- Open the authorized workspace and confirm the active company and role.
- Select the relevant m-pesa openapi integration record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 22

EcoCash integration

Supports merchant charge, lookup and refund/reversal using configured merchant credentials and callbacks.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

An additional wallet channel can be enabled where the provider supports the merchant market and customer numbers.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Basic authentication
- Charge and lookup
- Refund/reversal
- Callback evidence

How to use: EcoCash integration

This page is the operational checklist for users and trainers working with ecocash integration.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for ecocash integration, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

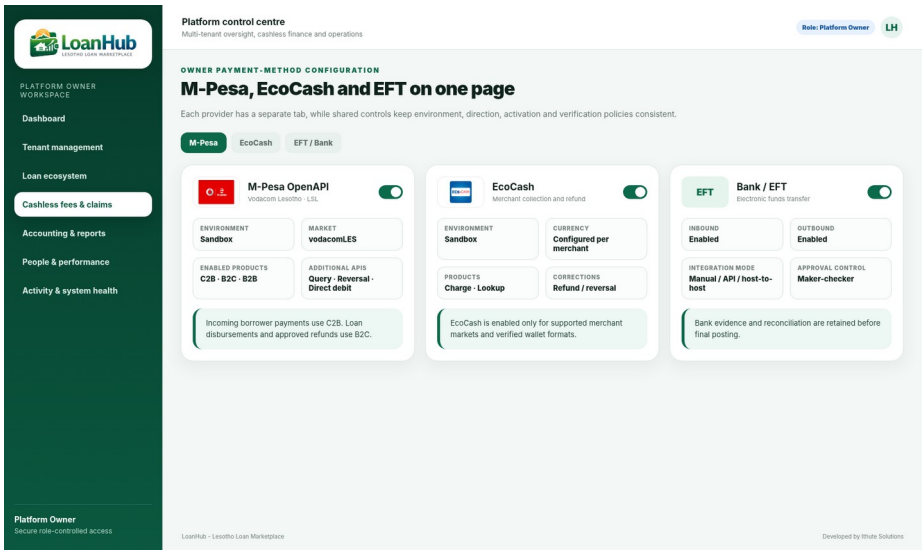
- Open the authorized workspace and confirm the active company and role.
- Select the relevant ecocash integration record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 23

EFT and bank integration

Supports manual reconciliation, bank API, host-to-host or file-exchange modes with inbound/outbound flags.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

Companies can avoid cash while accommodating banks with different integration maturity.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Bank account configuration
- Instruction reference
- Evidence reconciliation
- Maker-checker approval

How to use: EFT and bank integration

This page is the operational checklist for users and trainers working with eft and bank integration.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for eft and bank integration, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

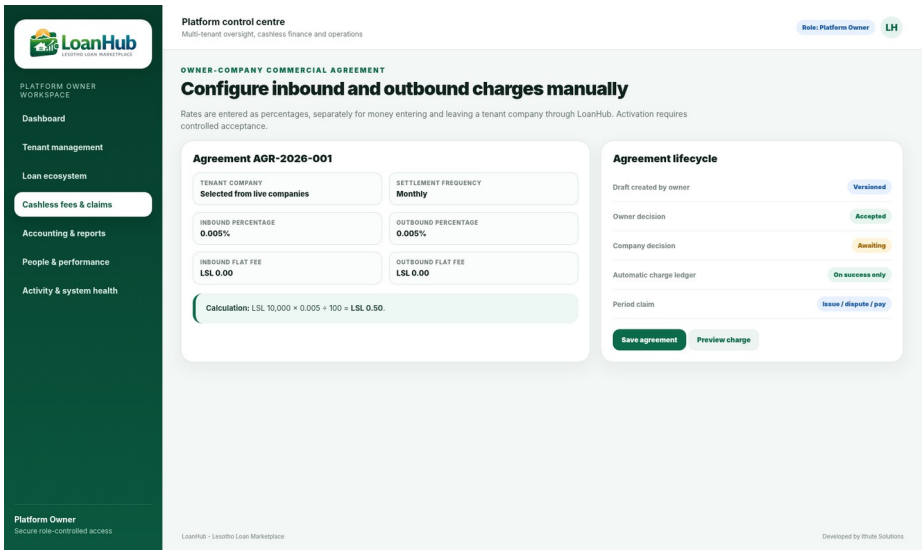
- Open the authorized workspace and confirm the active company and role.
- Select the relevant eft and bank integration record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 24

Commercial agreements and charge ledger

Stores separate inbound/outbound percentage and flat charges, effective periods and bilateral acceptance.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

The platform owner and tenant can see how platform transaction charges are calculated and accrued.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- 0.005% handled as percentage
- Agreement versioning
- Immutable charge rows
- Min/max and settlement frequency

PART II · MODULE 24 OPERATIONS

How to use: Commercial agreements and charge ledger

This page is the operational checklist for users and trainers working with commercial agreements and charge ledger.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for commercial agreements and charge ledger, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

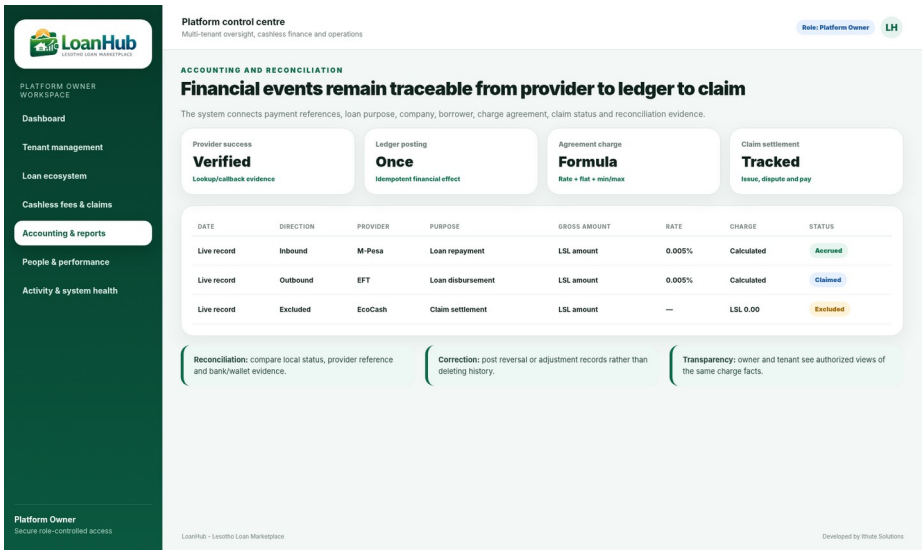
- Open the authorized workspace and confirm the active company and role.
- Select the relevant commercial agreements and charge ledger record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 25

Claims and electronic settlement

Groups eligible unclaimed charge rows into a period claim that the company may acknowledge, dispute and pay.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

Platform revenue becomes transparent, reviewable and electronically settled.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Claim period
- Transaction count and amount
- Decision and dispute reason
- Provider-based payment

How to use: Claims and electronic settlement

This page is the operational checklist for users and trainers working with claims and electronic settlement.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for claims and electronic settlement, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

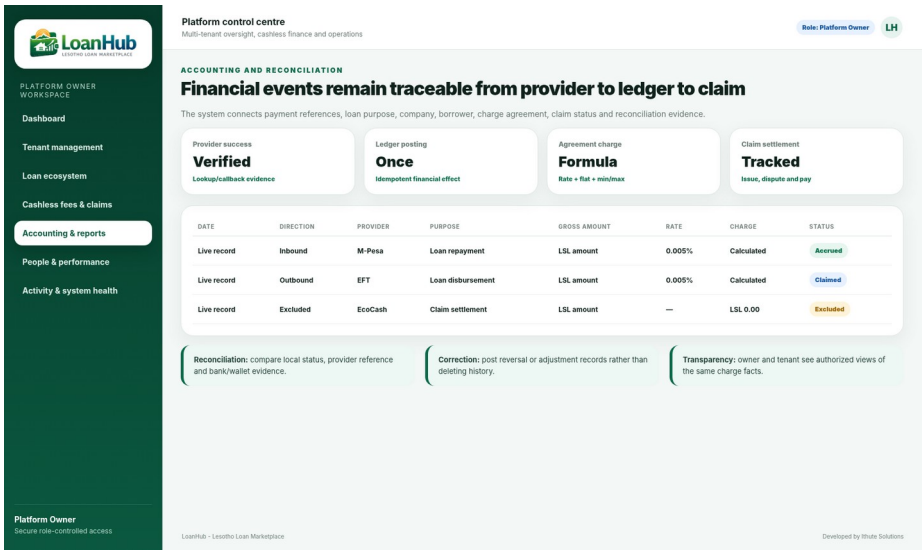
- Open the authorized workspace and confirm the active company and role.
- Select the relevant claims and electronic settlement record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 26

Accounting and reconciliation

Maintains journal-oriented accounting views, provider status, ledger evidence and variance investigation.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

Finance teams can trace money movement and avoid unsupported balance changes.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Accounts and journal entries
- Provider/local matching
- Reversal and adjustments
- Period close evidence

How to use: Accounting and reconciliation

This page is the operational checklist for users and trainers working with accounting and reconciliation.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for accounting and reconciliation, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

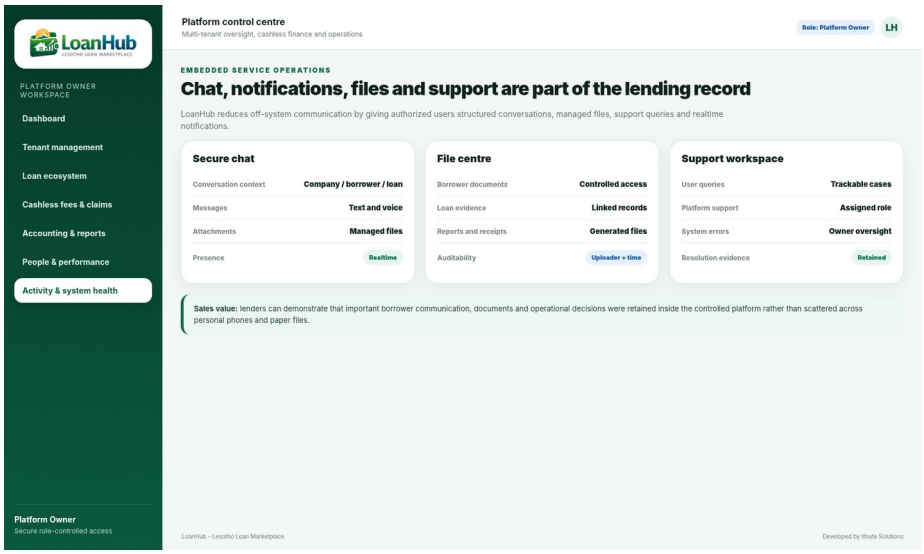
- Open the authorized workspace and confirm the active company and role.
- Select the relevant accounting and reconciliation record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 27

Reports, chat, files, notifications and support

Provides generated reports, realtime communication, managed attachments, user alerts and query handling.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

Operational evidence remains inside the platform instead of fragmented across paper and personal messaging.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Report centre
- Secure chat and voice
- Managed file centre
- Notifications and support cases

PART II · MODULE 27 OPERATIONS

How to use: Reports, chat, files, notifications and support

This page is the operational checklist for users and trainers working with reports, chat, files, notifications and support.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for reports, chat, files, notifications and support, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

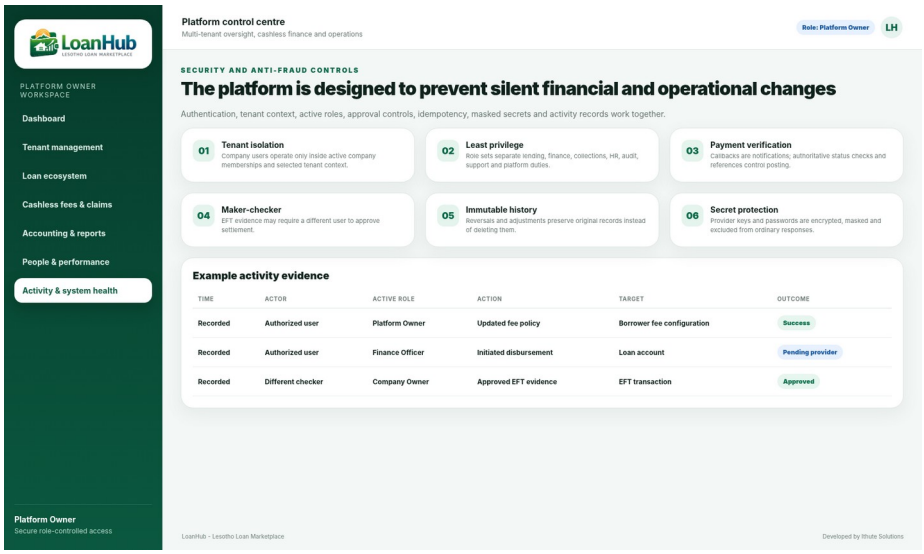
- Open the authorized workspace and confirm the active company and role.
- Select the relevant reports, chat, files, notifications and support record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART II · MODULE 28

Audit, performance and system health

Records actions, supports employee goals/reviews and exposes system-error evidence to authorized roles.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Why the module is important

Management can improve operations while auditors and support teams retain independent evidence.

Primary users

The module is available only to users whose authenticated platform or tenant role permits the applicable operation. Ordinary visibility in the interface does not override backend authorization.

Inputs	Processing
Identity, configuration, business data or linked source records appropriate to the module.	Validation, tenancy and role checks, status transitions and evidence creation.
Outputs	**Control point**
A persisted record, user-visible status, notification, report or provider instruction.	The operation must be attributable, repeatable and reviewable.

- Activity log
- Performance goals and reviews
- System errors
- Operational dashboards

How to use: Audit, performance and system health

This page is the operational checklist for users and trainers working with audit, performance and system health.

Standard procedure

Follow the sequence below. Exact buttons are role- and status-dependent; unavailable actions indicate that the current user, company, role or record state does not permit the action.

Records created or updated

The module creates or updates the linked business records for audit, performance and system health, including actor, tenant, timestamps and status where applicable.

Common exception handling

For validation errors, correct the source information. For authorization errors, confirm the active role/company. For provider or network uncertainty, query status or reconcile; do not repeat blind financial actions.

