HEXABANK

Group : - Arnaud Fernandes - Pavel-Dan Diaconu - Nathan Novier - Sara BenAbdelkader - Saber Dhib	

Step A — Problem & Outcome

1. Mission

« Given HexaBank’s portfolio of AI projects and their metadata (business owner, KPIs, MLOps status), the app returns a standardized dashboard showing performance, ROI, and governance maturity for each project — for executives and data teams. »

2. Input contract

File types : CSV or Excel export of AI projects (name, team, stage, KPIs).

Max size : 10 MB (~500 projects).

Example input :

Project	Owner	Stage	ROI (%)	Risk Level	Last Review
Credit Scoring v2	Risk Dept	Pilot	15	Medium	2025-05-12

3. Output contract

Format : Web dashboard + downloadable CSV / JSON

Example output :

Overall maturity = 2.7 / 5

ROI distribution by use case

Compliance gaps detected (e.g. “Missing bias check — 3 models”)

4. Constraints

Languages : English + French (bilingual UI).

Privacy : internal bank data → secured behind SSO.

Channel : web app (internal use).

Time budget : ≤ 6 h prototype (Streamlit / Retool).

5. Quality check

Metric : Governance Coverage = #AI projects with KPI + compliance metrics / total projects.

Target : ≥ 80 % coverage.

Assessment : via small golden set manually reviewed by compliance team.

💻 Step B — Interface Track via 6 boxes

Category	Choice	Justification
Channel	Web	Internal platform for execs/data teams
Speed feel	Streaming	Real-time metric refresh when uploading file
Dev time & skills	No/low-code	Prototype feasible in Streamlit ≤ 6 h
Stage	Pilot	Early internal testing
Sensitivity	High	Financial & regulatory data
Scale (near-term)	Hundreds	Covers ~300 projects across divisions
Track		

✅ Track A — No/Low-code (Streamlit or Retool)
→ fits “rapid prototype in 6 hours”.

Features + Capabilities

User-facing features :

✅ Suggested prompts/examples (“Show top 5 projects by ROI”)

✅ Clear actions (Download CSV / View governance report)

Core UX capabilities :

✅ Exportability (CSV/PDF)

✅ Latency UX (loading indicator + cancel button)

Wireframe (coquille) — description textuelle

Top bar : “AI Ops Navigator Dashboard”
Left pane : File upload → project table → filters (KPI range, stage, risk)
Main pane :

KPI cards (Avg ROI, Maturity, Coverage %)

Interactive chart ROI vs Compliance

Governance Heatmap per Business Unit
Bottom : “Download report” / “Generate Insights Summary”

Sara:

Assignment 2 — Part 1

Step A — Problem & Outcome

1. Mission (one sentence)
Given all AI project data and metrics across HexaBank, the *AI Ops Navigator* app returns real-time governance insights, risk diagnostics, and performance dashboards for AI project owners and compliance teams.

---

2. Input contract

- **File types:** CSV, XLSX, or JSON uploads from AI projects (metrics, logs, KPIs).
- **Max size:** 50 MB per file.
- **Example input:**
    - `ai_project_metrics.csv` with columns such as *project_name, model_accuracy, bias_index, retraining_date, ROI_score*.

---

3. Output contract

- **Format:** Interactive web dashboard (with downloadable CSV/PDF reports).
- **Example output:**

    - Summary of model risks per use case.
    - Compliance score (0–100) and trend graph.
    - Suggested mitigation actions (retrains, access control, explainability improvements).

---

4. Constraints

- **Languages:** English + French (bilingual).
- **Privacy:** Internal use only (HexaBank data).
- **Channel:** Web-based interface (internal portal).
- **Time budget:** ≤ 6 hours for initial prototype using Streamlit.

---

5. Quality check

- **Metric:** Accuracy of compliance diagnostics and KPI linkage.
- **KPI:** ≥ 90% match with expert human review on test set.
- **Assessment:** Comparison with “golden” compliance reports validated by risk officers.

