PAYMENTS · DATA · AI · COMPLIANCE

Embedded Payments Delivery and Support Runbook

For platforms, fintechs and their partner banks, from requirements to live L1, L2 and L3 support: models, flow of funds, shared responsibilities, ledger reconciliation, partner approvals, live pilot, alerts, disaster recovery and audit.

SP Sankar · Payment Product Consultant

sp@paymentconsultant.top · paymentconsultant.top · linkedin.com/in/spsankar

Version 2026 · Always confirm current rules with your sponsor bank, payments provider and legal advisers.

Contents

1. Purpose and how to use this runbook
2. Planning vs delivery alignment
3. Embedded payments basics for the team
4. Rules and regulations
5. The nine kinds of work, step by step
6. Exit criteria and sign-off: E2E and UAT
7. Proving it in production
8. Controls that run across every payment
9. Security, certificates and certification
10. Production support: L1, L2 and L3
11. Operational runbooks for common incidents
12. Disaster recovery
13. Internal and external audit
14. Measures to watch
15. Go-live checklist
16. Sources

Purpose and how to use this runbook

Embedded payments means putting payments inside a product that is not a bank: a software platform that lets its customers take card payments, a marketplace that pays its sellers, a payroll app that moves money, or an app that offers accounts and cards through a partner bank. This runbook takes an embedded payments product from idea to live production and support. It is written for product managers, delivery leads, engineers, testers, operations, finance, risk and compliance teams at platforms and fintechs, and for their partner banks.

Three things make embedded payments different:

- **Many parties share the work.** The platform, a payments provider or payment facilitator, a sponsor bank and often a ledger or banking-as-a-service vendor each own part of the flow, and of the risk.
- **The platform owns the customer experience but not the licence.** The bank or licensed provider stays responsible to regulators, so the platform must prove it runs the controls.
- **Your ledger must match the bank's money.** When customer funds sit in pooled ("for benefit of", or FBO) accounts, every customer's balance must be traceable to real money at the bank, every day. The 2024 collapse of the banking-as-a-service firm Synapse, where records and bank balances did not match, showed what happens when this fails.

Golden rules for Agile embedded payments delivery

- Work in sprints, but never skip the hard gates: partner bank and provider approval, E2E and UAT exit criteria, compliance sign-off and a live pilot.
- Agree in writing who does what (onboarding checks, monitoring, disputes, complaints, reconciliation) before building.
- Reconcile the ledger to the bank every day from day one.
- Design for the rails underneath (cards, ACH, instant, wires); each brings its own rules from the other runbooks in this series.

Planning vs delivery alignment

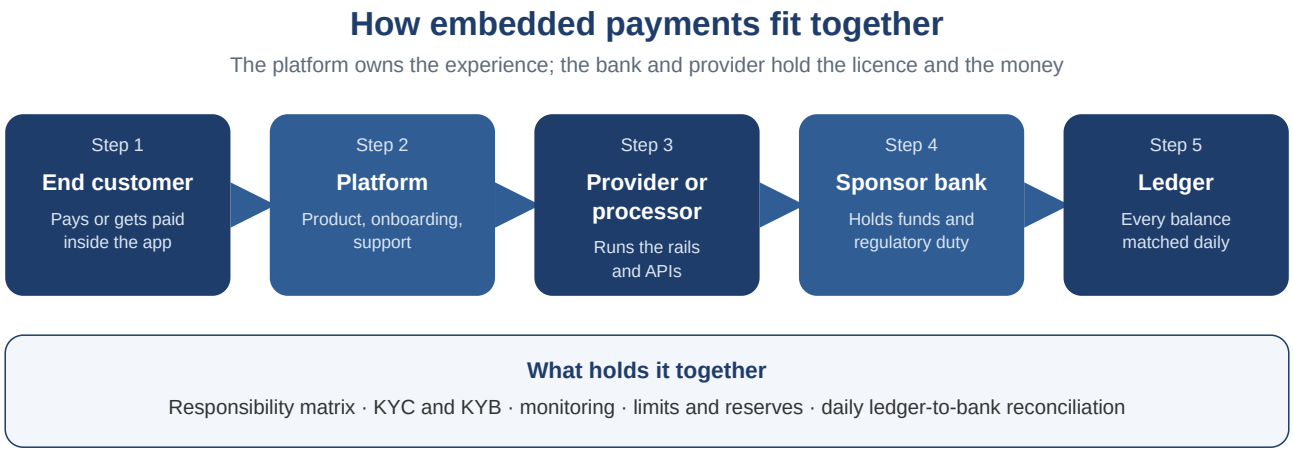
Level	What it holds	Who owns it	Reviewed
Product roadmap	Use cases, partner bank and provider milestones, regulatory changes	Product manager	Quarterly
Release or PI plan	Features committed, partner approvals, dependencies	Product manager, delivery lead	Every planning increment

Level	What it holds	Who owns it	Reviewed
Sprint plan	User stories for 2 weeks	Product owner and team	Every sprint
Release calendar	Deployment dates, freezes, partner release windows	Release manager	Weekly

- **Partner approvals are fixed dates:** program approval, marketing review and compliance testing by the sponsor bank often take weeks; plan them first.
- **Track outside dependencies:** sponsor bank, payments provider, card processor, ledger vendor, KYC and fraud vendors.
- **Measure it:** say/do ratio, feature predictability, scope change and milestone status, reported weekly.

