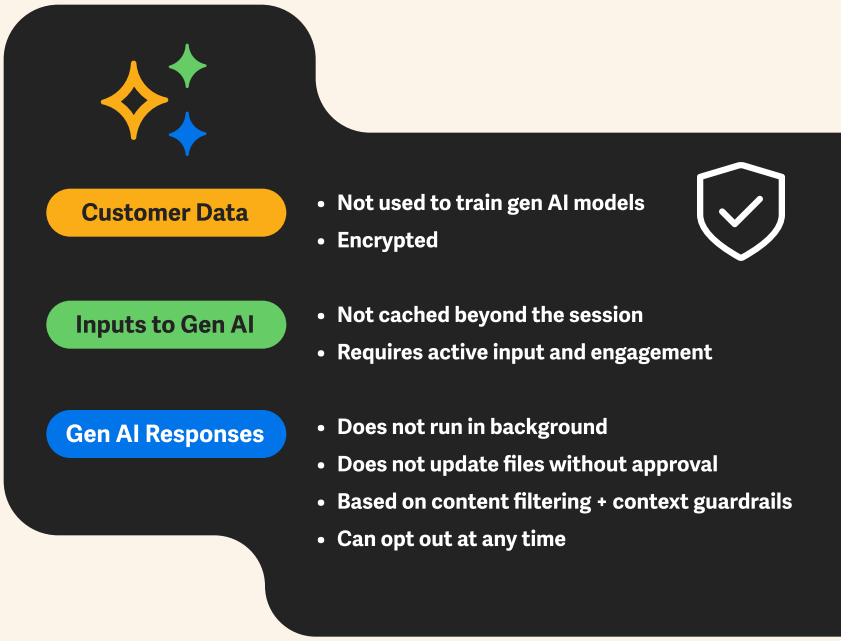
Delivering a secure gen AI experience

Generative AI revolutionizes the way you work, making content creation, editing, and brainstorming more efficient than ever. With the complex and sensitive work associated with financial reporting, ESG reporting, audit, and risk, responsible AI usage is paramount—particularly when it comes to data security, subject-matter expertise, and human oversight.

We've built a generative AI experience that brings you productivity gains backed by ethical and responsible implementation. Our goal is to provide you with the tools and support needed to achieve your best work while maintaining a high standard of data security, privacy, and human-centered decision-making.



Our commitment spans three crucial aspects: customer data, inputs to gen AI, and gen AI responses. None of these components are used to train the generative AI models, whether they are the foundational large language models (LLMs) or the industry-specific extensions exclusive to Workiva.

From enrollment to engagement, your data and your interactions with Workiva Gen AI are handled with the utmost care and responsibility.

AI, on your terms
You have the control to ask for AI's assistance when needed. This maintains the quality of your work but also reinforces the importance of human judgment and active input in the process.

Single platform security
Protect your data by using our built-in gen AI capabilities, rather than copying and pasting information in an unsecure AI service in the public domain.

Built to augment and enhance
Workiva Gen AI is designed to work alongside you as a virtual assistant, not a hands-off automation tool. Your expertise and creativity should help guide the process. And the more you engage with Workiva Gen AI, the better results you will get.

Your data stays your data
Your data, your inputs into the gen AI model, and the responses generated by the AI remain entirely distinct from the model training process. None of these elements are utilized to train the AI models. There is a clear separation between your data and the AI training process.

Frequently Asked Questions About Workiva Generative AI

Workiva

Operational security

What measures are in place to protect customer data during interactions with Workiva Gen AI?
To ensure data security and privacy, all data—including customer inputs and AI-generated responses—are encrypted during transmission. Gen AI session data is not cached beyond the duration of your session—which is set to a default of 10 minutes.

Data management

How do you prevent using my data for training your model?
Workiva does not train its own large language model (LLM). Instead, we partner with industry-leading LLM providers—such as Google, AWS, and Microsoft—to power Workiva Gen AI responses. Customer data, inputs, and responses are not stored or being used to train models by the LLM providers. Your data remains entirely separate from the AI training and tuning process, ensuring that it is not utilized for model improvement.

What data do you use to customize and improve results?
Customer data is not used to train or tune LLMs. We rely on retrieval augmented generation (RAG) to enhance prompts and responses. This involves using algorithms to search for and retrieve industry- and context-based information relevant to users' prompts. Workiva Gen AI leverages a narrower, defined set of sources for added security and reliability, and also provides citations for responses that can be cross-referenced to validate information.

