

Why Fragmented Payments Testing Undermines Change Assurance in Financial Services

A Practitioner's Perspective on Testing Transformation in Regulated Payments Environments

Giovanni Leonardi

December 2025



Why Fragmented Payments Testing Undermines Change Assurance in Financial Services

*Transformation · No. 429
December 2025*

1. The Problem Nobody Wants to Name

In financial services organisations that process high volumes of international payments, testing models have become collections of disconnected activities rather than coherent assurance mechanisms. Core payment engines, ancillary vendor platforms, internal development teams, QA functions, regression suites, end-to-end flows and UAT cycles each generate their own artefacts, yet none can demonstrate collectively that coverage is complete or that risk has been systematically reduced. The result is that change programmes proceed with technical outputs that satisfy individual phase gates while leaving material gaps in the ability to prove that payments will behave as expected once live.

This fragmentation persists because organisations continue to treat testing as a series of contractual deliverables rather than an integrated control. When a vendor completes its QA, an internal team runs UAT and a separate function manages end-to-end scenarios, accountability for overall integrity becomes diffused. Evidence of duplication is visible in overlapping test cases, repeated environment builds and conflicting defect logs, yet the underlying model remains unchallenged because each party can point to its own completed artefacts.

2. Why It Happens — Three Structural Reasons

Three structural conditions sustain the pattern. First, vendor contracts are written around isolated phase responsibilities without requiring integrated traceability. Payment system vendors deliver against their own development and QA milestones; downstream teams then recreate similar coverage because contractual acceptance criteria do not reference upstream artefacts. Second, test documentation standards remain phase-specific rather than ecosystem-wide. Without a single traceability framework that maps requirements through to field-level and data-level outcomes across every application in the payments hub, coverage claims cannot be validated. Third, test environments are funded and managed as tactical assets rather than strategic ones. The cost and complexity of maintaining consistent versioning across interconnected applications discourages investment in environments that could support higher-quality, automated testing.

These conditions are reinforced by delivery pressure. Programmes that must meet regulatory or market deadlines accept the existing model because redesigning it appears to add time rather than reduce risk.

3. What Good Looks Like — The Three-Level Fix

3.1 Governance and structural level

A central testing authority, independent of individual vendors and delivery teams, owns the end-to-end test strategy. This body defines the single set of coverage objectives, mandates artefact standards and holds contractual levers to require upstream vendors to produce evidence in a common format. Tactical improvements to environment provisioning are approved only when they demonstrably reduce duplication across phases.

3.2 Data, insight and measurement level

A unified traceability matrix becomes the primary control artefact. Every requirement, including those related to SWIFT messaging, ISO 20022 formats, AML screening and sanctions checks, is mapped to test cases at the appropriate level of granularity. Automation is prioritised where regression volume is highest and where field-level and data-level verification can be executed repeatedly without manual intervention. Metrics shift from phase completion percentages to measures of residual coverage gaps and defect escape rates between phases.

3.3 People, stakeholder and culture level

Capability is built through deliberate rotation of testers across vendor and internal teams, and through shared tooling that replaces fragmented instances of JIRA, ServiceNow and Confluence with a single source of truth. Success is defined by the ability of the combined testing community to produce a single, defensible statement of coverage rather than by the volume of test cases executed within any one phase.

4. The Sector-Specific Complication

Regulated payments environments add a further constraint: every testing decision must withstand regulatory scrutiny. Evidence of coverage must be auditable not only for functional correctness but also for compliance with sanctions screening, fraud controls and data integrity rules. This requirement makes superficial harmonisation dangerous; any new model must demonstrably strengthen, rather than dilute, the chain of evidence that regulators expect to see.

5. Conclusion

Organisations that continue to optimise individual testing phases while leaving the overall model untouched will keep delivering change that passes internal gates yet carries unexamined operational risk. The uncomfortable question is whether the next payments

transformation programme will still be accepted on the basis of phase-by-phase sign-off, or whether leadership will insist on a single, integrated view of testing integrity before any release is authorised.