D3: Agentic Workflow with LangGraph

🎯 Goal of D3

We built an **agentic workflow** that:

1. **Plans reconciliation steps**
2. **Calls the trained reconciliation model** (from D2) as a tool
3. **Generates a dispute explanation + draft email** (via LLM)
4. **Pauses for human approval** before finalizing

This creates a balance between **automation** and **human oversight**, which is exactly what enterprise workflows need.

🏗️ Workflow Components

1. Matcher Agent

- Uses the trained **RandomForest model** from D2.
- Input: features for a specific invoice (amount diff, date diff, vendor match, etc.).
- Output:
  - pred = 0 → Match
  - pred = 1 → Mismatch
  - prob = confidence score (0–1).

👉 Example: {'pred': 1, 'prob': 0.62}

---

2. Decision Node

- Business logic decides the next step:
- if pred == 1 or prob < threshold:
-   go to Explainer Agent
- else:
-   auto-approve

- Threshold default = **0.9** → only very confident matches are auto-approved.

---

3. Explainer Agent

- Triggered if:
  - Prediction = mismatch (1)
  - OR model confidence < 0.9
- Responsibilities:
  - Summarize reasons for mismatch (amount diff, vendor mismatch, date delay).
  - Draft a professional dispute email to vendor.

👉 This step turns **raw model output** into **business-friendly evidence**.

---

4. Human-in-the-Loop

- After generating explanation + email:
  - Workflow **stops**.
  - AP Officer must review and approve email before sending.
- Prevents AI from automatically sending wrong disputes.

👉 Shows **responsible AI** design — automation with guardrails.

🔀 Two Workflow Branches

1. **Auto-Approve Path**
   - Model predicts match (pred=0) with **confidence ≥ 0.9**.
   - Workflow ends immediately with:
   - Auto-approved: match detected with high confidence.
2. **Human-in-Loop Path**
   - Model predicts mismatch (pred=1) OR confidence < 0.9.
   - Workflow generates explanation + draft email.

    - Stops, awaiting human approval.

🖥️ What We Delivered in D3

✅ **LangGraph Workflow Code** (workflow_graph.py)

- Defines the graph nodes: MatcherTool, decision logic, ExplainerTool.
- Encapsulates the agent orchestration.

✅ **Run Script** (scripts/run_workflow.py)

- CLI tool: python scripts/run_workflow.py --invoice_id INV0134
- Fetches invoice → runs through workflow → prints results.

✅ **Unit Tests** (tests/test_workflow.py)

- Verifies:
    - Model loads and predicts.
    - Explainer outputs structured reasons + email.
    - End-to-end workflow runs without errors.

✅ **Transcript Examples**

- Console runs for mismatch (human-in-loop) and match (auto-approve).

✅ **Diagram** (D3_Workflow_Branch_Diagram.pdf)

- Clear visual of both paths.