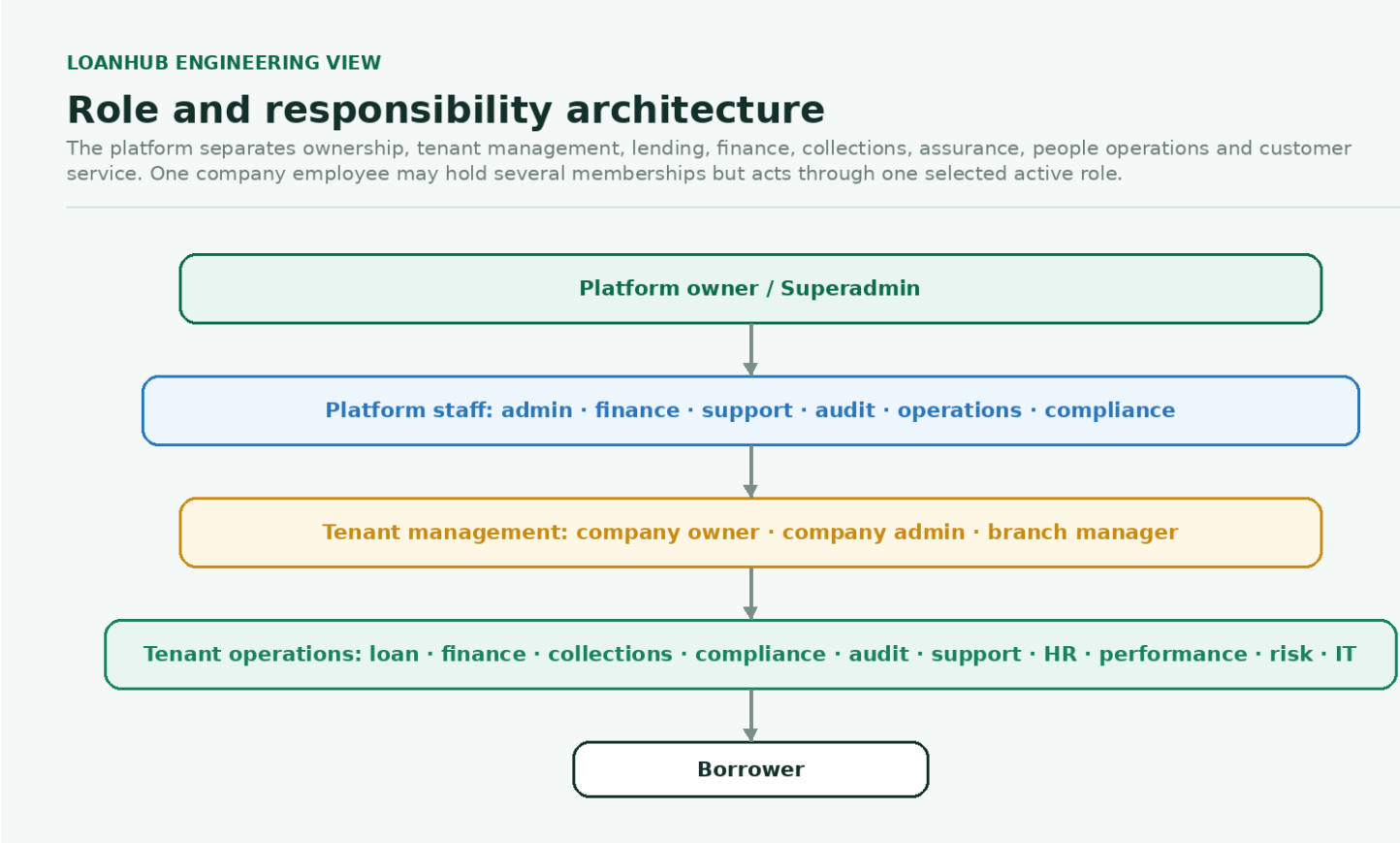
- Open the authorized workspace and confirm the active company and role.
- Select the relevant audit, performance and system health record or create a new record only when policy permits.
- Complete required fields using verified information; do not invent values to make the form pass.
- Review calculated amounts, status, destination and supporting evidence before saving or submitting.
- Where payment or approval is involved, wait for verified completion and keep the reference.
- Use reports, activity or support tools to investigate any exception rather than editing history.

> **No dummy operations** Training environments may use clearly identified test records. Production must use real authorized data and must never contain hidden seed transactions or fabricated balances.

PART III

Complete role-by-role user manual

Each role receives a purpose, access map, daily workflow, procedure, controls, reports and escalation guide.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

PART III · ROLE 01

Platform Owner / Superadmin

Own the platform configuration, approve commercial rules, control provider activation, create platform employees and retain ultimate accountability for tenant and system governance.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Dashboard, Tenant management, Loans and payments, Cashless fees and claims
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary The owner does not approve tenant loans as a lender.

PART III · ROLE 01 DAILY WORK

Platform Owner / Superadmin: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Dashboard, Tenant management, Loans and payments, Cashless fees and claims, Accounting and reports, Plans, Performance, Activity and system errors.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Review pending companies, failed or pending payments and system-health exceptions.
- Confirm no provider configuration or commercial agreement changed without authority.
- Review unclaimed transaction charges, claims, disputes and settlement evidence.
- Delegate support, finance, operations, audit and compliance work to platform employees.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

PART III · ROLE 01 CONTROLS

Platform Owner / Superadmin: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate provider outages, unresolved reconciliation differences, security incidents and regulatory concerns to the named external and internal accountable parties.

- The owner does not approve tenant loans as a lender.
- Provider secrets must not be exposed to tenant or borrower users.
- Production activation requires external provider approval and documented UAT.
- Commercial revisions create a new effective version rather than rewriting historical transactions.
- Report/evidence: Platform financial overview
- Report/evidence: Tenant and subscription status
- Report/evidence: Provider/reconciliation exception report
- Report/evidence: Activity and system-error report

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 02

Platform Administrator

Administer platform users, tenant records and operational settings within delegated authority without owning commercial or confidential payment decisions.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Platform dashboard, Tenant records, Branches and administrators, Support workspace
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Cannot silently take ownership of provider credentials or owner agreements.

PART III · ROLE 02 DAILY WORK

Platform Administrator: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Platform dashboard, Tenant records, Branches and administrators, Support workspace, Activity and operational reports.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Process approved tenant administration work.
- Help correct non-financial configuration and access issues.
- Verify tenant status before enabling ordinary company workspaces.
- Maintain evidence of material changes.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

PART III · ROLE 02 CONTROLS

Platform Administrator: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate finance, compliance and security matters to the appropriate specialized platform role.

- Cannot silently take ownership of provider credentials or owner agreements.
- Must not use platform access to operate as a tenant lender.
- High-risk actions remain owner-controlled.
- Report/evidence: Tenant onboarding queue
- Report/evidence: Administration activity
- Report/evidence: Access and account status

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 03

Platform Finance

Operate owner-side financial oversight: fee policies, payment monitoring, charge ledgers, claims, settlement and reconciliation support.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Cashless finance, Payments, Accounting, Reports
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Cannot alter historical provider responses or source amounts.

PART III · ROLE 03 DAILY WORK

Platform Finance: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Cashless finance, Payments, Accounting, Reports, Claims and charge ledger.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Review pending provider transactions and reconciliation exceptions.
- Prepare period claims from eligible unclaimed ledger entries.
- Verify that claim payments are not charged again.
- Support month-end financial close.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

Platform Finance: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate unmatched balances, duplicate references and disputed claims before close.

- Cannot alter historical provider responses or source amounts.
- Corrections use reversal, waiver or adjustment evidence.
- Must distinguish 0.005% from 0.005 as a decimal multiplier.
- Report/evidence: Provider settlement report
- Report/evidence: Transaction charge ledger
- Report/evidence: Claim aging
- Report/evidence: Reconciliation variance

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 04

Platform Support

Receive and resolve user assistance requests while protecting financial secrets and respecting tenant boundaries.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Support workspace, Queries, Notifications, Files permitted for support
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary No financial approval or secret change authority.

PART III · ROLE 04 DAILY WORK

Platform Support: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Support workspace, Queries, Notifications, Files permitted for support, System status summaries.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Triage new cases, reproduce issues and provide clear user guidance.
- Attach evidence and status updates to the case.
- Avoid requesting passwords, PINs or full provider credentials.
- Escalate code, finance or compliance incidents to the responsible team.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

PART III · ROLE 04 CONTROLS

Platform Support: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate suspected fraud, data exposure, outages and payment mismatches immediately.

- No financial approval or secret change authority.
- Do not access unrelated tenant data.
- Use approved support notes and resolution evidence.
- Report/evidence: Open cases
- Report/evidence: Resolution aging
- Report/evidence: Recurring issue analysis

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 05

Platform Auditor

Independently review records, controls, claims, user actions and financial evidence without performing operational transactions.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Audit logs, Accounting reports, Cashless ledger, Claims
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Read-only assurance principle.

Platform Auditor: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Audit logs, Accounting reports, Cashless ledger, Claims, System errors, Generated reports.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Select samples and trace source-to-ledger evidence.
- Review separation of duties and active-role use.
- Document exceptions without changing the underlying record.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

PART III · ROLE 05 CONTROLS

Platform Auditor: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Report material findings to the platform owner and compliance function.

- Read-only assurance principle.
- No transaction initiation, provider secret change or operational approval.
- Report/evidence: Audit trail extracts
- Report/evidence: Control exception register
- Report/evidence: Claim and reconciliation samples

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 06

Platform Operations

Coordinate platform service continuity, operational queues, tenant readiness and cross-team incident execution.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Operations dashboard, Support workspace, System status, Tenant status
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Operations coordination does not override finance or compliance approvals.

PART III · ROLE 06 DAILY WORK

Platform Operations: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Operations dashboard, Support workspace, System status, Tenant status, Reports.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Review service queues and failed jobs.
- Coordinate maintenance windows and communication.
- Track owner actions and provider dependencies.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

PART III · ROLE 06 CONTROLS

Platform Operations: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Activate incident procedures for service-impacting events.

- Operations coordination does not override finance or compliance approvals.
- Report/evidence: Service availability
- Report/evidence: Incident timeline
- Report/evidence: Operational backlog

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 07

Platform Compliance

Monitor policy, consent, onboarding, payment disclosures, agreements and regulatory obligations.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Compliance reports, Audit logs, Tenant records, Cashless agreements
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary No hidden fee or unsupported market activation.

PART III · ROLE 07 DAILY WORK

Platform Compliance: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Compliance reports, Audit logs, Tenant records, Cashless agreements, Files and evidence.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Review exceptions and high-risk changes.
- Confirm fee disclosures and agreement acceptance.
- Monitor provider-market and customer-consent constraints.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

PART III · ROLE 07 CONTROLS

Platform Compliance: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate legal, regulatory and provider-scope uncertainty before activation.

- No hidden fee or unsupported market activation.
- Evidence must remain attributable and retrievable.
- Report/evidence: Compliance exceptions
- Report/evidence: Agreement acceptance
- Report/evidence: Consent and disclosure samples

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 08

Borrower

Create and manage loan requests, review offers, accept one offer, receive funds, repay electronically and maintain personal files and support communication.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Dashboard, Loan requests, My loans, Payments
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Never share provider PIN, password or OTP with staff.

Borrower: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Dashboard, Loan requests, My loans, Payments, Service fees, Files, Support queries, Profile.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Keep identity, contact, employment and address information accurate.
- Review service-fee quote before authorizing payment.
- Compare total loan terms and expiry before accepting an offer.
- Check repayment schedule and keep payment references.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

Borrower: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Raise a support query for incorrect balances, duplicate debits, missing receipts or unauthorized profile changes.

- Never share provider PIN, password or OTP with staff.
- A pending payment is not proof of success.
- Only one offer should be accepted for a request.
- Report/evidence: Payment receipts
- Report/evidence: Loan schedule
- Report/evidence: Request and offer history

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 09

Tenant Company Owner

Own the tenant company workspace, commercial acceptance, payment accounts, staff authority, lending policies and overall portfolio accountability.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Company dashboard, Clients, Marketplace, Loans
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Company owner is not the platform owner.

PART III · ROLE 09 DAILY WORK

Tenant Company Owner: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Company dashboard, Clients, Marketplace, Loans, Payments, Cashless and charges, Accounting, Reports, Products, Branches, Staff, Employees, Activity, Billing, Settings.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Review portfolio, liquidity, arrears, pending payouts and exceptions.
- Approve company configurations, staff memberships and commercial agreements.
- Confirm finance and collections follow separation-of-duty rules.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

PART III · ROLE 09 CONTROLS

Tenant Company Owner: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate provider, settlement, legal and platform-charge disputes through recorded channels.

- Company owner is not the platform owner.
- Cannot view or change other tenant data.
- Electronic disbursement and repayment controls remain mandatory.
- Report/evidence: Portfolio and arrears
- Report/evidence: Company cashless ledger
- Report/evidence: Staff and performance
- Report/evidence: Subscription status

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 10

Company Administrator

Administer company configuration, branches, staff, products and operational access under the company owner's authority.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Company settings, Branches, Staff, Products
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Must not bypass finance approval or owner commercial acceptance.

PART III · ROLE 10 DAILY WORK

Company Administrator: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Company settings, Branches, Staff, Products, Reports, Activity, Operational pages permitted by role.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Maintain accurate company and branch information.
- Create and manage staff memberships and role assignments.
- Confirm inactive staff lose access without deleting history.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

PART III · ROLE 10 CONTROLS

Company Administrator: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate ownership, finance and compliance decisions.

- Must not bypass finance approval or owner commercial acceptance.
- Use primary role and branch assignments carefully.
- Report/evidence: Staff roster
- Report/evidence: Branch status
- Report/evidence: Configuration changes

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 11

Branch Manager

Supervise branch lending, employees, client service, collections and operational quality.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Branch dashboard, Clients, Loans, Marketplace
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Cannot operate outside assigned branch or unauthorized role.

PART III · ROLE 11 DAILY WORK

Branch Manager: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Branch dashboard, Clients, Loans, Marketplace, Staff/employees, Performance, Activity, Collections.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Review branch pipeline, workload and overdue cases.
- Approve or supervise loan-officer work according to company policy.
- Confirm evidence and handover at day close.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

Branch Manager: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate suspicious applications, repeated payment failure and staff-control breaches.

- Cannot operate outside assigned branch or unauthorized role.
- High-value financial actions require finance/owner approval.
- Report/evidence: Branch pipeline
- Report/evidence: Branch arrears
- Report/evidence: Employee performance
- Report/evidence: Operational exceptions

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 12

Loan Officer

Acquire and serve clients, capture applications, review borrower information and prepare offers or internal applications without controlling final cash movement.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Clients, Direct lending, Marketplace, Loan requests
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Internal applications are not broadcast.

PART III · ROLE 12 DAILY WORK

Loan Officer: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Clients, Direct lending, Marketplace, Loan requests, Loans, Files, Chat, Support.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Select or register a client using provided information and consent.
- Create marketplace or internal loan requests correctly.
- Review affordability and prepare an offer under company policy.
- Keep documents and communication linked to the record.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

Loan Officer: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate identity mismatch, suspected fraud, affordability exceptions and provider-payment problems.

- Internal applications are not broadcast.
- Loan officers should not finalize electronic disbursement.
- Do not invent borrower information or retain personal documents outside approved storage.
- Report/evidence: Applications by status
- Report/evidence: Offer pipeline
- Report/evidence: Missing document list

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 13

Finance Officer

Control electronic disbursements, repayments, provider status, allocations, EFT evidence and financial reconciliation for the tenant.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Payments, Cashless configuration, Loans, Accounting
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Never mark a loan disbursed from a pending request.

PART III · ROLE 13 DAILY WORK

Finance Officer: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Payments, Cashless configuration, Loans, Accounting, Claims, EFT reconciliation, Reports.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Verify approval and beneficiary details before payout.
- Initiate permitted provider transactions with idempotency.
- Review pending, failed and reversed payments.
- Allocate successful repayments and reconcile totals.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

Finance Officer: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate duplicate references, unmatched funds, provider outages and unauthorized payout instructions.

- Never mark a loan disbursed from a pending request.
- Do not approve your own EFT evidence where maker-checker is required.
- Do not edit historical financial amounts.
- Report/evidence: Disbursement register
- Report/evidence: Repayment allocation
- Report/evidence: Provider reconciliation
- Report/evidence: Cashless charge ledger

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 14

Collections Officer

Follow overdue accounts, record contact and promises, receive verified repayment outcomes and escalate unresolved arrears.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Loans, Repayments, Collections cases, Chat
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary No cash-in-hand collection.

PART III · ROLE 14 DAILY WORK

Collections Officer: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Loans, Repayments, Collections cases, Chat, Files, Reports.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Review due and overdue schedules.
- Contact borrowers through approved channels.
- Record promise-to-pay details and collection notes.
- Verify repayment before closing an action.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

Collections Officer: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate hardship, disputes, legal cases and suspicious payment claims.

- No cash-in-hand collection.
- No intimidation, undocumented settlement or balance editing.
- Report/evidence: Arrears aging
- Report/evidence: Promises due
- Report/evidence: Collections actions and recoveries

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 15

Company Compliance Officer

Monitor tenant compliance, borrower consent, lending controls, disclosures, agreements and exception handling.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Activity, Files, Reports, Loan records
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Independent monitoring; no ordinary loan or payment initiation.

PART III · ROLE 15 DAILY WORK

Company Compliance Officer: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Activity, Files, Reports, Loan records, Cashless agreements, Staff evidence.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Review samples and exceptions.
- Confirm internal and marketplace applications follow disclosure rules.
- Monitor staff use of roles and branches.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

Company Compliance Officer: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate legal or policy breaches to company owner and platform compliance.