Step B — Interface Track via 6 Boxes

1. Six Boxes

Dimension	Choice	Justification
Channel	Web	Centralized and accessible to internal teams.
Speed feel	Streaming	Users see metrics update dynamically.

Dev time & skills	1–2 devs	Feasible within 6h using Streamlit + Python.
Stage	Pilot	First internal version for feedback.
Sensitivity	High	Involves regulatory and AI risk data.
Scale (near term)	Hundreds	Covers all AI projects in the organization.

---

2. Pick your track

Track A — No/Low-code (Streamlit prototype)

Chosen to ensure rapid delivery and easy iteration with non-technical users.

---

3. Features and Capabilities

User-facing features:

- **Hybrid input (chat + key fields):** Allows users to upload files or query projects conversationally (“Show me high-risk models”).
- **Clear actions:** Download report, export dashboard, or refresh data.

Core UX capabilities:

- **Sessions & memory:** Keeps history of prior uploads and analyses.
- **Exportability:** Download compliance dashboards as PDF or CSV.

Justification:

These elements make the app practical and usable in compliance workflows, while ensuring transparency and auditability.

---

4. Coquille (Wireframe)

Page layout (text-based sketch):

```
------------------------------------------------------------
|  AI OPS NAVIGATOR — HexaBank Governance Dashboard         |
------------------------------------------------------------
| [Upload Project Metrics File] [Chat with AI Ops]          |
------------------------------------------------------------
| Risk Overview                                    |
|  - Projects: 12 active                           |
|  - High-risk: 3   | Medium: 5  | Low: 4                |
------------------------------------------------------------
| Compliance Score Trend                           |
|  [Line Chart]                                    |
------------------------------------------------------------
| Key Actions                                      |
|  [Download Report] [Export CSV] [Refresh Dashboard]       |
------------------------------------------------------------
| Chat Area (optional)                             |
|  User: "Show projects with bias index > 0.3"             |
|  AI Ops: "3 projects found: Retail Loan Model, KYC Bot..."|
------------------------------------------------------------
```

Assgn2 - AI Ops Navigator

Step A. Problem & Outcome

Mission:

Given HexaBank's internal AI projects and regulatory documentation, the app returns standardized AI project diagnostics, risk assessments, and compliance dashboards for managers and compliance officers.

The goal is to design a co-pilot for the industrialization and supervision of artificial intelligence projects that centralizes information and automates risk and compliance assessment for the bank's governance and compliance teams.

Input contract:

File types, max size/length, example input. Expected inputs are internal files containing project reports, regulatory documents, and model execution logs. Accepted formats are PDF, DOCX, or CSV, with a maximum size of a few megabytes per file, corresponding to a complete project. For example, a quarterly performance report for a credit scoring model is a typical input.

Output contract:

Format (text/table/JSON), example output. The output takes the form of explanatory text accompanied by a summary table or a file that can be exported in JSON format. For each project, it presents a risk assessment, identifies any potential deviations, and provides recommendations for action. An example of output is a table indicating that the credit scoring model presents a moderate risk, a delay in retraining, and the need to add loyalty metrics to comply with European AI regulations.

Constraints:

Languages, privacy, channel (web/Slack), time budget. The application must work in English and French. It handles sensitive banking data and must therefore be deployed in an internal, secure environment. It is accessible via a web interface integrated into Teams. Development time is limited to six hours, which means that a functional prototype focused on a single use case must be produced.

Quality check:

Metric (what you'll measure) + KPI (threshold/target) + how you'll assess (golden set / human review / proxy). Product quality will be assessed based on the accuracy of the diagnostics produced. The KPI selected is that 80% of the diagnostics generated must be validated by business experts. The assessment will be based on a cross-review by the Data and Compliance teams, using a reference set consisting of previous AI projects that have already been assessed manually.

Step B. Interface Track via 6 boxes

Channels:

Web. The application will be deployed on the web for secure internal use, accessible via a browser and integrated into the HexaBank corporate ecosystem.

