Report

Organization: **NEC Corporation**

https://www.nec.com/en/global/solutions/ai/index.html

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?

Risks are identified, analyzed, classified and assessed based on data flows during the AI lifecycles in line with the business models/processes. The results are integrated and mapped into the company-wide enterprise risks list, where and when necessary.

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

NEC Corporation (hereby, the company) has identified AI related risks at appropriate timing and recently has also been updating the latest AI risks based on the business processes. This activity involves CxOs, e.g., CRO: Chief Risk Officer and related CxOs, and executives/AI experts across division/departments.

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?

Red teaming: Conducting red teaming to assess model/system suitability for migration beyond the development phase.

Depending on the security levels, developers are required/recommended to conduct self-diagnose using vulnerability diagnostics and/or penetration tests delivered by internal security teams.

Independent external testing: Conducting independent external testing to assess the suitability of the models/systems for migration beyond/after the development phase.

Regarding the third-party evaluation (independent external tests), the organization can undergo a penetration test by an in-house or by security specialist teams in the group companies who are different entitles from the project.

Quantitative Assessment Test: Metrics are adopted for quantitative risk assessment in Upstream processes, the internal documents including "Cyber Security Checklists" are used for evaluations. The evaluation before shipment, the CVSS value are adopted.

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?

In upstream processes, the internal documents including "Cyber Security Checklists" are used for evaluations. The evaluation before shipment, the CVSS value are adopted.

A security incident escalation mechanism is in place for vulnerability reporting.

No incentive program to disclose vulnerabilities

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?

Conducting independent external testing to assess the suitability of the models/systems. Regarding the third-party evaluation (independent external tests), the organization can undergo a penetration test by an in-house or by security specialist teams in the group companies who are different entitles from the development/migration project.

The secure development processes and the operation check mechanism are utilized in accordance with the company-wide rules/guidelines.

Regarding generative AI, vulnerability assessments and reports related to security are externally conducted.

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?

The company has contributed to development of international standards by SDOs and best practices by industries globally.

NEC is ranked as one of the top companies according to the number of treatises between 2000 to 2022 at prestigious conferences such as NeurIPS, ICML, ECML-PKDD, KDD, and ICDM. The company also promote participation in global AI discussions at international organizations, and participate in standards activities for international standards (ISO, IEC, ITU, etc.), regional standards, domestic standards, etc.

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?

There are several guidelines internally to check risks and countermeasures in each business/service areas such as AI, System Integration, and products. Those requirements in the guidelines are normally operated with necessary combinations. When feedbacks and updates are made, it is shared with internal stakeholders and reflected to the guidelines on demand basis.

The Internal stakeholders are identified in each case and needs are shared across divisions/departments to cover from AI development (R&D) to sales. Risk mitigation measures are also implemented based on the above collaborations.

Section 2 - Risk management and information security

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

The processes are operated in the Research and Development (R&D) , for example;

-possible threats are listed at each phase in the AI lifecycle,

-verification and evaluation on the existing technologies are conducted to respond to the threats,

-R&Ds are investigated to new technologies,

-Risk assessments by external parties are regularly taken, and

-the original risk assessment methods are also developed internally.

As for the generative AI business, to identify risks, security assessments are taken by the external party and also quality assessments required by internal criteria are adopted.

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

Regarding the AI models, the risks identified by the external evaluation are shared with internal stakeholders in the AI model development division and business divisions, and countermeasures are consulted, by them.

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

Based on "the NEC Security Policy", as a prerequisite for service provision, evaluations are conducted in secure environments with required security measures, e.g., blocking networks from outside and authenticated accesses.

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

The company has introduced a system to check whether AI has harmful biases, and guardrails to detect biases in AI outputs, with the cooperation of partner companies.

The company has also created a dataset to detect biases internally, and use it to inspect AI at the time of shipment.

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

The company protects intellectual property by understanding the intellectual property systems and precedents of each country, acquiring intellectual property rights such as patents and trademarks, managing know-how, negotiating licenses, and handling disputes such as litigation. The company also respects the intellectual property of third parties, and investigate the rights of others to ensure that the company does not infringe on their rights in the company's own business activities. Furthermore, based on the “NEC Group AI and Human Rights Principles”, the company has established internal usage rules to protect the intellectual property of others, such as copyrights.

- NEC Group AI and Human Rights Principles

https://www.nec.com/en/press/201904/images/0201-01-01.pdf

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

The company makes necessary implementations in accordance with the AI and human rights principles and the internal personal information protection rules and guidelines which are applied to the company-wide and all group companies.

The company responds to the leakage of confidential or secret data in accordance with the Rules for Trade Secret Management. The company makes necessary implementations in accordance with the internal secure development guidelines. Surveys, research, and introduction studies of existing guardrail technologies to prevent leaks are also conducted.

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?**

g. Within the company, the security department is implementing measures in accordance with international frameworks such as the NIST Cyber Security Framework.

