PAYMENTS · DATA · AI · COMPLIANCE

Cross-Border Payments over SWIFT Delivery and Support Runbook

From requirements to live L1, L2 and L3 support: correspondent banking, ISO 20022 under CBPR+, structured data, sanctions, FX, live pilot per corridor, 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 SWIFT, your correspondents and your own bank policies.

Contents

1. Purpose and how to use this runbook
2. Planning vs delivery alignment
3. Cross-border 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

This runbook takes a cross-border payment change, for example a new international wire product, a new corridor or currency, a correspondent bank change or a SWIFT platform upgrade, from idea to live production and support. It is written for product managers, delivery leads, engineers, testers, operations, sanctions and compliance teams.

Cross-border payments add three things to a domestic wire:

- **More banks in the chain.** A payment can pass through one or more correspondent (intermediary) banks before it reaches the beneficiary's bank, each with its own checks, fees and cutoffs.
- **More rules.** Sanctions in several countries, foreign exchange, consumer remittance rules and the receiving country's own requirements.
- **A new message standard.** SWIFT ended the coexistence of old MT messages and ISO 20022 for cross-border payment instructions on November 22, 2025. MT103 and MT202 payment instructions are now replaced by pacs.008 and pacs.009 under the CBPR+ rules.

Golden rules for Agile cross-border delivery

- Work in sprints, but never skip the hard gates: SWIFT and correspondent testing, sanctions sign-off, E2E and UAT exit criteria, and a live pilot in every new corridor.
- Data quality is the product: structured names, addresses, purpose and remittance data decide whether a payment flows or stops.
- Test the whole chain, including returns, rejects and investigations, not just the first hop.
- Plan around SWIFT's yearly Standards Release (each November), holidays in every currency you send, and correspondent cutoffs.

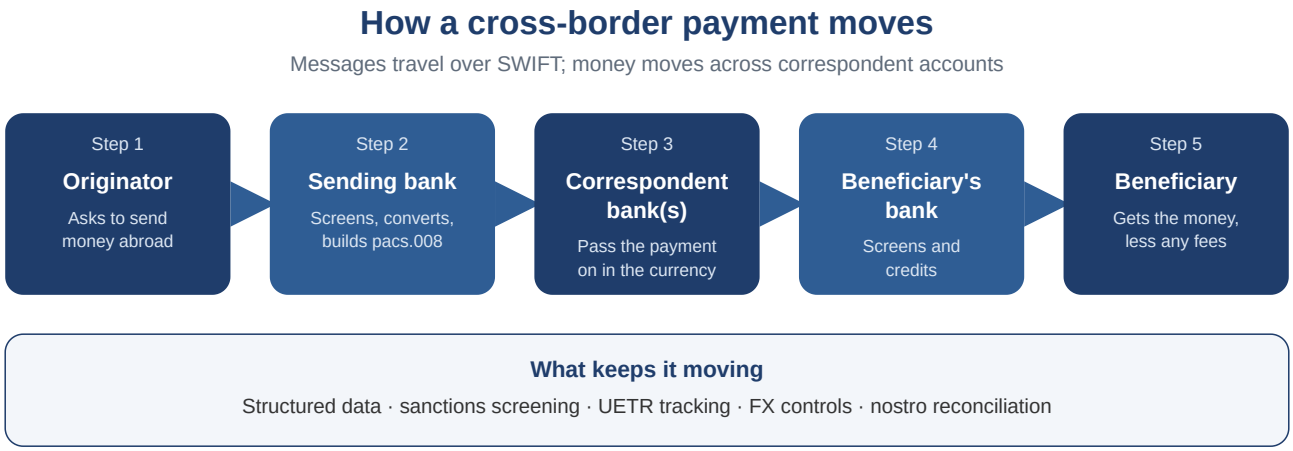
Planning vs delivery alignment

Level	What it holds	Who owns it	Reviewed
Product roadmap	Corridors, currencies, SWIFT Standards Release dates, regulatory changes	Product manager	Quarterly
Release or PI plan	Features committed, correspondent test slots, dependencies	Product manager, delivery lead	Every planning increment
Sprint plan	User stories for 2 weeks	Product owner and team	Every sprint
Release calendar	Deployment dates, freezes, SWIFT release weekend, holiday calendars	Release manager	Weekly