Speed feel:

Full answer. The system will return complete, summarized answers without resorting to streaming, as the user needs a consolidated, explanatory analysis rather than a progressive response.

Dev time & skills:

1–2 developers. Development will be carried out by one or two developers in order to quickly create a working prototype using a low-code environment.

Stage:

Pilot. The project will be launched as an internal pilot limited to a restricted scope of use cases in order to validate the added value of the product before its wider deployment.

Sensitivity:

High. The data handled is highly confidential as it concerns internal models and regulatory information specific to the bank.

Scale (near term):

Dozens. The application will initially be tested on around ten artificial intelligence projects, involving several dozen internal users.

Pick your track:

A No/Low-code: Retool/Softr/Bubble or Streamlit/Gradio. Scenario A is chosen to enable quick and easy implementation using a tool such as Streamlit or Gradio, without requiring complex infrastructure or advanced development skills.

User-facing features:

Hybrid input (chat + key fields). The interface will combine a conversational chat and structured fields to provide key information such as the project name or model type, facilitating interaction and clarity of queries. Each diagnosis will display the excerpts or documentary sources used in its calculation, in order to enhance transparency and user confidence, particularly for auditability reasons.

Core UX capabilities:

Sessions & memory (history, clear history). Le système conservera l'historique des analyses par projet, permettant à un chef de projet de suivre l'évolution des diagnostics dans le temps et de redémarrer une session au même point.

Exportability (CSV/PDF). Les utilisateurs pourront exporter leurs résultats au format CSV ou PDF, afin de faciliter leur diffusion auprès des équipes de conformité et des responsables de gouvernance.

Coquille (wireframe):

The interface is presented as a single page divided into several sections. At the top, users can upload a file and enter project metadata. In the center, a conversation window displays exchanges between the co-pilot and the user. Below, an area displays the diagnosis with a risk table, compliance alerts, and key performance indicators. Finally, buttons allow users to export results, download a report, or launch a new analysis.

Tableau récapitulatif des paramètres de conception:

Élément	Choix
Channel	Internal web
Response speed	Complete answer
Development resources	1 to 2 developers
Project status	Internal pilot
Data sensitivity	High
Deployment scale	Several dozen users
Development tool	Streamlit ou Gradio
Key features	Hybrid entry and citations
Key capabilities	Session memory and export of results
Quality indicator	80% of diagnoses validated by experts

Assignment 2 - Part 1

Step A — Problem & Outcome

Mission

Given HexaBank's internal AI project documentation and regulatory sources (EBA, ECB, EU AI Act, etc.), the app returns standardized compliance diagnostics, gap analyses, and actionable recommendations for managers and compliance officers.

The goal is to design RegIntel AI, a specialized LLM-powered compliance copilot that centralizes regulatory intelligence, automatically identifies policy gaps, and assists governance teams in maintaining continuous alignment with European AI regulations.

Input contract

Expected inputs include internal AI project documentation, regulatory texts, charters, procedures and model audit reports.

- ➢ Formats: PDF, DOCX, or CSV
- ➢ Maximum file size: a few megabytes per file, corresponding to a full project or regulatory document
- ➢ Example input: a procedure on a credit scoring model

Output contract

Output format: Text summary + structured table (exportable as JSON or CSV). Each output provides a compliance score, detected gaps, and recommended actions.

Example output:

Project	Compliance Score	Risk Level	Key Gaps	Recommendations
Credit Scoring v2	72%	Moderate	Missing fairness metrics	Retrain model, document bias test results, add ethical impact note.