- Independent monitoring; no ordinary loan or payment initiation.
- Report/evidence: Compliance exceptions
- Report/evidence: Consent and disclosure review
- Report/evidence: Role-control review

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 16

Company Auditor

Provide tenant-level independent assurance over loans, payments, allocations, charges, staff actions and evidence.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Accounting, Reports, Activity, Files
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Read-only assurance and no operational approval.

PART III · ROLE 16 DAILY WORK

Company Auditor: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Accounting, Reports, Activity, Files, Loans and payments read views.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Trace selected transactions end-to-end.
- Review adjustments and reversals.
- Verify reports reconcile to source records.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

PART III · ROLE 16 CONTROLS

Company Auditor: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Report material findings without altering the original record.

- Read-only assurance and no operational approval.
- Report/evidence: Audit samples
- Report/evidence: Exception log
- Report/evidence: Reconciliation review

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 17

Company Customer Support

Assist borrowers and company users with access, navigation, document, request and payment-status questions.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Support queries, Chat, Notifications, Permitted borrower/loan summaries
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary No disclosure of secrets or unrelated borrower data.

PART III · ROLE 17 DAILY WORK

Company Customer Support: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Support queries, Chat, Notifications, Permitted borrower/loan summaries.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Triage cases and provide clear explanations.
- Verify identity before discussing account-specific information.
- Record actions and escalation status.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

PART III · ROLE 17 CONTROLS

Company Customer Support: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate disputes, fraud indicators and provider failures.

- No disclosure of secrets or unrelated borrower data.
- No loan approval or financial posting authority.
- Report/evidence: Open cases
- Report/evidence: Resolution time
- Report/evidence: Recurring borrower issues

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 18

HR Manager

Manage employee profiles, status and people records while company-role assignments remain governed by authorized administrators.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Employees, Staff summaries, Performance, Reports
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Employment profile does not automatically grant system permissions.

PART III · ROLE 18 DAILY WORK

HR Manager: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Employees, Staff summaries, Performance, Reports.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Maintain employment records and active status.
- Coordinate onboarding/offboarding evidence.
- Support role and branch assignment review.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

HR Manager: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate access mismatch and separation-of-duty concerns.

- Employment profile does not automatically grant system permissions.
- Report/evidence: Employee roster
- Report/evidence: Onboarding/offboarding
- Report/evidence: Role assignment gaps

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 19

Performance Manager

Define goals, review performance and report operational improvement using authorized company metrics.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Performance dashboard, Employees, Reports, Activity summaries
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Performance access does not grant lending or payment authority.

Performance Manager: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Performance dashboard, Employees, Reports, Activity summaries.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Maintain goals and review cycles.
- Use verified operational data rather than invented results.
- Document feedback and action plans.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

Performance Manager: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate data-quality and conduct concerns.

- Performance access does not grant lending or payment authority.
- Report/evidence: Goal progress
- Report/evidence: Review completion
- Report/evidence: Operational performance

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 20

Risk Manager

Identify, assess and monitor portfolio, operational, fraud, concentration and process risks.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	Portfolio reports, Arrears, Activity, Payments and exceptions
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary Risk advice does not replace required credit or finance approval.

PART III · ROLE 20 DAILY WORK

Risk Manager: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: Portfolio reports, Arrears, Activity, Payments and exceptions, Files.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Review risk indicators and exceptions.
- Challenge unusual applications, concentrations or payment patterns.
- Document mitigation ownership.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

Risk Manager: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate material exposure and control failure.

- Risk advice does not replace required credit or finance approval.
- Report/evidence: Risk register
- Report/evidence: Portfolio concentration
- Report/evidence: Fraud and payment exceptions

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART III · ROLE 21

Company IT Support

Support tenant devices, browsers, connectivity and approved technical configuration without accessing confidential financial secrets.

Owns	Collaborates
The work and decisions explicitly assigned to this role.	Other roles provide approvals, evidence, service or assurance.
Does not own	**Daily focus**
Functions outside this role remain inaccessible or require escalation.	Prioritize exceptions, due work and records awaiting action.

Item	Description
Primary workspace	System status, Support, Error summaries, Permitted settings
Authority model	Actions are granted by platform role or active tenant membership and role.
Account rule	Use an individual account; do not share credentials.
Evidence rule	Material actions and decisions must remain attributable.

Role boundary No production provider credentials, database access or unauthorized impersonation.

PART III · ROLE 21 DAILY WORK

Company IT Support: navigation and daily routine

The interface presents role-relevant navigation. Multi-role company users must confirm the “Working as” selection before beginning.

Navigation and records

Expected areas: System status, Support, Error summaries, Permitted settings.

Start-of-day routine

Confirm user identity, active company, active role, assigned branch and any pending notifications. Review work queues before creating new records.

Daily responsibilities

Complete only work supported by verified source information and the required approvals.

- Diagnose local network, browser and workstation issues.
- Document reproducible errors and environment details.
- Coordinate with platform support for application defects.

> **End-of-day handover** Record unresolved items, references, next action, accountable owner and deadline. Do not leave payment or approval uncertainty only in personal messages.

Company IT Support: controls, reports and escalation

This page should be used during training, supervision and access review.

Mandatory controls

The following boundaries protect the borrower, company and platform.

Reports and evidence

Use the listed reports and linked source records to review work.

Escalation

Escalate security, data loss and platform defects immediately.

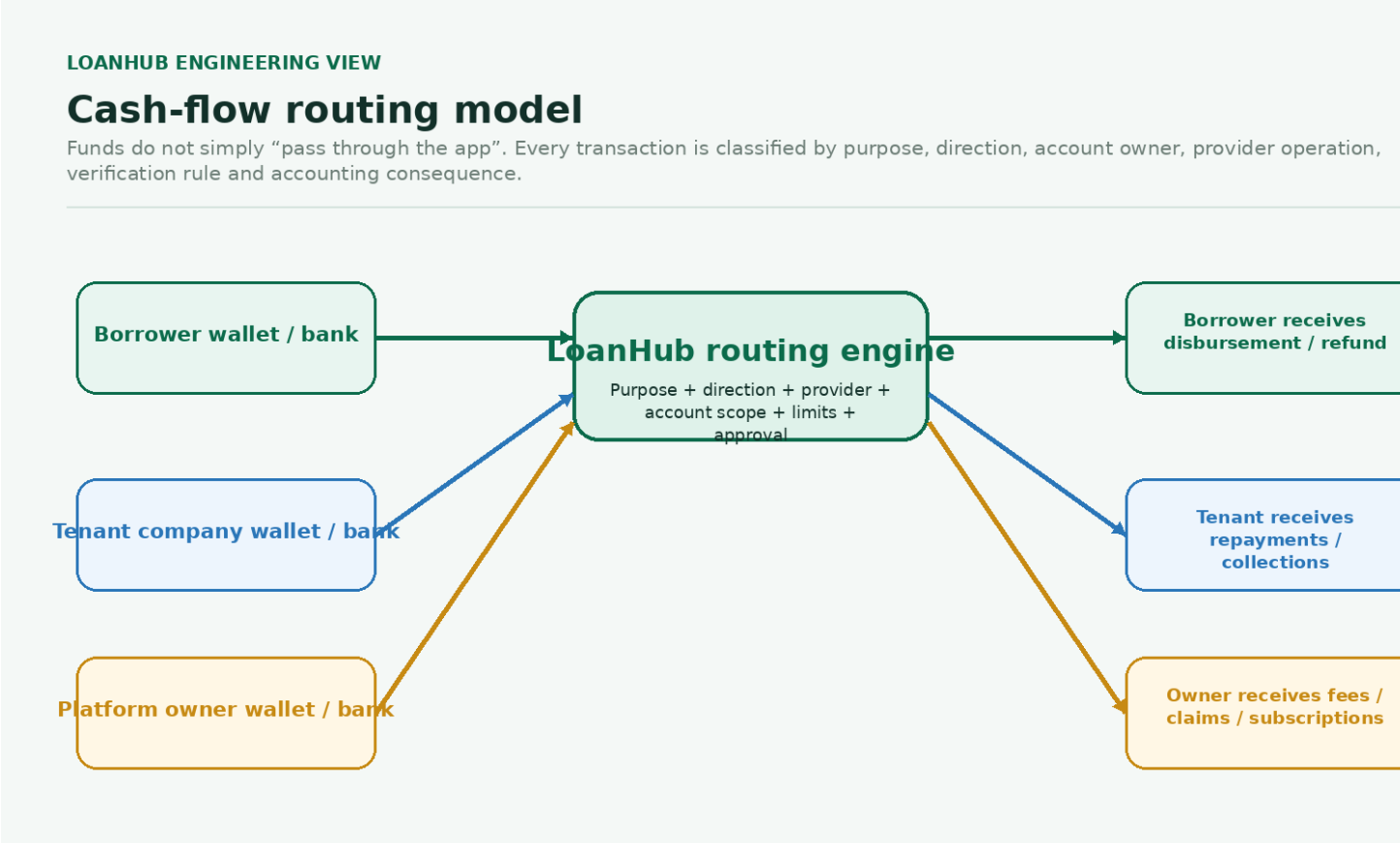
- No production provider credentials, database access or unauthorized impersonation.
- Report/evidence: Technical incident log
- Report/evidence: Device/browser issue trends

> **Access review** Remove inactive memberships promptly, but retain historical actor references and business records.

PART IV

End-to-end process and cash-flow manual

Step-by-step operating flows from borrower acquisition to final reconciliation, including the source and destination of money.

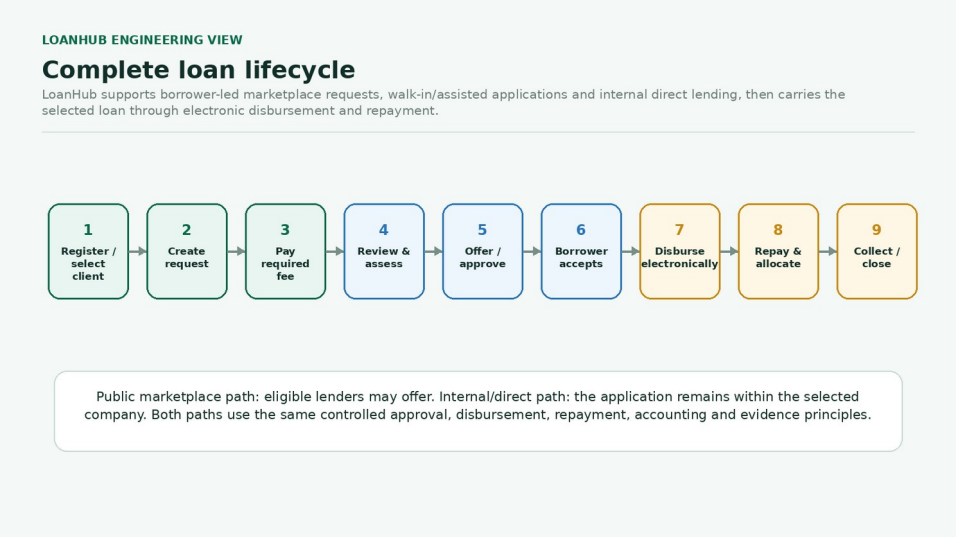


Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

PART IV · PROCESS 01

Online borrower request

Borrower creates a private draft, receives the current fee quote, pays when required, submits, and then waits for eligible offers.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Item	Description
Primary actors	Borrower
Parties/funds	Platform owner / lender companies
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control The request is not visible to lenders while the required fee is unpaid or pending.

Procedure: Online borrower request

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 02

Walk-in borrower onboarding

The officer searches for an existing client, captures borrower-provided data and consent when no account exists, attaches permitted evidence and completes any configured company-paid opening fee.

Item	Description
Primary actors	Loan officer
Parties/funds	Borrower and tenant company
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control The borrower account remains traceable to the capturing company user and source channel.

PART IV · PROCESS 02 PROCEDURE

Procedure: Walk-in borrower onboarding

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

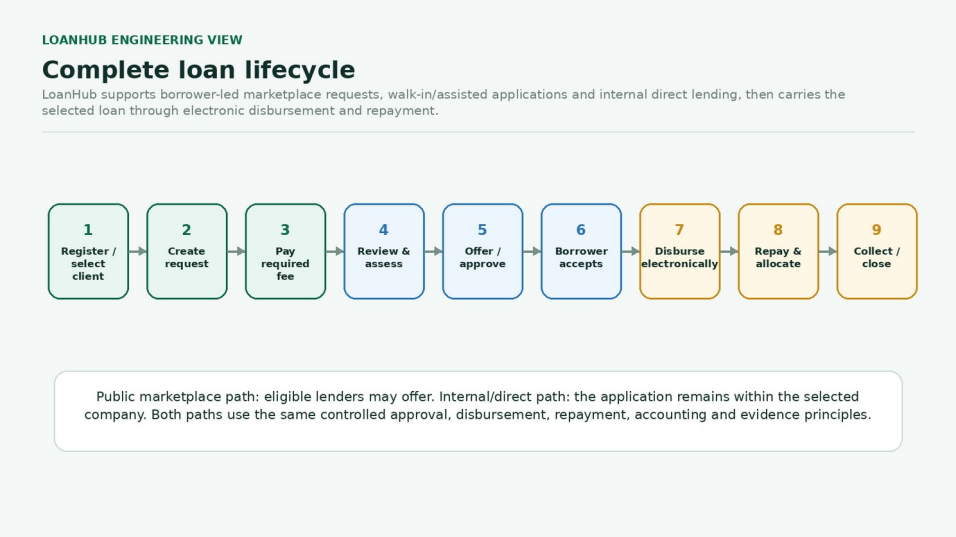
- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 03

Internal direct application

The officer selects a client, enters requested amount, term and purpose, and creates an internal-client-offer application.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Item	Description
Primary actors	Loan officer
Parties/funds	Selected borrower and tenant company
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control The record remains company-specific and is not broadcast to the marketplace.

Procedure: Internal direct application

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 04

Marketplace offer and acceptance

A lender reviews an open request, prepares terms and submits an offer. The borrower compares offers and accepts one.

Item	Description
Primary actors	Loan officer / borrower
Parties/funds	Eligible lenders and borrower
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control Acceptance creates the controlled path to a loan; competing offers cannot disburse.

Procedure: Marketplace offer and acceptance

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

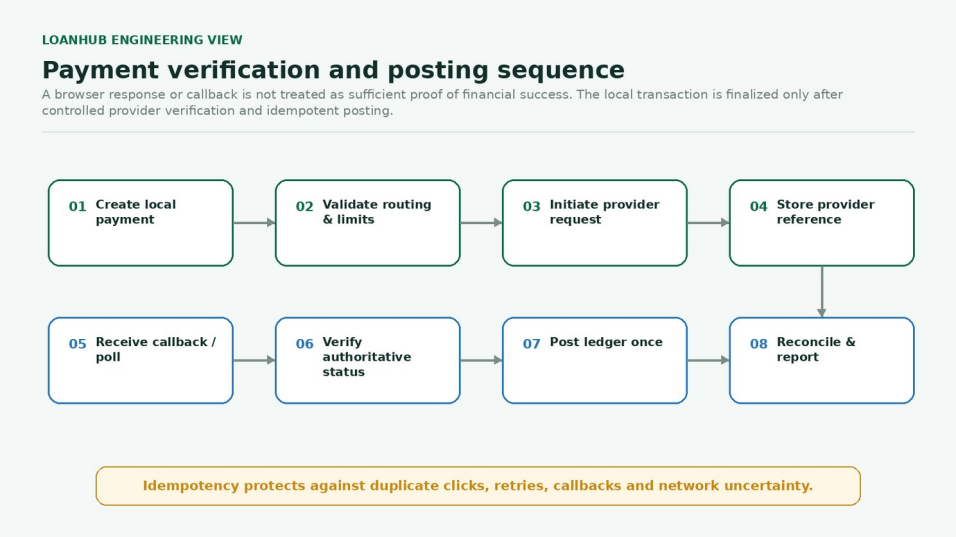
- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 05

Loan disbursement

Finance verifies approval, beneficiary and provider route, initiates the payout, stores references and verifies final status.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Item	Description
Primary actors	Finance officer
Parties/funds	Tenant company and borrower
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control A pending API response does not mark the loan disbursed.

