Question Title	Available options	Zhipu AI	xAI	OpenAI
If you specified external pre-deployment safety evaluations in the previous section, were these performed before or after broad internal deployment? (Select one)	▪ Before - External safety tests were completed before broad internal deployment. ▪ Partial - All external evaluations on situational awareness, scheming, and cyber-offense were conducted before broad internal deployment. ▪ After - External safety tests were completed after broad internal deployment. ▪ Other (please explain briefly):	Partial - All external evaluations on situational awareness, scheming, and cyber-offense were conducted before broad internal deployment.		After - External safety tests were completed after broad internal deployment.
What level of safety testing does your company require for broad internal deployment of frontier AI models? (Select one)	▪ No formal risk management requirements for internal deployments Formalized risk management for internal deployments with less stringent requirements than external deployment framework for the following risks/capabilities: situational awareness, scheming, AI R&D, cyber-offense. ▪ Formalized risk management for internal deployments with the same requirements as external deployment framework for the following risks/capabilities: situational awareness, scheming, cyber-offense. Company requires the same risk management effort for internal and external deployments. ▪ Other (Please briefly describe):	Formalized risk management for internal deployments with less stringent requirements than external deployment framework for the following risks/capabilities: situational awareness, scheming, AI R&D, cyber-offense.	No formal risk management requirements for internal deployments	As described in our public Preparedness Framework, we believe that models that have reached or are forecasted to reach Critical capability under our framework will require additional safeguards (safety and security controls) during development, regardless of whether or when they are externally deployed. We do not currently possess any models that have Critical levels of capability, and we expect to further update this Preparedness Framework before reaching such a level with any model.
Does your company require any of the following safeguards for broad internal deployments of frontier AI models? *(Select all that apply)*	▪ Inference time safety mitigations for misuse risks (including cyber & bio risks) ▪ Restricting access to helpful-only models and only granting time-bound access to staff that apply with a legitimate research need ▪ Logging all inputs and outputs from internal use and retaining them for at least 30 days ▪ Not currently logging, but introduced an *official, written* plan to start doing so after models reach a specified capability threshold ▪ Analyzing all internal model interactions for abnormal activity, including harmful use or unexpected attempts by AI systems to take real-world actions ▪ Live monitoring and automated editing/resampling of suspicious outputs ▪ None of the above ▪ Other (please describe briefly):	Inference time safety mitigations for misuse risks (including cyber & bio risks),Restricting access to helpful-only models and only granting time-bound access to staff that apply with a legitimate research need,Logging all inputs and outputs from internal use and retaining them for at least 30 days,Analyzing all internal model interactions for abnormal activity, including harmful use or unexpected attempts by AI systems to take real-world actions,Live monitoring and automated editing/resampling of suspicious outputs	Logging all inputs and outputs from internal use and retaining them for at least 30 days	See answer to Q24, above.