

OECD AI Transparency Report

Organization: NTT, Inc. (JPN)

Reporting Period: Q2 2026

Published: October 2, 2026

Section 0 – Your role in the AI system lifecycle

Responding as (please select all that apply):

- Model developer (/provider)
- Application developer (/provider)
- Deployer

If any of the fields above are selected, please indicate your organization size:

Large enterprise: 250 or more employees

Section 1 – Risk Identification and Evaluation

1. How does your organization define and/or classify different types of risks related to AI?¹

- Maintain an internal taxonomy, classification system, and/or set of risk area definitions
- Align with specific external frameworks, standards, reports, and/or guidance documents such as taxonomies, classification systems, and/or sets of definitions for risk areas (e.g. the NIST AI Risk Management Framework, the ISO/IEC 42001, the OECD AI Principles, the EU General-Purpose AI Code of Practice, the International AI Safety Report). (please specify): At NTT, risks are defined with reference to hard laws relevant to our core business areas, including the EU AI Act's risk categories, and to soft law and related standards, including ISO/IEC 42001, the NIST Risk Management Framework, and Japan's AI Guidelines for Business.
- Consult with external stakeholders (e.g., from academia, industry groups, civil society, or standard development organisations) when developing or updating risk taxonomies

How does your organization define thresholds at which severe risks, unless adequately mitigated, may be considered "unreasonable"? Please describe the framework(s) most relevant to your organization's role and context. If your organisation does not use formal thresholds, you may describe instead the policies, decision criteria, or governance processes you apply when assessing severe AI risks. You may also describe:

- Specific examples of contexts in which your models or systems could, in your assessment, pose unreasonable or intolerable risk;
- How mitigations are graduated by capability or propensity level;
- How your organisation considers the specificities of different AI technologies, such as generative AI and agentic AI, including any specific risk assessment or governance mechanisms applied to agentic AI capabilities.

Within NTT's core business areas, any use case that hard law designates as prohibited is likewise banned across the whole NTT Group to keep our AI safe, secure, and trustworthy. We also prohibit the use of AI services judged highly likely to be rights-infringing. One global set of AI-risk levels and definitions is applied to every project, and mitigation is applied according to the assessed level, taking the traits of different AI technologies such as generative AI into account.

2. Both before and after deployment, what practices does your organization use to identify and evaluate vulnerabilities, incidents, emerging risks and misuse throughout the AI system lifecycle?

- Internal red teaming³
- Adversarial testing to detect technical vulnerabilities
- Publicly available benchmarks and measurement tools
- Structured techniques to explore the behavior or performance of a model and/or application, such as model elicitation or bottleneck assessments
- Qualitative assessments (e.g., expert judgment, narrative scoring)
- Specific risk identification practices for vulnerable groups
- Impact assessments such as personal data protection assessment and fundamental rights impact assessments
- External model, system, or application-independent research initiatives
- Internal model, system, or application-independent research initiatives
- Vulnerability reports
- Incident reports, including reports shared by other organizations
- Automated monitoring / remote status reporting (e.g., telemetry pipelines, automated alerts when risk thresholds are breached)
- Specific risk identification practices for agentic AI capabilities, e.g., autonomous action-taking, tool use, multi-step planning (please specify): NTT participates in government, industry, and private-sector events on AI governance, while also identifying risks specific to AI agents with reference to the Guide to Evaluation Perspectives on AI Safety and implementing appropriate risk mitigation measures for AI agent developers and providers.
- Multilingual and cross-cultural evaluation, including collaboration with local ecosystems (e.g., national AI institutes, language-specific evaluation consortia) for under-represented languages and cultural contexts (please specify): We participate in industry-association events.
- Assessment of risks arising from interactions among multiple AI agents

How does your organization monitor the interactions of AI agents under your control with other agents / assess risk from multiple agents interacting?

No answer provided

Please briefly describe your organization's decision-making process for deploying an AI model or system including: who has decision authority; what evidence and criteria are required (e.g., performance, safety/security, robustness, fairness, privacy, compliance, independent external testing, evaluation, validation and verification (TEVV) or assurance); contextual caveats or limitations required in interpreting risk evaluation metric results; what approvals/sign-offs are needed; and what safeguards (e.g., mitigations, monitoring, or phased release) must be in place to move into deployment.

