Sage uses the power of AI (Artificial Intelligence) to support Small and Mid-sized Businesses

Sage, a UK FTSE50 tech company, is a market leader in accounting, financial, HR and payroll technology for small and mid-sized businesses (SMBs), enabling them to streamline operations, make more informed decisions and be more productive. Our ambition is to be the trusted network for small and mid-sized businesses.

Despite record numbers choosing to start and grow a business, business owners still face barriers to growth:

- Sustained economic uncertainty means businesses are looking for better, quicker insight of their financial position and to make commercial decisions with confidence.
- Regulation and compliance are viewed as a growing area of risk and uncertainty especially around tax and employment law.
- Competing for talent and being an employer of choice coupled with pressure on wages creates an additional strain.

Digitisation with advancements in AI has the potential to free business owners and their workforce from repetitive administration tasks to deliver more strategic higher-value tasks, ultimately increasing productivity. AI will progress from automation of tasks to managing entire workflows.

How Sage is using AI today:

- To automate manual processes such as invoice processing. SMBs embracing Accounts Payable (AP) Automation report a 2X – 3X improvement in productivity, which creates more capacity within their accounting teams.
- Our Outlier Detection solution is the first real-time AI-driven tool for general ledger error detection, reviewing more than 15 million transactions per week, helping accounting teams catch and correct thousands of accounting errors before they are posted.
- We are using AI to power Sage Earth, our carbon accounting solution to classify expenses according to specific carbon emissions categories, so we can more accurately predict their environmental impact. This is helping SMBs manage and reduce their carbon emissions.
- Sage Accounting uses AI to automatically categorize bank transactions for digital tax filing.

- With Generative AI we can use LLMs (Large Language Models) to provide a better user experience and digital assistance.

Sage is focusing on using AI to give business leaders real-time, trusted information about their organisation's financial performance. We will empower SMBs to make faster, smarter, more confident decisions, to create more time and space for users to focus on growing and scaling their businesses.

AI and Trust

We have spoken extensively to SMBs globally about AI, and just as they are looking for technology to help drive growth, equally there is a long way to go before SMBs feel familiar with, and trust AI.

Whilst US SMBs are most likely to see the potential of AI (54% in US vs 39% UK/31% France), our research shows that trust is the most important consideration for SMBs when looking to increase their adoption of AI. Delivering promised results, proof of the benefits and confidentiality are all seen as key.

Sage's software offerings assist our customers in making critical decisions across diverse domains, including human resources, accounting and taxation and financial management. Erroneous or "hallucinated" data could pose considerable risks to our clients, particularly for small enterprises. These businesses often operate at an accelerated pace and possess limited capacity for peer-review of the decisions being made.

Our view is that operational decisions suggested by AI should not inadvertently favour or disadvantage certain groups. Transparency in how AI processes financial data is key as financial predictions might be based on incomplete or outdated data, leading to unreliable forecasts. HR (Human Resources) recommendations must be rational and justifiable (especially where harm can be brought to an individual or group) and handling of HR data must respect the jurisdiction and nationalities of relevant individuals.

SMBs will need to feel a strong sense of security before using AI for their business-critical tasks, they need proof that any answers generated will be correct and want to ensure employees have had the right training to use AI without creating additional risks.

That is why Sage will never use AI in a way that erodes a customer's trust in Sage or our products. We are working hard to embed a philosophy of trusted AI among the SMBs we serve. People will only transition their work to technology if they trust the technology to do the job safely and competently.

Standards and Regulation

Sage believes a common framework and nomenclature for AI risks, internationally recognised standards and where appropriate, regulation, will play a significant role in driving innovation forward whilst maintaining public confidence in AI systems. For these reasons, Sage welcomes international collaboration by public and private stakeholders to establish clear, effective guardrails for AI.

Governments considering creating standards for, or, regulating AI should do so in a way which recognises the scope and objectives of the existing standards and regulatory landscape (both domestic and where relevant, internationally) and focuses on enabling and guiding companies to respond effectively to specific harms in the context of their AI development, while allowing for advances in technology and innovation. That includes efforts to align around common parameters and consider the scope of AI, taking a risk-based, context-specific approach to governing AI, and evaluating existing laws and regulations to determine whether there are gaps requiring incremental new rules for AI.

A regulatory model which clarifies the split of responsibility between foundation model developers, application developers (like Sage) and end users (like SMBs) will be key. This could be similar to the widely used *shared responsibility model* for cloud computing, which has been successful at providing clarity for consumers of cloud infrastructure and services.

