الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

أكاديمية كاوست
KAUST ACADEMY

GRC Agent – A Bilingual AI Assistant for Saudi Cybersecurity Compliance and Governance Regulations

Jana Mowaffaq Shata
Janashata26@gmail.com

Fatimah Ibrahim Abuharb
fatima6868@outlook.com

Tala Mohammed Alhadawi
Talamh6@gmail.com

Maitha Waleed Almuharrami
H00499170@hct.ac.ae

Nour Reda Jamjoom
jamjoomnour@gmail.com

Supervised By:
Dr.Salma Kharrat
salma.kharrat@kaust.edu.sa

***Abstract*—This project focuses on developing the GRC Agent, a corporate AI assistant designed to support Governance, Risk, and Compliance (GRC) specialists in both Arabic and English. In alignment with Saudi Arabia's vision for digital transformation and robust cybersecurity frameworks, the agent leverages Retrieval-Augmented Generation (RAG) to provide accurate, context-driven answers based on regulatory documents issued by the National Cybersecurity Authority (NCA). The bilingual interface ensures accessibility, while advanced retrieval and memory mechanisms allow for continuous conversational interaction. The project not only reduces manual workload for GRC professionals but also contributes to building stronger cybersecurity practices across organizations in Saudi Arabia.**

I. INTRODUCTION

Governance, Risk, and Compliance (GRC) is one of the fundamental subfields of cybersecurity, ensuring that organizations adhere to regulatory frameworks, security standards, and legal requirements. National authorities (such as cybersecurity agencies) and international organizations publish official documents that contain controls, guidelines, and best practices that must be followed. GRC professionals are responsible for continuously referring to these documents, assessing their organization's compliance, and producing reports that highlight strengths, gaps, and areas for improvement. However, these tasks rely heavily on repetitive manual work, as employees are required to review hundreds of regulatory documents and official tools. This process is time-consuming, exhausting, and prone to human error, especially with the continuous evolution of regulatory requirements.

To address these challenges, we propose "GRC Agent": an AI-powered assistant designed to automate and accelerate the retrieval and interpretation of compliance documents. The agent leverages Natural Language Processing (NLP) techniques and Retrieval-Augmented Generation (RAG) to provide employees with quick, context-aware answers, enabling them to focus on strategic decision-making rather than repetitive manual searches.

II. PROBLEM STATEMENT

Governance, Risk, and Compliance (GRC) specialists in Saudi Arabia face growing challenges in managing complex cybersecurity requirements. Regulations and frameworks are detailed, frequently updated, and available in both Arabic and English, which makes manual searching, interpretation, and application time-consuming, inconsistent, and inefficient. Existing solutions often lack bilingual support, are not tailored to the Saudi cybersecurity context, and fail to provide real-time, context-aware assistance. This creates barriers for organizations trying to meet the standards of the National Cybersecurity Authority (NCA) while aligning with Saudi Arabia's Vision 2030 digital transformation goals.

III. OBJECTIVE

The main objective of the GRC Agent project is to develop a bilingual AI assistant capable of understanding and responding to GRC-related queries in both Arabic and English. By leveraging Retrieval-Augmented Generation (RAG) and advanced large language models, the system is designed to deliver accurate, context-aware answers directly linked to official NCA documents. In doing so, the agent helps reduce the manual workload of GRC specialists, allowing them to focus on higher-value tasks such as decision-making and compliance strategy. The project also aims to improve accessibility and efficiency through a user-friendly web interface that enables seamless interaction and instant responses.

IV. METHODOLOGY

The development of the GRC Agent follows a structured methodology consisting of four main stages:

1. Data Collection and Preparation

Collected a set of cybersecurity regulatory documents from the National Cybersecurity Authority (NCA) in both Arabic and English languages, followed by cleaning and preprocessing these documents to convert them from their original .pdf format to clean, structured, machine-readable format (plain .txt).

2. Preprocessing and Chunking

Designed a custom chunking algorithm that is able to detect control ID patterns (e.g. Domain 1, control 1-1, Sub-control 1-1-1, etc.) in text files and segment text accordingly, so that each chunk represents exactly one, full control.

3. Representation and Storage

Use multilingual embedding models to represent the semantic meaning of texts (in both Arabic and English), and store the embeddings in a vector database (Qdrant) to enable fast similarity search and advanced metadata filtering. Each entry in the vector store contains:

- The original chunk text.
- Embedding.
- Metadata tags, such as control ID, relevant control IDs (the predecessors and successors of the ID), and regulation source.

This structure supports hierarchical navigation and promotes accurate retrieval.

4. Retrieval

Designed a custom retrieval algorithm that leverages both similarity search and metadata filtering in the following way:

- If the user query contains a specific control ID (e.g. "What are the expected deliverables of control 3-2-5?"), the algorithm is able to detect this ID pattern in the user query, perform metadata filtering on the stored documents to retrieve the exact document corresponding to that control ID with its relevant controls, utilize similarity search with the user query to rank the retrieved documents based on their similarity score, and return the top K documents.
- If the user query does not contain an explicit control ID (e.g. "What are the requirements for incident response?"), perform regular similarity search and return the top K similar documents to the user query.

