

Phase 3 Requirements (Minimum Viable Release: External Launch)

The following must be completed before launching a full version of the agent to users externally.

1. Describe the results of estimated agent effectiveness and return on investment based on phase 2 findings. Ensure that statistical findings examine relevant evidence with relevant statistical control group(s):
2. Summarize the key feedback received during phase 2, improvements made (or backlogged for future versions), and any outstanding major issues that were not addressed or only partially mitigated:
3. Describe whether you plan to make the tool free and fully available, or whether it will require user registration and/or chargebacks for credits consumed. If limited, describe how you plan to manage user registrations. If not limited, describe how you plan to manage costs:
4. Summarize the launch plan, any potential risks you foresee to launching the agentic tool, and your plan to mitigate those risks. Describe how you will monitor agent performance after launch and address any performance issues that arise:
5. Describe how you plan to continually monitor, measure, and report on the following statistics: correctness, groundedness, explainability and clarity, completeness, reliability under variation, cost per completed task, outcome gap, decision gap, and bias gap. In addition, define thresholds under which these statistics may merit pausing or reconsidering the public use of the agent, if different from the thresholds considered in phases 1 and 2:
6. Describe the key points in the agent process where human intervention is needed, if any. If human intervention is necessary:
 - a. Describe how the appropriate staff members have been identified and trained:
 - b. Describe how you plan to monitor and measure the rate of “rubber-stamping” (insufficient human review):

7. If any items from the phase 1 and 2 documentation have changed, describe those changes here:
8. Describe how you plan to monitor and mitigate the following cybersecurity risks on an ongoing basis:
Unauthorized actions or excessive agency, sensitive information disclosure, knowledge source poisoning/indirect injection, and any other threats surfaced by red teaming in phase 2:
9. Check the boxes below to affirm the following:
- ☐ I will make this document, apart from security information deemed sensitive by myself or the security lead, available to all users of the agent.
 - ☐ I will make a plan for how to update this document when changes are made.

As the accountable owner, I affirm the above to be true and accurate as of

Accountable owner signature: _____

As the security lead, I affirm the above to be true and accurate as of

Security lead signature: _____

As the responsible agentic AI lead, I and the relevant internal governance committee approve the release of this agent as of

Responsible agentic AI lead signature: _____