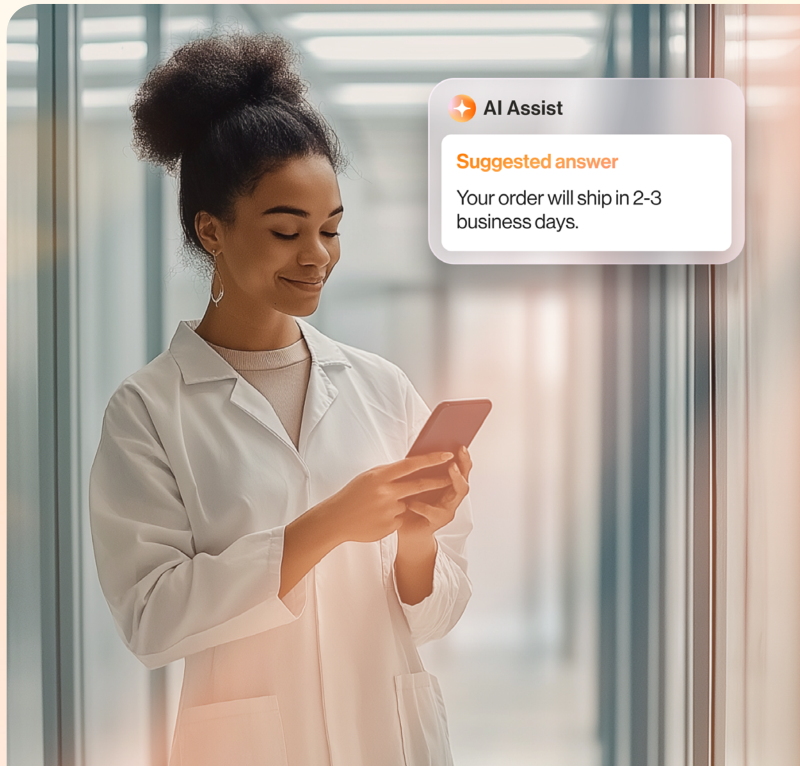
Responsible AI, governance, and trust in workplace communications



GenAI has vast potential, already demonstrating tremendous value for improving productivity and effectiveness. AI tools are obliterating old assumptions about what is possible with computing technologies, changing how we think about business processes and the future of work.

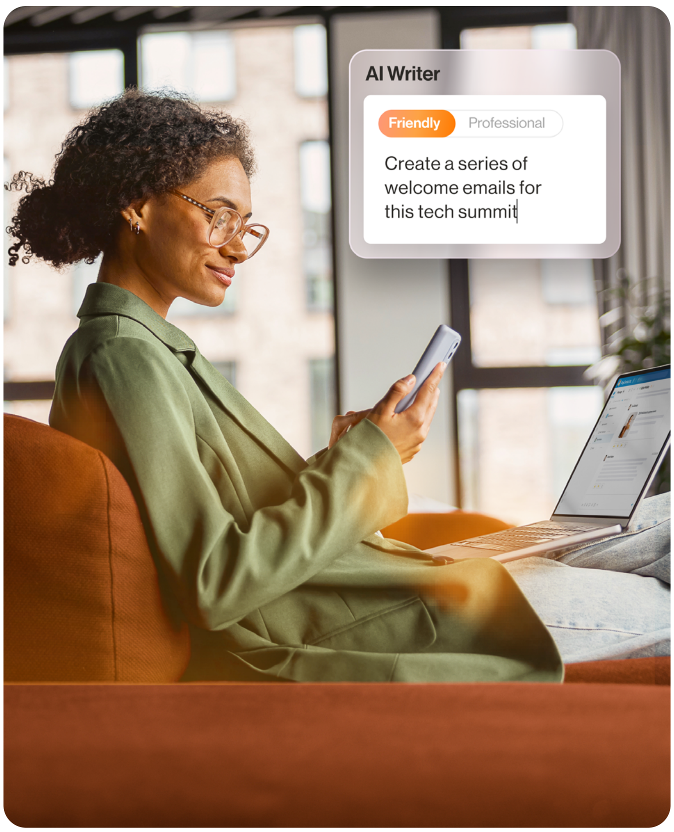
At the same time, there is a growing awareness that AI technology requires careful oversight. In many respects, this is still uncharted territory. As businesses forge ahead, it is essential to remain mindful of potential pitfalls and develop frameworks for governance and trust.