- **SWIFT release first:** every November's Standards Release brings mandatory changes; plan backwards from it.
- **Track outside dependencies:** SWIFT, each correspondent bank, the FX provider and the sanctions screening vendor, each with an owner and date.
- **Measure it:** say/do ratio, feature predictability, scope change and milestone status, reported weekly.

Cross-border basics for the team

Who is involved



How a cross-border payment moves

How to read this picture: Read left to right: each box is one bank or person a cross-border payment passes through. There can be more than one correspondent bank in the middle. The band at the bottom lists what keeps the payment from stopping: good structured data, sanctions checks at every bank, and tracking with the UETR.

Party	Role
Originator	The customer sending money abroad
Sending bank	Checks the request, screens it, converts currency if needed, sends the payment
Correspondent (intermediary) banks	Hold accounts for other banks and pass the payment on in a currency
SWIFT	The secure messaging network banks use to send payment instructions; it does not hold or settle money
Beneficiary's bank	Receives the payment and credits the beneficiary

Party	Role
Beneficiary	The person or business receiving the money

Key facts

Topic	What to know
Message standard	ISO 20022 under CBPR+ since November 22, 2025: pacs.008 for customer payments, pacs.009 for bank payments and cover, pacs.004 for returns, camt.056 and camt.029 for cancellations, camt.052/053/054 for reports
Tracking	Every payment carries a UETR (unique end-to-end transaction reference); SWIFT gpi lets banks track the payment and its fees along the chain
Addresses	Structured or "hybrid" addresses (with at least town and country) are now expected; fully unstructured addresses are being retired. SWIFT has extended the original November 2026 deadline, so check the current SWIFT timeline
Settlement	Money moves across correspondent accounts; in US dollars the last step usually settles over CHIPS or Fedwire
Security	SWIFT's Customer Security Programme requires a yearly attestation against its security controls

Rules and regulations

Rule	What it means for delivery
SWIFT CBPR+ usage guidelines and Standards Releases	How every cross-border message must be built; yearly changes
SWIFT Customer Security Programme (CSP)	Yearly security attestation for your SWIFT environment
UCC Article 4A	Governs commercial funds transfers in the US
Regulation E, Subpart B (Remittance Transfer Rule)	Consumer cross-border payments: pre-payment disclosure of fees and exchange rate, receipt, 30-minute cancellation, error resolution
OFAC and other countries' sanctions	Screen every party, bank, country and free text; block or reject as required
BSA/AML, Travel Rule and correspondent due diligence	Keep and pass originator and beneficiary data ($3,000 and above), know your correspondents, file SARs

Rule	What it means for delivery
Receiving-country rules	Purpose codes, tax IDs and local data requirements in some corridors

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

- Corridors, currencies and products (consumer remittance, business payment, bank-to-bank).
- FX: rate source, margin, quote validity and when the rate is locked.
- Fees: who pays (sender, receiver or shared) and how they are shown.
- Data needed per corridor: structured addresses, purpose codes, IDs.
- Consumer remittance disclosures and receipts where Reg E applies.

Exit: requirements signed by product, operations, sanctions, compliance and treasury.

Phase 2: Design

- Routing: which correspondent for each currency and country; backup routes.
- Sanctions screening on every field, including free text, with clear hit handling.
- Building ISO 20022 messages to CBPR+ rules; cover payments where needed.
- Investigations and exceptions: cancellations, returns, queries, gpi tracking.
- Reconciliation of nostro accounts (your accounts at correspondents).

Exit: architecture, security and sanctions design reviews passed.

Phase 3: Development

- Build to CBPR+ usage guidelines; validate every message before sending.
- Store the UETR for every payment and show tracking to customers where offered.
- Code review, static analysis and dependency scanning on every change.

