

OECD AI Transparency Report

Organization: Infosys (IND)

Reporting Period: Q3 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

- 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): Infosys aligns its AI risk classification and management approach with internationally recognized frameworks and standards, including the NIST AI Risk Management Framework (AI RMF), ISO/IEC 42001, OECD AI Principles, relevant EU AI regulatory requirements, and broader Responsible AI, privacy, cybersecurity, and risk management practices. Risks are categorized across areas such as fairness, safety, security, privacy, transparency, explainability, accountability, compliance, robustness, and societal impact.
- Consult with external stakeholders (e.g., from academia, industry groups, civil society, or standard development organisations) when developing or updating risk taxonomies
- Maintain an internal taxonomy, classification system, and/or set of risk area definitions

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.

Our organization does not rely on a single quantitative threshold to determine when AI risks become unreasonable. Instead, severe risks are assessed through a risk-based governance framework aligned with ISO/IEC 42001, NIST AI Risk Management Framework (AI RMF), ISO/IEC 23894, OECD AI Principles, and applicable regulatory requirements, including the EU AI Act. Risks may be considered unreasonable or intolerable when they have the potential to cause significant harm to individuals, society, organizations, or critical systems and cannot be reduced to an acceptable level through technical, operational, legal, or organizational controls.

Risk assessments evaluate factors such as potential impact severity, likelihood of occurrence, scale of affected stakeholders, reversibility of harm, regulatory implications, human rights impact, safety concerns, privacy implications, cybersecurity risks, and the effectiveness of available mitigations. AI systems identified as presenting severe residual risk are subject to enhanced governance review, additional controls, deployment restrictions, or may be prohibited from deployment until risks are adequately mitigated.

Examples of potentially unreasonable or intolerable risks include:

- AI systems that could cause significant safety impacts to individuals or critical infrastructure.
- Systems that may result in unlawful discrimination, bias, or denial of fundamental rights.
- AI applications involving unauthorized processing or exposure of sensitive personal or confidential information.
- Autonomous or agentic systems capable of taking consequential actions without appropriate human oversight, accountability, or control mechanisms.
- Systems that could materially facilitate cyber-attacks, fraud, misinformation, or other harmful activities.

Mitigations are applied proportionate to the level of risk and AI capability. Our organization uses a Responsible AI framework aligned with the EU AI Act, classifying use cases as Prohibited, High, Medium, or Low Risk in our AI Management System(AIMS). Prohibited (Unacceptable Risk) use cases, or those whose risks cannot be adequately mitigated, are considered unreasonable and may be redesigned, or rejected. The Responsible AI Assessment Team provides independent oversight, with high risk use cases requiring stronger controls, including enhanced risk assessments, human-in-the-loop approvals, explainability measures, security testing, privacy reviews, monitoring, escalation procedures, and executive-level governance oversight.

The organization recognizes the distinct risk profiles of different AI technologies. Generative AI systems are assessed for risks such as hallucinations, misinformation, intellectual property concerns, privacy exposure, toxicity, and prompt injection attacks. Agentic AI systems receive additional scrutiny due to their ability to autonomously plan, make decisions, interact with external systems, or execute actions. Such systems are subject to stronger governance controls, approval gates, human oversight requirements, access restrictions, monitoring, and periodic reassessments before and after deployment.

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
- Specific risk identification practices for agentic AI capabilities, e.g., autonomous action-taking, tool use, multi-step planning (please specify): Infosys evaluates AI systems through structured adversarial testing, including automated and manual red-teaming, to identify vulnerabilities and ensure ethical, secure, and resilient performance. Findings inform remediation and compliance checks under Responsible AI governance before production deployment, aligning with ISO 42001 and global safety standards.
- Impact assessments such as personal data protection assessment and fundamental rights impact assessments
- Vulnerability reports
- Automated monitoring / remote status reporting (e.g., telemetry pipelines, automated alerts when risk thresholds are breached)

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.

Deployment decisions for AI systems follow a structured review process involving the use case team and relevant stakeholders. AI systems are assessed through established questionnaires covering areas such as fairness, privacy, security, explainability, and model characteristics, with identified risks documented and supported by appropriate mitigation plans. Deployment approval is granted only after all required assessments are completed and recommended mitigations are implemented, ensuring that necessary safeguards, controls, and compliance requirements are in place before the AI system moves to production.

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.

The incident reports including external reports feed into our Responsible AI risk management process, informing updates to governance controls, risk registers, and compliance frameworks, ensuring continuous improvement and alignment with ethical, secure, and regulatory standards.

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

Yes, both receiving and sharing

If yes, please indicate which stakeholders reporting mechanisms may be accessible to, recognising specifics will depend on the nature of the report and risk level. For each, indicate whether access is on a standing basis (Always), activated based on context (Ad hoc/as relevant), or not currently accessible.