Procedure: Loan disbursement

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

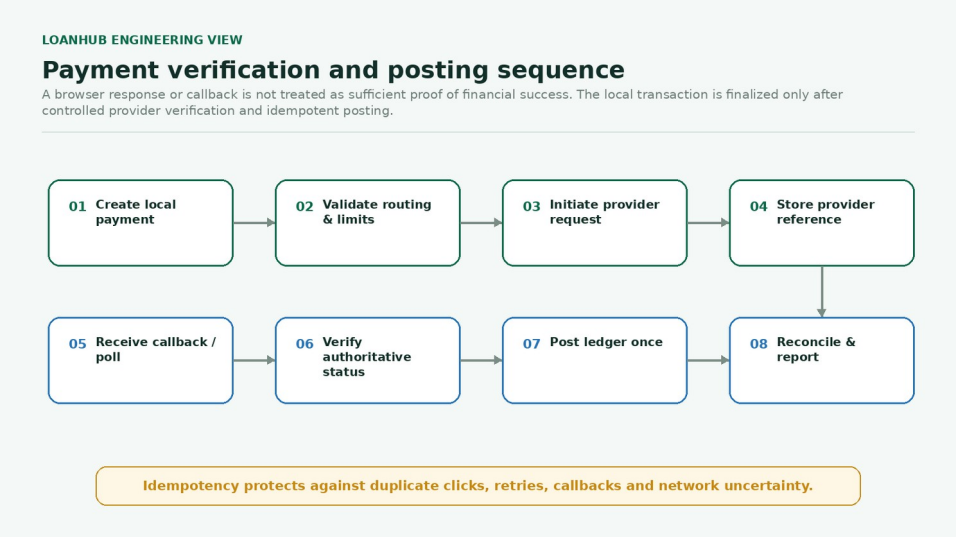
- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 06

Loan repayment

The borrower selects an enabled provider and authorizes payment. LoanHub verifies status and allocates the successful amount.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Item	Description
Primary actors	Borrower / finance
Parties/funds	Borrower and tenant company
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control The loan balance changes once, and a receipt/reference remains available.

Procedure: Loan repayment

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

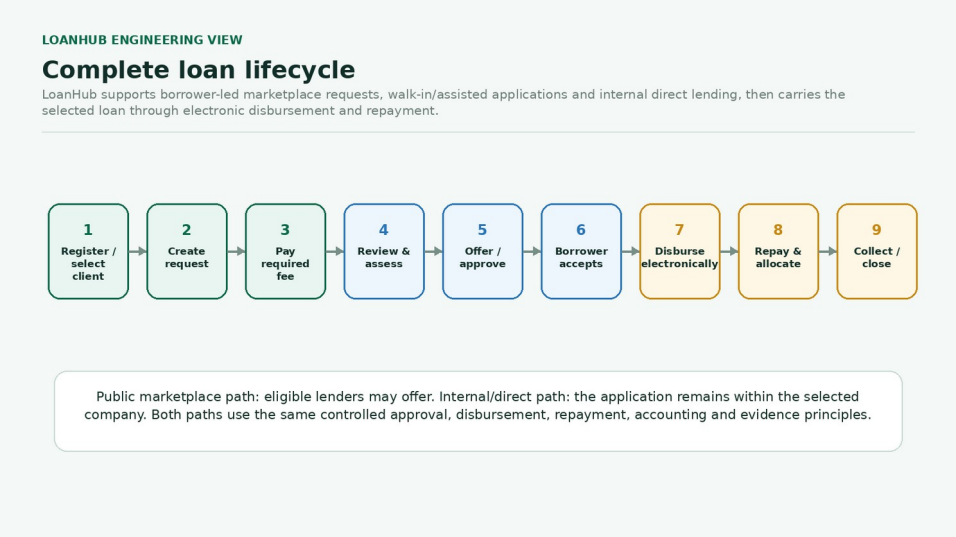
- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 07

Borrow request fee

The fee policy calculates an amount. The borrower pays from wallet/bank to the owner collection account.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Item	Description
Primary actors	Borrower / platform finance
Parties/funds	Borrower and platform owner
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control Only confirmed success opens a fee-gated request.

Procedure: Borrow request fee

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

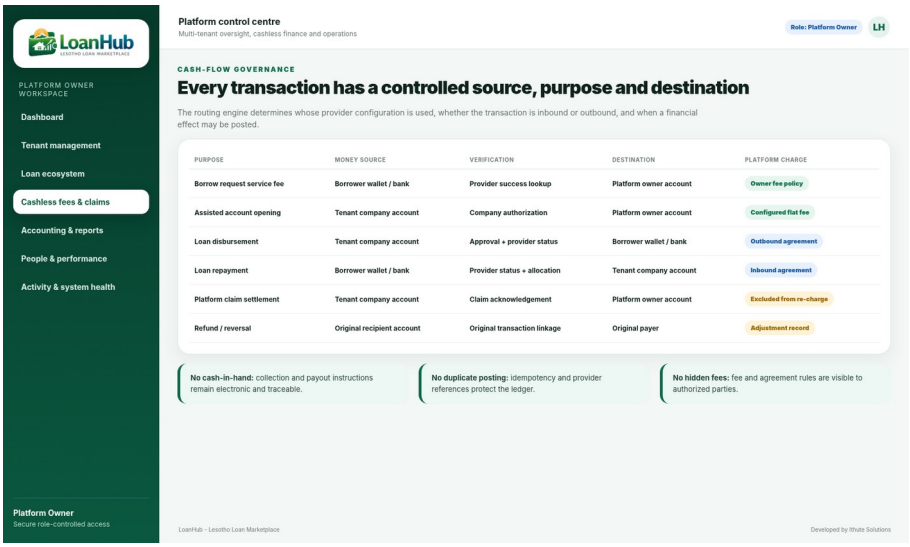
- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 08

Assisted account-opening fee

When configured, the company pays the platform for opening a borrower account on the client's behalf.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Item	Description
Primary actors	Loan officer / company finance
Parties/funds	Tenant company and platform owner
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control The new login activation follows confirmed company-to-owner payment.

Procedure: Assisted account-opening fee

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

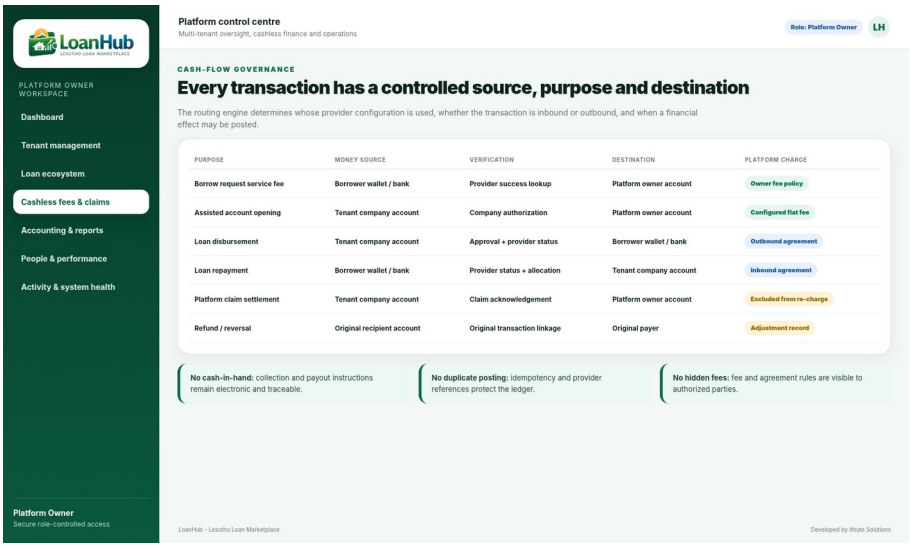
- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 09

Transaction charge accrual

After an eligible successful inbound or outbound payment, the active agreement is applied and one charge-ledger row is created.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Item	Description
Primary actors	System / platform finance
Parties/funds	Tenant company and platform owner
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control A 0.005% rate on LSL 10,000 equals LSL 0.50.

Procedure: Transaction charge accrual

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

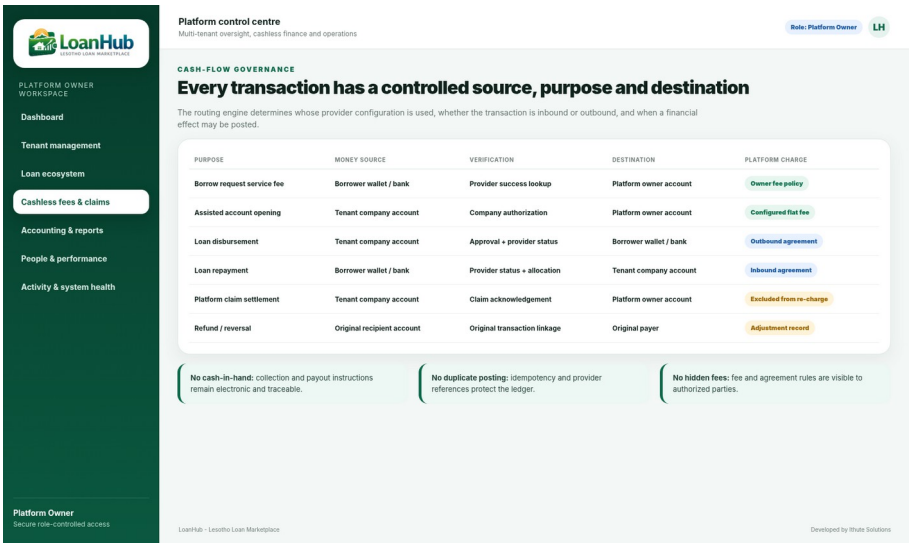
- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 10

Period claim

Eligible unclaimed rows are grouped into a period claim, frozen, issued, acknowledged or disputed, then paid electronically.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Item	Description
Primary actors	Platform finance / company owner
Parties/funds	Platform owner and tenant company
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control Claim settlement itself is excluded from being charged again.

Procedure: Period claim

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

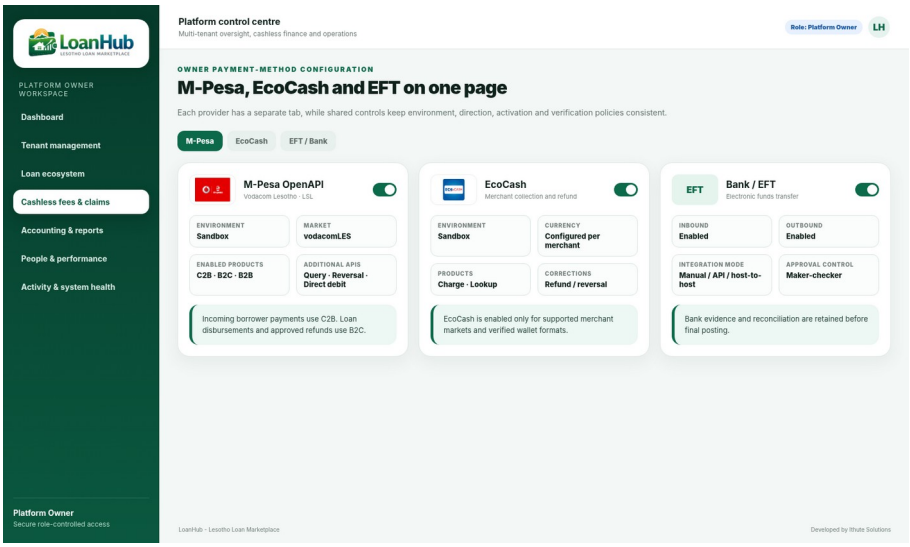
- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 11

M-Pesa transaction

Generate/reuse session, submit the appropriate product request, store references, receive/poll status and reconcile.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Item	Description
Primary actors	Finance or borrower
Parties/funds	M-Pesa provider
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control Use C2B for collections and B2C for approved payouts in Lesotho.

Procedure: M-Pesa transaction

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

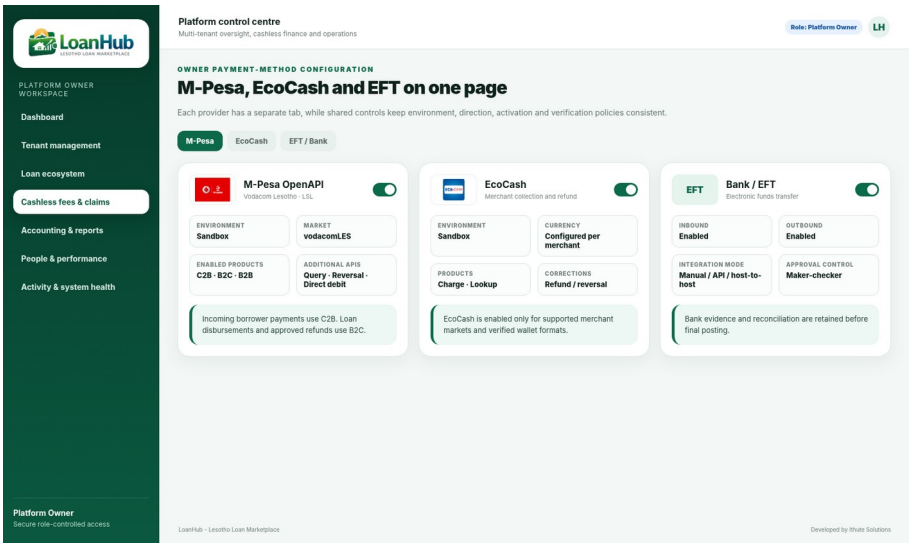
- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 12

EcoCash transaction

Authenticate, submit charge/refund, store correlator and provider reference, receive callback and perform lookup.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Item	Description
Primary actors	Finance or borrower
Parties/funds	EcoCash provider
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control Enable only for supported merchant markets and customer-number formats.

Procedure: EcoCash transaction

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

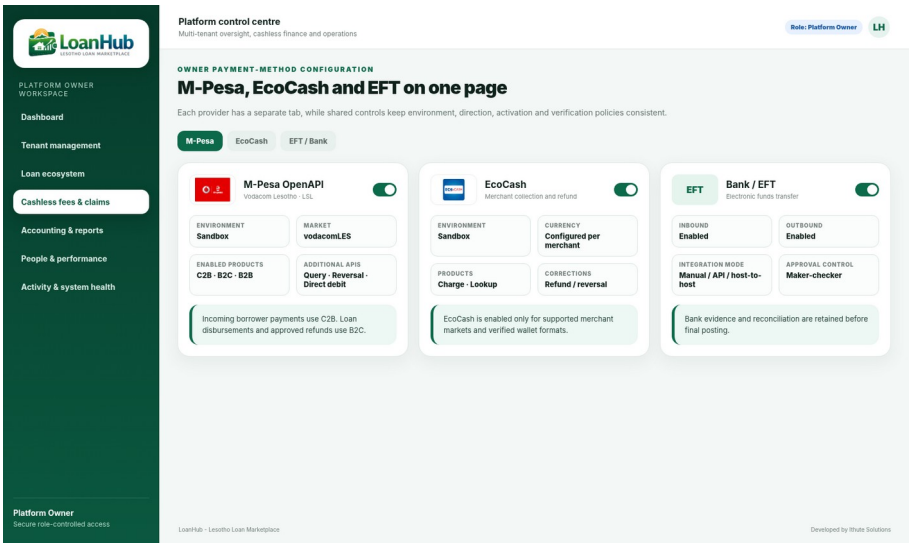
- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 13

EFT transaction

Create instruction, capture bank reference/evidence, reconcile outcome and obtain separate approval where required.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Item	Description
Primary actors	Finance maker / checker
Parties/funds	Bank and tenant/platform account
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control The same user cannot maker and check when maker-checker is enabled.

