Banking Workflow Compliance Documentation — Template

The audit-ready documentation pack every AI workflow needs before it goes live in production. Mapped to OCC, FDIC, Fed, FinCEN, GLBA, NYDFS, and SOC 2. One template, repeat for every flow.

From HitLai Institute — Module B2: "Banking AI Workflows — KYC, AML, and Beyond"

WHAT THIS IS FOR

The difference between a bank that survives an exam on AI and a bank that gets an MRA is the documentation pack behind each AI workflow. Examiners do not ask "do you have AI?" They ask "show me the documentation for THIS specific use case."

This template is the documentation pack. Fill it in once per workflow, refresh on a defined cadence, and you have what every internal auditor, examiner, and large customer's vendor risk team expects to see. Adapt to your bank's existing documentation standards.

HOW TO USE THIS TEMPLATE

For every AI workflow in the bank's inventory (see [[B2-01-Banking-Workflow-Catalog]]):

1. Complete each section below.
2. Get the named approvers' signatures (electronic or physical, per the bank's standard).
3. Store in the bank's policy / procedure / model risk repository alongside related policies.
4. Refresh on the cadence in Section 12.
5. Cross-reference from the Regulatory Mapping Matrix ([[B1-02-Regulatory-Mapping-Matrix]]) and the AI Governance Policy.

If you cannot fill in a section honestly, the workflow is not ready for production.

SECTION 1 — WORKFLOW IDENTIFICATION

Workflow name: _____

Workflow ID: _____

Business unit: _____

Business owner (name, title): _____

Technical owner (name, title): _____

Date of initial deployment: _____

Latest refresh / review date: _____

Workflow category: ☐ KYC ☐ AML ☐ Sanctions ☐ Lending ☐ Payments ☐ Customer Service ☐ Treasury ☐ Audit/Compliance ☐ Other: _____

SECTION 2 — PURPOSE AND SCOPE

One-sentence description: _____

WHAT AI DOES IN THIS WORKFLOW:

-
-

WHAT AI DOES NOT DO IN THIS WORKFLOW (EXPLICIT CEILING):

-
-

Who is the verifier (role) for each AI-assisted step: | Step | AI action | Verifier role | Verification method |
|——|————|————————|——————————|||||||||||

Trust setting: ☐ AI watches ☐ AI suggests ☐ AI acts, you approve ☐ AI handles routine

SECTION 3 — DATA HANDLING

Data classifications handled by this workflow: ☐ Public ☐ Internal ☐ Confidential ☐ NPI / Customer ☐ Investigation / SAR-sensitive

Data residency: _____

Deployment architecture: ☐ Self-hosted (firm network) ☐ Private-tenant cloud ☐ Hybrid ☐ Other: _____

If private-tenant cloud, name vendor, region, and no-training contract reference: _____

If self-hosted, model used (e.g., Llama 3.x, Qwen, Mistral via Ollama / vLLM): _____

Encryption in transit: _____

Encryption at rest: _____

Access controls: _____

Retention period for prompts, responses, and audit log: _____

SECTION 4 — REGULATORY MAPPING

(See [[B1-02-Regulatory-Mapping-Matrix]] for the cross-bank matrix; this section is the per-workflow specifics.)

Framework	In scope?	Obligation	Control	Evidence reference
OCC SR 11-7 / 2011-12	☐			
FDIC consumer / third-party	☐			
Fed SR 11-7 / SR letters	☐			
SEC (if applicable)	☐			
FinCEN BSA / AML	☐			
GLBA Safeguards Rule	☐			
NYDFS Part 500 (or state equiv.)	☐			
SOC 2 TSC	☐			
State banking law	☐			

SECTION 5 — MODEL RISK (IF APPLICABLE)

Is this workflow treated as a model under the bank's model risk management framework? ☐ Yes ☐ No

If Yes: - Model inventory ID: _____ - Model risk tier: ☐ Tier 1 (high) ☐ Tier 2 (medium) ☐ Tier 3 (low) - Initial validation date and reference: _____ - Validation owner: _____ - Ongoing monitoring schedule: _____ - Periodic review cadence: _____ - Compensating controls (where validation is limited, e.g., proprietary LLM): _____

If No, document the position: - Rationale signed by: _____ (CRO / Head of MRM / equivalent) - Date: _____ - Trigger for revisiting position: _____

SECTION 6 — SUPERVISION PROTOCOL

Per-transaction verification: Describe how the assigned human verifies each AI output before it has effect. _____

Sampling and quality assurance: Frequency, sample size, escalation criteria.

_____

Aggregate monitoring: Dashboards reviewed, frequency, owner.

_____

Exception / incident escalation path: Who is paged, what threshold, time-to-acknowledge SLA.