Gartner estimates that by 2027, more than 50 percent of enterprises will have implemented a governance framework for the responsible use of AI.[1] Today, that number is less than two percent.

As AI innovation accelerates in the coming years, organizations must develop mature governance frameworks to incorporate ethical deployment, transparency, and regulatory compliance into their planning and implementation of AI technologies. Doing so will enable organizations to fully enjoy the benefits of AI without compromising ethical standards and values.

1. Gartner, A Comprehensive Guide to Responsible AI

Defining and implementing responsible AI



Responsible AI is built upon a clear set of principles that guide ethical decisions. These include but are not necessarily limited to:

- **Transparency**, which ensures that the processes and decisions made by AI systems are open and understandable, fostering trust among users and stakeholders by allowing them to see and understand how decisions are made.
- **Fairness**, which aims to eliminate bias and discrimination, ensuring that AI systems deliver rational outcomes that apply equal standards to all stakeholders, regardless of their background or characteristics.
- **Accountability**, which establishes clear lines of responsibility for the actions and outcomes impacted by AI systems, ensuring that there are mechanisms in place to address any issues or errors and hold parties responsible as needed.
- **Privacy**, which safeguards personal data, ensuring that personal or organizational information is not misused or disclosed without consent. This is essential for maintaining user trust and for legal compliance.
- **Safety**, which involves designing and deploying AI systems in a manner that prevents harm to individuals, groups, or society as a whole. AI must function reliably and predictably, staying within clearly defined ethical and legal boundaries.

Each of these principles contributes to trust and confidence, safeguarding the interests of the organization, its employees, its customers, and other stakeholders.

In the context of business communications, responsible AI must ensure that automated decision-making and data processing are fully explainable and justifiable to users.

Each organization must forge its own path, tailoring its definition of responsible AI, including guiding principles, to address its unique circumstances and ethical considerations. Organizations must formulate a plan for integrating those principles into the complete lifecycle of their AI projects, from strategy and development to execution and ongoing operations. This will help them to achieve their goals of enhancing productivity and collaboration while also aligning with the organization's fundamental values. It will also set them up for success as AI regulation takes shape in the coming months and years.

Privacy and data security by design

GenAI requires training. To mimic human thought and language, the large language models (LLMs) upon which GenAI is built must ingest and process large amounts of information. In other words, these models use human input to continuously improve their understanding of linguistic nuance and gain factual knowledge.

But what happens to that input when it includes potentially sensitive information? GenAI is often described as an "intelligent assistant," but what happens when that assistant shares a bit too much information with people outside the office, or even with unauthorized users within their own organization?

This is precisely why privacy and security have emerged as key elements in responsible AI governance frameworks. At RingCentral, we believe that privacy should never be an afterthought. Our privacy team is deeply involved with every product and service we develop, ensuring that it meets our stringent standards for privacy and data security. Our product development process includes multiple privacy reviews to ensure transparency, privacy, and explainability. We explore each new requirement and AI feature at length to determine how it could impact our customers and users. Our privacy team identifies risks, recommends mitigation strategies, and documents how our AI works.

Perhaps just as importantly, this "Privacy by Design" practice extends to our third-party partners. We perform rigorous AI assessments as part of our vendor management process, from initial due diligence to ongoing reviews. RingCentral will only work with partners whose standards and practices fully conform to our "privacy by design" philosophy.

