CashLine ERP

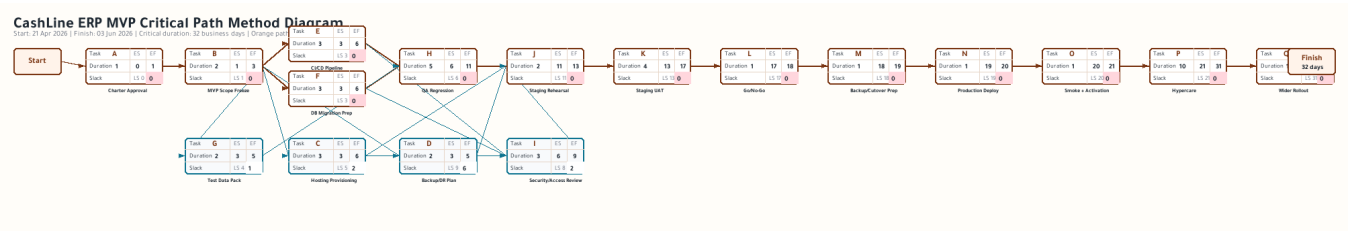
MVP Production Deployment Plan

Development -> QA -> Staging/Pre-production -> Controlled Production MVP -> Stabilization -> Wider rollout

Document Field	Value
Version	1.0 - Branded Cloudflare Share Pack
Document Date	2026-04-20
Formats	Word, HTML, PDF
Release Position	Controlled production MVP planning baseline
Typography	Tajawal

CPM Network Diagram

The following diagram applies the Critical Path Method concept to the real CashLine MVP production nodes. Orange nodes represent the zero-slack critical path; blue nodes represent supporting work with float.



CashLine ERP MVP Production Deployment Plan

Document date: 2026-04-20

Document status: Controlled production MVP planning baseline

Prepared for: Business owners, product owners, implementation leads, engineering, QA, infrastructure, security, operations, and release governance

Release path:

Development -> QA -> Staging/Pre-production -> Controlled Production MVP -> Stabilization -> Wider rollout

---

1. Executive Summary

CashLine ERP V1 should move to production through a controlled MVP deployment model rather than a full enterprise big-bang launch. The objective is to protect workflow integrity, user access control, data quality, operational credibility, and business confidence while allowing the platform to start real controlled usage.

The recommended strategy is to operate a clean environment chain from Development through QA, Staging/Pre-production, Controlled Production MVP, Stabilization, and then Wider rollout. Each environment must have a clear purpose, controlled data rules, deployment gates, and release sign-off criteria.

Production must only receive builds that have already passed equivalent deployment, migration, workflow, API, user-role, UI, reporting, desktop, backup, and rollback checks in staging.

2. Target Release Path

Stage	Purpose	Exit Condition
Development	Engineering implementation, local verification, and feature preparation	Code compiles, unit-level checks pass, and feature is ready for QA
QA	System testing, regression, negative testing, API validation, and test-data execution	Functional, API, workflow, permission, and reporting tests pass against controlled test data
Staging/Pre-production	Production-like rehearsal and business approval environment	Production deployment package, migration, rollback, desktop, reporting, and UAT sign-off are complete
Controlled Production MVP	Limited real operational use with approved users and clean production data	Production smoke test passes, users are activated, and hypercare monitoring starts
Stabilization	First post-go-live monitoring, defect triage, support, and release correction	Critical issues are closed or controlled, user feedback is processed, and daily operations stabilize
Wider rollout	Expansion to broader user groups, additional modules, and higher transaction volume	MVP is stable, controls are proven, and business approves expansion

3. Environment Strategy

Environment	Primary Purpose	Data Type	Access Model	Production Similarity
Development	Engineering changes and local validation	Synthetic development data	Developers and technical team only	Low to medium
QA/System Test	Functional, regression, API, negative, and workflow testing	Controlled synthetic test data	QA, product, engineering, selected business testers	Medium
Staging/Pre-production	Final production rehearsal and business sign-off	Sanitized production-like data or approved test data	Product owners, QA, release approvers, technical release team	High
Production MVP	Controlled live business operation	Real live operational data	Approved business users and approved support roles only	Final
Backup/Recovery	Restore validation and continuity support	Backup replica or recovery copy	Technical administrators only	Recovery-dependent

Staging must mirror production as closely as possible. It should use the same build type, same database engine, same role model, same authentication rules, same environment-variable structure, same integration mode, same desktop package behavior, same reporting/export model, and the same release gates.

4. Deployment Pipeline

The deployment pipeline should be gated and repeatable. No deployment should move forward based on manual confidence alone.

