Report

Organization: **West Lake research & education service, a division of Palo Alto Research**

https://paloaltoresearch.org/anp.htm

Publication date: Apr 22, 2025, 09:00 AM PDT

Reporting period: 2025

Section 1 - Risk identification and evaluation

a. How does your organization define and/or classify different types of risks related to AI, such as unreasonable risks?

Palo Alto Research has several technical committees in the fields of AI, wireless, mobile and cybersecurity, and we use thousands of experts to review the proposals to reduce risks based on technical discussions.

b. What practices does your organization use to identify and evaluate risks such as vulnerabilities, incidents, emerging risks and misuse, throughout the AI lifecycle?

Palo Alto Research utilized the resources of World Wireless Congress, West Lake education and research services, and several of our Task Forces throughout the AI lifecycle. Please visit https://paloaltoresearch.org for details.

c. Describe how your organization conducts testing (e.g., red-teaming) to evaluate the model's/system's fitness for moving beyond the development stage?

Palo Alto Research has its own small model testbed plus other clients' large model testbeds in the Silicon Valley to test the model's performance.

d. Does your organization use incident reports, including reports shared by other organizations, to help identify risks?

Yes

e. Are quantitative and/or qualitative risk evaluation metrics used and if yes, with what caveats? Does your organization make vulnerability and incident reporting mechanisms accessible to a diverse set of stakeholders? Does your organization have incentive programs for the responsible disclosure of risks, incidents and vulnerabilities?

Yes, Palo Alto Research has complete procedures for such risk evaluation and reporting mechanism.

Palo Alto Research is a scientific research organization working closely with our partners and sponsors in the AI R&D.

f. Is external independent expertise leveraged for the identification, assessment, and evaluation of risks and if yes, how? Does your organization have mechanisms to receive reports of risks, incidents or vulnerabilities by third parties?

Palo Alto Research works with our partners, clients and sponsors for this issue.

g. Does your organization contribute to the development of and/or use international technical standards or best practices for the identification, assessment, and evaluation of risks?

Palo Alto Research contributes to the best practices for the identification, assessment, and evaluation of risks

at Stanford AI Best Practice Summit.

h. How does your organization collaborate with relevant stakeholders across sectors to assess and adopt risk mitigation measures to address risks, in particular systemic risks?

Palo Alto Research uses its West Lake education and research services to address this issue.

Any further comments and for implementation documentation

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards and manage risks in the United States and worldwide.

Section 2 - Risk management and information security

a. What steps does your organization take to address risks and vulnerabilities across the AI lifecycle?

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

b. How do testing measures inform actions to address identified risks?

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

c. When does testing take place in secure environments, if at all, and if it does, how?

PAR started testing well before 2020, and has been continuing testing in Silicon Valley in our own Testbed.

d. How does your organization promote data quality and mitigate risks of harmful bias, including in training and data collection processes?

PAR utilized Stanford University best practice procedure for this process.

e. How does your organization protect intellectual property, including copyright-protected content?

PAR utilized Mobile DNA technology to protect IP in the AI data flow.

---

f. How does your organization protect privacy? How does your organization guard against systems divulging confidential or sensitive data?

PAR utilized Mobile DNA technology to protect privacy and sensitive data in the AI data flow.

---

g. How does your organization implement AI-specific information security practices pertaining to operational and cyber/physical security?

- **i. How does your organization assess cybersecurity risks and implement policies to enhance the cybersecurity of advanced AI systems?**
- **ii. How does your organization protect against security risks the most valuable IP and trade secrets, for example by limiting access to proprietary and unreleased model weights? What measures are in place to ensure the storage of and work with model weights, algorithms, servers, datasets, or other relevant elements are managed in an appropriately secure environment, with limited access controls in place?**
- **iii. What is your organization's vulnerability management process? Does your organization take actions to address identified risks and vulnerabilities, including in collaboration with other stakeholders?**
- **iv. How often are security measures reviewed?**
- **v. Does your organization have an insider threat detection program?**

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

---

h. How does your organization address vulnerabilities, incidents, emerging risks?

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

Any further comments and for implementation documentation

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

Section 3 - Transparency reporting on advanced AI systems

a. Does your organization publish clear and understandable reports and/or technical documentation related to the capabilities, limitations, and domains of appropriate and inappropriate use of advanced AI systems?

- i. How often are such reports usually updated?
- ii. How are new significant releases reflected in such reports?
- iii. Which of the following information is included in your organization's publicly available documentation: details and results of the evaluations conducted for potential safety, security, and societal risks including risks to the enjoyment of human rights; assessments of the model's or system's effects and risks to safety and society (such as those related to harmful bias, discrimination, threats to protection of privacy or personal data, fairness); results of red-teaming or other testing conducted to evaluate the model's/system's fitness for moving beyond the development stage; capacities of a model/system and significant limitations in performance with implications for appropriate use domains; other technical documentation and instructions for use if relevant.

PAR regularly publishes its reports thru its own project websites.

---

b. How does your organization share information with a diverse set of stakeholders (other organizations, governments, civil society and academia, etc.) regarding the outcome of evaluations of risks and impacts related to an advanced AI system?

PAR shared these information in Linkedin platform as well its own websites.

---

c. Does your organization disclose privacy policies addressing the use of personal data, user prompts, and/or the outputs of advanced AI systems?

Yes.

---

d. Does your organization provide information about the sources of data used for the training of advanced AI systems, as appropriate, including information related to the sourcing of data annotation and enrichment?

Yes.

---

e. Does your organization demonstrate transparency related to advanced AI systems through any other methods?