Phase 4: Unit testing

- Message building, validation rules, FX and fee calculations, cutoff and holiday logic per currency.

Phase 5: Performance testing

- Peak volumes (month end, payroll days in other countries) with screening switched on.

Exit: peak volume handled with headroom, no message loss.

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

- Send and receive through SWIFT test environments and with correspondent banks.
- Returns, rejects, cancellations, investigations, sanctions hits and repairs.
- FX booking, fees, nostro reconciliation and customer receipts.

Phase 7: User acceptance testing (UAT)

- Operations, sanctions and investigation teams run real cases.
- Customer journeys: quote, disclosure, send, receipt, tracking, cancellation.

Phase 8: Release management

- Change approval, rollback plan; align with the SWIFT Standards Release weekend.

Phase 9: Deployment

- Deploy, smoke test, then a live pilot per corridor (see "Proving it in production"); hypercare.

Exit criteria and sign-off: E2E and UAT

E2E exit criteria

- [ ] All CBPR+ messages validated; correspondent testing passed for each corridor
- [ ] 100% of planned test cases run; at least 95% passed; no open Severity 1 or 2 defects
- [ ] Sanctions screening tested on all fields, including free text
- [ ] Returns, cancellations and investigations work end to end
- [ ] FX, fees and nostro reconciliation balanced

UAT exit criteria

- [ ] Business scenarios signed by the business owner
- [ ] Operations, sanctions and investigation procedures tested by the people who use them
- [ ] Reg E disclosures and receipts checked where they apply

Sign-off matrix

Who signs	What they confirm
Product owner	Features meet acceptance criteria

Who signs	What they confirm
QA lead	Exit criteria met, evidence stored
Operations head	Team trained, procedures ready
Sanctions and compliance	OFAC, AML, Travel Rule and Reg E met
Treasury	FX and nostro funding ready
Information security	SWIFT CSP controls in place
Change manager	Release approved

Proving it in production

1. Send a small live payment in each new corridor and currency to an account you control or a friendly correspondent.
2. Track it end to end with the UETR and confirm the fees deducted along the way.
3. Confirm the beneficiary was credited with the right amount, name and reference.
4. Receive a small incoming payment and post it correctly.
5. Run a cancellation or return.
6. Reconcile the nostro accounts and the general ledger.

Exit: pilot payments settled and reconciled in every corridor; sign-off by product, operations, sanctions and treasury.

Controls that run across every payment

Control	What good looks like
Sanctions screening	Every party, bank, country and free-text field screened before release
Data quality checks	Structured addresses, purpose and IDs present before sending
Dual approval and callback	As for domestic wires: second approver and callback for new or changed instructions
Limits	Per payment, per day, per customer and per corridor
Correspondent due diligence	Reviewed at onboarding and on a set cycle
FX controls	Rate source, approval of margins, limits on open positions

Control	What good looks like
Nostro reconciliation	Daily, with breaks investigated
SWIFT security (CSP)	Controls in place and attested every year

Security, certificates and certification

- **Access:** least privilege, quarterly reviews, PAM, NIST SP 800-63B for passwords and multi-factor authentication. SWIFT operator roles split so no one person can create and release.
- **SWIFT environment:** follow the CSP controls; protect the secure zone, keys and HSMs; track certificate and key expiry with alerts at 60, 30 and 7 days.
- **Certification:** SWIFT and correspondent testing for new message types and corridors; keep evidence.
- **Vendors, licences and open source:** SWIFT interface and screening software versions, support dates and licences; scan dependencies on every build.