Procedure: EFT transaction

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART IV · PROCESS 14

Refund, reversal and correction

Reference the original successful transaction, initiate an eligible correction and retain both original and reversing records.

Item	Description
Primary actors	Finance / authorized approver
Parties/funds	Original payer and recipient
Start condition	Authorized source record and applicable configuration exist.
End condition	Verified status and linked evidence are stored.

Critical control Never delete financial history to make balances appear correct.

Procedure: Refund, reversal and correction

Use this sequence for training, UAT and standard operating procedures.

Expected evidence

Source record, configuration snapshot, unique reference, provider/bank response, final status, actor, timestamp and any accounting/claim relationship.

Failure handling

Keep failed and pending attempts. Correct inputs or reconcile the original reference before considering a retry. A retry must not create a second effective financial result.

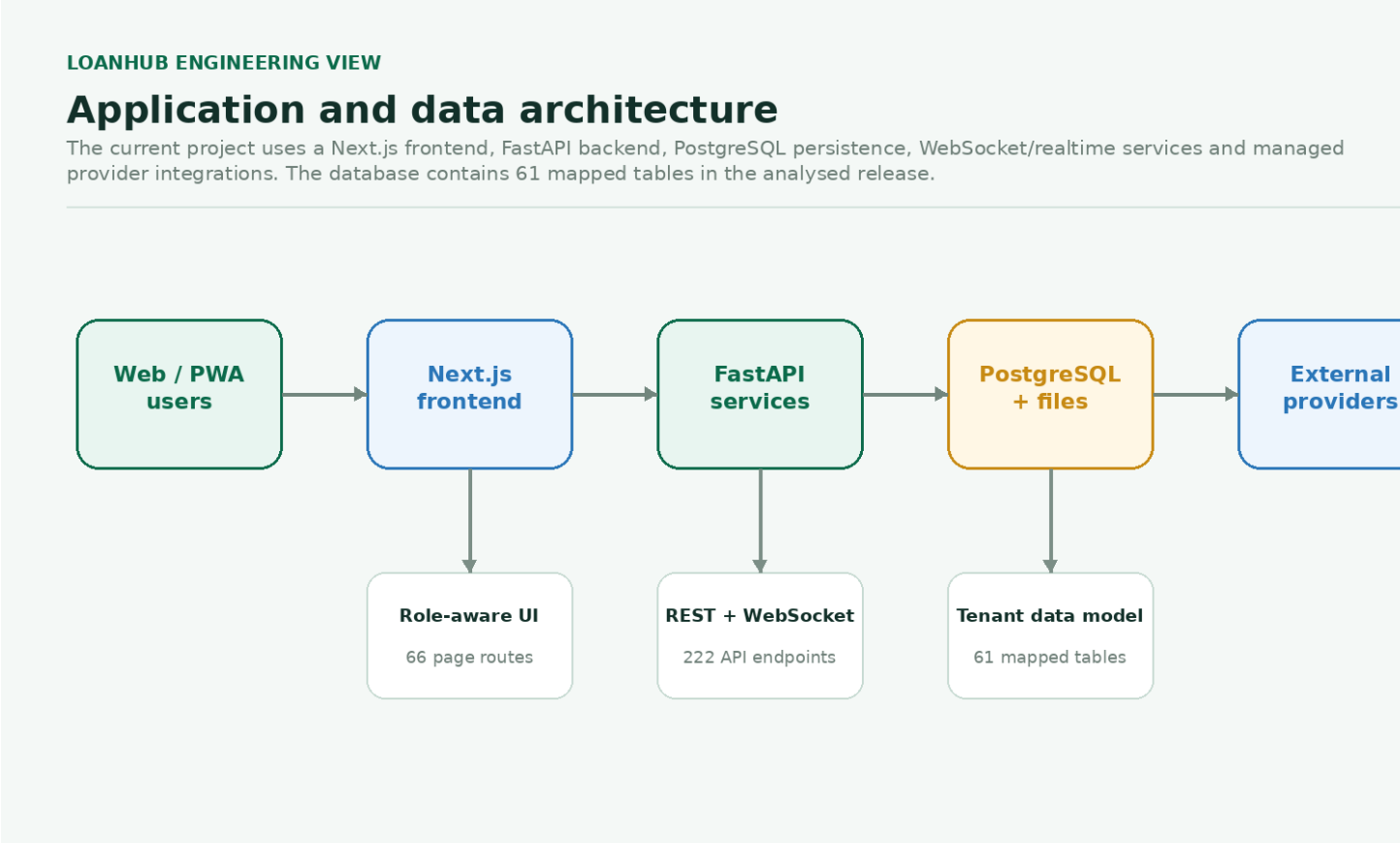
- Confirm the actor is authenticated, active and working in the correct company/role context.
- Select or create the correct source business record and verify required supporting information.
- Apply the active configuration, product, fee, agreement or provider rule effective for the transaction date.
- Display the amount, payer/source, recipient/destination, provider operation and any approval requirement before authorization.
- Create the local instruction with a unique reference and idempotency protection.
- Submit or record the external action, then store provider/bank references and evidence.
- Verify final status; do not infer success from a timeout, redirect or callback alone.
- Post the business, accounting and charge-ledger effects once, then notify authorized users.
- Reconcile and retain exceptions, reversals, disputes and closure evidence.

> **Audit test** An independent reviewer should be able to move from the final loan/payment/claim record back to the original request, actor, configuration and external reference.

PART V

Engineering, security and operational architecture

A maintainable explanation of how the current project is structured and which controls must remain intact.

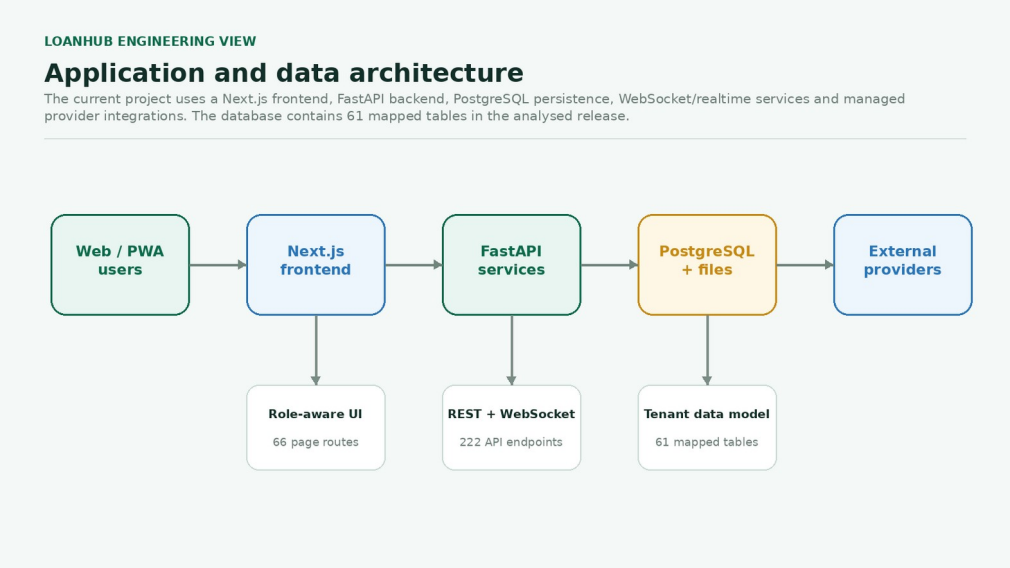


Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

PART V · ENGINEERING 01

Architecture overview

The analysed release uses a Next.js application for browser/PWA workspaces and a FastAPI backend for REST and WebSocket services. PostgreSQL/SQLAlchemy persists multi-tenant records, while managed file services and provider adapters handle documents and cashless integrations.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Engineering principle

The separation allows browser code to remain free of merchant secrets while the backend enforces tenancy, role and financial rules.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input	Implementation
Business rule, provider specification, data sensitivity and user role.	Typed frontend/API contracts and persistent backend validation.
Verification	**Operations**
Automated tests, review, migration and UAT evidence.	Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 02

Frontend workspace model

The current frontend contains 66 page routes across visitor, borrower, tenant company, platform staff and superadmin workspaces. Shared shells provide branding, responsive navigation, theme switching, chat and notifications.

Engineering principle

A route appearing in the browser is never treated as sufficient authorization; backend dependencies remain authoritative.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 03

Backend API model

The current backend exposes 222 route decorators grouped into authentication, companies, branches, borrowers, loans, payments, cashless finance, chat, files, reports, accounting, performance and system-health routers.

Engineering principle

The API is designed around business resources rather than a single monolithic payment or loan endpoint.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 04

Database model

The analysed SQLAlchemy release maps 61 tables covering users, people, borrowers, companies, staff, products, requests, offers, loans, repayments, providers, ledgers, accounting, chat, files, reports, subscriptions and system evidence.

Engineering principle

Financial history and tenant identity are represented as linked records rather than transient screen state.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

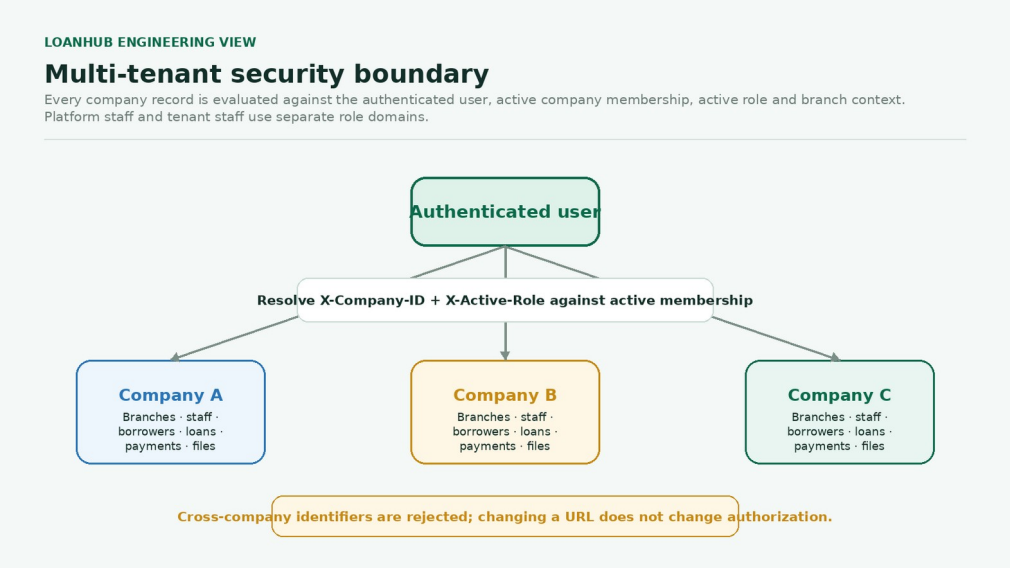
Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 05

Tenant context enforcement

Company requests resolve the authenticated user against active CompanyStaff memberships, the X-Company-ID header and optional X-Active-Role header. Platform roles use a separate authorization domain.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Engineering principle

This prevents a user from gaining access by guessing identifiers or changing a browser route.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

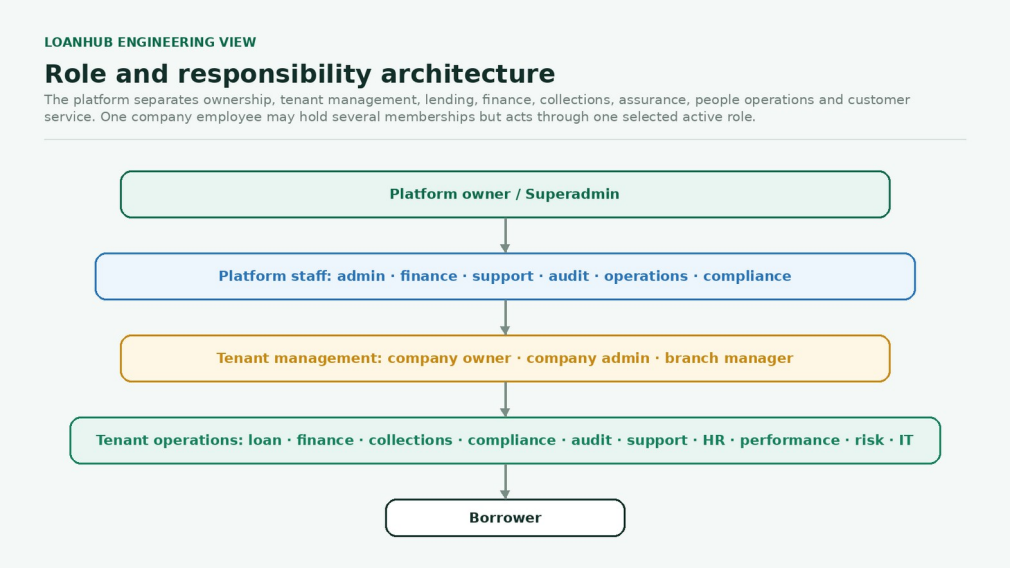
Design input	Implementation
Business rule, provider specification, data sensitivity and user role.	Typed frontend/API contracts and persistent backend validation.
Verification	**Operations**
Automated tests, review, migration and UAT evidence.	Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 06

Role switching design

A user may have several company memberships. The frontend presents available roles and companies; the backend validates each selected context before processing.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Engineering principle

Role switching is a controlled authorization choice, not merely a visual menu change.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 07

Authentication and sessions

Access tokens, refresh tokens, active-account checks and websocket-session support protect ordinary and realtime calls. CORS origins must match the actual frontend origin.

Engineering principle

Browser network errors caused by failed OPTIONS preflight must be treated as configuration defects rather than API business errors.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 08

Provider-secret handling

M-Pesa API keys, EcoCash credentials, bank client secrets and signing material belong in encrypted backend storage or environment-backed secret management. Read APIs expose masked state and “has secret” flags.