Embedded payments basics for the team

Common models



How embedded payments fit together

How to read this picture: Read left to right: each box is one party in an embedded payments product, from the customer using the app to the ledger that records every balance. The band at the bottom lists

> what must be shared and proven across all of them, above all a daily match between the ledger and the money at the bank.

Model	What it means	Who holds the main licence or bank role
Payments provider integration	The platform uses a provider's API to take payments for its users	The provider and its acquiring bank
Payment facilitator (PayFac)	The platform signs up sub-merchants under its own merchant account	The platform, registered with the card networks through a sponsor acquirer
Banking as a service	The platform offers accounts, cards or transfers through a partner bank	The partner (sponsor) bank
Marketplace payouts	The platform collects from buyers and pays sellers	The provider or bank, plus money transmission rules to check

Who is involved

Party	Role
End customer	Pays or gets paid inside the platform
Platform (you)	Owns the product, the experience and often onboarding and support
Payments provider or processor	Runs the payment rails and APIs
Sponsor (partner) bank	Holds the funds and the regulatory responsibility
Ledger or BaaS vendor (optional)	Keeps customer balances and connects to the bank

Open banking note: the CFPB's Section 1033 rule on consumers' access to their financial data was finalized in October 2024, but a federal court stopped its enforcement in October 2025 while the CFPB reconsiders it. Check its status before relying on it for account linking.

Rules and regulations

Rule	What it means for delivery
Interagency guidance on third-party relationships (2023)	Banks must oversee their fintech partners; expect due diligence, monitoring and audits
Card network rules (for PayFacs) and PCI DSS	Sub-merchant onboarding, monitoring and card data security

Rule	What it means for delivery
Nacha Operating Rules (for ACH)	Third-party sender duties, risk assessments and audits
State money transmission laws	May apply if the platform holds or moves customer money
BSA/AML, OFAC and KYC/KYB	Customer and business checks, monitoring, SARs, often shared with the bank
Regulation E and Regulation Z	Consumer error resolution and credit rules where they apply
UDAAP and marketing review	Clear, fair product messages; many banks review all marketing
Section 1033 (open banking)	Under reconsideration and enjoined; follow updates

The nine kinds of work, step by step

These are not waterfall phases. In sprints they overlap; the gates are what matter.

Phase 1: Requirements

- Use cases, rails and money flows (draw the flow of funds for every case).
- Who does what: a responsibility matrix covering onboarding, monitoring, disputes, complaints and reconciliation.
- Onboarding: KYC for people, KYB for businesses, risk ratings and limits.
- Fees, payouts timing, reserves and negative balance handling.

Exit: requirements and the flow of funds approved by the platform, provider and sponsor bank.

Phase 2: Design

- API integration with the provider; webhooks; idempotency.
- Ledger design: one entry per movement, balances by customer, daily match to the bank's FBO account.
- Onboarding and monitoring flows with clear handoffs to the bank.
- Data sharing with the bank for oversight and audits.

Exit: architecture, security and partner design reviews passed.

Phase 3 to 5: Development, unit and performance testing

- Build in the provider's sandbox; secrets in a vault.
- Unit tests for ledger entries, fees, limits and status changes.
- Performance tests for payout days and sale events.

Phase 6: End-to-end (E2E) testing

- Every money flow end to end: pay in, hold, pay out, refund, dispute, return, reversal.
- Onboarding approvals, declines and reviews; limits and reserves.
- Ledger to bank reconciliation with real-looking volumes.

Phase 7: User acceptance testing (UAT)

- Operations, support, risk and finance run real cases, including a dispute and a negative balance.
- Sponsor bank reviews customer journeys, disclosures and marketing.

Phase 8 and 9: Release and deployment

- Partner sign-off, change approval and rollback plan.
- Deploy, smoke test, then a live pilot (see "Proving it in production"); hypercare.

Exit criteria and sign-off: E2E and UAT

E2E exit criteria

- [ ] 100% of planned test cases run; at least 95% passed; no open Severity 1 or 2 defects
- [ ] Every money flow traced from the customer to the bank account and back
- [ ] Ledger to bank reconciliation balanced to the cent
- [ ] Onboarding, monitoring and limits behave as designed
- [ ] Disputes, returns and refunds work end to end

UAT exit criteria

- [ ] Business scenarios signed by the business owner
- [ ] Support, risk and finance procedures tested by the people who use them
- [ ] Disclosures and marketing approved by the sponsor bank

Sign-off matrix

Who signs	What they confirm
Product owner	Features meet acceptance criteria
QA lead	Exit criteria met, evidence stored
Finance	Ledger and reconciliation ready
Risk and compliance	KYC/KYB, AML, consumer rules met

Who signs	What they confirm
Sponsor bank and provider	Program approved for launch
Information security	Security testing passed
Change manager	Release approved

Proving it in production

1. Onboard a small group of friendly customers (often employees and a few trusted businesses).
2. Run real low-value payments in every flow: pay in, pay out, refund, dispute.
3. Check fees, payout timing and notifications.
4. Reconcile the ledger to the bank account every day of the pilot.
5. Review the pilot with the sponsor bank before opening to more customers.