In terms of security measures in operations, cyber security measures, physical security measures, and risk hunting, appropriate security measures and secure development are implemented according to the critical level of the system based on various internal evaluation standards.

g-i. Within the company, the security department evaluates compliance with international frameworks such as the NIST Cyber Security Framework and implements policies.It is mandated/recommended that action items from developers' self-diagnose using vulnerability diagnostics to penetration testing by internal security teams, should be performed, depending on security level.

In terms of security measures in operations, cyber security measures, physical security measures, and risk hunting, appropriate security measures and secure development are implemented according to the critical level of the system based on various internal evaluation standards.

g-ii. Within the company, the Three Lines Model is used to manage important information, and each business owner defines important information and manages it strictly.

The company has a mechanism for detecting insider risks and monitoring information leakage channel. Through the mechanism, risky behavior including internal improprieties can be detected and visualized in order to check and prevent information leakage. Alerts are issued in case external leakage of critical information or unusual behavior.

It is mandated/recommended that action items from developers' self-diagnose using vulnerability diagnostics to penetration testing by internal security teams, should be performed, depending on

security level.

In terms of security measures in operations, cyber security measures, physical security measures, and risk hunting, appropriate security measures and secure development are implemented according to the critical level of the system based on various internal evaluation standards.

g-iii. It is mandated/recommended that action items from developers' self-diagnose using vulnerability diagnostics to penetration testing by internal security teams should be performed and identify and respond to vulnerabilities in the system. In addition, the system for collecting vulnerability information on the company's products and the customer-delivered items, and deploying patch information is internally developed and operated to perform vulnerability management

Actions are taken against the identified risks and vulnerabilities through the security incidents escalation process .

(Cooperation with other parties concerned is on a case-by-case basis)

g-iv. Internal: Vulnerability diagnostics are performed quarterly (four times/year) on servers exposed to the internet. In addition, the company's security measures are reviewed at the Information Security Strategy Meeting, which is held twice a year.

External: Penetration tests are performed at the environment construction phase and thereafter it will be performed when necessary.

g-v. The company has a mechanism for detecting insider risks and monitoring information leakage channel. Through the mechanism, risky behavior including internal improprieties can be detected and visualized in order to check and prevent information leakage. Alerts are issued in case external leakage of critical information or unusual behavior.

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

Monitorings are implemented based on the internal quality guidelines.

As for the part related to general IT systems, vulnerability measures are taken on a case-by-case basis during system construction.

The company has a process for obtaining explanations and agreements with customers, and has agreed with them on this. The company also has a program for monitoring logs in the maintenance and operation support, and takes measures according to risks.

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.

a. Corporate Policies

- NEC Group AI and Human Rights Principles

https://www.nec.com/en/press/201904/images/0201-01-01.pdf

- ESG

https://www.nec.com/en/global/sustainability/report/index.html

-Digital Trust Advisory Council

https://www.nec.com/en/global/sustainability/social/ai.html#anc-03

-AI Governance

https://www.nec.com/en/global/techrep/journal/g23/n02/230221.html

a-i. The documents are reviewed and updated when necessary. The type of annual reports, e.g., the ESG reports, are published regularly. See:

https://www.nec.com/en/global/sustainability/report/index.html

a-ii. Update is considered when necessary or appropriate, for example, when any new significant release is needed, incorporation and/or update is considered.

a-iii. Currently, the company publishes the corporate principles on AI and human rights and this is applicable to the company-wide including group companies.

https://www.nec.com/en/global/sustainability/social/ai.html

The rules/guidelines for governances including AI governance and procedures are equipped, operated and updated regularly. Those documents are for internal use with confidential (Undisclosed).

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?

It is customary for each customer providing the AI system to report and explain, and if there are any problems, to implement improvements. The content, scope and frequency of information sharing for each customer are not disclosed.

General information is shared through activities with external stakeholders including governments, industrial associations, experts communities and academia; the company actively contributes to such initiatives, e.g., member of government research institutions for the creation of machine learning quality management guideline, members of government committee by ministries, activities at the Governance Association, researching with various universities and research institutes, and participants various academic conferences.

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

The company discloses and shares information regarding the use of personal data, prompts and other privacy policies with relevant parties. The information is confidential and not disclosed outside the parties.

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?

Basically, the company does not disclose or provide the data itself, but if requested by a customer or other party, the company will provide the information appropriately in response to the request.

---

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

The company has a mechanism to report and explain to each customer that we provide, and if there is a problem, it will be improved. It is not specifically focusing on transparency related AI systems, but also include other elements. Regarding the AI system specific part, collaborations with external parties are being considered.

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?

AI risks are managed based on the following AI governance principles in addition to the internal rules/guidelines (nondisclosure: confidential) :

https://www.nec.com/en/global/techrep/journal/g23/n02/230221.html

AI and human rights principles

https://www.nec.com/en/global/sustainability/social/ai.html

The company currently reviews and updates AI risks and AI governance accordingly to support generative AI and the latest AI business environment.