	Always	Ad hoc / as relevant	Not currently accessible
Relevant employees (security, legal/compliance, etc.)	☐		

	Always	Ad hoc / as relevant	Not currently accessible
Public authorities (e.g., public reporting offices for security incidents or data breaches)		☐	
Supervisory authorities (e.g., data protection authorities)		☐	
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, etc.)		☐	
Specific civil society organizations		☐	
Media / general public (people or communities indirectly impacted)		☐	
Other		☐	

Please describe how your organisation determines when and how reporting mechanisms are made accessible to different stakeholders (e.g. based on legal or regulatory requirements, internal policies, or risk level). Please also provide public URLs or details on how to submit reports. If none, write “Not applicable”

We generate market scan reports every month which gives a snapshot of the AI market (especially enterprise AI), including trends, regulatory shifts, risks, opportunities, and how organizations can adopt AI responsibly. Infosys shares information on vulnerabilities to all the relevant teams over email and incidents, AI risks through internal governance forum, the AI War Room, Market scan reports and cross-functional reviews involving Legal, Risk, and Security teams to ensure timely awareness and coordinated action.

How does your organization share relevant information as appropriate?

- Reporting to regulatory authorities as relevant
- Information-sharing partnerships (with confidentiality agreements as appropriate)
- Publicly

Please describe what type of information is shared.

Infosys shares information on vulnerabilities to all the relevant teams over email and incidents, AI risks through internal governance forum, the AI War Room, Market scan reports and cross-functional reviews involving Legal, Risk, and Security teams to ensure timely awareness and coordinated action. We also generate market scan reports every month which gives a snapshot of the AI market (especially enterprise AI), including trends, regulatory shifts, risks, opportunities, and how organizations can adopt AI responsibly.

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

- Not applicable

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)
- Industry-led best practices or codes of conduct
- Framework Convention on AI and Human Rights, Democracy and the Rule of Law (Council of Europe)
- OECD Due Diligence Guidance for Responsible AI
- General Purpose AI Code of Practice
- NIST AI Risk Management Framework (AI RMF)
- Other international or regional standards (please specify): EU AI Act

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	☐		

	Always-on	Ad hoc / as relevant	No current collaboration
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.

Yes — Infosys collaborates with civil society, academia, and community organizations to develop AI solutions that support the UN SDGs. For example, we co-developed the AI-powered Sustainability Atlas with Economist Impact ([Economist Impact and Infosys Launch The Sustainability Atlas to Help Businesses Navigate a Sustainable Future](#)) to advance climate and social decision-making, and through the Infosys Foundation’s Aarohan Social Innovation Awards, we support NGOs and social innovators building technology for education, healthcare, and environmental sustainability. These partnerships ensure our AI initiatives address real community needs and contribute to inclusive and sustainable development.

Any further comments and implementation documentation.

No answer provided

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.

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).

Our organization has a comprehensive ISO 42001 certified AI Governance Program. The program provides end-to-end oversight across the AI lifecycle, covering risk management, accountability, transparency, human oversight, data governance, and regulatory compliance. These are updated annually or when triggered by regulatory changes, emerging risks, audits, or technological advancements, ensuring alignment with ISO 42001 standards and global best practices.

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).

Infosys ensures data quality through rigorous validation, provenance checks, and ethical sourcing. Bias mitigation includes diverse dataset curation, fairness audits, and algorithmic reviews during training and collection stages. These measures align with Responsible AI principles and ISO 42001 standards, promoting transparency and reducing harmful bias risks.

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

- Isolated and secure test environments
- Locally hosted testing environments
- Human-in-the-loop controls for higher-risk test cases
- Access controls, including roles-based permissions
- Containment measures for prompt-injection and jailbreak attempts
- Network isolation from external access
- Isolation of staging environments (from production / operational environments)

- Restrictions on outbound Internet or API access, including a list of permitted domains or APIs
- Controlled environments for red-teaming and adversarial testing
- Controlled security vulnerability testing
- Rate limits and resource caps
- Audit logging and monitoring
- Disabling, restricting or simulating high-impact capabilities during testing
- Use of “AI-safe” test-data, as appropriate
- Use of synthetic, anonymized, or dummy data, as appropriate

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.

Responsibility for secure testing is shared across multiple teams. The Information Security/Cybersecurity team oversees secure testing standards and vulnerability management, while Engineering, QA, and Product teams execute testing and remediation activities. Governance and risk management functions provide oversight to ensure compliance with organizational policies and regulatory requirements.

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
- 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
- Engage in AI training that comprises a non-consumptive use of any underlying data
- 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:

- Filtering results using keyword or image-based restrictions to reduce risks of misuse
- 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.