Production support: L1, L2 and L3

Level	Who	What they do	Target
L1	Payment operations and investigations	Repair payments, answer queries, gpi tracking, first triage	Acknowledge within 15 minutes
L2	Application and SWIFT support	Diagnose message, connection and screening issues	Respond within 30 minutes
L3	Engineering and vendors	Code fixes, hotfixes, root cause	Engaged within 1 hour for Sev 1

Severity levels

Severity	Example	Response
Sev 1	SWIFT connection down; screening down; payments can't leave before cutoff	Bridge within 15 minutes
Sev 2	One corridor or correspondent failing; rejects rising	Within 30 minutes
Sev 3	Single payment query	Next business day

Alerts and notifications: alerts to Slack or Teams and paging for SWIFT connection loss, messages stuck, NAKs (negative acknowledgements) or rejects rising, screening queue age, nostro balance low, and

certificate expiry. Email stakeholders for Sev 1 and Sev 2 every 30 minutes.

Escalation: L1 to L2 at 15 minutes; L2 to L3 and the incident manager at 30 minutes; senior leaders for any Sev 1 or a missed currency cutoff.

Hotfixes: emergency change with a named approver, peer review, test in a lower environment and a review within 5 business days.

Operational runbooks for common incidents

1. Payments rejected after the ISO 20022 switch

1. Read the reject reason; most are data quality (address, name, purpose code).
2. Repair and resend with the same UETR rules; fix the source data, not just the message.

2. Payment stuck at a correspondent

1. Track it with the UETR in gpi; contact the correspondent's investigations team.
2. Tell the customer what you know and when you will update them.

3. Sanctions hit after release (late match)

1. Follow your sanctions procedure at once; involve compliance.
2. Report to OFAC within the required time if funds are blocked.

4. Customer cancels a consumer remittance

1. Check the Reg E 30-minute cancellation right and refund as required.
2. If already sent, send a cancellation request (camt.056) and track the answer.

Disaster recovery

Item	Example target
Recovery time objective (RTO)	2 to 4 hours, and before the key currency cutoffs
Recovery point objective (RPO)	Zero for accepted payments

- [ ] Backup SWIFT connection and site tested
- [ ] Screening available at the backup site
- [ ] DR test at least once a year, with evidence
- [ ] After failover, reconcile every payment by UETR to avoid duplicates

Internal and external audit

Internal audit checklist

- [ ] Cross-border policies and procedures current and approved
- [ ] SWIFT CSP attestation submitted on time and supported by evidence
- [ ] Sanctions screening complete; hits decided and documented
- [ ] Travel Rule data present; correspondent due diligence current
- [ ] Reg E remittance disclosures, cancellations and errors handled on time
- [ ] Dual approval and callback controls working (sample payments)
- [ ] Access reviews quarterly; no direct database changes without approved tickets
- [ ] Nostro reconciliation daily; breaks closed
- [ ] DR test in the last 12 months

External audit and exam checklist

- [ ] Evidence index linking each control to its evidence
- [ ] Payment population lists ready to sample
- [ ] Change records with approvals, testing and pilot evidence
- [ ] Access lists and review sign-offs
- [ ] Incident records and root cause reviews
- [ ] BSA/AML, OFAC and correspondent banking policies, training and independent testing
- [ ] Vendor SOC reports
- [ ] Open findings tracker with owners and dates

Measures to watch

Measure	Why it matters
Straight-through processing rate	Payments that need no repair
Reject and return rate by corridor	Data quality and routing problems
Time to credit the beneficiary (gpi)	What customers care about
Sanctions queue age	Delays and cutoff misses
Nostro breaks	Must be zero at end of day
Customer queries per 1,000 payments	Signs of unclear fees or slow payments

Go-live checklist

- [ ] SWIFT and correspondent testing complete
- [ ] E2E and UAT exit criteria met and signed
- [ ] Live pilot payments settled and reconciled in each corridor
- [ ] Sanctions screening, limits, dual approval and callback live
- [ ] FX and nostro funding ready
- [ ] Alerts, on-call and escalation tested
- [ ] DR path tested
- [ ] Operations and investigations teams trained

Sources

- SWIFT: CBPR+ and the end of MT/ISO 20022 coexistence (November 22, 2025); Payments Market Practice Group guidance on structured and hybrid addresses
- Regulation E Subpart B; UCC Article 4A; BSA recordkeeping rules (31 CFR 1010.410); OFAC