HLRD

High-Level Requirements Document (HLRD)

Project Title: Control Review Agent

Version: 1.0

Prepared by: [Your Name]

Date: [Insert Date]

Owner: Enterprise Risk, Bank of Montreal (example)

1. Purpose

The purpose of this document is to define the high-level business and technical requirements for the Control Review Agent — an AI-powered assistant designed to support internal control reviews across banking domains. The agent enables intelligent querying, analysis, and documentation of control data, thereby accelerating compliance reviews, audit preparedness, and operational risk assessments.

2. Scope

2.1 In Scope

- A LangChain-based conversational agent for interactive control review.
- Analysis types supported: 5W (Who, What, Where, When, Why), Operational Effectiveness (OE), and Design Effectiveness (DE).
- Filtering and retrieval of controls using a structured dataset (`controls.json`).
- Real-time prompt customization for each analysis type.
- CLI interface via `interactive_chat.py`.

2.2 Out of Scope (for v1)

- Integration with live audit platforms or ticketing systems.
- UI-based deployment (e.g., web app).
- Review beyond 10 controls per session (performance bound).

3. Stakeholders

Role	Name/Group	Responsibility
Product Owner	Risk Transformation Lead	Business alignment and outcome validation
Technical Lead	AI Platform Team	Architecture, API integration, deployment
End Users	Risk Analysts, Auditors	Use the agent to review internal controls
Compliance	Internal Audit & Regulatory	Validate outputs meet compliance standards

4. Functional Requirements

ID	Requirement Description
FR1	The system shall accept natural language input from users to review internal controls.
FR2	The system shall load control data from `controls.json` and allow filtering by ID or attributes.
FR3	The system shall provide structured reviews of controls using 5W, OE, and DE frameworks.
FR4	The system shall support up to 10 controls per batch review.
FR5	The system shall allow dynamic updating of prompt templates at runtime.
FR6	The system shall provide explanations for review methodologies (5W, OE, DE).
FR7	The system shall support a CLI-based interface for querying and reviewing.
FR8	The system shall log all tool invocations and LLM decisions during execution.

5. Non-Functional Requirements

ID	Requirement Description
NFR1	The system shall respond to user inputs within 5 seconds for basic queries.
NFR2	The system shall maintain modular, extensible architecture for adding tools and prompts.
NFR3	The agent shall support Claude models via Anthropic's API with configurable parameters.
NFR4	The `.env` file shall store all sensitive configuration values.
NFR5	The system shall support basic error handling for data loading and invalid input.

6. Technical Architecture (Summary)

- **LLM Provider:** Anthropic (Claude 3 family via LangChain)
- **Core Components:**
  - `src/agent.py` – orchestrator and tool binding
  - `src/tools.py` – tool logic and LLM chains
  - `src/prompts.py` – template management
  - `src/data_loader.py` – control data ingestion and filtering
- **Execution Mode:** CLI-based via `interactive_chat.py`
- **Data Format:** JSON (list of control objects)

7. Assumptions

- Control data is static per session and loaded from a pre-curated `controls.json`.
- Users will operate the agent in a secured internal environment with access to the Anthropic API.
- Prompt templates can be modified by users who have basic understanding of LLM prompting syntax.

8. Constraints

- No more than 10 controls can be processed per batch to avoid token limit overflow.
- System is CLI-only in v1; no GUI/web interface included.
- External data sources are not dynamically accessed in v1 (no live integration with internal systems).

---

9. Future Considerations

- Integrate with audit management systems (e.g., Archer, Resolver).
- Expand to include Risk and Control Self-Assessment (RCSA) logic.
- Support department-specific prompt tuning based on domain context (e.g., Market Risk, Credit Risk).
- Add fine-tuned summarization for long control descriptions and historical evaluations.

---

10. Acceptance Criteria

ID	Description
AC1	The agent successfully processes and returns control reviews using 5W, OE, or DE prompts.
AC2	The user can apply filter criteria and receive correct control subsets.
AC3	The prompt update tool must reflect real-time changes in reviews.
AC4	CLI interface must operate without crashing and show clear feedback to the user.