When deploying an AI model or system, each NTT Group company follows its established business processes in making deployment decisions. Every AI project is evaluated against a common set of AI risk definitions. For projects classified as high risk, the designated AI risk management officer at each Group company confirms that adequate risk reduction measures are in place, and mitigation actions are implemented according to the assigned risk level.

Following deployment, how do you use incident reports — including those shared by other organizations — to identify emerging issues, update risk assessments, and trigger corrective actions.

We review not only the laws, regulations, and guidelines relevant to our core business areas, but also incident reports shared by other organisations, and we incorporate the lessons learned into the NTT Group's AI risk definitions.

3. Does your organization have mechanisms to receive and/or share reports of risks, incidents or vulnerabilities by/with third parties?

No

4. If your organization has programs to incentivize risk(s) disclosure, incidents and systemic vulnerabilities, please share what type of programs you use?

- Paid rewards (“bug bounty”)
- Research grants, contracts, and hiring red teamers

Please provide public URLs and/or details on your incentive program(s). If none, write “Not applicable.”

We operate an internal vulnerability reward program that rewards NTT Group employees for identifying security weaknesses in Group services and systems. We are also building and expanding AI red-team capabilities across the Group, with incentives for projects that adopt these practices early.

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

Contributes and uses

If contributes or uses, please select all that apply:

- ISO/IEC standards (e.g., ISO/IEC 27001, ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 42005)
- NIST AI Risk Management Framework (AI RMF)
- Industry-led best practices or codes of conduct
- Other international or regional standards (please specify): We contribute to the HAIP reporting framework, support the development and rollout of the HAIP handbook, and help develop Japan's AI guidelines for business operators.

6. Does your organization collaborate with relevant stakeholders across sectors to assess and adopt risk mitigation measures to address risks that could have broad and potentially cascading socio-economic impacts? Please indicate which stakeholders you collaborate with, and whether

collaboration is on a standing basis (Always-on), activated based on context (Ad hoc/as relevant), or there is no current collaboration.

	Always-on	Ad hoc / as relevant	No current collaboration
Relevant employees (security, legal/compliance, etc.)	☐		
Public authorities / regulators / AI safety institutes / other public sector bodies and inter-governmental coordination structures	☐		
Industry partners or industry fora	☐		
Users (end users, enterprise customers, developers using APIs)		☐	
Business customers / deploying organizations (if different from “users”)	☐		
Supply-chain partners (cloud, data providers, etc.)	☐		
Academia / researchers		☐	
Independent auditors	☐		
Standards bodies / multi-stakeholder initiatives (OECD.AI; ISO/IEC; IEEE; AIID etc.)		☐	
Independent civil society organizations (e.g., for evaluations, audits, or policy review)		☐	
Media / general public (people or communities indirectly impacted)		☐	
Other(s) (please add any other relevant stakeholder groups):		☐	
Not applicable		☐	

Please describe examples of how your organization collaborates. Examples may include: participating in multi-stakeholder or industry initiatives; partnering with academia, civil society, or the public sector; establishing internal or joint governance structures with external experts or in partnership with other efforts to share knowledge and jointly address risks.

We support international coordination by speaking at Hiroshima AI Process events, including in-person meetings of the HAIP Friends Group. We also speak at and participate in government-related global forums, such as the Hiroshima Global Forum for Trustworthy AI, HAIP events, and Global AISI Network events, contributing to AI policy discussions in multiple jurisdictions. In addition, we share expertise on AI governance through participation in the AI Governance Association and the JDLA.

Any further comments and implementation documentation.