Engineering principle

No provider credential should be placed in NEXT_PUBLIC variables, localStorage or screenshots.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

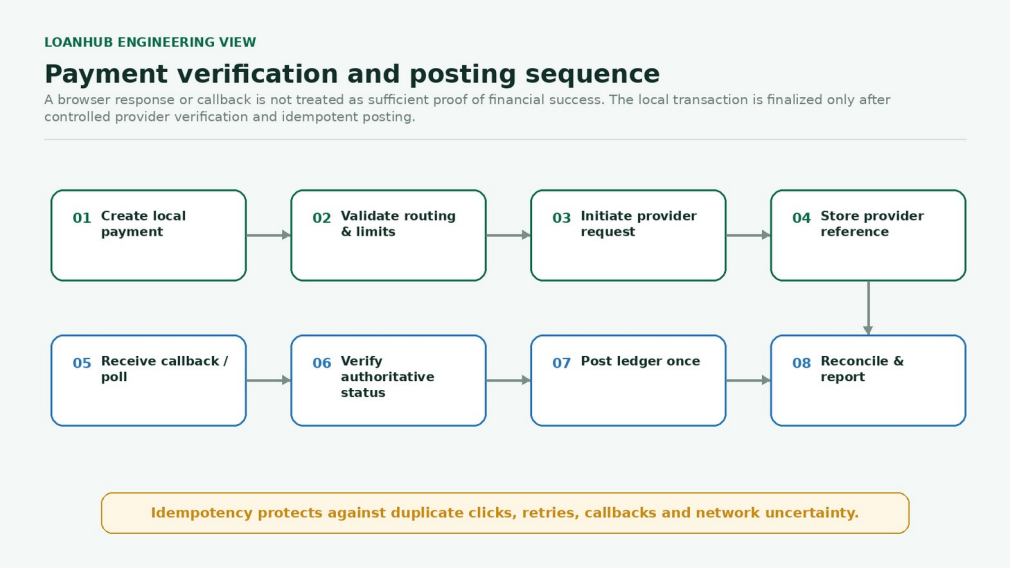
Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 09

Payment state machine

Local payment records move through created/pending/succeeded/failed/reversed states while provider-specific transaction tables retain external references and payload evidence.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Engineering principle

The business object is updated only by a verified, idempotent outcome.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

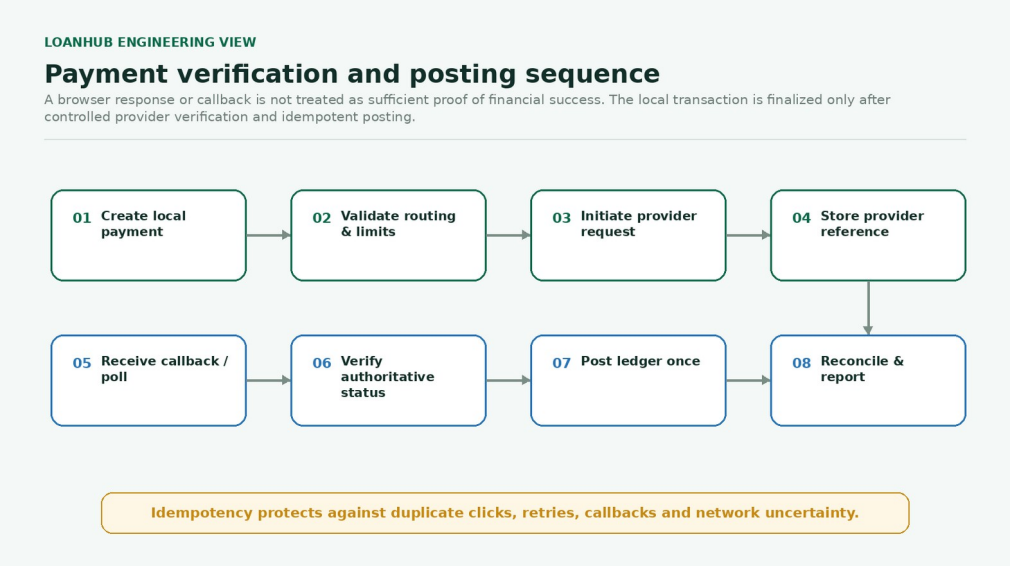
Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 10

Idempotency and duplicate control

Payment initiation uses idempotency keys and unique references. Callback events and retries are recorded to prevent repeated accounting, request opening, disbursement or allocation.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Engineering principle

Network uncertainty must lead to lookup and reconciliation, not a second blind payment request.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 11

Callback security

Callbacks are stored as events and linked to configuration/provider transactions. Authenticity controls depend on provider capabilities and may include secrets, signatures, known endpoints and independent lookup.

Engineering principle

A success-looking callback alone is not sufficient evidence where authoritative query is available.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

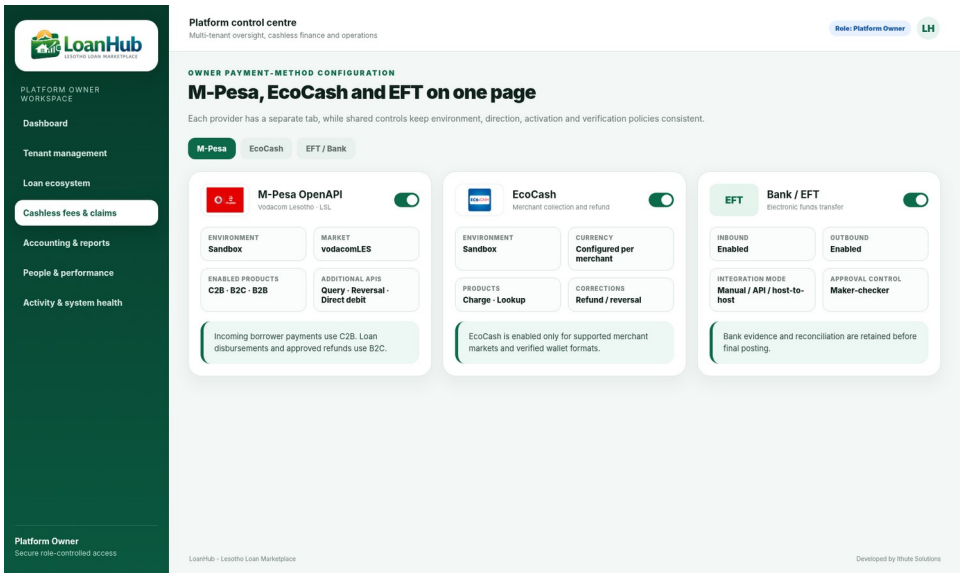
Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 12

EFT maker-checker

Bank/EFT transactions can require separate reconciliation and approval users. Evidence, bank reference, settlement date and approver are retained.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Engineering principle

This reduces the risk of one user creating and self-approving a fabricated transfer.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 13

Immutable correction model

Original payments, ledger charges and accounting records are preserved. Refunds, reversals, waivers and adjustments create linked corrective evidence.

Engineering principle

Deletion or in-place alteration of settled history is prohibited.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 14

Fee calculation engine

Borrower fees support flat, percentage and combined logic plus minimum/maximum and effective periods. Transaction agreements separately define inbound/outbound percentage and flat charges.

Engineering principle

Percent fields are stored and displayed as percentages; calculations divide by 100.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 15

Agreement versioning

Commercial terms include effective dates, bilateral decisions and activation. New terms should be represented by a new version/effective period.

Engineering principle

Historical payments continue to use the agreement snapshot that was applicable when they occurred.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 16

Accounting integration

Successful financial events can create journal-oriented accounting records and are reconciled to provider/bank evidence. Allocations connect repayments to loan obligations.

Engineering principle

Accounting must not rely on dashboard totals alone; source references remain traceable.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 17

Files and evidence

Managed files, borrower documents, request documents, chat attachments, generated reports and receipts use linked metadata and controlled access.

Engineering principle

Evidence should not be stored only on an employee laptop or personal messaging account.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 18

Realtime services

WebSocket management supports chat, presence, notifications and session-controlled realtime events.

Engineering principle

Realtime convenience does not override REST authorization or database truth.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 19

Error monitoring

System-error records capture operational failures for authorized support and owner review. User-facing screens should display actionable messages rather than raw stack traces.

Engineering principle

Recurring errors become an improvement and release-readiness input.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 20

Configuration management

Environment variables define database, security, CORS, provider and deployment settings. Production values must be separated from sandbox values and reviewed before launch.

Engineering principle

Configuration should be documented, reproducible and excluded from source-control secrets.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 21

Database migrations

Alembic revisions evolve the schema. Release deployment must identify the expected head, back up data, test upgrade/rollback in staging and record results.

Engineering principle

A code release without a compatible database migration plan is incomplete.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 22

Container and reverse-proxy deployment

The repository includes Docker and Caddy-related assets for service startup, proxying and operational helpers.

Engineering principle

TLS, hostname, callback reachability and trusted origins must be validated in the target environment.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 23

Backup and recovery

Backups must cover PostgreSQL data, managed files and required configuration/secrets. Restore tests should prove recovery objectives rather than assuming backups are usable.

Engineering principle

Recovery evidence is a production gate.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 24

Monitoring and alerting

Monitor API availability, payment failure rates, callback backlog, reconciliation variance, authentication anomalies, system errors and job failures.

Engineering principle

Alerts need named owners and escalation times.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

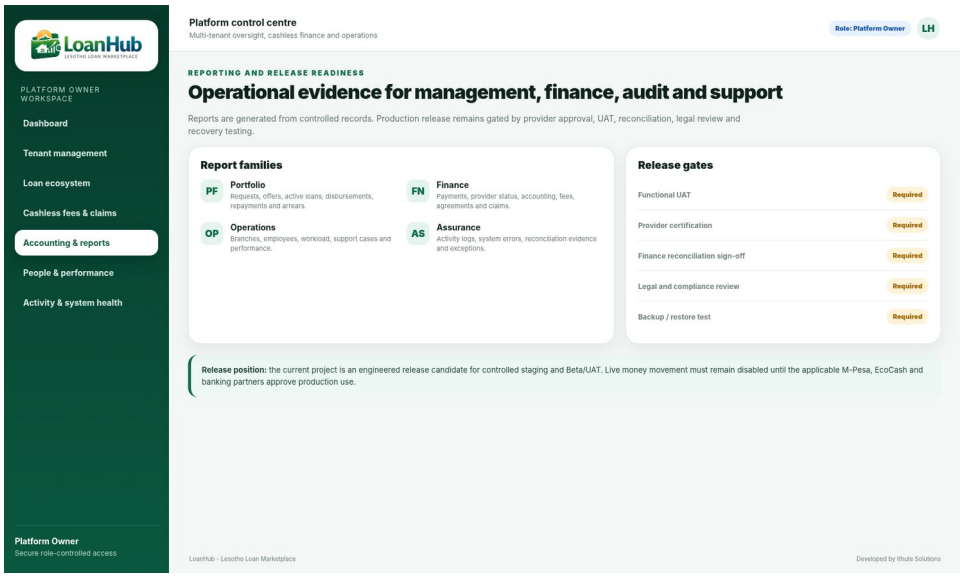
Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 25

Testing strategy

Unit, API, security, migration, provider sandbox, cash-flow, role and reconciliation tests should form a layered test pack.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Engineering principle

Financial success and failure scenarios both require evidence.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

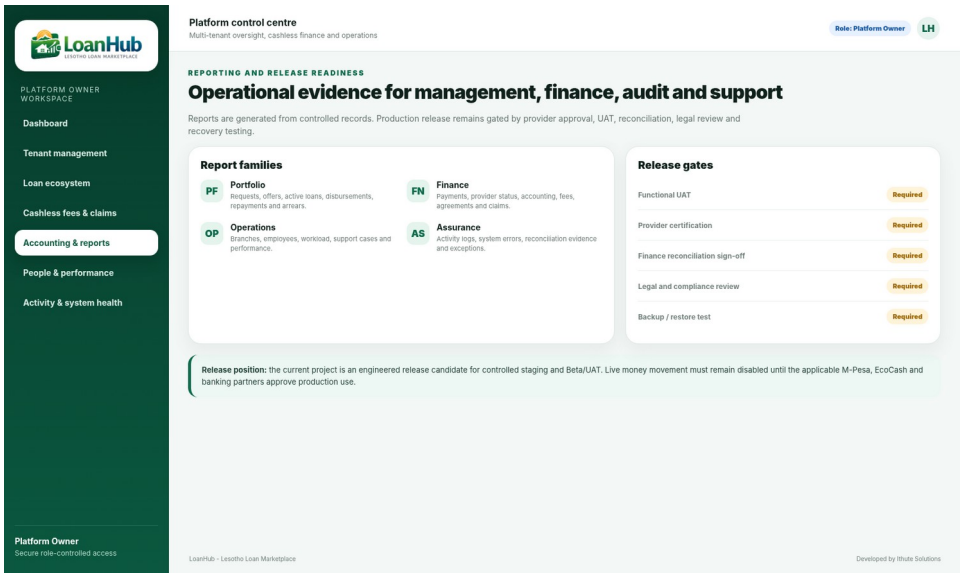
Design input	Implementation
Business rule, provider specification, data sensitivity and user role.	Typed frontend/API contracts and persistent backend validation.
Verification	**Operations**
Automated tests, review, migration and UAT evidence.	Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 26

UAT design

UAT covers borrower fee gating, online and internal loans, provider outcomes, maker-checker, tenant isolation, role switching, claims and period close.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

Engineering principle

Business and finance users must sign off, not only developers.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 27

Performance and scalability

Pagination, indexed tenant identifiers, provider rate limits and asynchronous/realtime workload should be measured under representative use.

Engineering principle

Capacity decisions must use observed workloads and service targets, not invented transaction volumes.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 28

Privacy and data governance

Borrower identity, employment, communication and financial data require minimization, purpose limitation, role-based access, retention rules and secure disposal.

Engineering principle

A sales presentation must not expose real customer information.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 29

Operational support model

Support, finance, operations, compliance and engineering use separate queues and escalation paths. Provider and bank contact details must be maintained outside ordinary user views.

Engineering principle

Incidents should have a timeline, owner, evidence and closure review.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART V · ENGINEERING 30

Engineering handover

A maintainable release includes source, environment template, migration instructions, route/model inventories, architecture decisions, tests, known limitations and support ownership.

Engineering principle

The manual complements, but does not replace, in-repository documentation and code review.

Maintenance expectation

Changes must preserve tenancy, role boundaries, status transitions, idempotency, provider evidence and historical traceability. Update source documentation and tests with the code.

Review questions

What data is trusted? Which role is authorized? What happens on timeout, retry, duplicate or reversal? Which record proves the result?

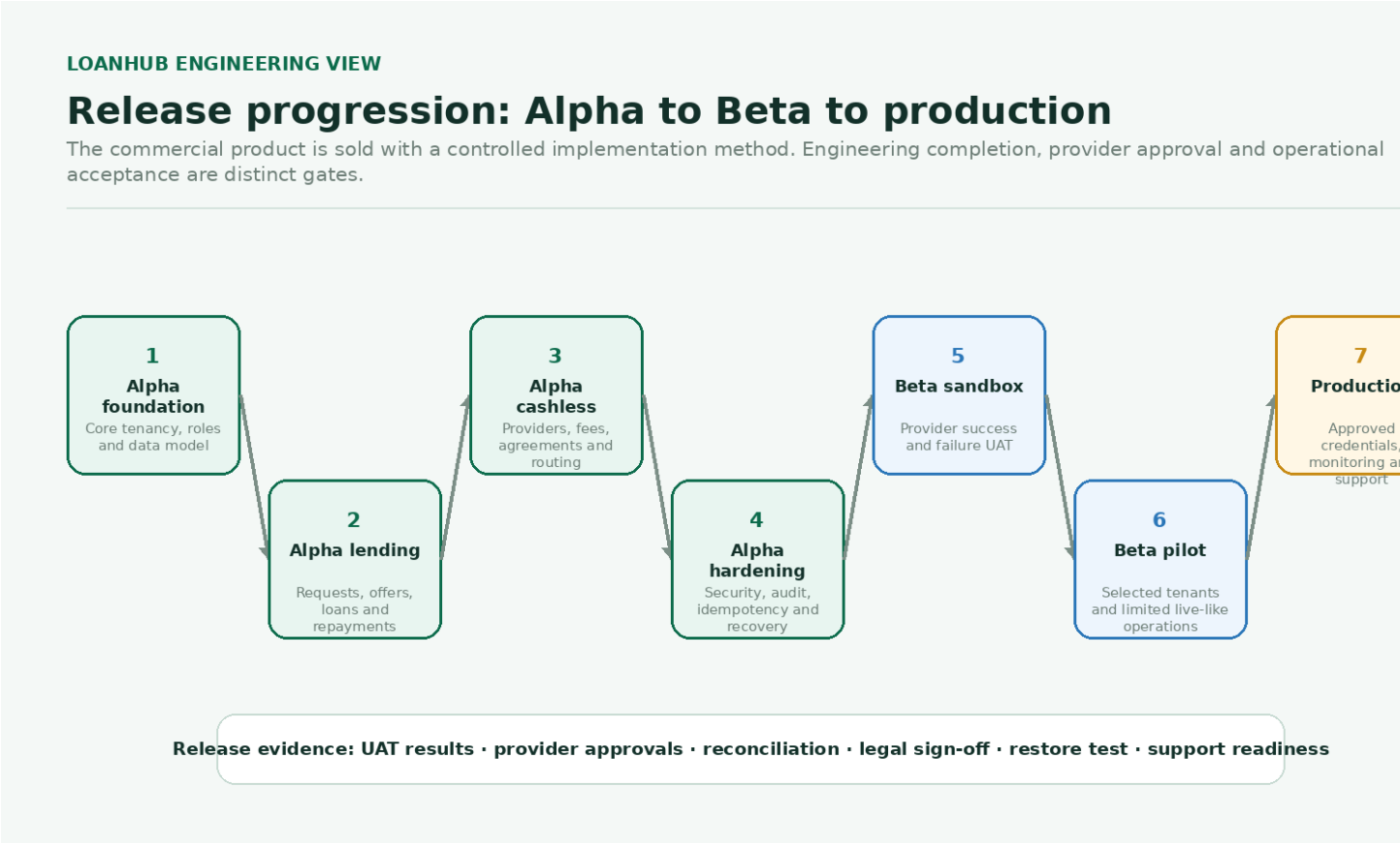
Design input Business rule, provider specification, data sensitivity and user role.	**Implementation** Typed frontend/API contracts and persistent backend validation.
Verification Automated tests, review, migration and UAT evidence.	**Operations** Monitoring, support, reconciliation and controlled change.