Constraints

- Languages: English and French

- Privacy: sensitive internal and regulatory data, hosted in a secure, on-premise environment with restricted access

- Channel: internal web app integrated with Microsoft Teams

- Time budget: ≤ 6 hours of development. Prototype focused on a single representative use case

Quality check

- Metric: diagnostic accuracy (alignment between AI-generated and expert-reviewed compliance reports)

- KPI target: ≥ 80% of RegIntel AI diagnostics validated by compliance experts

- Evaluation method: human review by both data and compliance teams using a “golden set” of previously audited project

Step B — Interface Track via 6 Boxes

Category	Choice	Justification
Channel	Web	Deployed internally via a secure web interface accessible through Teams
Speed feel	Full answer	Compliance assessments require complete, structured reports rather than progressive outputs
Dev time & skills	1–2 developers	Rapid prototype achievable in ≤6 hours using a low-code tool
Stage	Pilot	Initial deployment for a limited set of internal AI projects
Sensitivity	High	Confidential regulatory and risk-related information
Scale (near term)	Dozens	Tested on ~10 AI projects involving a few dozen internal users

Track selection - Track A: No/Low-code

Chosen to enable rapid prototyping and easy deployment without requiring a complex infrastructure. Streamlit's flexibility supports hybrid inputs and dynamic compliance reports.

Features and Capabilities

User-facing features

1. Hybrid input

Combines conversational input (e.g., "Analyze credit scoring compliance report") with structured fields (project name, department, document type) to enhance usability and context understanding.

2. Citations / evidence chips

Each diagnostic includes traceable excerpts from regulatory texts or internal policies, increasing transparency and auditability for compliance officers.

Core UX capabilities

1. Sessions & memory

Enables users to revisit previous analyses, compare diagnostics across time, and resume ongoing reviews.

2. Exportability

Allows exporting of compliance summaries and recommendations for inclusion in official governance reports or audit submissions.

Wireframe (Conceptual Layout)

Top section:

- File upload widget (PDF/DOCX/CSV)
- Project metadata fields (Project name, Department, Model type)

Center panel (chat area):

- Conversational interface with RegIntel AI
- Suggested prompts (e.g., *“Check EU AI Act alignment for this document”*)

Bottom panel (results dashboard):

- Compliance scorecard and visual risk indicators
- Table of detected gaps and recommended mitigation actions
- “Download report” and “Start new analysis” buttons

Assignment 2 - Part 2

Part 1 — Our Technique Choice, RAG

RegIntel AI needs to analyze internal regulatory documents and provide traceable, source-based explanations. Simple prompting would not ensure verifiable compliance outputs.

Part 2 — Debate & Decide (B – RAG)

1. **Why do we need our own documents / sources?**

To ground the LLM's responses in official EU regulations (EBA, ECB, EU AI Act) and internal HexaBank policies, ensuring factual, auditable recommendations.

2. **Is RAG compatible with our interface (track A/B/C)?**

Yes. Streamlit or Gradio can embed a lightweight RAG pipeline (PDF upload → vector store → LLM response with citations).

3. **Which documents or knowledge bases will we start with?**

HexaBank AI governance charter, EU AI Act text, and ACPR guidelines.

4. **How will we chunk and tag them (size, metadata)?**

Chunk ≈ 500 tokens per segment, tagged by document name, section title and publication date (metadata stored with embedding).

5. **Which embedding model fits language + budget?**

text-embedding-3-small (OpenAI), multilingual, cost-efficient for EN & FR.

6. **Which vector store (pgvector, Chroma, Pinecone) can we set up fast?**

ChromaDB (local), open-source, simple to run within Streamlit.

7. **Which LLM will generate answers and why this one?**

gpt-4-mini (OpenAI) — high reasoning quality, strong multilingual support, low latency for prototype.

8. **How will we show citations or evidence in the UI?**

Inline “evidence chips” below each answer + expandable side panel linking to original PDF passages.

9. **How do we keep data private (PII, access rights)?**

Metrics: Hit Rate (≥ 85 %), Source Coverage (≥ 80 %), Average Latency ≤ 4 s. Validation via expert review on a golden set of 5 projects.

10. **How will we know RAG works (hit rate, source coverage, latency)?**

Local vector DB (no cloud storage); SSO-based access; on-premise hosting with encrypted uploads and automatic deletion after session.