This customized algorithm ensures better retrieval accuracy and greater alignment with users queries, hence enhanced results.

5. Agent Development and Integration

Built a Retrieval-Augmented Generation (RAG) system powered with an AI agent. The agent uses `deepseek-chat` (`DeepSeek-V3.1`) model as its core LLM, and has access to the custom retrieval function as its tool. This enables the agent to intelligently decide whether or not the user query requires a documents retrieval action, as well as empowering it with the ability to call the retrieval tool with reformatted queries to contribute to delivering better, more accurate responses.

The agent is also equipped with a customized prompt template that ensures that responses are structured, source-backed, and aligned with official documents, and has a memory component to keep track of conversations histories and interact more naturally.

Finally integrated the system into a simple user interface that allows employees to ask questions in natural language and receive optimized responses in smooth conversational flows.

V. RESULTS & DISCUSSION

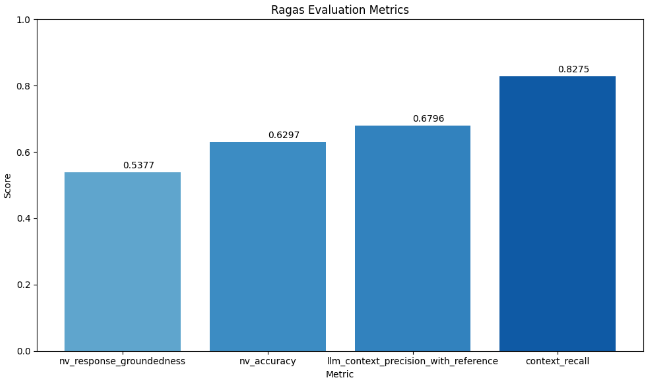

Figure 1. Summary of the system's performance across several aspects.

Constructed a custom bilingual evaluation dataset consisting of 100 entries, where each entry contains a question, ground-truth answer, and ground-truth contexts, and utilized the “llm-as-a-gudge” approach to conduct a multifaceted system evaluation with these settings:

- LLM: `deepseek-chat` (`DeepSeek-V3.1`).
- K (number of retrieved chunks): 10

Figure 1 summarizes the system performance from different perspectives. Key insight to note is the system’s relatively excellent recall score of 0.8275, which represents the core evaluation metric, as it demonstrates how well the system is able to recall relative chunks based on the user query, which directly corresponds to the effectiveness of combining the custom retrieval algorithm with an intelligent AI agent as its tool.

A precision score of 0.6796 reflects the impact of fixing the K hyperparameter to 10, and suggests that fine-tuning it can produce better evaluation results and contribute to enhancing the system’s performance by eliminating the inclusion of redundant contexts.

Finally, the accuracy metric measures the alignment of generated responses with the ground-truth answer, and the groundness measures how well the generated answers are supported by the retrieved contexts. Their scores of 0.6297 and 0.5377 respectively directly relate to the LLM capabilities in comprehending information and responding effectively, which is the `deepseek-chat` (`DeepSeek-V3.1`) model in this setting. Although these metrics are not inherently stable, they can slightly indicate that further experiments to explore and choose better LLMs for the system can contribute to achieving enhanced responses.

VI. CHALLENGES & OBSTACLES

Throughout the project, several challenges were faced, particularly related to data collection, retrieval performance, and evaluation:

A. **Document Accessibility & Availability:** Initially, organization-specific regulations were inaccessible, and most external datasets lacked Arabic support. This was resolved by shifting the focus to official NCA documents, which provide bilingual and highly relevant material.

B. **PDF Parsing Issues:** Extracting clean text from PDFs was difficult due to formatting errors and unreadable sections. To address this, the team manually preprocessed documents into .txt format to ensure high-quality input.

C. **Knowledge Base Size & Processing Speed:** Chunking, embedding, and storing large datasets locally were slow. The solution was to use GPUs via Ibex to accelerate processing.

D. **Retrieval Accuracy:** Basic text-splitting led to irrelevant matches since control numbers and metadata were not considered. The team improved performance by adding metadata tagging and implementing hybrid search strategies, as well as switching from Chroma to Qdrant for enhanced filtering.

E. **Conversation Flow:** Early prototypes could not maintain memory across queries. This was improved by adopting `langgraph`, which introduced persistent conversation flows and system interaction logging.

F. **Evaluation Dataset Gap:** No suitable dataset existed for GRC-related Q&A in the Saudi context. The team addressed this by building a custom bilingual dataset derived from NCA regulations.

G. **LLMs Availability:** The initial chosen LLM for the system, `gemini-2.6-flash`, had very few free tokens and did not provide subscriptions for non-business accounts. Addressing this problem was by subscribing in the deepseek platform and utilizing the `deepseek-chat` (`DeepSeek-V3.1`) as the system’s LLM.