Response quality and reliability

What are you doing to ensure Workiva Gen AI results are safe, ethical, and reliable?
Our select LLM providers have several safeguards in place to create a safe and responsible gen AI experience—for example, bias prevention. Please refer to our individual **LLM providers' documented principles and policies** for details on their stance.

How do you prevent inappropriate or unreliable results?
Workiva Gen AI employs content filtering and anchoring to effectively prevent the processing or generation of inappropriate or sensitive content, as well as limit hallucinations. For more details, refer to the "How Workiva Generative AI Works" diagram on the following page.

Oversight and control

Will Workiva Gen AI automatically add content to my documents?
We do not generate content without your action. After each response, you have full control to add the generated content, modify it, or discard it altogether.

What should users do with responses from Workiva Gen AI?
Every response generated by Workiva Gen AI should undergo human review to ensure that the content aligns with your intent, is accurate in the context of your work, and meets your quality standards.

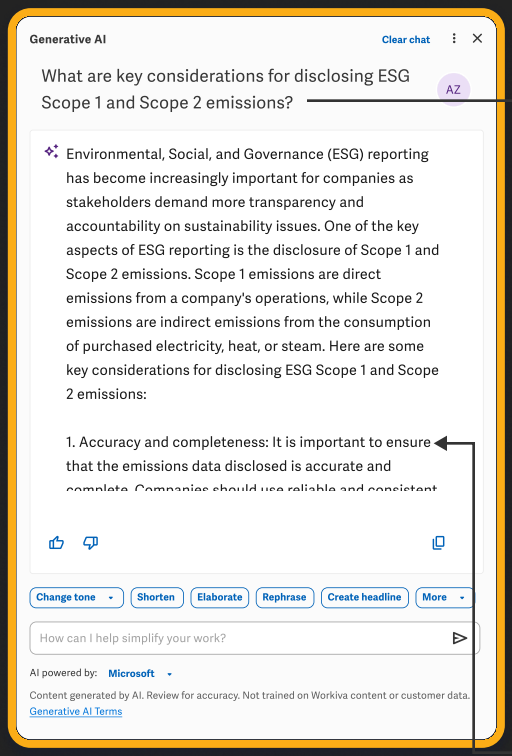
Can we opt out of using Workiva Gen AI?
Customers have to actively enable Workiva Gen AI in the account settings. If you have any concerns or simply prefer not to engage with Workiva Gen AI, you have the freedom to opt out at any time.

How do we get started using Workiva Gen AI?
Before enabling Workiva Gen AI for your organization, we ask that you review the **Workiva Generative AI Terms of Use**, which include specific terms of our LLM providers. For more information on the systems and controls we have in place, Workiva customers can also **access our SOC reports here**.

For a full list of FAQs with more details, visit workiva.com/genai-security

How Workiva Generative AI works

We prioritize safety, quality, and user-friendliness to provide you with the best gen AI experience possible. The following steps ensure that the responses you receive are appropriate for your needs while also maintaining a high level of security and compliance.



Prompt Filter

User inputs are filtered to adhere to guidelines, eliminating off-limit requests.

Guardrails

Boundaries are set for generating responses, using factors like context, intent, and persona. As a result, responses generated are more relevant and aligned with your needs.

Grounding

We leverage embeddings and retrieval augmented generation (RAG), consider the solution and file type being used, and offer templates for specific Workiva-exclusive extensions, such as Workiva Support or ESG European Sustainability Reporting Standards content. We also provide citations and references for responses, indicating their source.

Prompt Generation

Prompts and model parameters create a user-friendly experience—including predefined commands like "shorten" or "elaborate," as well as prompt-tuning with industry terms to avoid confusion (i.e., 10-K report vs. 10-K run).

Response Generation

Responses are generated based on advanced AI models from industry leaders such as Google, Microsoft, and AWS. **Click here for a list of our current LLM providers.**