Exit: pilot money flows reconciled; sign-off by product, finance, compliance and the sponsor bank.

Controls that run across every payment

Control	What good looks like
Responsibility matrix	Every control has a named owner across platform, provider and bank
KYC/KYB and risk rating	Every customer checked before they can move money
Transaction monitoring	Fraud and AML monitoring with clear escalation to the bank
Limits and reserves	Set by risk level; reviewed regularly
Ledger reconciliation	Daily match of every customer balance to bank funds
Complaint handling	Logged, tracked and shared with the bank
Data protection	Least data, encrypted, shared only as agreed

Security, certificates and certification

- **Access:** least privilege, quarterly reviews, PAM, NIST SP 800-63B and multi-factor authentication.
- **API keys and certificates:** in a vault, rotated; track expiry with alerts at 60, 30 and 7 days.
- **Partner certification:** provider and bank testing before launch and after major changes; PCI DSS where card data is in scope.

- **Vendors, licences and open source:** SOC reports from every partner; dependency scanning on every build.

Production support: L1, L2 and L3

Level	Who	What they do	Target
L1	Platform support and operations	Customer queries, first triage	Acknowledge within 15 minutes
L2	Application support	Diagnose API, webhook, ledger and payout issues	Respond within 30 minutes
L3	Engineering, provider and bank	Code fixes, hotfixes, root cause	Engaged within 1 hour for Sev 1

Severity levels: Sev 1 when payments or payouts fail for many customers or the ledger and bank don't match (bridge within 15 minutes, partner bank told); Sev 2 for one flow failing or payouts delayed (30 minutes); Sev 3 for a single payment (next business day).

Alerts: to Slack or Teams and paging for payment success rate below normal, API errors, webhook backlogs, payout file failures, reconciliation breaks and fraud spikes. Agree with the sponsor bank which incidents they must hear about and how fast.

Escalation and hotfixes: L1 to L2 at 15 minutes; L2 to L3, provider and bank at 30 minutes; senior leaders for any Sev 1. Hotfixes follow the emergency change process with a review within 5 business days.

Operational runbooks for common incidents

1. Ledger and bank don't match

1. Stop payouts if the gap is material; tell the sponsor bank.
2. Find the cause (missed webhook, duplicate entry, returned payment); correct with approved entries only.

2. Payout file failed

1. Check the provider or bank reject reason; fix and resend once.
2. Tell affected customers when they will be paid.

3. Fraud ring among new sign-ups

1. Freeze affected accounts; tighten onboarding rules.
2. Report to the bank; file SARs as agreed in the responsibility matrix.

Disaster recovery

Item	Example target
Recovery time objective (RTO)	Under 1 to 4 hours, agreed with the bank
Recovery point objective (RPO)	Zero for ledger entries

- [ ] Ledger backed up and replicated; restore tested
- [ ] Backup region can reach the provider and bank
- [ ] DR test at least once a year, with evidence
- [ ] After failover, reconcile the ledger to the bank before reopening payouts

Internal and external audit

Internal audit checklist

- [ ] Responsibility matrix current and agreed with all partners
- [ ] KYC/KYB complete for sampled customers
- [ ] Monitoring alerts worked and escalated as agreed
- [ ] Daily ledger to bank reconciliation done; breaks closed
- [ ] Complaints logged and shared with the bank
- [ ] Access reviews quarterly; no direct database changes without approved tickets
- [ ] DR test in the last 12 months

External audit and partner review checklist

- [ ] Evidence index linking each control to its evidence
- [ ] Sponsor bank oversight reports and findings
- [ ] Customer, payment and complaint population lists ready to sample
- [ ] Change records with approvals, partner sign-off and pilot evidence
- [ ] BSA/AML program, training and independent testing
- [ ] Partner SOC reports and PCI attestations
- [ ] Open findings tracker with owners and dates

Measures to watch

Measure	Why it matters
Payment and payout success rate	The product working for users
Reconciliation breaks	Customer money must always match the bank
Onboarding approval and fraud rates	Growth versus risk
Disputes and complaints	Customer harm and partner concern
Partner findings open	Health of the bank relationship

Go-live checklist

- [ ] Sponsor bank and provider approval received
- [ ] E2E and UAT exit criteria met and signed
- [ ] Pilot money flows reconciled
- [ ] KYC/KYB, monitoring, limits and reserves live
- [ ] Daily reconciliation running
- [ ] Alerts, on-call and partner escalation tested
- [ ] DR path tested

Sources

- Federal banking agencies: Interagency Guidance on Third-Party Relationships (June 2023)
- CFPB: Personal Financial Data Rights (Section 1033) rule (October 2024) and reconsideration; court injunction (October 2025)
- Card network PayFac rules, PCI DSS v4.0.1, Nacha Operating Rules