VII. CONCLUSION

The development of the GRC Agent marks an important step toward leveraging artificial intelligence to strengthen cybersecurity governance and compliance in Saudi Arabia. By combining bilingual support, Retrieval-Augmented Generation (RAG), and official NCA regulations, the system provides accurate, context-aware assistance to GRC specialists and reduces the burden of manual work. Despite challenges in document processing, retrieval accuracy, and dataset availability, the team successfully built a functioning prototype that demonstrates the potential of AI to transform regulatory compliance. The solutions applied—such as metadata tagging, hybrid search, and custom dataset creation—paved the way for a more robust and scalable system. Looking ahead, integrating the GRC Agent with organizational infrastructures, expanding its dataset, and optimizing its models will ensure broader adoption and real-world impact. Ultimately, this project contributes to Saudi Arabia's Vision 2030, enabling organizations to adopt smarter, more efficient approaches to cybersecurity compliance and governance.

VIII. FUTURE WORK

The future of the project focuses on scaling, enhancing accuracy, and expanding the capabilities of the GRC Agent to serve organizational needs better:

- **Integration with Organizational Systems:** Connecting the agent with internal databases, knowledge repositories, and digital infrastructures to generate more tailored, context-aware answers, while maintaining strict privacy, security, and compliance standards.

- **Dataset Expansion & Document Coverage:** Continuously enlarging the bilingual dataset by incorporating additional NCA frameworks, regulations, standards, guidelines, and case studies. This expansion will enhance coverage, enabling the agent to respond with greater depth and accuracy across a broader range of compliance scenarios.

- **Model Optimization and Accuracy Improvements:** Experimenting with different LLMs (such as Gemini models) and/or finetuning open-source LLMs and the system's hyperparameters to enhance linguistic precision, contextual accuracy, and relevance of responses.

- **Efficiency & Performance:** Optimizing the RAG pipeline, indexing methods, and retrieval strategies to reduce response times, improve retrieval quality, and enable the agent to handle large-scale document collections more effectively.

- **User Experience Enhancements**: Extending the bilingual web interface with advanced features such as voice-based queries, uploading files, and other personalized recommendations, and dashboard analytics to deliver a more engaging and practical user experience.

- **Impact and Adoption:** Evaluating the system's real-world effects by deploying it in enterprise environments, measuring improvements in compliance efficiency, risk reduction, and decision-making speed, and gathering feedback for continuous refinement.

- **Scaling Implementation:** Transitioning from prototype to enterprise-grade deployment, with performance monitoring, scalability testing, and security hardening to support large organizations across multiple industries.

IX. RESOURCES & TOOLS

The GRC Agent project was designed to ensure performance and scalability by leveraging a combination of advanced AI technologies and development tools. For language processing, `deepseek-chat` (`DeepSeek-V3.1`) was used to enable bilingual responses, while the `intfloat/multilingual-e5-large` embedding model from `HuggingFace` generated text-level vector representations of each chunk to support accurate retrieval. The system's generation backbone relied on `deepseek-chat` (`DeepSeek-V3.1`), ensuring high-quality contextual outputs in both Arabic and English. For storage and retrieval, a `Qdrant` vector database was implemented, enabling semantic search enhanced with metadata filtering for improved accuracy. The RAG pipeline and conversational memory were orchestrated using `LangChain` and `LangGraph`, while the user interface was developed in `Streamlit`, offering bilingual support for seamless user interactions. Finally, Visual Studio Code (`VSCode`) served as the primary development environment for coding, and debugging, while Google Colab was utilized to host the evaluation pipeline.

X. GITHUB LINK

The link for our Project on GitHub: https://github.com/MaithaAlmuharrami/GRC_Agent/tree/main

XI. REFERENCES

[1] Gu, Jiawei & Jiang, Xuhui & Shi, Zhichao & Tan, Hexiang & Zhai, Xuehao & Xu, Chengjin & Li, Wei & Shen, Yinghan & Ma, Shengjie & Liu, Honghao & Wang, Yuanzhuo & Guo, Jian. (2024). A Survey on LLM-as-a-Judge. 10.48550/arXiv.2411.15594.

[2] Kowsik, Alexander. (2024). Optimizing a Retrieval-Augmented QA Chatbot for HR Support using LLMs. 10.48550/arXiv.2411.15594

[3] Chen, Jiajing & Bao, Runyuan & Zheng, Hongye & Qi, Zhen & Wei, Jianjun & Hu, Jiacheng. (2024). Optimizing Retrieval-Augmented Generation with Elasticsearch for Enhanced Question-Answering Systems. 10.48550/arXiv.2410.14167.

[4] Lima, Rafael & Gupta, Shubham & Berrospi Ramis, Cesar & Mishra, Lokesh & Dolfi, Michele & Staar, Peter & Vagenas, Panagiotis. (2024). Know Your RAG: Dataset Taxonomy and Generation Strategies for Evaluating RAG Systems. 10.48550/arXiv.2411.19710.

[5] Li, Siran & Stenzel, Linus & Eickhoff, Carsten & Bahrainian, Seyed. (2025). Enhancing Retrieval-Augmented Generation: A Study of Best Practices. 10.48550/arXiv.2501.07391.

[6] https://github.com/topics/retrieval-augmented-generation

[7] https://nca.gov.sa/ar/regulatory-documents/