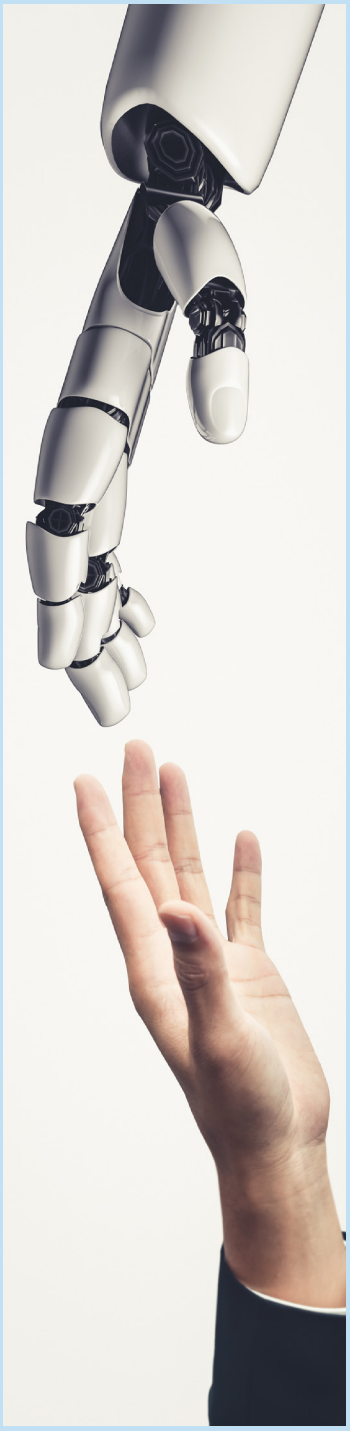
VIEW POINT



FROM COMPLIANCE TO A COMPETITIVE EDGE — THE RISE OF RESPONSIBLE AI

Abstract

As artificial intelligence (AI) adoption accelerates globally, the gap between availability and trustworthiness has become a critical challenge. While 66% of people use AI worldwide, only 46% trust it, underscoring the urgency of embedding ethical principles into AI systems from the outset. Responsible AI offers a framework to bridge this gap. Organisations can draw on established frameworks for better implementation and to overcome common pitfalls. Ultimately, responsible AI is not merely a regulatory obligation but a strategic differentiator. Companies that build trustworthy, ethical AI systems are best positioned for long-term competitive success.

Infosys®
Navigate your next

Water, water, everywhere / Nor any drop to drink" - Samuel Coleridge in the Rime of the Ancient Mariner.

Coleridge was, in 1798, referring to the water of the oceans when he wrote this poem about sailors dying from thirst, while being stuck on the high seas. But the analogy is quite apt in 2026 when we look around us at the digital oceans and see "unusable" AI everywhere. Stories of AI going rogue are rising, as are mounting evidence of AI pilots failing.

One of the key reasons for this problem with plenty — the lack of usable AI — lies in the concept of "responsible AI": a phrase that refers to the design and implementation of AI systems that have built-in principles of ethics, fairness, transparency and accountability, with an intent to minimise harm and maximise benefit to society. It is not just about technical performance: it goes well beyond that to ensure AI systems align with human values.

In fact, responsibility in AI systems starts where compliance ends, when the precept is about human values and protecting the safety of humans who interact with the systems. Some of the key pillars of responsible AI systems include:

- **Explainability:** AI decisions must be understood by humans
- **Reliability and safety:** The ability to handle edge cases without failure
- **Bias mitigation:** Ensuring the training data is diverse and representative
- **Accountability:** Clear responsibility for outcomes, via monitoring and audits
- **Privacy:** Safeguarding user data

The one precept that is vital over and above all of these is that of human oversight, which remains essential to ensure that high-stakes sectors like healthcare or finance are not fully automated.

Responsible AI matters for many reasons, the fundamental one being that it builds trust throughout the value chain. AI is here to stay. While 66% of people use AI globally, only 46% trust the systems. 7 in 10 people believe stronger regulations are needed.

When generative models influence decisions at scale, risks like discrimination or misinformation can rise. Responsible AI systems address such risks. Compliance is supported as well, keeping pace with evolving regulations and promoting inclusivity across diverse communities

When responsible AI is embedded into governance frameworks, it becomes part of sustainable AI adoption.

How to get started

To embed responsible AI into systems in practice, enterprises must frame ethical principles and design guardrails for AI deployments. They must examine the entire AI lifecycle and embed the principles via governance and assessments, as well as continuous monitoring. Market leaders, such as Microsoft and Google, and industry experts have established structured frameworks that may be assessed and integrated into an organisation's systems.

Some of the popular frameworks include:

- Google's AI Principles that focus on societal benefit and avoidance of bias
- Microsoft standards that emphasise privacy, reliability, and accountability
- PwC's risk management toolkit
- Huron's seven actions that cover safety, validity, transparency, fairness, privacy, accountability, and human-centred design.

The endeavour starts with leadership. Leaders must align on several foundational precepts:

- Core vision and accountability standards that the organisation must follow
- Robust cybersecurity and data privacy safeguards
- The plan must include ongoing impact evaluations and approval gates
- There must be rigorous documentation of all changes
- It is important to engage stakeholders to ensure inclusivity and compliance with the regulations of the geographies the organisation operates in.

Common pitfalls

The endeavour to build responsibility into AI systems is not without challenges.

- Foremost among them is treating the implementation of responsible AI frameworks as mere checkboxes. This can lead to a very superficial adoption and embed persistent risks into the system such as bias or a lack of accountability.
- Lack of clear ownership of the endeavour, and not drawing clear lines of accountability can also hamper the project. Outcomes may remain undefined or ill-defined, and diffused across multiple teams.
- As outlined previously, leadership backing is crucial for success. If leaders do not provide sufficient resources, such underfunded initiatives serve as mere lip service to the brand, with very little enforcement. Shoddy integrations may also create new silos, creating clashes between ethics reviews and rapid development cycles.
- On the technical side, data quality issues, bias and representativeness issues in data may lead to unreliable or skewed models. Data that is scarce, or inaccessible high-quality data, may create similar issues.
- Monitoring needs to be an ongoing process, along with auditing. Neglecting these may create conditions for model drift or emerging biases going unchecked after deployment. One of the common problems is insufficient human oversight, leading to errors, non-compliance, and ethical gaps.

- On the culture side, challenges include inadequate training and not combating resistance to change. This leaves teams unprepared and exposes firms to legal or ethical problems. The downstream effects may include fines or reputational damage. Trust in the company's products and services may erode, especially with customer-facing applications.

Given the gamut of challenges and complexities, enterprises may opt to work with strategic partners who have the experience and expertise to support them with responsible AI framework design, deployment, as well as post-deployment monitoring and compliance.

Responsible AI is not just a matter of compliance. Building ethical and fair standards in AI systems and maintaining bias-free models and applications that depend on these models is a competitive advantage for companies. In a fast-moving marketplace filled with increasing AI-driven capabilities, tools and technologies, companies that actually take the time and effort to build responsible AI systems will prove to be winners in the long run.

How Infosys BPM can help

Infosys BPM offers a comprehensive suite of responsible AI and AI safety solutions. These include AI support services such as developing Gen AI classifiers, automating prompt moderation, output filtering and Gen AI red teaming; AI enablement for LLM chatbots, review of AI results curation and output accuracy review. Whether it is with exploratory data analysis, model fine tuning, and review or model inference and monitoring, enterprises can rely on Infosys BPM to build in responsible safeguards into their AI systems.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next