The company reviews and considers update policies/principles and related rules/guidelines regularly and at necessary timing, e.g., when new threats are recognized due to the evolution of technologies or changes by social environments.

As an example, the policies on image generation services was updated due to getting possible higher risks of piracy and other copyright infringement than traditional text generation.

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

Various web-based and individual training programs exist for internal and company-wide personnel including all employees.

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

Same as "Section 3.a".

(Corporate Policies

- NEC Group AI and Human Rights Principles

https://www.nec.com/en/press/201904/images/0201-01-01.pdf

- ESG

https://www.nec.com/en/global/sustainability/report/index.html

-Digital Trust Advisory Council

https://www.nec.com/en/global/sustainability/social/ai.html#anc-03

-AI Governance

https://www.nec.com/en/global/techrep/journal/g23/n02/230221.html)

In addition, the explanatory leaflets for customers on "the NEC Group AI and Human Rights Principle" are prepared and provided to each related project so that the principles and practices can be shared with customers.

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

Procedures are documented and maintained internally with regard to the security incident escalation rules as answered in Section 1.e.

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

It is customary for each customer providing AI systems to report and explain problems and make improvements if there are any.

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?

It is customary for each customer providing AI systems to report and explain problems and make improvements if there are any. Not publicly shared.

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

The company collaborate with domestic and global NEC Group research institutes including R&D division, Labs around the world, to address and mitigate AI related risks. The research details and best practices are shared and published as internal and technical reports.

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

Adopted examples are (not limited to):

best practices in collaboration with third parties of international standards and the perspective of globally recognised standards such as OWASP.

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?

EULA (End User License Agreement) is prepared for each AI model and AI system.

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?

For the business perspective, the company's business are basically B2B. It is assumed that the generated contents are explained to the company's customers in advance.

Adopted examples are (not limited to):

best practices in collaboration with third parties of international standards and the perspective of globally recognised standards such as OWASP.

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?

In R&D, researches are on-going at the areas of, but not limited to:

-test data and experimental programs for bias detection and fairness,

-false information detection systems, and

-the systems to ensure explainability and interpretability based on the identification of hallucination points by checking with the original text are being carried out.

---

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

The company invests technologies on misinformation output detection, fact checking, AI output content detection, etc. at in-house global laboratories has been researching by laboratories at the global scale and level .

---

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?

Yes.

Examples are:

i. Support for democratic values and respect for human rights

Ethical/Bias Risk Assessment Dataset Development

ii. Protection of children and vulnerable groups

Ethical/Bias Risk Assessment Dataset Development

iii. protection of intellectual property rights

AI output content detection

iv. protection of privacy

Personal information secrecy and privacy protection technology

v. Avoidance of harmful bias

Development of Ethical/Bias Risk Assessment Data Sets

vi. Avoiding false alarms, disinformation, and information manipulation

Fact-checking support and misinformation output detection

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

Yes.

Examples are:

i. Support for democratic values and respect for human rights

Ethical/Bias Risk Assessment Dataset Development

ii. Protection of children and vulnerable groups

Ethical/Bias Risk Assessment Dataset Development

iii. protection of intellectual property rights

AI output content detection

iv. protection of privacy

Personal information secrecy and privacy protection technology

v. Avoidance of harmful bias

Development of Ethical/Bias Risk Assessment Data Sets

vi. Avoiding false alarms, disinformation, and information manipulation

Fact-checking support and misinformation output detection

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.

Yes.

Examples are:

i. Support for democratic values and respect for human rights

Ethical/Bias Risk Assessment Dataset Development

ii. Protection of children and vulnerable groups

Ethical/Bias Risk Assessment Dataset Development

iii. protection of intellectual property rights

AI output content detection

iv. protection of privacy

Personal information secrecy and privacy protection technology

v. Avoidance of harmful bias

Development of Ethical/Bias Risk Assessment Data Sets

vi. Avoiding false alarms, disinformation, and information manipulation

Fact-checking support and misinformation output detection

---

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.

Yes.

The company provide various corporate-wide education programs for AI and LLM to raise literacy levels.

"NEC Academy" provides training service externally in specialized areas including highly professional areas. Measures for literacy improvement are also provided and implemented in the industry-academia collaboration program.

---

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.

The company takes actions and contributes to achieve SDGs. Please see:

https://www.nec.com/en/global/sdgs/index.html

In generative AI, the company has developed and provides models with lightweight configurations that take environmental impacts into account considering decarbonization.

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.

The company promotes collaboration with internal and external stakeholders, such as the Japan Data Scientist Society, the AI Governance Association, public-private dialogues led by Ministries (the government) , Universities, and taking leadership position for those initiatives.

Advisory board meetings with external multi-stakeholders professionals are also arranged, e.g., Digital Trust Advisory Council.

https://www.nec.com/en/global/sustainability/social/ai.html