Yes.

Any further comments and for implementation documentation

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

Section 4 - Organizational governance, incident management and transparency

a. How has AI risk management been embedded in your organization governance framework? When and under what circumstances are policies updated?

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

b. Are relevant staff trained on your organization's governance policies and risk management practices? If so, how?

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

c. Does your organization communicate its risk management policies and practices with users and/or the public? If so, how?

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

d. Are steps taken to address reported incidents documented and maintained internally? If so, how?

Yes.

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

e. How does your organization share relevant information about vulnerabilities, incidents, emerging risks, and misuse with others?

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

f. Does your organization share information, as appropriate, with relevant other stakeholders regarding advanced AI system incidents? If so, how? Does your organization share and report incident-related information publicly?

Yes.

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

g. How does your organization share research and best practices on addressing or managing risk?

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

PAR and West Lake regularly publish the report mostly in PAR's websites, and sometimes in Linkedin pages.

h. Does your organization use international technical standards or best practices for AI risk management and governance policies?

Yes, mostly on best practices.

Any further comments and for implementation documentation

Palo Alto Research, rooted in the heart of Silicon Valley, has over 50 partners and clients to work together to set standards, define tasks, conducting tests and manage risks, etc in the United States and worldwide.

Our division - West Lake education and research services, is in charge of the subject AI Policy and Code of Conduct issue.

PAR and West Lake regularly publish the report mostly in PAR's websites, and sometimes in Linkedin pages.

Section 5 - Content authentication & provenance mechanisms

a. What mechanisms, if any, does your organization put in place to allow users, where possible and appropriate, to know when they are interacting with an advanced AI system developed by your organization?

PAR focuses on trademark to tell those who are interacting with PAR's AI solutions.

b. Does your organization use content provenance detection, labeling or watermarking mechanisms that enable users to identify content generated by advanced AI systems? If yes, how? Does your organization use international technical standards or best practices when developing or implementing content provenance?

PAR uses trademark rights and Mobile DNA technology to protect content owners' rights.

Any further comments and for implementation documentation

PAR uses trademark rights and Mobile DNA technology to protect content owners' rights.

Section 6 - Research & investment to advance AI safety & mitigate societal risks

a. How does your organization advance research and investment related to the following: security, safety, bias and disinformation, fairness, explainability and interpretability, transparency, robustness, and/or trustworthiness of advanced AI systems?

Palo Alto Research and its division - West Lake education and research services, invest huge amount of funds every year in research and development on all topics of AI technology in the heart of San Francisco Bay Area. PAR has over 50 partners and clients on this critical AI mission. Visit https://paloaltoresearch.org for details.

b. How does your organization collaborate on and invest in research to advance the state of content authentication and provenance?

Palo Alto Research and its division - West Lake education and research services, invest huge amount of funds every year in research and development on all topics of AI technology in the heart of San Francisco Bay Area. PAR has over 50 partners and clients on this critical AI mission. Visit https://paloaltoresearch.org for details.

c. Does your organization participate in projects, collaborations, and investments in research that support the advancement of AI safety, security, and trustworthiness, as well as risk evaluation and mitigation tools?

Palo Alto Research and its division - West Lake education and research services, invest huge amount of funds every year in research and development on all topics of AI technology in the heart of San Francisco Bay Area. PAR has over 50 partners and clients on this critical AI mission. Visit https://paloaltoresearch.org for details.

d. What research or investment is your organization pursuing to minimize socio-economic and/or environmental risks from AI?

Palo Alto Research and its division - West Lake education and research services, invest huge amount of funds every year in research and development on all topics of AI technology in the heart of San Francisco Bay Area. PAR has over 50 partners and clients on this critical AI mission. Visit https://paloaltoresearch.org for details.

Section 7 - Advancing human and global interests

a. What research or investment is your organization pursuing to maximize socio-economic and environmental benefits from AI? Please provide examples.

PAR works with California state government to address this issue.

Palo Alto Research and its division - West Lake education and research services, invest huge amount of funds every year in research and development on all topics of AI technology in the heart of San Francisco Bay Area. PAR has over 50 partners and clients on this critical AI mission. Visit https://paloaltoresearch.org for details.

b. Does your organization support any digital literacy, education or training initiatives to improve user awareness and/or help people understand the nature, capabilities, limitations and impacts of advanced AI systems? Please provide examples.

West Lake education division is in charge of this issue.

Palo Alto Research and its division - West Lake education and research services, invest huge amount of funds every year in research and development on all topics of AI technology in the heart of San Francisco Bay Area. PAR has over 50 partners and clients on this critical AI mission. Visit https://paloaltoresearch.org for details.

c. Does your organization prioritize AI projects for responsible stewardship of trustworthy and human-centric AI in support of the UN Sustainable Development Goals? Please provide examples.

Yes. We work with related team in US, EU, China and Malaysia, etc for this issue.

Palo Alto Research and its division - West Lake education and research services, invest huge amount of funds every year in research and development on all topics of AI technology in the heart of San Francisco Bay Area. PAR has over 50 partners and clients on this critical AI mission. Visit https://paloaltoresearch.org for details.

d. Does your organization collaborate with civil society and community groups to identify and develop AI solutions in support of the UN Sustainable Development Goals and to address the world's greatest challenges? Please provide examples.

Yes, we work with local county for this issue.

Palo Alto Research and its division - West Lake education and research services, invest huge amount of funds every year in research and development on all topics of AI technology in the heart of San Francisco Bay Area. PAR has over 50 partners and clients on this critical AI mission. Visit https://paloaltoresearch.org for details.