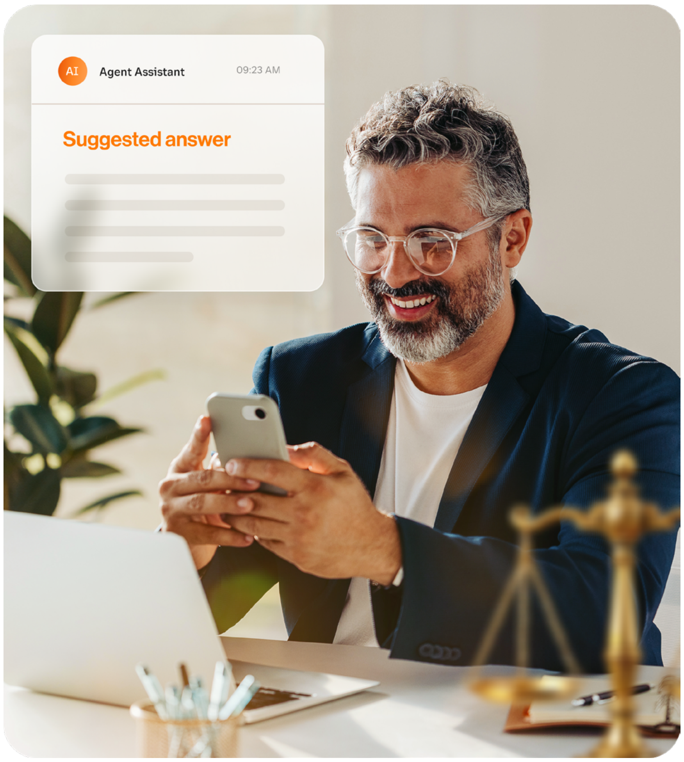
Transparency forward

Trustworthy AI means protecting stakeholders and safeguarding their data. This includes full transparency regarding how data is collected and used. At RingCentral, for example, we do not use our customer's data to train our AI models, nor do we allow our third-party vendors to use it to train their AI models. As part of our commitment to AI transparency, we make Product Privacy Datasheets available on our RingCentral Trust Center. This keeps our customers and prospects fully informed about how RingCentral uses their data, including the specific purposes and outputs for which it may be used.

This empowers our customers, in turn, to establish and maintain trust and transparency with their own stakeholders.RingCentral's AI Transparency Whitepaper offers more detail about our approach to trustworthy AI, including how our products use and feature AI.

Removing bias from AI

Several years ago, a large US bank sent pre-approved credit card applications to thousands of people, setting predictive credit limits calculated by AI algorithms. It soon came to light that the bank's AI systems were offering lower credit limits to women than to men. Since then, numerous other news stories have underscored the potential for bias in AI.



AI clearly has the potential to get it wrong. That doesn't merely apply to potential discrimination, though; AI can also provide output that is inappropriate to the circumstances.

Responsible AI must incorporate safeguards to eliminate that possibility, first by establishing limits and boundaries within the technology itself, then via feedback loops that correct the AI algorithms. Assessing and eliminating potential bias during the development process is an important first step, but as customers use our products and services, we aim for continuous improvement.

In RingCentral's Smart Notes feature, for example, it is possible to programmatically infer whether or not the AI output is correct. If a user is performing many edits, that provides an indication that our AI output needs to be adjusted.

RingCentral's processes include extensive testing for potential bias and undesirable outputs. We also test for equality and accessibility across multiple demographics, and we perform legal and stakeholder reviews to assess the inclusiveness of our products for every one of our customers.

Choosing the right vendors and partners

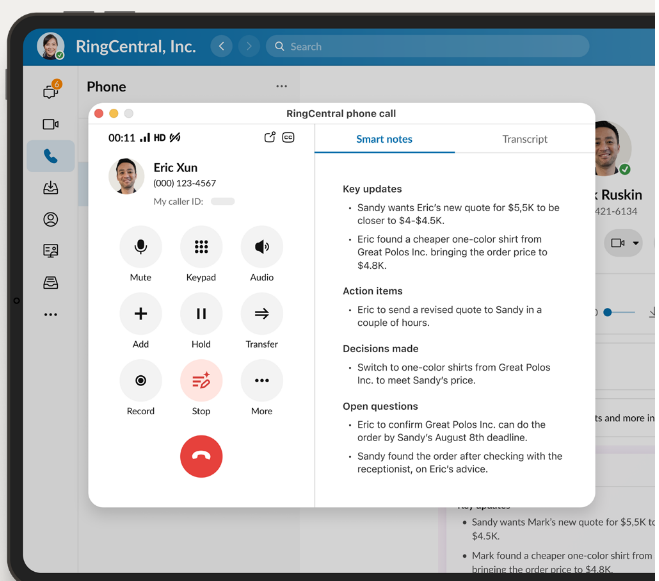
Responsible AI must account for the interdependent relationships among all the organizations that share the use of a particular instance and the vendors that contribute to the technology stack. Therefore, it is critical that enterprises carefully select their technology vendors, ensuring that they not only "talk the talk" but can actively demonstrate a commitment to responsible AI practices.