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)
- Apply Privacy-Enhancing Technologies (PETs) where applicable (e.g. differential privacy, federated learning, synthetic data generation, homomorphic encryption)

Describe key privacy measures and data-protection standards applied.

Our organization protects privacy by restricting the use of personal, sensitive or confidential data and enforcing strict Responsible AI checks with required approvals before any data is used. We document and validate data sources, rights, and security controls to prevent unauthorized disclosure and ensure compliance with privacy requirements throughout the AI lifecycle. Every use case is assessed by data privacy office and controls are implemented as per recommendations by DPO.

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
- These responsibilities are delegated contractually to model or infrastructure providers

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

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
- Provide staff training on cybersecurity best practices and AI-specific threats
- Monitor for unauthorized internal access or suspicious activity
- Implement insider-risk escalation or response procedures
- These responsibilities are delegated contractually to model or infrastructure providers

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

Infosys assesses cybersecurity risks through continuous vulnerability scans, penetration testing, and threat modeling for AI systems. Policies enforce encryption, secure coding, and access controls. Governance aligns with ISO 42001 and Responsible AI principles, ensuring resilience against evolving threats and safeguarding advanced AI systems throughout their lifecycle.

Infosys protects critical IP and trade secrets through secure environments with strict access controls, encryption, and role-based permissions. These are managed within client environments for client projects and through licenses for Infosys IP. Proprietary model weights, algorithms, and datasets are stored in isolated infrastructure within client environment with monitoring and compliance checks under Responsible AI governance and ISO 42001 standards, ensuring confidentiality and integrity.

Infosys reviews security measures regularly through scheduled audits, governance reviews, and compliance checks. Assessments occur at least annually and during major system updates, or on demand depending on the severity of the risk, ensuring alignment with Responsible AI principles, ISO 42001 standards, and evolving cybersecurity best practices for AI systems.

Infosys has an insider threat detection program integrated into its information security framework. It includes continuous monitoring, and strict access controls for sensitive AI assets. These measures align with Responsible AI governance and ISO 42001 standards to prevent unauthorized access and safeguard critical information.

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)
- Reporting to regulators / authorities when relevant
- Defined escalation criteria and follow-on actions for identified vulnerabilities (e.g., for external reporting or information sharing)

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

- 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.

- 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
- Constraints on the agent's action space (e.g., tool-use permissions, environment sandboxing, allowlists/blocklists of resources, scope limits per task)

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?

Yes

15.A. If yes, which of the following information is included in your organization's publicly available documentation for any of your AI products?

- Risk management policies
- Summary of results from evaluations of safety, security, and societal risks including potential adverse impacts on individuals or groups (e.g. impacts on human rights, privacy or differential outcomes across user groups).
- Plain-language or non-technical summaries

Please provide links or references showing where this information is made public.

Infosys communicates its risk management policies to users through Responsible AI documentation, and to public through various public events. These includes publishing ethical guidelines, participating in industry forums, events, awards and sharing governance practices via consortiums and regulatory platforms, ensuring transparency and alignment with ISO 42001 standards

15.B. If yes, how often are such reports usually updated?

Other (e.g., triggered by material changes, incidents, or new risks)

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
- Regulatory reporting as relevant
- Direct engagement with AI safety institutes, civil society or academic partners
- Protected information sharing

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.

Infosys shares AI risk and impact evaluation outcomes, where appropriate, through customer communications, regulatory engagements, industry forums, standards initiatives, academic collaborations, research publications, and responsible AI governance disclosures. Information is shared subject to confidentiality, privacy, security, and contractual obligations, ensuring transparency while protecting sensitive information.

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.

<https://www.infosys.com/privacy-statement.html>

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?

- Regulatory reporting as relevant

Please provide links to any publicly available information.

NA

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

Yes

If yes, describe additional method(s), including where relevant transparency measures related to AI agents

Infosys demonstrates transparency through Responsible AI governance disclosures, privacy notices, client communications, public research and thought leadership, participation in industry forums and standards initiatives, and disclosures regarding AI capabilities, risks, safeguards, and oversight mechanisms.

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?

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

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).

Infosys integrates AI risk management into its enterprise governance framework through cross-functional oversight involving Responsible AI, Legal, Privacy, Security, Compliance, Risk Management, and business stakeholders. Advisory responsibilities are shared across these functions, while approval and decision-making authority rests with designated governance bodies and accountable business owners. Final accountability for AI risk decisions lies with the relevant business and governance authorities. AI-related policies and controls are reviewed periodically and updated to address regulatory changes, emerging risks, audit findings, and evolving technology.

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).

