Below are some example use cases to use in your lab.

1. Resume summarization

In this use case, a human resources department would like to use a large language model (LLM) to create brief summaries of job applicant resumes to help deal with a large volume of applications. Summarization is one of the most common use cases for LLMs. However, this use case can pose some risks:

- Resumes traditionally contain personal data, some of which may be considered sensitive
- Hallucinations and other incorrect summarizations could negatively affect the perception of a candidate's viability
- Any attempt to introduce AI into hiring decisions will always be met with extra scrutiny

2. Hiring recommendation

In this use case, a human resources department would like to use a traditional machine learning (ML) model to assist in hiring decisions. Candidates are scored in a variety of categories, and the model attempts to predict which ones will be successful employees based on those scores. This is a binary classification model. This model has the following risks associated with it:

- Models of this nature are at risk for unfair bias based on biased training data
- Decisions made by the model can impact hiring decisions, and are subject to higher scrutiny
- Auditors are likely to request that any decisions the model made be explained
- Any attempt to introduce AI into hiring decisions will always be met with extra scrutiny

3. Credit risk

In this use case, the corporate finance department would like to evaluate applications for credit cards using a traditional machine learning (ML) model. This model has the following risks associated with it:

- Models of this nature are at risk for unfair bias based on biased training data
- Decisions made by the model can impact financial decisions, and are subject to higher scrutiny
- Auditors are likely to request that any decisions the model made be explained
- Financial data used by the model is considered highly confidential

4. Auto insurance risk

In this use case, an insurance company would like to evaluate the riskiness of auto insurance policies based on a number of factors, including age and gender of the driver,

make and model of the vehicle, previous insurance claims, and proximity of the driver's home address to locations where traffic accidents frequently occur. This model has the following risks associated with it:

- Models of this nature are at risk for unfair bias based on biased training data
- Decisions that reject policies as too risky will likely be subject to audits for explainability
- Personal information such as home addresses will be used in the model
- Indirect bias may exist when judging distance to areas with frequent traffic accidents, if those areas are near neighborhoods with high minority populations

5. Human resources chatbot

In this use case, the company's human resources department would like to use retrieval-augmented generation (RAG) to answer questions regarding employee benefits, compensation and health insurance. This model has the following risks associated with it:

- The model will accept direct input from users, so data poisoning attacks are possible
- The model will need to guard against any hateful, aggressive, and profane (HAP) speech
- The model must be monitored to ensure it does not unwittingly leak personal identifiable information (PII) for other users
- Hallucinations are possible, so the model must be able to provide citations for relevant information