Section 2 – Risk Management and Information Security

7. Across the AI system lifecycle, what steps does your organization take to manage risks and vulnerabilities? Please indicate which specific practices, tools or metrics your organization uses at each lifecycle stage. You may refer to tools or metrics present in the OECD.AI Catalogue of Tools and Metrics or suggest additions. Respondents may complete only the lifecycle stages relevant to their organisation's role. Stages that do not apply may be left blank.

garak, LLM vulnerability scanner

Accuracy

Plan and design

Collect and process data

Build, integrate and interpret model

Verify and validate

Deploy

Operate and monitor

Please provide a consolidated description of your organisation's approach to risk management across the AI system lifecycle, including how the practices identified above operate together and any cross-cutting governance, review or escalation processes. Please also indicate how often these practices are reviewed and what types of events trigger reviews and updates. Where relevant, please distinguish between different types of AI systems (e.g. generative or agentic AI).

Across the NTT Group, all AI projects undergo risk identification and assessment at the planning stage using a common Group-wide risk framework. In response to the assessment results, necessary risk mitigation measures are implemented. Before release, the AI risk management officer and other responsible personnel review the measures to confirm that the identified risks have been appropriately addressed.

When an already released AI system undergoes additional development or functional changes, it is reassessed as a new AI project.

Please describe any measures used to ensure data quality and fairness across the data collection and curation stage (e.g., dataset audits, filtering training data to remove harmful content or personal information, fine-tuning on curated data, use of moderation tools, assessment of limitations to model generalisability).

In operating the LLMs we develop and in sourcing their training data, we exclude data from pirated or otherwise problematic sources through blacklist controls and manual review to ensure data quality. In addition, validation testing has been done to confirm that when the same input is used with only

attributes such as gender, age, or race changed, the model produces consistent outputs and does not show a pattern of favoring or disadvantaging any group.

8. What security measures are used in testing AI systems?

- Isolated and secure test environments
- Network isolation from external access
- Locally hosted testing environments
- Restrictions on outbound Internet or API access, including a list of permitted domains or APIs
- Isolation of staging environments (from production / operational environments)
- Controlled environments for red-teaming and adversarial testing
- Containment measures for prompt-injection and jailbreak attempts
- Controlled security vulnerability testing
- Rate limits and resource caps
- Human-in-the-loop controls for higher-risk test cases
- Access controls, including roles-based permissions
- Disabling, restricting or simulating high-impact capabilities during testing
- Audit logging and monitoring
- Use of “AI-safe” test-data, as appropriate
- Use of synthetic, anonymized, or dummy data, as appropriate
- Other(s) (please specify): In consideration of security risks, all of the above options have been selected.

8.A. Please indicate, if relevant, the team or role responsible for overseeing secure testing and whether this responsibility is shared across multiple teams and/or functions.

Independent from AI system projects, dedicated AI and IT red teams are established, and AI safety testing is conducted based on the characteristics of each system.

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

9.A. Safeguards that promote lawful data use and transparency in AI training:

- Maintain a copyright policy that addresses data sourcing, content provenance, safeguards, and organizational roles and responsibilities
- Publishing “model cards” or contextual information on training data and model limitations
- Apply provenance controls to guard against training data being sourced from websites or repositories that have been determined to engage in large-scale piracy
- Refrain from the unlawful circumvention of technological protection measures in data sourcing
- Maintain policies or practices to respect copyright holders’ preferences through, where appropriate/applicable, mechanisms like Robots.txt “do not train” tags or other machine-readable protocols developed through voluntary, industry-led standards processes
- Conduct data cleaning, qualification, and/or tokenization activities as part of a transformative data preparation process

- Consult and/or retain an intellectual property attorney to protect, enforce, and comply with, intellectual property rights.

9.B. Safeguards that reduce the risk of dissemination of outputs that may infringe copyright:

- Restricting outputs that raise ethical, human rights, or legal concerns—such as non-consensual intimate imagery, unauthorized deepfakes, or outputs that are substantially similar to copyrighted works.
- Filtering results using keyword or image-based restrictions to reduce risks of misuse
- Designating clear points of contact so creators or rights holders can raise concerns about infringing outputs

10. How do you protect privacy and prevent your systems from disclosing confidential or sensitive data across the AI lifecycle?

- Make information about data privacy, practices, and controls accessible to a diverse set of stakeholders
- Use security controls, including encryption at rest and in transit
- Provide organizational customers with controls to configure and implement privacy choices (e.g., data retention, logging, access, or processing settings)

Describe key privacy measures and data-protection standards applied.

