**Questions to be asked regarding the use case**

1. Nature of use case: These use case encompass a wide range of functions, including chatbots for interactive communication, extracting structured information from data, translating languages, generating code, producing news articles, summarizing content, automating email responses, analyzing sentiment in text, building knowledge bases, creating synthetic datasets, implementing question answering systems, analyzing documents, and automating the generation of reports. Collect information on nature of use case, number of intended user interactions per month.

2.Nature of data: The nature of data can vary widely, and it can be categorized into different types based on how it is collected and processed. Data can be "scraped," which means it is gathered from various online sources using automated techniques. Alternatively, data can be "curated," indicating that it has been carefully selected, organized, and maintained to ensure its quality and relevance. Another category is "instructed" data, where information is generated or collected based on specific guidelines or instructions provided to data collectors. These distinctions in the nature of data highlight the importance of understanding how data is sourced and handled, as it can impact its accuracy, reliability, and usability in various applications. Collect information on nature of use case.

3. User group: The intended users for a project can be grouped into four categories: the general public, internal organization members, focus groups, and specialist teams. Each of these user groups has unique characteristics and requirements, and considering their needs is essential for successful project development and implementation. Further the user group contributes to efforts to determine the risk level of the use case. For instance, use cases which are shared publicly will have a certain level of risk depending on the purpose of the use case. Collect information on the intended user group for the use case.

4. Purpose of the use case: Use cases serve multiple purposes, including benefits assessment, information sharing, manual effort optimization, creativity facilitation, and information management. They help organizations make informed decisions, promote collaboration, streamline processes, encourage innovation, and ensure effective data handling. The purpose also helps understand the extent of risk posed by the use case. Collect intended purpose of the use case.

5. Nature of LLMs used: The nature of models in the context of language processing can be categorized into three main types: open source LLMs, private LLMs, and closed LLMs. These distinctions are crucial in understanding how language models are developed, distributed, and utilized. Open source LLMs are publicly accessible and can be used and modified by anyone, fostering collaboration and innovation in the AI community. Private LLMs, on the other hand, are developed and maintained by organizations for their specific purposes, often with restricted access. Closed LLMs are proprietary models that are not openly available, and their inner workings are typically kept confidential. Each type has its own advantages and limitations, shaping the landscape of language model development and deployment in the context of a use case. Collect information on nature of LLMs used for the use case.

6. Embedding approach: The "embedding approach" is a versatile method that encompasses various techniques for representing and organizing data. These techniques include word embeddings, table embeddings, and graph embeddings. Each of these approaches involves transforming raw data into a structured and meaningful format that can be used for various tasks such as natural language processing, data analysis, and network analysis. Word embeddings convert words into numerical vectors to capture their semantic meaning, table embeddings enable the representation of tabular data in a condensed form for analysis, and graph embeddings transform graph structures into numerical representations for graph-based applications. The embedding approach is a fundamental concept in data science and machine learning, offering a powerful way to make complex data more manageable and accessible for computational tasks. Collect information on embedding approach adopted for the use case.

7. Vector stores: Vector stores are specialized systems for managing high-dimensional vectors. Popular options include Pinecone for real-time and managed use, Weaviate for semantic graph modeling, Faiss for efficient similarity search, MongoDB for flexibility in mixing data types, ElasticSearch for text and vector search, and RedisStack for low-latency caching. Collect information on vector stores used in the use case, including the reason for such choice.

8. Prompt engineering: The Prompt Engineering approach encompasses a diverse set of techniques and methodologies designed to enhance the capabilities of AI systems. These techniques include Prompt Chain, which involves a sequence of prompts to guide AI behavior; Meta Prompting, where AI can generate prompts for itself; Self-Ask, enabling AI to seek clarification or additional information; Re-act, which focuses on responsive AI behavior; Symbolic Reasoning and Pal, which involves symbolic manipulation for problem-solving; Sequential Prompting, a step-by-step guidance method; Self-Consistency Prompting, ensuring AI responses remain internally coherent; and Automatic Reasoning & Tool Use, allowing AI to perform complex reasoning tasks and utilize external tools effectively. Together, these elements form a comprehensive framework for shaping AI behavior and enhancing its capabilities in various applications. Method of prompting used in these will also have an impact on the level of risk posed by the use case. Collect information on prompting approach used for the use case and the reason for such choice.