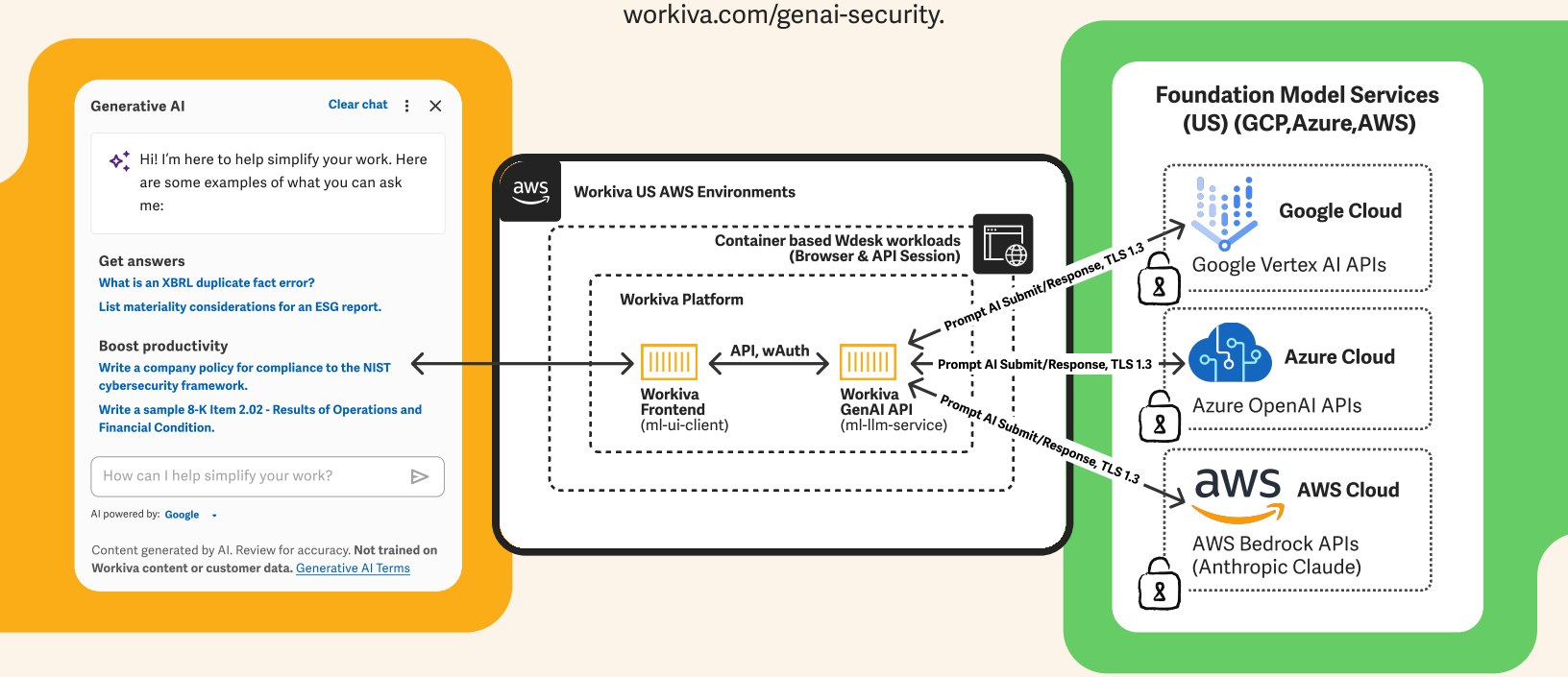
Response Filter

Responses are filtered to exclude inappropriate or prohibited content, such as unethical terminology. **Visit our Gen AI security hub for our vendors' ethical AI policies.**

Security is baked into every step. For more information, visit workiva.com/genai-security

Workiva Generative AI Architecture

More information about the large language models (LLM) Workiva uses in their gen AI experience can be found at workiva.com/genai-security.



Data security measures throughout the experience:

- Encrypted at rest
- Encrypted in transport
- Not cached outside a session with our secure LLM providers

Data security measures with each LLM provider:

- Providers cannot access customer prompts or data
- Data enters and leaves only through API calls

Put the productivity and security of Workiva Generative AI to work for you.
Learn more at workiva.com/genai-security

"This is exactly the kind of generative AI implementation we want to use from a data security standpoint."

CIO, SVP of Internal Audit
Commercial & Consumer Finance Company

WORKIVA.COM/CUSTOMERS

About Workiva

Workiva Inc. (NYSE:WK) is on a mission to power transparent reporting for a better world. We build and deliver the world's leading cloud platform for assured integrated reporting to meet stakeholder demands for action, transparency, and disclosure of financial and non-financial data. Workiva offers the only unified SaaS platform that brings customers' financial reporting, environmental, social, and governance (ESG), and governance, risk, and compliance (GRC) together in a controlled, secure, audit-ready platform. Our platform simplifies the most complex reporting and disclosure challenges by streamlining processes, connecting data and teams, and ensuring consistency. Learn more at workiva.com.

20231020

The information contained herein is proprietary to Workiva and cannot be copied, published, or distributed without express prior written consent. Copyright 2023 Workiva Inc. Workiva is a registered trademark of Workiva Inc. All rights reserved.

workiva.com | info@workiva.com