✓ 100 XP

Operate a responsible generative AI solution

3 minutes

When you have identified potential harms, developed a way to measure their presence, and implemented mitigations for them in your solution, you can get ready to release your solution. Before you do so, there are some considerations that help you ensure a successful release and subsequent operations.

Complete prerelease reviews

Before releasing a generative AI solution, identify the various compliance requirements in your organization and industry and ensure the appropriate teams are given the opportunity to review the system and its documentation. Common compliance reviews include:

- Legal
- Privacy
- Security
- Accessibility

Release and operate the solution

A successful release requires some planning and preparation. Consider the following guidelines:

- Devise a *phased delivery plan* that enables you to release the solution initially to restricted group of users. This approach enables you to gather feedback and identify problems before releasing to a wider audience.
- Create an *incident response plan* that includes estimates of the time taken to respond to unanticipated incidents.
- Create a *rollback plan* that defines the steps to revert the solution to a previous state in the event of an incident.
- Implement the capability to immediately block harmful system responses when they're discovered.

- Implement a capability to block specific users, applications, or client IP addresses in the event of system misuse.
- Implement a way for users to provide feedback and report issues. In particular, enable users to report generated content as "inaccurate", "incomplete", "harmful", "offensive", or otherwise problematic.
- Track telemetry data that enables you to determine user satisfaction and identify functional gaps or usability challenges. Telemetry collected should comply with privacy laws and your own organization's policies and commitments to user privacy.

Next unit: Exercise - Explore content filters in Azure OpenAI

Continue >