

Preserving Segregation of Duties in Agentic Payments Delivery

A Joint Control Method for Bank Managers

Phil Hatch | Akholi

October 23, 2026

Bank payment and vendor-access managers should preserve independently enforced preparation, approval, and execution when provider agents act. Different agent names do not establish separation if one credential or administrator can control the entire transaction.

Test the Transaction Rather Than the Role Chart

The bank's payments control owner should require proof that a provider agent cannot prepare, approve, and execute the same consequential transaction outside the bank's authorized design. A role matrix is useful only when the systems enforce it. Two agent labels can conceal a single credential, shared permissions, or an administrator able to bypass both roles.

Start with one payment or account-maintenance workflow. Identify what creates the instruction, validates the beneficiary, approves the amount, releases the transaction, and reconciles the result. Include amendments and cancellation, because a post-approval change can alter the substance of an apparently authorized payment without requiring a new approval.

The study records respondents' accounts of agents using shared service accounts or staff credentials. Those reports do not verify the underlying permissions, but they justify testing whether actual identities preserve attribution and control. Managers should reconstruct the access path before accepting the provider's statement that duties are separated.¹

¹ Phil Hatch, *Agentic AI Outsourcing at Tier 1 Financial Institutions: Full Study Report*, version 1.8.2 (Akholi, forthcoming manuscript dated November 1, 2026), Part 3, Financial Institution Readiness, sec. 4.1, "Ability to Provision Access and Identities for Agents," indicator C108, <https://doi.org/10.2139/ssrn.7164559>.

Bind Approval to the Action That Executes

The approval record should identify the transaction attributes it authorizes: beneficiary, destination, currency, amount, value date, and relevant case reference. The bank should define which changes invalidate approval. The execution system should compare the proposed action with that approval rather than trust a narrative assertion that the payment was previously reviewed.

A hypothetical agent could prepare a valid payment, obtain approval, and then update the destination before release. The control must reject the changed transaction or obtain a fresh independent approval. Recording the approver's identity without binding the approval to the released instruction leaves the manager unable to establish what was approved.

Delegation requires the same discipline. A provider's orchestrating agent should not gain approval authority by asking another agent it controls to approve the request. The bank needs a decision about independence, credentials, administrative control, and allowed delegation, with an enforcement point outside the preparing agent's ability to modify.

Create a Joint Transaction Authority Record

Figure 1 proposes a transaction authority record that managers can complete with bank IAM, payments operations, and provider leads. Each stage should identify the principal performing it, the authority granted, the control preventing incompatible access, and the record proving execution. The record should name the firm that owns each enforcement point.

The allied agent-security guidance recommends distinct identities, bounded delegation, and codified separation of duties. It supports the control direction without prescribing a bank-specific payment architecture. Managers still need to test their own systems, payment rules, and exception routes rather than treat guidance conformity as evidence that a transaction is protected.²

NIST's identity and authorization initiative also distinguishes identification, authorization, auditing, and non-repudiation as design questions. Its concept-paper status matters: a vendor cannot use the announcement as certification of its identity scheme. Require the actual grant chain and observed denial of an incompatible action.³

² Australian Signals Directorate's Australian Cyber Security Centre et al., *Careful Adoption of Agentic AI Services* (Australian Signals Directorate, May 1, 2026), "Manage third-party components," "Identity management," "Resilience," and "Human in the loop," <https://www.cyber.gov.au/publication/careful-adoption-of-agentic-ai-services>.

³ National Institute of Standards and Technology, "New Concept Paper on Identity and Authority of Software Agents," National Institute of Standards and Technology, February 5, 2026, project status and identification, authorization, auditing, and non-repudiation questions, <https://www.nist.gov/news-events/news/2026/02/new-concept-paper-identity-and-authority-software-agents>.

Figure 1. Prove separation through the complete transaction

Stage	Required authority boundary	Manager evidence
Prepare	Cannot independently approve own instruction	Originator identity and content
Approve	Independent permitted approval	Approved transaction attributes
Execute	Release only the approved instruction	Execution identity and exact match
Amend or recover	Reapproval or authorized exception	Change record and reconciliation

Author's proposed operating framework. Adapt to the service and applicable jurisdiction; not an empirically validated standard.

Source: Phil Hatch, proposed framework developed for this paper.

Challenge the Routes That Bypass the Normal Flow

Test shared accounts, emergency access, batch interfaces, duplicate submissions, stale approvals, and configuration changes. A control that works in the ordinary application may fail through an administrative API or a retained provider credential. Record who can modify the approval rules and whether that person can also release transactions without an independent check.

