Regulated Agent Harness Architecture

Authority, action controls and evidence for financial-services agents

Owner grants authority → agent proposes action → identity and scope → policy → validation / human decision → controlled execution → evidence

CONTROL / KLA SURFACE AND DEPLOYMENT ACCEPTANCE TEST

01 Authority	**Agent Registry; governed request identity** Unrecognized or out-of-scope agent cannot perform the action.
02 Tool and data scope	**Tool Catalog; Data Boundaries** Restricted tool, record and tenant requests are rejected.
03 Pre-action policy	**Policy Builder; KLA Policy Engine** Exercise allow, warn, require_approval and block on the integrated path.
04 Validation	**Simulation; workflow-specific checks** Invalid output and unsafe state transitions fail before release.
05 Human escalation	**Decision Desk** Rejection and expiry prevent the approved-action path from executing.
06 Monitoring	**Assurance Center; Lineage Explorer** A control failure becomes an owned finding with a response.
07 Evidence	**Audit Trail; Evidence Room** Reconstruct request, decision, human review and actual execution outcome.

Boundary: KLA maps to configured governed paths. Verify alternate credentials, direct calls and delegated actions. Assign network isolation and sandboxing to the host environment.

Standards preparation: Risk: prEN 18228; cybersecurity: prEN 18282; logging: prEN 18229-1. Quality-management processes sit around these controls. Topic-level KLA mapping; no conformity or certification claim.

Informed by the Bank of England's 2 September 2026 cyber-defence harness note. The seven-control grouping is KLA's interpretation. The note creates no new supervisory expectations and does not endorse KLA.