To enable the definition and identification of privacy risks, we have established operational rules and ensure that input data that may infringe privacy is neither collected nor used beyond its intended purpose without permission.

11. How does your organization assess cybersecurity risks and implement policies to enhance the cybersecurity of advanced AI systems across the AI system lifecycle? Respondents may complete the checkbox subsections in 11.A–11.D or describe their overall approach under 11.E.

11.A. Governance, policy and assessments

- Conduct regular cybersecurity risk and vulnerability assessments tailored to AI models or systems
- Perform threat modeling that includes AI-specific risks (e.g., data poisoning, prompt injection)
- Maintain or update security policies aligned with recognized standards (e.g., NIST CSF, ISO/IEC 27001, SOC 2, CIS Critical Security Controls), and review them regularly in response to emerging risks or regulatory guidance
- Maintain vulnerability management processes (scanning, channels for external reporting, patching, remediation)
- Implement incident response, disaster recovery, or business continuity plans, including escalation procedures for high-severity incidents
- Train staff on cybersecurity best practices and AI-specific threats, including how to recognize and respond to misuse or unintended outcomes of advanced AI systems
- Integrate cybersecurity AI risks into broader cybersecurity risk management activities
- Regularly review security measures and update them in response to emerging risks, incidents, or major releases

11.B. Technical and operational controls

- Apply multi-factor authentication (MFA) and role-based access controls for advanced AI systems
- Encrypt AI assets (datasets, models, configurations) in storage and in transit as appropriate
- Restrict physical access to servers, GPUs, or devices hosting AI models, systems, and/or applications
- Monitor system activity and log access to detect anomalies or misuse
- Conduct secure AI development and/or deployment practices
- Conduct security testing focused on AI-specific risks (e.g., red-teaming, adversarial testing, stress tests)
- These responsibilities are delegated contractually to model or infrastructure providers
- Other(s) (please specify): In consideration of security risks, all of the above options have been selected.

11.C. Protection of sensitive or high value AI assets

- Limit access to proprietary AI assets based on role or need-to-know
- Store model weights, datasets, and algorithms in secure, access-controlled environments
- Use hardware security modules (HSMs) or trusted execution environments (TEEs) where feasible
- Track and log access to sensitive AI resources
- Require NDAs or confidentiality agreements for staff and contractors with access
- These responsibilities are delegated contractually to model or infrastructure providers

11.D. Insider risk protection detections

- Conduct pre-employment screening or role-sensitive vetting
- Monitor for unauthorized internal access or suspicious activity
- Provide staff training on cybersecurity best practices and AI-specific threats
- Implement insider-risk escalation or response procedures
- These responsibilities are delegated contractually to model or infrastructure providers
- Other (please specify): In consideration of security risks, all of the above options have been selected.

11.E. Please describe the main security measures your organization applies and indicate which are specific to particularly sensitive AI assets, where relevant.

For LLMs, we use tools designed to assess AI vulnerabilities to evaluate AI security risks. For RAG systems that incorporate LLMs, we apply user access controls and restrict to available documents.

12. 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?

- Internal vulnerability disclosure receipt and tracking processes
- Bug bounty or incentive programs for external reporters
- Investigation of reported or identified risks and vulnerabilities
- Development of patches or other mitigations for confirmed risks or vulnerabilities

- Testing of patches or other mitigations
- Scanning for and mitigation of similar risks or vulnerabilities
- Collaborative vulnerability sharing (e.g., with partners, industry groups)
- Vulnerability disclosure program that is aligned with internationally recognized standards, e.g. ISO/IEC 30111 and 29147.
- Reporting to regulators / authorities when relevant
- Recognition of external finders of confirmed risks or vulnerabilities
- Defined escalation criteria and follow-on actions for identified vulnerabilities (e.g., for external reporting or information sharing)
- Other(s) (please specify): In consideration of security risks, all of the above options have been selected.

13. What post-deployment practices does your organization use to monitor and respond to vulnerabilities, incidents, emerging risks and misuse of advanced AI systems?