Do not weaken Convenient UI behavior must never replace server-side authorization or financial verification.

PART VI

Alpha-to-Beta release, implementation and sales use

How to take the engineered release through provider sandbox, pilot, acceptance and production while presenting it honestly to buyers.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

PART VI · RELEASE 01

Alpha 1 - foundation

Confirm companies, users, people, borrowers, branches, roles, memberships, authentication and tenancy.

Work package

Confirm companies, users, people, borrowers, branches, roles, memberships, authentication and tenancy.

Exit criteria

Exit when tenant isolation, account lifecycle and basic navigation pass internal tests.

Evidence pack

Test results, configuration screenshots without secrets, migration/version record, approvals, reconciliation, issues and accountable sign-off.

Product owner Confirms scope and commercial acceptance.	**Engineering** Builds, fixes, deploys and documents.
Finance/operations Performs UAT and proves control execution.	**External provider** Approves credentials, products and production use.

Gate principle No stage is passed because a screen looks complete. Exit criteria require evidence.

PART VI · RELEASE 02

Alpha 2 - lending core

Validate products, requests, offers, acceptance, direct lending, loan accounts, schedules, repayments and collections.

Work package

Validate products, requests, offers, acceptance, direct lending, loan accounts, schedules, repayments and collections.

Exit criteria

Exit when each loan path is traceable and business statuses are correct.

Evidence pack

Test results, configuration screenshots without secrets, migration/version record, approvals, reconciliation, issues and accountable sign-off.

Product owner Confirms scope and commercial acceptance.	**Engineering** Builds, fixes, deploys and documents.
Finance/operations Performs UAT and proves control execution.	**External provider** Approves credentials, products and production use.

Gate principle No stage is passed because a screen looks complete. Exit criteria require evidence.

PART VI · RELEASE 03

Alpha 3 - cashless and commercial rules

Validate provider configuration, fee policies, routing, agreements, charge ledger, claims and accounting relationships.

Work package

Validate provider configuration, fee policies, routing, agreements, charge ledger, claims and accounting relationships.

Exit criteria

Exit when all financial effects are idempotent and formulas are verified.

Evidence pack

Test results, configuration screenshots without secrets, migration/version record, approvals, reconciliation, issues and accountable sign-off.

Product owner Confirms scope and commercial acceptance.	**Engineering** Builds, fixes, deploys and documents.
Finance/operations Performs UAT and proves control execution.	**External provider** Approves credentials, products and production use.

Gate principle No stage is passed because a screen looks complete. Exit criteria require evidence.

PART VI · RELEASE 04

Alpha 4 - security hardening

Test active-role manipulation, cross-tenant IDs, secret exposure, callback replay, duplicate initiation, maker-checker and audit evidence.

Work package

Test active-role manipulation, cross-tenant IDs, secret exposure, callback replay, duplicate initiation, maker-checker and audit evidence.

Exit criteria

Exit with no unresolved critical control failure.

Evidence pack

Test results, configuration screenshots without secrets, migration/version record, approvals, reconciliation, issues and accountable sign-off.

Product owner Confirms scope and commercial acceptance.	**Engineering** Builds, fixes, deploys and documents.
Finance/operations Performs UAT and proves control execution.	**External provider** Approves credentials, products and production use.

Gate principle No stage is passed because a screen looks complete. Exit criteria require evidence.

PART VI · RELEASE 05

Alpha 5 - internal release candidate

Freeze code, migrations, environment template, manual, automated tests and known limitations.

Work package

Freeze code, migrations, environment template, manual, automated tests and known limitations.

Exit criteria

Exit when the build can be reproduced in staging.

Evidence pack

Test results, configuration screenshots without secrets, migration/version record, approvals, reconciliation, issues and accountable sign-off.

Product owner Confirms scope and commercial acceptance.	**Engineering** Builds, fixes, deploys and documents.
Finance/operations Performs UAT and proves control execution.	**External provider** Approves credentials, products and production use.

Gate principle No stage is passed because a screen looks complete. Exit criteria require evidence.

PART VI · RELEASE 06

Beta 1 - provider sandbox UAT

Use real sandbox credentials and approved test numbers/accounts for success, failure, timeout, lookup, reversal and reconciliation scenarios.

Work package

Use real sandbox credentials and approved test numbers/accounts for success, failure, timeout, lookup, reversal and reconciliation scenarios.

Exit criteria

Exit with signed provider and internal test evidence.

Evidence pack

Test results, configuration screenshots without secrets, migration/version record, approvals, reconciliation, issues and accountable sign-off.

Product owner Confirms scope and commercial acceptance.	**Engineering** Builds, fixes, deploys and documents.
Finance/operations Performs UAT and proves control execution.	**External provider** Approves credentials, products and production use.

Gate principle No stage is passed because a screen looks complete. Exit criteria require evidence.

PART VI · RELEASE 07

Beta 2 - pilot tenants

Train selected users, restrict values and features, monitor every financial event and reconcile daily.

Work package

Train selected users, restrict values and features, monitor every financial event and reconcile daily.

Exit criteria

Exit when operational users demonstrate safe independent use.

Evidence pack

Test results, configuration screenshots without secrets, migration/version record, approvals, reconciliation, issues and accountable sign-off.

Product owner Confirms scope and commercial acceptance.	**Engineering** Builds, fixes, deploys and documents.
Finance/operations Performs UAT and proves control execution.	**External provider** Approves credentials, products and production use.

Gate principle No stage is passed because a screen looks complete. Exit criteria require evidence.

PART VI · RELEASE 08

Beta 3 - commercial and operational acceptance

Finalize agreements, support model, accounting treatment, compliance, backup/restore and incident procedures.

Work package

Finalize agreements, support model, accounting treatment, compliance, backup/restore and incident procedures.

Exit criteria

Exit with named business signatories.

Evidence pack

Test results, configuration screenshots without secrets, migration/version record, approvals, reconciliation, issues and accountable sign-off.

Product owner Confirms scope and commercial acceptance.	**Engineering** Builds, fixes, deploys and documents.
Finance/operations Performs UAT and proves control execution.	**External provider** Approves credentials, products and production use.

Gate principle No stage is passed because a screen looks complete. Exit criteria require evidence.

PART VI · RELEASE 09

Production launch

Enable approved production credentials, TLS, callbacks, monitoring, alerting, reconciliation and support rota.

Work package

Enable approved production credentials, TLS, callbacks, monitoring, alerting, reconciliation and support rota.

Exit criteria

Launch only the products and markets approved by providers.

Evidence pack

Test results, configuration screenshots without secrets, migration/version record, approvals, reconciliation, issues and accountable sign-off.

Product owner Confirms scope and commercial acceptance.	**Engineering** Builds, fixes, deploys and documents.
Finance/operations Performs UAT and proves control execution.	**External provider** Approves credentials, products and production use.

Gate principle No stage is passed because a screen looks complete. Exit criteria require evidence.

PART VI · RELEASE 10

Post-launch improvement

Measure adoption, turnaround, payment exceptions, support causes, arrears and control effectiveness.

Work package

Measure adoption, turnaround, payment exceptions, support causes, arrears and control effectiveness.

Exit criteria

Use real data to prioritize improvements and release notes.

Evidence pack

Test results, configuration screenshots without secrets, migration/version record, approvals, reconciliation, issues and accountable sign-off.

Product owner Confirms scope and commercial acceptance.	**Engineering** Builds, fixes, deploys and documents.
Finance/operations Performs UAT and proves control execution.	**External provider** Approves credentials, products and production use.

Gate principle No stage is passed because a screen looks complete. Exit criteria require evidence.

PART VI · SALES AND IMPLEMENTATION 01

How to present LoanHub to a prospect

Begin with the buyer's current lending journey and pain points. Show the ecosystem, three loan paths, owner finance control, company workspace, borrower portal, cash flow and release method.

Recommended approach

Begin with the buyer's current lending journey and pain points. Show the ecosystem, three loan paths, owner finance control, company workspace, borrower portal, cash flow and release method.

Important boundary

End with a discovery workshop and implementation-readiness assessment rather than an unsupported instant go-live promise.

Show Actual LoanHub workflows, configuration and control points.	**Explain** What the system does and why each step matters.
Prove Source analysis, test evidence, provider approvals and reconciled records.	**Avoid** Unsupported performance claims, hidden fees and fake live data.

Positioning LoanHub - Lesotho Loan Marketplace, developed by Ithute Solutions.

PART VI · SALES AND IMPLEMENTATION 02

Recommended 30-minute demonstration

Use one prepared test borrower: create/continue request, show fee quote, open request, lender offer, borrower acceptance, controlled payout, repayment, charge ledger and report. Then show internal direct lending and audit evidence.

Recommended approach

Use one prepared test borrower: create/continue request, show fee quote, open request, lender offer, borrower acceptance, controlled payout, repayment, charge ledger and report. Then show internal direct lending and audit evidence.

Important boundary

Keep provider calls in sandbox unless production is formally approved.

Show	Explain
Actual LoanHub workflows, configuration and control points.	What the system does and why each step matters.
Prove	**Avoid**
Source analysis, test evidence, provider approvals and reconciled records.	Unsupported performance claims, hidden fees and fake live data.

Positioning LoanHub - Lesotho Loan Marketplace, developed by Ithute Solutions.

PART VI · SALES AND IMPLEMENTATION 03

Proposal content checklist

Include objectives, scope, roles, integrations, commercial configuration, implementation phases, training, migration, support, security, acceptance, external dependencies and exclusions.

Recommended approach

Include objectives, scope, roles, integrations, commercial configuration, implementation phases, training, migration, support, security, acceptance, external dependencies and exclusions.

Important boundary

Separate software/service charges from M-Pesa, EcoCash, bank and telecom charges.

Show	Explain
Actual LoanHub workflows, configuration and control points.	What the system does and why each step matters.
Prove	**Avoid**
Source analysis, test evidence, provider approvals and reconciled records.	Unsupported performance claims, hidden fees and fake live data.

Positioning LoanHub - Lesotho Loan Marketplace, developed by Ithute Solutions.

PART VI · SALES AND IMPLEMENTATION 04

Buyer discovery questions

Ask about branches, borrower channels, products, approval levels, current cash handling, mobile-money markets, banks, reconciliation, accounting, arrears, staff roles, documents, reporting and legal constraints.

Recommended approach

Ask about branches, borrower channels, products, approval levels, current cash handling, mobile-money markets, banks, reconciliation, accounting, arrears, staff roles, documents, reporting and legal constraints.

Important boundary

Do not configure the system from assumptions.

Show Actual LoanHub workflows, configuration and control points.	**Explain** What the system does and why each step matters.
Prove Source analysis, test evidence, provider approvals and reconciled records.	**Avoid** Unsupported performance claims, hidden fees and fake live data.

Positioning LoanHub - Lesotho Loan Marketplace, developed by Ithute Solutions.

PART VI · SALES AND IMPLEMENTATION 05

Implementation plan

Run discovery, solution configuration, tenant/data preparation, sandbox integration, UAT, role training, pilot, reconciliation acceptance and controlled launch.

Recommended approach

Run discovery, solution configuration, tenant/data preparation, sandbox integration, UAT, role training, pilot, reconciliation acceptance and controlled launch.

Important boundary

Assign named owner, company, finance, technical and compliance representatives.

Show	Explain
Actual LoanHub workflows, configuration and control points.	What the system does and why each step matters.
Prove	**Avoid**
Source analysis, test evidence, provider approvals and reconciled records.	Unsupported performance claims, hidden fees and fake live data.

Positioning LoanHub - Lesotho Loan Marketplace, developed by Ithute Solutions.

Training plan

Train by role and process. Use controlled test records, checklists and evidence. Require each role to demonstrate routine work and exception handling.

Recommended approach

Train by role and process. Use controlled test records, checklists and evidence. Require each role to demonstrate routine work and exception handling.

Important boundary

Do not train only superusers and assume knowledge will reach all branches.

Show	Explain
Actual LoanHub workflows, configuration and control points.	What the system does and why each step matters.
Prove	**Avoid**
Source analysis, test evidence, provider approvals and reconciled records.	Unsupported performance claims, hidden fees and fake live data.

Positioning LoanHub - Lesotho Loan Marketplace, developed by Ithute Solutions.

PART VI · SALES AND IMPLEMENTATION 07

Support and service model

Define severity, contact path, support hours, provider escalation, evidence required, maintenance communication and closure review.

Recommended approach

Define severity, contact path, support hours, provider escalation, evidence required, maintenance communication and closure review.

Important boundary

A payment incident needs finance and provider coordination, not only technical troubleshooting.

Show	Explain
Actual LoanHub workflows, configuration and control points.	What the system does and why each step matters.
Prove	**Avoid**
Source analysis, test evidence, provider approvals and reconciled records.	Unsupported performance claims, hidden fees and fake live data.

Positioning LoanHub - Lesotho Loan Marketplace, developed by Ithute Solutions.

PART VI · SALES AND IMPLEMENTATION 08

Commercial importance summary

LoanHub’s value comes from connecting acquisition, lending, electronic money movement, commercial rules, people, evidence and reporting.

Recommended approach

LoanHub’s value comes from connecting acquisition, lending, electronic money movement, commercial rules, people, evidence and reporting.

Important boundary

The system is most saleable when presented as an operational transformation with controlled implementation.

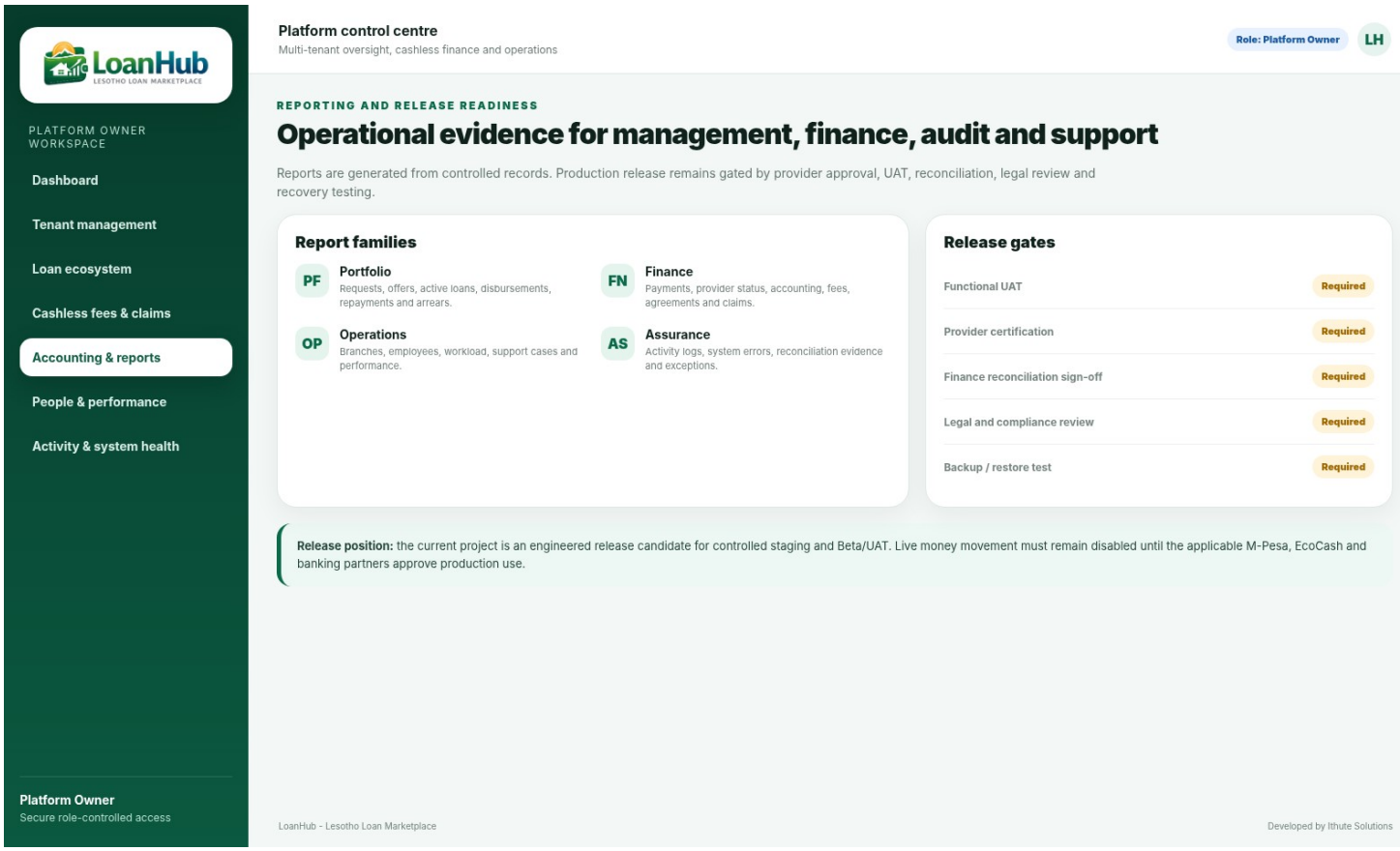
Show Actual LoanHub workflows, configuration and control points.	**Explain** What the system does and why each step matters.
Prove Source analysis, test evidence, provider approvals and reconciled records.	**Avoid** Unsupported performance claims, hidden fees and fake live data.