This requires a clear statement of commitment to responsible AI, backed by a governance framework that includes privacy, security, and transparency. Regulators are only just beginning to pay attention to AI, relatively speaking. Recent actions by the European Union signal that closer scrutiny of AI systems and practices is inevitable. It is likely to happen fast. Those companies that proactively govern their AI will be ahead of the curve as new regulations take effect. For many, that simply means working with vendors whose commitment to responsible AI is likewise ahead of the curve.

Technology vendors are rapidly incorporating AI into their products. Business communication tools offer one of the most powerful use cases for AI, with applications across every industry, and for companies of all sizes. When selecting a business communications vendor, enterprises should assess each candidate's AI governance framework carefully. Ask about each company's ethical standards and guiding principles for AI. Find out how they handle third-party vendor relationships, including initial due diligence and periodic reviews.

Companies that do their homework and hold their vendors to high standards will engender trust among their customers and employees. They can set the stage for a smooth adoption of emerging regulations and standards for AI, stimulating growth and rapid adoption of AI systems throughout their organizations. By partnering with forward-thinking vendors that demonstrate a strong commitment to responsible AI, companies can build trust, improve their organization's reputation, and contribute to a safer, more ethical digital environment.

RingCentral is committed to ensuring a strong framework for responsible AI in all our AI-enabled products. To learn more about how to safely and responsibly adopt AI solutions into your business communications, read our white paper entitled "Navigating AI with RingCentral."



A Checklist for IT decision makers: responsible AI and governance

Responsible AI ensures trust, reduces compliance risk, increases adaptability, and improves the outcomes produced by AI-enabled systems. Here are some guidelines to help ensure your success:

1. Assessing vendors for responsible AI

- ☐ Does the vendor provide transparency about its AI-enabled systems and outputs to the users who interact with those systems?
- ☐ Do the vendor's AI-enabled systems maintain confidentiality, integrity, and availability through protection mechanisms that prevent unauthorized access and use?
- ☐ Do the vendor's AI-enabled systems comply with applicable security regulations, industry standards, and internal company policies?
- ☐ Are the vendor's AI-enabled systems developed and used in compliance with privacy laws like GDPR, HIPAA, CCPA, and a written vendor privacy policy?
- ☐ Does the vendor's AI technology adequately address equality and equity, preventing harmful bias and discrimination?

2. Implementing governance frameworks

- ☐ Define clear AI governance policies that outline how AI will be used in your organization, including roles, responsibilities, and ethical guidelines.
- ☐ Create a dedicated AI Governance Committee within your organization whose mission is to oversee AI, ensuring ethical implementation and usage, monitoring security and privacy, and ensuring compliance.
- ☐ Perform periodic reviews to monitor performance, identify potential security and compliance concerns, and gather stakeholder feedback.

3. Preparing for regulatory change

- ☐ Start by implementing AI technologies that can be easily modified to comply with future regulatory shifts. Look for industry-leading platforms that prioritize responsible AI and governance.
- ☐ Monitor emerging AI regulatory frameworks at local, national, and international levels. Assign a team to track updates and assess how proposed changes may impact your organization.
- ☐ Engage your legal department and risk & compliance officer to ensure that your AI-enabled systems meet current and pending regulations, with an eye to potential changes on the horizon as well.

For more information, please contact a sales representative. Visit ringcentral.com or call 855-774-2510.

RingCentral Inc. (NYSE: RNG) is a leading provider of AI-driven cloud business communications, contact center, video and hybrid event solutions. RingCentral empowers businesses with conversation intelligence, and unlocks rich customer and employee interactions to provide insights and improved business outcomes. With decades of expertise in reliable and secure cloud communications, RingCentral has earned the trust of millions of customers and thousands of partners worldwide.. RingCentral is headquartered in Belmont, California, and has offices around the world.

RingCentral

RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002. ringcentral.com

09/2024