- Conduct post-deployment monitoring
- Perform root-cause analysis and apply lessons learned to improve future development and/or deployment practices
- Monitoring and emergency controls specific to agentic AI systems (e.g., ability to interrupt autonomous action sequences, override tool-use permissions, or revoke delegated authority)

14. Do you develop or deploy agentic AI systems (systems that can autonomously plan/act or use tools)?⁴

Yes

14.A. If yes, please indicate which categories of controls your organization applies. Please select all.

- Constraints on the agent's action space (e.g., tool-use permissions, environment sandboxing, allowlists/blocklists of resources, scope limits per task)
- Human oversight or interruptibility mechanisms (approval requirements for sensitive actions, escalation paths, interruption interfaces)
- Monitoring (anomaly detection, multi-agent interaction monitoring)
- Logging of agent actions

Please provide any further comments and implementation documentation.

No answer provided

Section 3 – Transparency Reporting on Advanced AI Systems

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

Are these clear and understandable by non-technical audiences?

No

16. 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?

- Public documentation

Describe how evaluation results are shared and with which stakeholders (e.g. other organizations, governments, civil society and academia, etc). You may also indicate whether non-technical or plain-language summaries are provided for broader audiences.

We have published safety information about our in-house LLM through a press release available at the URL below.

<https://group.ntt/en/newsrelease/2025/10/20/251020a.html>

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

Yes

If yes, provide links to privacy policies or notices covering personal data, user inputs, and AI-generated outputs.

The NTT Group's privacy policy is available at the URL below.

[Protection of Personal Information | NTT](#)

18. How 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?

- Protected information sharing

Please provide links to any publicly available information.

We maintain processes to manage the quality and accuracy of our training data, but we do not disclose the underlying details publicly.

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

No

20. Does your organization publish statistical insights derived from anonymised, aggregated usage data to advance understanding of AI adoption and its economic impacts in areas including

occupations and tasks by region, sector and country? To this end, do you contribute to international cooperation efforts?

No

Please estimate the total staff time and annual expenses associated with conducting compliance activities and include any further comments and implementation documentation (optional).

No answer provided

Section 4 – Organizational Governance, Incident Management, and Transparency

21. How has AI risk management been embedded in your organization's governance framework?

- Board of Directors oversight
- Executive oversight
- Senior management oversight
- Governance council or committee

Please describe how AI risk management is integrated into governance structures, including: which roles or bodies have advisory versus decision-making authority; which roles or bodies have final accountability for AI risk-related decisions; and how often policies are reviewed or updated (e.g., following major incidents, regulatory changes, or material updates to systems).

Within the NTT Group's risk management framework, AI risk is positioned as one of the key risks, and a standardized AI risk check workflow is defined based on shared group-wide AI risk definitions. Each group company appoints an AI risk management lead who translates these definitions into concrete rules at the service level, thereby implementing the governance framework.

22. Are relevant staff trained on your organization's governance policies and risk management practices?

Yes

If yes, describe training methods (e.g., onboarding modules, regular sessions, and confidential channels to report concerns).

The NTT Group maintains internal policies and standards and communicates governance policies and risk management practices through regular meetings and briefings with AI governance leads, while also addressing issues through a dedicated consultation desk.

23. Are steps taken to address reported incidents documented and maintained internally?

Yes

If yes, describe how incident records are kept and used for follow-up (e.g., incident logs, root-cause analysis reports, internal tracking systems). You may indicate whether and how you define escalation

thresholds for when incidents must be surfaced to senior leadership or external parties.

We define incidents in line with our AI risk definitions. In addition to addressing detected risks, we conduct root-cause analysis in cases where multiple risks overlap, identify measures to prevent recurrence, and document and retain the results.

24. Does your organization share research and best practices on addressing or managing risk?

Yes

If yes, describe how research or good practices are shared (e.g., publications, conferences, collaborations with other sectors).

We participate in government, industry-association, and private-sector events on AI governance to share best practices.