Emergency access should have a defined purpose, expiry, monitoring, and retrospective review by someone outside the emergency action. The bank should decide which actions remain prohibited even during an incident. A broad break-glass privilege can make the control appear available while removing the separation it was intended to preserve.

Managers should also test access withdrawal during an unfinished transaction. Revoking the parent agent may leave a delegated credential or queued release active. Reconcile the transaction's final state before replaying work; otherwise, a recovery attempt can create a duplicate payment. Use safe test environments and approved synthetic transactions.

Connect Local Control Duties to the Shared Service

The operational record can be common across the bank's jurisdictions, while the legal and supervisory conclusions remain local. FINMA's observations on AI accountability, documentation, and independent review provide a Swiss reference for the assurance

discussion. They do not establish that the same approval design satisfies every bank's payment obligations.⁴

A useful negative test begins with a valid approval and then changes one protected attribute before execution. The receiving system should reject the mismatch, retain the attempted change, and preserve the original approval for investigation. Repeat the scenario through an administrative or batch route where permitted in the test scope. The test is stronger when it proves the enforced boundary directly, rather than infer separation from the names of the agents or reviewers involved.

For EU, UK, and US entities, the bank's compliance and payments specialists should identify applicable obligations and the functions retained by the bank. The provider should receive explicit instructions about authority, evidence, and changes. Managers should resolve conflicting local requirements before a shared agent can route or release the affected work.

Avoid solving an access delay by informally lending a staff identity. If the approved agent identity cannot be provisioned, the service owner should choose an authorized fallback and record the cost and service impact. Hidden workarounds weaken attribution and can leave assurance based on a workflow that nobody is using.

Require a Demonstrated Denial Before Release

Before production approval, the bank and provider should demonstrate that an unauthorized preparation, approval, amendment, or release is denied. The test should preserve the action request and the resulting system state. Retest when privileges, delegations, payment interfaces, or approval rules change.

The manager's acceptance decision should state which transaction scope is protected, which exceptions remain, and who owns remediation. Separation of duties is established by incompatible authority being prevented and independently evidenced throughout the transaction. That is the basis for expanding an agent's role in payment delivery.

⁴ Swiss Financial Market Supervisory Authority, *Governance and Risk Management When Using Artificial Intelligence* (Swiss Financial Market Supervisory Authority, December 18, 2024), FINMA Guidance 08/2024, secs. 2.1–2.7, https://www.finma.ch/~media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmittelungen/20241218-finma-aufsichtsmittelung-08-2024.pdf?hash=60E2745D7AC1D7F4E06CE43474539F68&sc_lang=en.

Evidence and Source Note

The study is a nonrepresentative cross-section of 850 vendor delivery-team respondents on 150 engagements serving Tier 1 financial institutions, collected during January–June 2026. Neither banks nor vendors corroborated the accounts. It establishes reported experience, not causation, legal breach, or market prevalence. The author-supplied version 1.8.2 is dated November 1, 2026 and is cited as a forthcoming manuscript consulted October 23, 2026.⁵

This is an analytical decision paper based on the supplied study and selected primary public sources checked through October 23, 2026. The original contribution is a joint transaction authority record and a set of negative tests for payment preparation through recovery. The proposed method has not been independently validated. Legal requirements depend on the entity, activity, jurisdiction, and effective provisions; supervisory observations, research, and professional commentary have distinct authority.

Bibliography

Australian Signals Directorate's Australian Cyber Security Centre et al.. *Careful Adoption of Agentic AI Services*. Australian Signals Directorate, May 1, 2026. <https://www.cyber.gov.au/publication/careful-adoption-of-agentic-ai-services>.

Hatch, Phil. *Agentic AI Outsourcing at Tier 1 Financial Institutions: Full Study Report*. Version 1.8.2. Akholi. Forthcoming manuscript dated November 1, 2026. Author-supplied manuscript consulted October 23, 2026. <https://doi.org/10.2139/ssrn.7164559>.

National Institute of Standards and Technology. "New Concept Paper on Identity and Authority of Software Agents." National Institute of Standards and Technology. February 5, 2026. <https://www.nist.gov/news-events/news/2026/02/new-concept-paper-identity-and-authority-software-agents>.

Swiss Financial Market Supervisory Authority. *Governance and Risk Management When Using Artificial Intelligence*. Swiss Financial Market Supervisory Authority, December 18, 2024. https://www.finma.ch/~media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmittelungen/20241218-finma-aufsichtsmittelung-08-2024.pdf?hash=60E2745D7AC1D7F4E06CE43474539F68&sc_lang=en.

⁵ Hatch, *Agentic AI Outsourcing*, Introduction, "Executive Summary" and "Evidentiary Basis and Its Limits."