_____

SECTION 7 — AUDIT LOG

For this workflow, the audit log captures: - ☐ User identity and business unit - ☐ Prompt sent to AI - ☐ Model used and version - ☐ Output received - ☐ Verifier identity and verification timestamp - ☐ Customer / account / matter reference (if applicable) - ☐ Approval / rejection decision and reason - ☐ Downstream system actions taken - ☐ Any errors, retries, or fallbacks invoked

Retention period: _____

Tamper-evidence method (hash chain, WORM storage, write-once, etc.):

_____

Search SLA — examiner-grade query "what did AI do on matter X on date Y" returns in:

_____

SECTION 8 — TRAINING

WHO MUST COMPLETE TRAINING BEFORE BEING GRANTED ACCESS TO THIS WORKFLOW:

-
-

Training reference (course name, version, system of record):

_____

Acknowledgment captured (date, system of record): _____

Refresh cadence: _____

SECTION 9 — VENDOR / THIRD-PARTY (IF APPLICABLE)

AI vendor(s) used in this workflow: _____

Third-party risk file reference: _____

Contract clauses verified (date, reviewer): - ☐ No training on bank data - ☐ No retention beyond stated retention - ☐ Sub-processor transparency - ☐ Breach notification - ☐ Audit rights - ☐ Data residency commitment - ☐ Termination assistance

Annual reassessment due: _____

SECTION 10 — RISKS AND COMPENSATING CONTROLS

Risk	Likelihood	Impact	Compensating control	Residual rating
AI hallucination on customer data				
Unauthorized data egress				
Model drift / performance degradation				
Vendor disruption or contract change				
Unauthorized use beyond approved scope				
Fair-lending / UDAAP exposure (if applicable)				
Regulatory finding or MRA				
Other: _____				

SECTION 11 — INCIDENT RESPONSE

DEFINED INCIDENT CATEGORIES FOR THIS WORKFLOW:

-
-

Incident playbook reference: _____

Regulatory reporting triggers (e.g., NYDFS 72-hour cyber, FinCEN SAR-related): _____

Customer-notification triggers: _____

Lessons-learned process: _____

SECTION 12 — REVIEW CADENCE AND APPROVALS

Documentation refresh cadence: ☐ Quarterly ☐ Semi-annual ☐ Annual ☐ Event-driven

Triggers for off-cycle refresh: model change, vendor change, scope expansion, incident, regulatory update affecting scope.

Last refresh date: _____

Next scheduled refresh: _____

Approvers (signature, date): - Business owner: _____ - AI Governance Owner: _____ - Chief Compliance Officer: _____ - Chief Risk Officer: _____ - Head of Internal Audit (notified, not approver): _____ - General Counsel (if customer-facing or regulator-facing): _____ - Board / Risk Committee (if Tier 1 model or material change): _____

APPENDIX A — SAMPLE OUTPUTS

Attach a representative sample of AI outputs (de-identified if necessary) from the workflow's production use. Useful for examiner walk-throughs.

APPENDIX B — TESTING EVIDENCE

For workflows treated as models, attach the validation report, monitoring dashboards, and most recent independent challenge. For non-model workflows, attach the QA sampling results from the latest review cycle.

APPENDIX C — KNOWN LIMITATIONS

Document AI limitations specific to this workflow that informed the trust setting and supervision protocol. Examples: model context-length limits affecting long documents, language coverage gaps, geographic data sparsity, etc.

THE DOCUMENTATION DISCIPLINE

A bank running this template across all its AI workflows has, by virtue of the discipline:

- A single source of truth for each workflow
- A clear lineage from regulatory obligation → control → evidence
- A predictable refresh cycle that reduces ad-hoc scrambles before exams
- Defensible positions on model-vs.-non-model designations
- An incident response that is ready before, not built during, the incident

This is what auditable AI looks like. It is not impressive. It is boring. Boring is what survives.

THE HITLAI / AICTRLNET ANSWER, IN ONE LINE

> AI tools, your team, your systems — running together, safely.

For a bank: AI extracts, pre-screens, and drafts; your specialists do the work AI cannot; supervisors review; customer data stays inside your bank's network — including with self-hosted, air-gapped local AI via Ollama or vLLM. Every workflow has this documentation pack; every prompt and verification step lands in the audit log; every step auditable for OCC, FDIC, Fed, SEC, FinCEN, GLBA, NYDFS, and SOC 2.

Want a working session on filling this template in for your first 2-3 banking workflows? That's the second half of Module B2 — the 120-minute live-build session. → **hitlai.net/institute/banking**

This template is not legal, regulatory, or audit advice. It is operational guidance intended for internal bank planning under the supervision of compliance, audit, risk, and your primary regulator.