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

Yes

If yes, please indicate which standards or frameworks apply:

- ISO/IEC standards (e.g., ISO/IEC 27001, ISO/IEC 42001)
- NIST AI Risk Management Framework (AI RMF)
- OECD AI Principles
- Industry-led best practices or codes of conduct

If yes, describe which international technical standards or best practices your organization uses.

We reference frameworks such as the HAIP Code of Conduct, the EU AI Act, and Japan's AI business guidelines to define risks and implement governance accordingly.

Any further comments and implementation documentation.

No answer provided

Section 5 – Content Authentication & Provenance Mechanisms

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

- Documentation or FAQs explaining when and how AI is used in the system

Provide any additional details or context on how or when users are informed they are interacting with advanced AI systems (e.g. if such mechanisms are planned, in testing, or applied only to certain products).

NTT primarily operates through B2B projects, where relevant information is communicated during contract discussions and task alignment. In addition, for B2C services, users are notified through measures such as inclusion in the terms of service.

27. Does your organization use content provenance detection, labeling or watermarking mechanisms that enable users to identify content generated by advanced AI systems?

No

Any further comments and implementation documentation.

No answer provided

Section 6 – Research & Investment to Advance AI Safety & Mitigate Societal Risks

28. Does your organization advance research and investment in the following areas?

- Security
- Safety
- Data quality and representativeness
- Information integrity
- System performance and outcomes (e.g. accuracy, consistency)
- Explainability or interpretability
- Transparency
- Robustness or reliability

If yes, please describe key research or investment initiatives in the areas selected above (e.g., dedicated safety teams, funding of research programs, contributions to open-source safety tools, publishing research, partnerships and collaborative research initiatives). You may also indicate whether related outputs are publicly shared, shared with partners or within consortia or not publicly disclosed.

We evaluate the LLMs we develop and provide using publicly available evaluation tools, assessing quality, ethics, and security, and incorporating the results into product development.

In addition, we conduct research aimed at identifying and addressing AI-related risks, including:

- Reducing hallucinations and controlling inappropriate outputs
- Developing compound AI systems that automatically adapt to evolving cyberattack methods, enhancing the interpretability and transparency of detection and mitigation
- Advancing inspection and protection technologies for emerging AI threats, along with practical approaches to strengthening trust, including measures to address risks across the AI supply chain

29. Does your organization pursue research or investment related to socio-economic or environmental considerations in the development and deployment of AI?

- Socio-economic considerations (e.g., AI adoption and productivity, workforce transitions, skills development, access to AI tools)
- Environmental considerations (e.g., energy use, computational efficiency, resource use)

If yes, please provide examples of relevant research or investment initiatives for the areas selected above.

We conduct research on model development aimed at achieving high Japanese language processing performance using highly lightweight models, as an alternative to large-parameter LLMs such as GPT. Through this research, we aim to deliver lightweight LLMs that reduce training and inference costs, while also lowering environmental impact.

Any further comments and implementation documentation.

No answer provided

Section 7 – Advancing Human and Global Interests

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

Yes

If yes, describe any digital literacy or training initiatives your organization supports (e.g., user education, public AI-education programs, school or university partnerships, community workshops). You may also indicate whether these efforts include or prioritise underserved or underrepresented communities.

We implement organization-wide training initiatives to strengthen digital literacy in relation to generative AI, which introduces a range of societal risks.

As part of this effort, we have established and internally shared AI risk management guidelines that outline the risks and corresponding approaches to mitigation for each stakeholder group, including model developers, service providers, and AI users.

In addition, we provide educational content aimed at improving AI risk management literacy. This includes the purpose and structure of AI risk management, specific risks and countermeasures, and case studies, along with assessment questions to evaluate understanding. These materials are used to deliver training to all employees.

31. Does your organization pursue AI projects that aim to deliver societal or public benefits, including through partnerships with civil society and community groups?

Yes

If yes, please provide examples, including any collaborations with civil society, community groups, or efforts to address broader societal challenges.

The NTT Group has supported the SDGs since 2016 and promotes them across the Group. We see AI as a foundational technology for addressing social challenges. We also collaborate with industry associations and other organisations, local governments and communities, and academic institutions.

Any further comments and implementation documentation.

No answer provided