Pipeline Step	Required Outcome
Release branch freeze	Scope is locked and no unapproved changes are introduced
Static checks	Code quality, dependency validation, naming, and structure checks complete
Backend build	API/backend package builds successfully
Frontend build	Web portal package builds successfully
Desktop package build	Desktop shell/package is produced and smoke-testable
Database migration dry-run	Schema changes run successfully outside production first
API regression testing	Core endpoints return expected responses and errors
Role/permission testing	User visibility and access are enforced by role and backend authorization
Workflow/state transition testing	Status changes, approvals, returns, holds, and rejections persist correctly
UI smoke testing	Web screens load, navigate, and render without production-blocking UI issues
Desktop smoke testing	Desktop app launches and follows the same role and navigation rules
Reporting/export validation	PDF/Excel/export behavior works for MVP reports
Backup and rollback package	Recovery path is available before production deployment
Staging deployment	Full package is deployed to staging and validated
Business UAT sign-off	Product/business owner confirms readiness
Production approval	Release owner approves controlled production deployment
Production deployment	Package is deployed to production
Post-deployment smoke test	Critical production paths are verified immediately
Hypercare monitoring	First stabilization window begins

5. Database Deployment Strategy

The database must be treated as a controlled release asset. Production schema changes must never be performed informally.

Mandatory rules:

- Use versioned database migrations only.
- Do not perform manual production schema edits.
- Run every migration first in QA and staging.
- Validate migration ordering and repeatability.
- Take a production backup immediately before deployment.
- Confirm backup availability before applying changes.
- Separate reference/seed data from transactional data.
- Keep UAT/demo/test data out of production.
- Store migration execution evidence as part of the release record.
- Maintain a rollback or recovery strategy for each production deployment.

6. Database Test Loading

QA and staging should use repeatable, script-loaded test data. Test data should not depend on manual screen-by-screen creation.

Data Category	QA	Staging/Pre-production	Production MVP
Synthetic onboarding cases	Yes	Yes	No
Supplier/customer sample journeys	Yes	Yes	No
Admin/System Owner accounts	Yes	Yes	Yes, controlled
Role/function/menu configuration	Yes	Yes	Yes
Reference and lookup data	Yes	Yes	Yes
Notification templates	Yes	Yes	Yes, production-approved only
Report definitions	Yes	Yes	Yes, production-approved only
Demo guidance or UAT support content	No	No	No
Sample transactional data	Yes	Optional, sanitized only	No
Live operational records	No	No, unless sanitized and approved	Yes

7. Production Data Loading

Production must start clean. Only approved operational data and configuration should be loaded.

Production load should include:

- System Owner account.
- Approved Administrator account.
- Approved initial business users.
- Role, function, permission, and side-menu governance configuration.
- Required workflow configuration.
- Required lookup/reference tables.
- Required report definitions.
- Required notification templates.
- Required audit and operational settings.
- Required integration configuration in production-safe mode.
- Islamic Finance controlled/disabled/preparatory flags if Islamic Finance is not active in MVP.

Production load must exclude:

- UAT users.
- Demo users.
- Sample supplier/customer records.
- Historical test cases.
- Static guideline cards.
- Demo banners.
- Placeholder records.
- Training-only instructions.
- Non-operational service-layer explanations.

8. System Test Loading

The QA and staging test pack should cover all core MVP journeys and control points.

Test Area	Required Scenario Coverage
Supplier onboarding	Supplier submits onboarding, KYC, documents, review, approval, activation, and portal access
Customer onboarding	Customer submits onboarding, review, approval, activation, and portal access
Internal operations	Review, approve, reject, return, hold, reopen, and status tracking
Supplier to procurement to AP settlement	Supplier profile, procurement event, payable creation, settlement status, reporting impact
Customer to sales to AR receipt	Customer profile, sales event, receivable creation, payment receipt, reporting impact
Administrator governance	Create user, suspend, hold, revoke, delete, mandatory reason capture, report output
System Owner governance	Create/govern Administrator only, with no business-module access
Role/function governance	Assign/remove functions and validate sidebar/API enforcement
Notifications	Create, deliver, retry, fail, recover, and expose notification status
Reports	Dashboard to report to drilldown consistency and PDF/Excel export
Negative access	Unauthorized routes, hidden menu items, invalid role access, and API denial
Validation	Missing required fields, invalid formats, duplicate records, and blocked status transitions
Web/Desktop parity	Same role, navigation, visibility, and action behavior across web and desktop

9. Staging/Pre-production Exit Criteria

Staging is ready for production promotion only when all of the following are true:

- Backend health checks pass.
- Frontend loads correctly.
- Desktop app launches correctly.
- Login works for all approved MVP roles.
- System Owner sees only Administrator governance.
- Administrator sees only user creation and function administration.
- Supplier users see only Supplier-permitted functions.
- Customer users see only Customer-permitted functions.
- Internal users see only role-permitted functions.
- Workflow transitions persist correctly.
- Notifications are generated and visible.
- Reports export to PDF and Excel.
- No UAT/demo/guideline content is visible.
- Arabic and English UI behavior is acceptable.
- Database migration has been tested.
- Rollback or recovery plan has been tested.
- Production deployment package is frozen.
- Business owner and release owner sign-off is recorded.