We believe it is important the burden of any AI regulation is not carried by SMBs using AI features in our products.

NIST (National Institute of Standards and Technology) Request for Information

We are pleased to respond to the NIST Request for Information (RFI) Related to NIST's Assignments Under Sections 4.1, 4.5 and 11 of the Executive Order Concerning Artificial Intelligence (Sections 4.1, 4.5, and 11) to **produce guidelines and taking other actions to advance the safe, secure, and trustworthy development and use of AI** and to reinforce a US leadership position in responsible AI innovation as first safety legislation.

We welcome the key role NIST is playing in shaping responsible AI globally b:

- Creating a risk management framework for AI, the NIST AI RMF, which can be tailored to businesses' specific contexts and scaled to encompass a wide range of use cases.
- Setting new secure development standards for software and practices for labelling synthetic content (AI-generated material).
- Providing comprehensive resources for use by the AI community while working on additional guidelines for Generative AI.

Developing Guidelines, Standards, and Best Practices for AI Safety and Security

Sage is planning to adopt the NIST Risk Management Framework (RMF) and companion Adversarial Machine Learning guidance. More specifically, we plan to use the RMF Playbook to augment our Enterprise Risk Management Framework and support and complement our existing governance, risk management and cyber security processes for secure software development of our AI/ML systems and services.

Sage's AI and ML (Machine Learning) Secure Coding Standard is informed by the Open Worldwide Application Security Project (OWASP) Machine Learning Top 10 and OWASP Top 10 for LLM (Large Language Model) Applications projects and our testing processes are designed to confirm the absence of Top 10 issues and validate completeness against the Top 10s.

We intend to develop bespoke validation and verification tests to cover all the AI Risks and Trustworthiness principles in the RMF and would be happy to share this.

More broadly, Sage is adopting the Secure by Design Principles for software development, issued by the Cybersecurity and Infrastructure Security Agency (CISA) in 2023. Our commitment to these principles shapes the way we integrate security into the fabric of our design processes, well before the development, configuration, and deployment stages of our products and services.

Our view is that new NIST standards or frameworks created for AI should be designed to be employed with this important work from CISA to ensure a comprehensive approach to secure AI software development.

Sage believes AI red teaming plays an important role in managing AI risks and providing assurance to creators and consumers of AI systems. As with cyber security red teaming and penetration testing, we believe AI red teaming is most successful and effective when it is:

- Delivered against a consistent and transparent framework and methodology, used to determine the objectives and scope of testing.
- Available as an in-house capability or external service provider, or a blend of the two, subject to the level of assurance which is being sought.
- Delivered by practitioners who have validated their skills and experience through independent certification bodies, and where possible, in the specific context of the testing being undertaken.

We envisage Sage’s AI red teaming will involve tests to simulate potential adversarial scenarios to identify vulnerabilities, biases, or unexpected behaviours. However, these tests are also requirement outputs of a threat modelling exercise that must take place much sooner. The tests must be realistic, cover ethics, iterative in our software development lifecycle process and provide sufficient coverage (i.e. including data integrity, model robustness, output validation, and response to edge cases).

Professions, skills, and disciplinary expertise organizations need to effectively govern generative AI

Companies can build on the existing skills and expertise they have today that address risk, cyber and policy to effectively implement AI governance. However, AI ethics is a collective endeavour and requires a deep understanding of the impact of AI on customers and colleagues.

Understanding of risks and application of frameworks should be a company-wide initiative which will require upskilling colleagues across the business, from the Board of Directors down. The support of organizations like NIST in training and awareness will be very valuable.

Similarly, we see government as having a key role to play in supporting nascent professions such as AI assurance.

Reducing the Risk of Synthetic Content

Content provenance is applicable in accounting and payroll software for generating authentic invoices or payslips. Provenance tracking or watermarking can help prevent fraud such as fake invoices. Technical standards in this area should cover business related content (e.g. fake statements or invoices) as well as citizen facing content (e.g. deep fake videos, misinformation).

Useful techniques include digital signatures which are already a legal requirement in a few jurisdictions, plus immutable ledgers as mentioned above e.g. AWS (Amazon Web Services) QLDB. AI content generator software products could store the signatures for the content they generate on a publicly searchable blockchain solution. For example, this blockchain security testing company is maintaining a public list of their audits https://hacken.io/audits/.

ML powered detection models could be trained by public synthetic data and multi-model watermarking.

Effective assurance will be needed for certain critical sectors so new techniques can be audited effectively.