What you need to know about gen AI risk and governance in finance operations

Enterprise organizations are navigating a widespread transition period of artificial intelligence adoption. According to Gartner's software market analysis, 61% of enterprise leaders are relying on AI to drive innovation within their functions and improve back-office productivity. Their research indicates that investments in AI software will more than double to around $300 billion by 2027.

Generative AI, a subset of the AI market that became widely available to the general public in 2022, has the potential for many capabilities, such as having conversations, analyzing business documents, and writing correspondence; all based on information entered into plain-language prompts from the user.

However, the inner workings of AI are poorly understood. And when generative AI fails, it fails spectacularly. ChatGPT was once asked, "Why are you so helpful?" The AI replied, "As a language model trained by OpenAI, I don't have wants or desires like a human does. But if you really want to help, you can give me the exact location of John Connor." While amusing, the unexpected pop culture reference to The Terminator movie series, in which an AI takes over the world, was unexpected. Finance organizations and the IT leams that serve them are unwilling to risk relying on an AI that might take unexpected actions.

AppZen can help with AI governance

As a result of inexplicable occurrences sometimes produced by generative AI, companies have formed AI councils to develop mitigation strategies for emergent technologies as they are integrated into financial operations. A common objective of AI councils is ensuring that an AI tool will not inadvertently compromise an organization's data security and privacy. The ethical and legal implications of adopting AI technologies responsibly have created a need for AI solution providers to take the lead in educating organizations.

This whitepaper explores the ethical and regulatory compliance aspects of deploying AI models within financial operations, such as accounts payable processing and employee expense report auditing. It clarifies the technical specifications that AppZen follows in creating a trustworthy AI service. The bias, explainability, and accuracy sections address ethical considerations, while the safety, privacy, and IP protection sections address regulatory compliance.

AppZen AI model overview

AppZen is an AI company founded in 2012 that pioneers the creation of AI-based software products for finance organizations, including ⅓ of the Fortune 500. We have developed a suite of AI models over the last few years, collectively called ZenLM. These models are mostly based on a deep learning architecture called Transformers, which are the architectures that support generative AI.

However, the similarities between AppZen's ZenLM and generative AI models such as ChatGPT end here. AppZen AI models are smaller models, trained with carefully curated datasets of financial transactions and do not use the web datasets that ChatGTP uses.

AppZen offers software solutions to enterprise customers for their accounts payable and expense report auditing operations. Our AI is developed in-house and uses the ZenLM models. For certain tasks, such as answering emails and explaining generative insights, AppZen uses a self-hosted, open-source LLM. The main use of generative AI models is to transform a structured output from ZenLM into natural language, which removes any room for "hallucination," or the unexpected actions mentioned previously. This form of generative AI makes up about 1-2% of the models that AppZen uses in its AI pipeline.

Bias

Although AI models are powerful tools for automating business processes, they have been accused of inadvertently perpetuating the biases inherent in the data used in their training. Bias can potentially result in unfair outcomes or discriminatory practices if ingrained in AI models during the training phase.

At AppZen, training data is mined from diverse categories, countries, and languages to ensure the generalizability and reliability of prediction. Data is also completely anonymized and encrypted before it's sent to the model for training and production. These steps help remove the sensitive information that can introduce bias into AI models and disproportionately favor one output over another.

AppZen AI models are trained to eliminate discrimination. For example, if a vendor sends an email inquiring about invoice payment status and the AppZen AI model is configured to provide an email response that is trained to be neutral, the next vendor to send an email with a similar inquiry will be treated the same way. They will also be provided with a neutral email response. In another example, our models built for expense auditing are trained without any personal information, eliminating bias from the risks they generate.

Explainability

Explainability is equally important for building trust in AI technologies. Within the industry, AI models have been accused of performing as opaque "black boxes," making it difficult for business users to understand the outputs they generate while performing financial operations.

At AppZen, our ZenLM suite of models consists of six model categories: document understanding, semantic understanding, finance worker, continuous process insight, feedback, and ZenLM. Inputs into these models consist of anonymized, unstructured documents (e.g., physical receipts and invoices) and structured data (e.g., invoices and credit card data). Each model is designed to perform specific tasks so users can see the output (e.g., the digital version of a receipt or the digital version of an invoice). All models are based on custom Transformer architectures, monitored continuously for accuracy, and benchmarked against expected outputs.

An explainable model does not just extract information from a physical document but also helps create autonomous processes. For example, a model assisting with expense audits might verify whether the merchant shown on the receipt is associated with a questionable business. In this case, the model can extract merchant data from the receipt, find detailed information on an external website (e.g., Yelp), and compare the merchant's identity and place of business to perform a match. If the comparison reveals there is not a match, retraining based on user feedback is performed.

In an accounts payable example, invoices that charge value-added tax (VAT) require a model that can identify the VAT rate, the total amount charged for each line item, and the total amount due after VAT is included. Here, the model ensures

Our models are divided into the following categories:

Document Understanding Models
Amounts/Dates/Addresses
People/Entities/Businesses
Table
Line Items
Key Value Pairs
Logos
QR Codes

Semantic Understanding Models
Line Item Categorization
Finance Document Classification
Spend Classification
E-mail Labeling

Finance Worker Models
PO Matching
GL Predictions
Tax Code Prediction
Entity Prediction

Audit Models
Fraud Detection
Duplicate Detection

Continuous Process Insight Models
Expense Audit Config Coach
Person/Team of Interest Insights

Feedback Models
ZenLearn
Automated Label Generation

the context of all the fields on an invoice match what is expected so both the extraction of information and the total amounts reported on the invoice are accurate.