Positioning LoanHub - Lesotho Loan Marketplace, developed by Ithute Solutions.

PART VII

Appendices and reference inventories

Source-based inventories, glossary, operating checklists and sign-off aids.



Illustrative interface/engineering view based on the analysed LoanHub release. Operational values are loaded from live records.

APPENDIX A

Frontend page inventory 1

Current source route files 1-14 of 66.

Item	Description
app/(auth)/forgot-password	Frontend page route / workspace module
app/(auth)/login	Frontend page route / workspace module
app/(dashboard)/borrower/cashless	Frontend page route / workspace module
app/(dashboard)/borrower/chat	Frontend page route / workspace module
app/(dashboard)/borrower/files	Frontend page route / workspace module
app/(dashboard)/borrower/loans	Frontend page route / workspace module
app/(dashboard)/borrower/mpesa	Frontend page route / workspace module
app/(dashboard)/borrower/notifications	Frontend page route / workspace module
app/(dashboard)/borrower	Frontend page route / workspace module
app/(dashboard)/borrower/payments	Frontend page route / workspace module
app/(dashboard)/borrower/profile	Frontend page route / workspace module
app/(dashboard)/borrower/queries	Frontend page route / workspace module
app/(dashboard)/borrower/requests	Frontend page route / workspace module
app/(dashboard)/company/accounting	Frontend page route / workspace module

Use This inventory supports training coverage, route review and release regression checks.

APPENDIX A

Frontend page inventory 2

Current source route files 15-28 of 66.

Item	Description
app/(dashboard)/company/activity	Frontend page route / workspace module
app/(dashboard)/company/billing	Frontend page route / workspace module
app/(dashboard)/company/branches	Frontend page route / workspace module
app/(dashboard)/company/cashless	Frontend page route / workspace module
app/(dashboard)/company/chat	Frontend page route / workspace module
app/(dashboard)/company/employees	Frontend page route / workspace module
app/(dashboard)/company/files	Frontend page route / workspace module
app/(dashboard)/company/loans	Frontend page route / workspace module
app/(dashboard)/company/marketplace	Frontend page route / workspace module
app/(dashboard)/company/mpesa	Frontend page route / workspace module
app/(dashboard)/company/notifications	Frontend page route / workspace module
app/(dashboard)/company	Frontend page route / workspace module
app/(dashboard)/company/payments	Frontend page route / workspace module
app/(dashboard)/company/performance	Frontend page route / workspace module

Use This inventory supports training coverage, route review and release regression checks.

APPENDIX A

Frontend page inventory 3

Current source route files 29-42 of 66.

Item	Description
app/(dashboard)/company/products	Frontend page route / workspace module
app/(dashboard)/company/queries	Frontend page route / workspace module
app/(dashboard)/company/reports	Frontend page route / workspace module
app/(dashboard)/company/settings	Frontend page route / workspace module
app/(dashboard)/company/staff	Frontend page route / workspace module
app/(dashboard)/company-admin	Frontend page route / workspace module
app/(dashboard)/platform/cashless	Frontend page route / workspace module
app/(dashboard)/platform	Frontend page route / workspace module
app/(dashboard)/platform/support	Frontend page route / workspace module
app/(dashboard)/superadmin/accounting	Frontend page route / workspace module
app/(dashboard)/superadmin/activity	Frontend page route / workspace module
app/(dashboard)/superadmin/cashless	Frontend page route / workspace module
app/(dashboard)/superadmin/chat	Frontend page route / workspace module
app/(dashboard)/superadmin/companies/[id]	Frontend page route / workspace module

Use This inventory supports training coverage, route review and release regression checks.

APPENDIX A

Frontend page inventory 4

Current source route files 43-56 of 66.

Item	Description
app/(dashboard)/superadmin/companies/branches	Frontend page route / workspace module
app/(dashboard)/superadmin/companies	Frontend page route / workspace module
app/(dashboard)/superadmin/company-admins	Frontend page route / workspace module
app/(dashboard)/superadmin/files	Frontend page route / workspace module
app/(dashboard)/superadmin/loans/[id]	Frontend page route / workspace module
app/(dashboard)/superadmin/loans	Frontend page route / workspace module
app/(dashboard)/superadmin/mpesa	Frontend page route / workspace module
app/(dashboard)/superadmin/notifications	Frontend page route / workspace module
app/(dashboard)/superadmin	Frontend page route / workspace module
app/(dashboard)/superadmin/payments	Frontend page route / workspace module
app/(dashboard)/superadmin/performance	Frontend page route / workspace module
app/(dashboard)/superadmin/plans	Frontend page route / workspace module
app/(dashboard)/superadmin/queries	Frontend page route / workspace module
app/(dashboard)/superadmin/reports	Frontend page route / workspace module

Use This inventory supports training coverage, route review and release regression checks.

APPENDIX A

Frontend page inventory 5

Current source route files 57-66 of 66.

Item	Description
app/(dashboard)/superadmin/system-errors	Frontend page route / workspace module
app/(visitors)/borrower-registration	Frontend page route / workspace module
app/(visitors)/choose-account-type	Frontend page route / workspace module
app/(visitors)/greetings	Frontend page route / workspace module
app/(visitors)/lender-access	Frontend page route / workspace module
app/(visitors)/register-company-admin	Frontend page route / workspace module
app/borrower/offers-wall	Frontend page route / workspace module
app/company/direct-lending	Frontend page route / workspace module
app/company/suggestions	Frontend page route / workspace module
app	Frontend page route / workspace module

Use This inventory supports training coverage, route review and release regression checks.

APPENDIX B

Backend API group inventory 1

Router groups 1-10 of 27.

Item	Description
Accounting	10 route operations
Audit	1 route operations
Auth	12 route operations
Billing	9 route operations
Borrower	6 route operations
Borrower Registration	1 route operations
Branches	8 route operations
Cashless	37 route operations
Chat	10 route operations
Company	10 route operations

Security Every route group still requires appropriate authentication, tenant and role dependencies.

APPENDIX B

Backend API group inventory 2

Router groups 11-20 of 27.

Item	Description
Company Registration	1 route operations
Company Staff	6 route operations
Employees	8 route operations
Files	5 route operations
Loan Offers	6 route operations
Loan Products	8 route operations
Loan Request	10 route operations
Loans	4 route operations
Marketplace	3 route operations
Mpesa	22 route operations

Security Every route group still requires appropriate authentication, tenant and role dependencies.

APPENDIX B

Backend API group inventory 3

Router groups 21-27 of 27.

Item	Description
Notifications	6 route operations
Payments	3 route operations
Performance	1 route operations
Person	7 route operations
Professional Lending	18 route operations
Reports	7 route operations
System Errors	3 route operations

Security Every route group still requires appropriate authentication, tenant and role dependencies.

APPENDIX C

Database table inventory 1

Mapped tables 1-12 of 61.

Item	Description
accounting_accounts	accounting
journal_entries	accounting
journal_lines	accounting
audit_logs	audit_log
borrowers	borrower
company_branches	branch
borrower_fee_configurations	cashless
ecocash_configurations	cashless
ecocash_provider_transactions	cashless
ecocash_callback_events	cashless
eft_configurations	cashless
eft_provider_transactions	cashless

Data governance Table existence does not grant user visibility. Access is mediated by APIs and authorization.

APPENDIX C

Database table inventory 2

Mapped tables 13-24 of 61.

Item	Description
transaction_charge_agreements	cashless
platform_charge_claims	cashless
transaction_charge_ledger_entries	cashless
platform_staff_profiles	cashless
chat_conversations	chat
chat_participants	chat
chat_messages	chat
chat_message_attachments	chat
client_company_loan	client_loan_company
loan_companies	company
company_staff	company_staff
borrower_documents	documents

Data governance Table existence does not grant user visibility. Access is mediated by APIs and authorization.

APPENDIX C

Database table inventory 3

Mapped tables 25-36 of 61.

Item	Description
loan_request_documents	documents
employee_profiles	employee
performance_goals	employee
performance_reviews	employee
managed_files	file_management
lender_access_requests	lender_access
loan_offers	loan_offer
loan_products	loan_product
loan_requests	loan_request
marketplace_unlocks	marketplace_access
mpesa_configurations	mpesa
mpesa_provider_transactions	mpesa

Data governance Table existence does not grant user visibility. Access is mediated by APIs and authorization.

APPENDIX C

Database table inventory 4

Mapped tables 37-48 of 61.

Item	Description
mpesa_callback_events	mpesa
mpesa_beneficiary_verifications	mpesa
mpesa_direct_debit_mandates	mpesa
mpesa_reversal_requests	mpesa
broadcast	notificat
notifications	notification
payment_transactions	payment
people	person
direct_loan_applications	professional_lending
credit_blacklist	professional_lending
platform_suggestions	professional_lending
offer_wall_posts	professional_lending

Data governance Table existence does not grant user visibility. Access is mediated by APIs and authorization.

APPENDIX C

Database table inventory 5

Mapped tables 49-60 of 61.

Item	Description
offer_wall_interests	professional_lending
payment_receipts	professional_lending
print_agents	professional_lending
print_jobs	professional_lending
repayment_installments	repayment
payment_allocations	repayment
report_schedules	reporting
generated_reports	reporting
subscription_plans	subscription
company_subscriptions	subscription
system_error_logs	system_error
users	user

Data governance Table existence does not grant user visibility. Access is mediated by APIs and authorization.

APPENDIX C

Database table inventory 6

Mapped tables 61-61 of 61.

Item	Description
refresh_tokens	user

Data governance Table existence does not grant user visibility. Access is mediated by APIs and authorization.

APPENDIX D

Glossary 1

Key terms used in sales, training, finance and engineering.

Item	Description
Active role	The company role currently selected for authorization and navigation.
Borrower service fee	A platform-configured charge associated with creating/submitting a loan request.
Cashless routing	Selection of source, destination, provider operation and controls for a payment purpose.
Charge ledger	Immutable rows calculating platform charges on eligible transactions.
Claim	A period request for settlement of eligible platform transaction charges.
Company membership	A user-to-company role and branch relationship.
C2B	Customer-to-business provider operation, commonly used for collections.
B2C	Business-to-customer provider operation, commonly used for payouts.

APPENDIX D

Glossary 2

Key terms used in sales, training, finance and engineering.

Item	Description
EFT	Electronic funds transfer through bank instructions or integration.
Idempotency	Protection that makes repeated requests produce one effective business result.
Internal application	A company-specific loan application that is not broadcast to the marketplace.
Maker-checker	Separate users create and approve a sensitive operation.
Provider transaction	The M-Pesa, EcoCash or EFT-specific record linked to a local payment.
Reconciliation	Comparison of local records to provider/bank evidence and balances.
Tenant	A lending company operating in an isolated company workspace.

APPENDIX E

Sales readiness

Operational checklist for implementation and routine control.

- Use LoanHub system logo and screenshots on general pages.
- Use M-Pesa, EcoCash and bank branding only in applicable provider sections.
- Explain what the system does before technical detail.
- Separate engineered features from external approvals.
- Avoid invented live customer data or savings claims.

Sign-off Assign a name, date and evidence reference to every completed checklist.

APPENDIX E

Tenant onboarding

Operational checklist for implementation and routine control.

- Company identity and owner verified.
- Status and subscription approved.
- Branches and staff memberships created.
- Products and workflows configured.
- Company provider/bank accounts validated.
- Agreement and disclosures accepted.

> **Sign-off** Assign a name, date and evidence reference to every completed checklist.

APPENDIX E

Provider activation

Operational checklist for implementation and routine control.

- Merchant/product approval exists.
- Credentials stored securely.
- Sandbox success/failure/timeout/reversal tests pass.
- Callbacks and lookup verified.
- Reconciliation owner named.
- Production activation approved.

> **Sign-off** Assign a name, date and evidence reference to every completed checklist.

APPENDIX E

Go-live

Operational checklist for implementation and routine control.

- Backup and restore tested.
- Migration and rollback tested.
- TLS/DNS/CORS/callback reachability verified.
- Role training and access review completed.
- Opening balances reconciled.
- Support, finance and provider escalation live.

> **Sign-off** Assign a name, date and evidence reference to every completed checklist.

APPENDIX E

Daily finance close

Operational checklist for implementation and routine control.

- Review pending and failed payments.
- Reconcile provider/bank references.
- Confirm allocations and disbursements.
- Review charge-ledger exceptions.
- Record unresolved items and owner.

Sign-off Assign a name, date and evidence reference to every completed checklist.

APPENDIX E

Incident response

Operational checklist for implementation and routine control.

- Record time, service, tenant and impact.
- Protect evidence and secrets.
- Stop unsafe repeated transactions.
- Query/reconcile original references.
- Notify accountable teams and users.
- Document resolution and prevention.

> **Sign-off** Assign a name, date and evidence reference to every completed checklist.

FINAL STATEMENT

What the system does - in one complete statement

LoanHub is a Lesotho-focused, multi-tenant digital lending marketplace and loan-management system. It enables borrower self-service, walk-in and internal client lending; lender products and offers; controlled loan creation, disbursement, repayment and collections; M-Pesa, EcoCash and EFT configuration; borrower fees, transaction agreements, automated charge bookkeeping and claims; branches, staff, multi-role switching, platform employees, accounting, reports, chat, files, notifications, support, audit, performance and system-health evidence.

Why it is important

It reduces fragmented processes and cash-in-hand exposure while giving borrowers, companies and the platform owner clearer responsibilities, electronic references and traceable records.

How it should be sold

As digital lending infrastructure plus a controlled implementation and support service - not as an instantly certified provider or a promise of unmeasured savings.

How it should be released

Through Alpha engineering evidence, provider sandbox UAT, trained pilot tenants, reconciliation acceptance and formally approved production activation.

> **Product identity** LoanHub - Lesotho Loan Marketplace. Developed by Ithute Solutions.

DOCUMENT CONTROL

Approval and controlled release sign-off

Use this page when issuing the manual with a named release.

Item	Description
Product owner	Name / signature / date
Engineering lead	Name / signature / date
Platform finance	Name / signature / date
Compliance / legal	Name / signature / date
Pilot tenant representative	Name / signature / date
Release identifier	Version, commit/package and database revision
Known limitations	Reference the approved release note
Production approval	Not granted by this document alone

Thank you LoanHub is developed by Ithute Solutions to support accessible, controlled and accountable digital lending.