9. Fine-tuning: Fine-tuning in machine learning includes techniques like instruction fine-tuning, adaptive fine-tuning, and parameter-efficient fine-tuning. These methods help adapt pre-trained models for specific tasks. Techniques within fine-tuning involve updating the output, encoder, or additional layers and adjusting hyperparameters. Use fine-tuning when you have limited data or want to leverage pre-trained knowledge, but avoid it when you have enough data, the pre-trained model isn't relevant, or resources are limited. Fine-tuning is a flexible approach to enhance model performance, depending on the specific context and requirements. It also contributes to decreasing or increasing the risk in the context of a use case. For instance, if the number of records on which the model was fine tuned on are very limited as against the number of intended user interactions, then the outputs may not be as desired. Collect information on fine-tuning approach adopted and the reason for the adopted strategy or technique.

10. Type of evaluations: Downstream evaluation methods in natural language processing (NLP) and GenAI include fluency metrics, similarity metrics, human evaluation, and domain-specific metrics. Fluency metrics assess language flow and correctness, similarity metrics measure text resemblance, human evaluation gauges quality subjectively, and domain-specific metrics cater to specialized applications. Use fluency metrics for language quality, similarity metrics for text resemblance, human evaluation for comprehensive quality assessment, and domain-specific metrics for specialized domains. Avoid over-relying on any one method and choose based on task requirements and resources. Collect information on type of evaluations done for the use case.

11. Guardrails applied: The term "guardrails" encompasses a wide range of important considerations in various domains, including bias, security, intellectual property (IP), privacy, trustworthiness, safety, and faithfulness. These guardrails serve as essential guidelines and protective measures to ensure that systems, technologies, or processes operate in a responsible and ethical manner. They help prevent or mitigate issues related to bias, data security breaches, unauthorized use of intellectual property, invasion of privacy, and uphold the principles of trustworthiness, safety, and faithfulness in the design, development, and deployment of various applications and systems. By adhering to these guardrails, organizations and individuals can create more responsible and reliable solutions in today's technology-driven world. Collect information on the guard rails applied.

12. Monitoring and Moderating: There are various methods and practices for monitoring and moderating systems. These methods include input and output validation, ensuring the system's explainability and interpretability, incorporating human oversight, implementing safeguards, promoting transparency, and upholding accountability. These measures collectively aim to ensure the reliability, transparency, and responsible operation of systems for the benefit of users and stakeholders. Collect information on the nature of monitoring approach adopted and reason for such choices.

13. Deployment model: Modern software deployment encompasses various approaches, including microservices, containerization, cloud deployment, and RESTful APIs. Microservices involve breaking applications into smaller, independent services, while containerization ensures consistency and portability. Cloud deployment offers scalability and accessibility through cloud platforms. RESTful APIs enable seamless communication between software components. These approaches help developers efficiently deploy and manage applications in today's software landscape. Collect information on nature of deployment model considered for the use case.

14. Human-in-the-loop approach: Human-in-the-loop approaches encompass a range of strategies and processes that involve human participation in various stages of a system or technology's development and operation. These approaches include annotation, validation, oversight, user feedback, and safeguards evaluation. Annotation involves humans adding labels or metadata to data to improve machine learning algorithms. Validation ensures the accuracy and reliability of automated systems through human assessment. Oversight entails continuous monitoring and control by humans to maintain system performance and ethical standards. User feedback is crucial for refining systems based on user experiences and needs. Safeguards evaluation involves human assessment of security and safety measures within the technology. Together, these elements form a cohesive framework for integrating human expertise and guidance into the development and deployment of advanced technologies. Collect information on the nature of humans in loop adopted for the use case.

15. Logging and feedback mechanism: Logging and Feedback mechanism likely involves tracking and recording activities or events related to the downstream application and providing feedback or data regarding its performance or behavior. The goal is to monitor and improve the functionality and effectiveness of the downstream application by leveraging LLM technology. Collect information on logging and feedback mechanism applied in the use case.

16. The sensitivity of a use case, the type of data involved (specifically, personally identifiable information or PII), and the deployment scenario are crucial considerations when implementing a downstream application that utilizes Large Language Models (LLM). These factors collectively shape the overall context and approach for integrating LLM technology into various applications. Balancing the sensitivity of the use case, protecting PII, and choosing an appropriate deployment scenario are fundamental aspects of ensuring the successful and responsible utilization of LLM in downstream applications. Collect information about the sensitivity of use case, data used (Personally identifiable information) and deployment scenario