Infosys uses onboarding programs, mandatory compliance training, role-based learning, periodic awareness sessions, and ongoing communications to educate employees on ethics, security, privacy, risk management, and Responsible AI. Employees and third parties can raise concerns through confidential and anonymous reporting channels, including the Infosys Ethics Line (Whistleblower mechanism), supported by a non-retaliation policy. A data subject can raise Privacy concerns on privacy@infosys.com

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.

Infosys maintains incident records through internal incident management and tracking systems, supported by incident logs, investigation records, corrective action plans, and root-cause analysis reports. Incidents are monitored through closure, with lessons learned used to improve controls and governance. Escalation thresholds are generally based on severity, risk, business impact, regulatory obligations, and customer impact, with significant incidents escalated to senior leadership and, where required, reported to appropriate external stakeholders

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 generate market scan reports every month which gives a snapshot of the AI market (especially enterprise AI), including trends, regulatory shifts, risks, opportunities, and how organizations can adopt AI responsibly.

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:

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

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

Infosys aligns its Responsible AI framework with global standards, such as ISO 27001, ISO 27701, ISO/IEC 42001, NIST AI Risk Management Framework, EU AI Act, and UNESCO ethical principles, ensuring robust governance, risk mitigation, and compliance across AI lifecycle etc.

Any further comments and implementation documentation.

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?

- User disclosure (e.g., text notice, verbal statement, or system label)
- Documentation or FAQs explaining when and how AI is used in the system
- Persistent visual or audio indicators (e.g., watermark, icon, chime, banner) during AI interaction
- Disclosure to end-users when an AI system is acting autonomously or executing actions on their behalf (e.g., making purchases, sending communications, modifying files)

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).

Infosys advocates transparency by implementing clear AI interaction disclosures. Users are informed when engaging with AI systems through explicit notifications and labeling mechanisms, aligned with Responsible by Design principles for ethical and accountable AI deployment. These include visible disclosures, onboarding messages, and accessible documentation. For sensitive use cases, consent options and ability to engage a human are provided. The implementation of these are per the client and project requirements.

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

Yes

27.A. If yes, how?

- Detection tool(s) for hidden provenance signals (e.g., watermark or metadata checks)
- Use of international or industry standards (e.g., C2PA)

27.B. If yes, does your organization use international technical standards or best practices when developing or implementing content provenance?

Yes

27.C. Does your organization collaborate on or invest in research to advance content authentication and provenance?

Yes

Describe how provenance mechanisms are implemented and which standards or tools are used, and any collaborations or investments to improve content authentication (e.g., C2PA credentials, joint R&D projects, open-source initiatives, standard-setting groups). You may also indicate whether these mechanisms are tested for robustness against removal, tampering, or circumvention.

Infosys collaborates with global forums and invests in research to strengthen content authentication and provenance. Initiatives include partnerships, open-source tools, and adherence to guidance provided by Coalition for Content Provenance and Authenticity (C2PA) and ISO/IEC.

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

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.

Yes. Infosys actively participates in global collaborations and research projects to advance AI safety, security, and trustworthiness. Investments include participation in and contributions to working groups of EU AI Office, NIST, WEF, ISO and UNESCO.

Outputs are shared through appropriate channels based on the collaboration model and confidentiality requirements. Certain research findings, standards contributions, and thought leadership materials are publicly available, while consortium-specific, partner-related, or proprietary outputs are shared only with authorized participants and are not publicly disclosed.

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.

Infosys invests in Responsible AI research to reduce socio-economic and environmental risks by promoting fairness, inclusivity, and sustainability. Initiatives include bias mitigation, energy-efficient AI practices, and alignment with global standards like UNESCO recommendations for Ethical AI and sustainable AI development. Infosys invests in sustainable AI research by promoting ethical, efficient, and responsible AI development, including autonomous systems, that are designed to optimize resources and reduce the overall carbon footprint.

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.

Yes. Infosys supports digital literacy and AI education through initiatives like Infosys Springboard and AI training programs, helping users understand AI's capabilities, limitations, and impacts. These programs promote responsible AI awareness and ethical use globally.

Infosys prioritizes underserved and underrepresented communities through programs such as Infosys Springboard, which offers free digital learning, technology, and career-readiness content to learners from diverse backgrounds, helping bridge the digital skills gap and promote inclusive access to education and employment opportunities.

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.

Yes. Infosys undertakes AI-enabled and digital innovation initiatives aimed at generating societal and public benefits across education, healthcare, sustainability, and digital inclusion. Through Infosys Springboard, the organization provides free access to digital, and AI learning opportunities. Infosys Foundation collaborates with civil society organizations, NGOs, educational institutions, healthcare providers, and government agencies to improve educational outcomes, healthcare access, environmental sustainability, and community resilience. Infosys also supports social innovation initiatives that encourage technology-driven solutions to societal challenges, particularly in underserved and vulnerable communities.

Any further comments and implementation documentation.

No answer provided