10. Production Deployment Day Plan

Sequence	Activity	Owner
1	Announce release freeze	Release owner
2	Stop non-essential deployments	Engineering lead
3	Take database backup	DBA/technical lead
4	Validate backup restore point	DBA/technical lead
5	Deploy backend package	Engineering/release team
6	Run database migrations	DBA/release team
7	Deploy frontend package	Engineering/release team
8	Deploy desktop package or release installer	Desktop/release team
9	Apply production configuration	Technical lead
10	Load approved production seed/reference data	DBA/release team
11	Run production smoke tests	QA/release team
12	Validate System Owner and Administrator login	QA/product owner
13	Validate one Supplier and one Customer path where users are ready	QA/business owner
14	Validate reports and exports	QA/product owner
15	Confirm monitoring and logs	Technical operations
16	Release to controlled MVP users	Release owner/business owner
17	Start hypercare monitoring	Support and release team

11. Monitoring And Hypercare

The first production MVP phase must include active monitoring and daily governance review.

Monitor at minimum:

- Login failures.
- Unauthorized access attempts.
- Role/menu mismatch.
- Failed API calls.
- Failed workflow transitions.
- Notification failures.
- Report/export failures.
- Database errors.
- Slow requests.
- Desktop launch or rendering issues.
- User action audit trail.
- Administrator actions.
- System Owner actions.

Hypercare should run daily for the first one to two weeks, or longer if business volume, defect count, or operational risk requires it.

12. Rollback And Recovery Strategy

Rollback must be planned before production deployment begins.

Required controls:

- Pre-deployment database backup.
- Release package archive.
- Previous frontend package archive.
- Previous backend package archive.
- Desktop package rollback option.
- Migration execution record.
- Known rollback limitations documented before approval.
- Emergency decision owner identified.
- Communication path for business users.

Rollback should be used when a production issue blocks login, corrupts data, breaks role access, prevents critical workflows, or creates unacceptable business or compliance risk.

13. MVP Scope Control

The MVP must remain controlled and not expand silently during deployment.

Production MVP includes:

- Clean login and role-based access.
- Supplier and Customer onboarding foundations.
- Operations review and activation workflows.
- Administrator user/function governance.
- System Owner Administrator governance.
- Core portal navigation and read models.
- Notifications foundation.
- Reporting and export foundation.
- Web/Desktop consistency.
- Audit and operational traceability.

Production MVP excludes unless separately approved:

- Full Islamic Finance live execution.
- Automated credit decisioning.
- Live lender offer generation.
- Full Murabaha transaction execution.
- Oracle production parity.
- Unqualified external production integrations.
- Historical test/demo data.
- Broad user rollout without stabilization sign-off.

14. External Integration Go-Live Uncertainty Paths

ETA/e-invoicing, Fawry, and Paymob are formal MVP go-live uncertainty paths. They are currently treated as held/conditional production capabilities because their activation depends on third-party credentials, merchant/account access, authority access, endpoint configuration, certification evidence, callback readiness, and owner sign-off.

These integrations may still be added to the controlled MVP at any time if the relevant third party activates the required credentials or access during MVP preparation, staging, production cutover, stabilization, or early production. This must be read as an explicit project risk and readiness dependency, not as a permanent exclusion.

External Path	Current MVP Status	Activation Trigger	Deployment Control
ETA / e-invoicing	Held / conditional	ETA credentials, authority access, target endpoint, and submission evidence become available	Change request, staging test, tax/finance sign-off, rollback plan, production approval
Fawry	Held / conditional	Fawry merchant credentials, API access, callback configuration, and payment test evidence become available	Change request, payment-flow test, reconciliation check, rollback plan, production approval
Paymob	Held / conditional	Paymob merchant credentials, API access, callback configuration, and payment test evidence become available	Change request, payment-flow test, reconciliation check, rollback plan, production approval

If any of these third-party paths become available unexpectedly, the project team must not activate them informally. They must pass impact assessment, security review, staging/pre-production validation, integration owner approval, business owner approval, and release-governance evidence before being enabled in production.

15. Release Governance

Each production release should have a documented release record that includes:

- Release version.
- Scope.
- Environment deployed.
- Migration version.
- Test evidence.
- Open defects.
- Accepted risks.
- Rollback plan.
- Business approver.
- Technical approver.
- Deployment timestamp.
- Post-deployment smoke-test result.

Production promotion requires approval from both business and technical ownership.

16. Recommended Strategy

CashLine should proceed with a controlled production MVP deployment using the following path:

Development -> QA -> Staging/Pre-production -> Controlled Production MVP -> Stabilization -> Wider rollout

This strategy gives the business a credible live operating platform while protecting the system from uncontrolled go-live risk. It also keeps advanced modules, heavier integrations, and broader rollout behind proper readiness gates.

The immediate focus should be to finalize environment readiness, database migration discipline, staging sign-off, production seed-data controls, smoke-test automation, rollback preparation, and hypercare governance before opening the platform to controlled MVP users.