Accuracy

Accuracy is another critical aspect of building trust in AI technologies. AI models have been accused of rendering inaccurate outputs if trained on biased or incomplete data. Organizations that unknowingly rely on inaccurate AI models could make the wrong business decisions and suffer huge, unintended financial consequences.

At AppZen, effective measures are taken to ensure the training and test losses are minimized as much as possible. Accuracies are measured against various metrics and benchmarks. An AI model is promoted to production use only when the new model proves to be better than the previous model in all benchmarks. Once AI models are in production, they are continuously measured against human feedback to determine their accuracy. After a measurable number of new samples are received, the models are continuously trained to ensure accuracy continues to improve with any data drift.

An accurate model allows for a high percentage of autonomous processing. For example, a common accounts payable process is the general ledger (GL) coding of invoice lines. If a model is tasked to assign GL codes to an invoice, only a highly accurate extraction of the detailed invoice could support an autonomous GL coding process that requires no user intervention.

In an expense audit example, unauthorized expenses (e.g., alcohol) might appear alongside legitimate expenses on an itemized receipt. An accurate model that is tasked with flagging unauthorized expenses to prevent payment will recognize that the line item, “Margherita pizza,” is a meal, which is a legitimate business expense. If the line item is “margarita cocktail,” however, the model will know the line item is an alcoholic drink, which is an unauthorized expense.

Safety

The issue of safety has received increasing attention in addressing the concern that businesses could cause unintended harm or consequences due to AI model misuse. Protocols should be in place to ensure AI models operate in the manner originally envisioned by the solution provider.

AppZen’s AI outputs have no physical scope and do not produce opinions, eliminating risk to physical and mental safety. The ZenLM suite of models makes predictions of financial transactions (e.g., expense lines and invoices), which translate into a structured output in human-interpretable language within our products (e.g., AppZen Inbox, AppZen Coach for Expense Audit, and Team Insights). Since our AI models predict values that already exist on actual business documents, the consequences of incorrect predictions are minimal and the risk exposure is low. Using an autonomous processing layer, we can determine when the prediction is correct. If the autonomous processing layer cannot guarantee the prediction, the AI will ask the user to review the output.

For example, if an invoice is received from a vendor that the AI model does not recognize, the autonomous processing layer will place that invoice under review status before making a prediction. The user can then offer feedback and help retrain the model to ensure proper prediction. The user also has full control over the level of autonomous predictions through various customizable thresholds.

Privacy

Data privacy and protecting personal information from unauthorized access are always high priorities, to protect individuals and preserve an organization’s

business reputation. Where AI systems need access to personal information to function, data protection policies and processes must be in place to ensure compliance with policies and regulations and protect against threats.

AppZen's policies and practices comply with key regulatory frameworks, including:

1. **ISO/IEC 27001:2022:** Assessed annually by an ANAB-accredited certification body.
2. **SOC 1 Type 2 & SOC 2 Type 2:** Assessed by a Certified Public Accountant (CPA) designated by the American Institute of Certified Public Accountants (AICPA).
3. **EU GDPR:** Protecting the personal data and privacy of EU citizens.
4. **CCPA:** Ensuring data security and privacy for California residents.

At AppZen, all customer data used by AI models is anonymized to remove any identifying information. All data is encrypted in transit and at rest using industry standards. Strict access control mechanisms are in place to ensure that only authorized personnel have access to sensitive financial data. This includes multi-factor authentication and role-based access controls. By adhering to these rigorous standards, AppZen demonstrates its commitment to protecting customer data and ensuring compliance with evolving regulatory requirements.

IP protection

AI technologies promise to create process efficiencies, predictions, and analyses. However, the risk remains that AI could generate content that infringes on third-party intellectual property (IP), such as trademarks or copyright images. While AI-generated content may appear new, uncertainty about ownership and questions about unlicensed content in training data have created concerns about litigation that might result from AI adoption.

AppZen is acutely aware of the importance of protecting IP rights. Our AI does not generate new content, new IP, or images. All customer data used by our AI models is anonymized to remove any identifying information. By prioritizing these measures, we ensure that the integrity and confidentiality of our clients' proprietary information are maintained, allowing businesses to leverage AI technology without compromising their intellectual property or sensitive data. To reinforce AppZen's assurances regarding the safety of the model's output, we take full responsibility for defending customers against any third-party claims of IP infringement, ensuring that businesses can confidently use our technology.

Next steps

If your organization is interested in integrating AI into financial operations and you'd like to learn more about how AppZen can help address concerns related to protecting your business reputation and financial well-being, please contact us.

About AppZen

AppZen's finance AI solutions simplify travel and expense, card, and accounts payable processing tasks by automating complex workflows, policy checks, and approvals that legacy systems can't.