

Exploring the risks of AI across the accounting profession

Exploring the risks of AI across the accounting profession

The recent declaration issued by countries attending the AI Safety Summit hosted by the UK Government at Bletchley Park in November 2023 encapsulates the twin features of AI that make its increasing use by businesses inevitable but challenging. The Bletchley Declaration notes that AI presents “enormous global opportunities” yet “alongside these opportunities, AI also poses significant risks”.

This short paper is intended as a brief summary of those risks for accountancy firms. For those with a deeper interest in this subject we will be jointly hosting a seminar in Spring 2024.

AI and the new technological horizon

The use of AI can benefit professional services firms significantly. For accountancy firms, smart intuitive platforms are being used to support digital audit, to analyse processes and controls, for pattern detection, to search large numbers of journal entries for anomalies, to relate and cluster data, or perform payroll processes. Such capabilities enable businesses to synthesise, segment and translate data, automate processes, and transform the execution of tasks. As platforms evolve, AI interface is likely to transform all elements of business activities, services, solutions, products, as well as the means of execution and delivery, in unimaginable ways.

For example, there is likely to be greater adaption of AI capability within the tax function in terms of identifying and implementing appropriate tax planning scenarios, and performing tax compliance processes, and tax management, all enhancing efficiency. However, this needs to be considered in the context of developing sufficiently sophisticated operational AI models for scenarios involving the provision of complex prescriptive advice on matters such as tax.

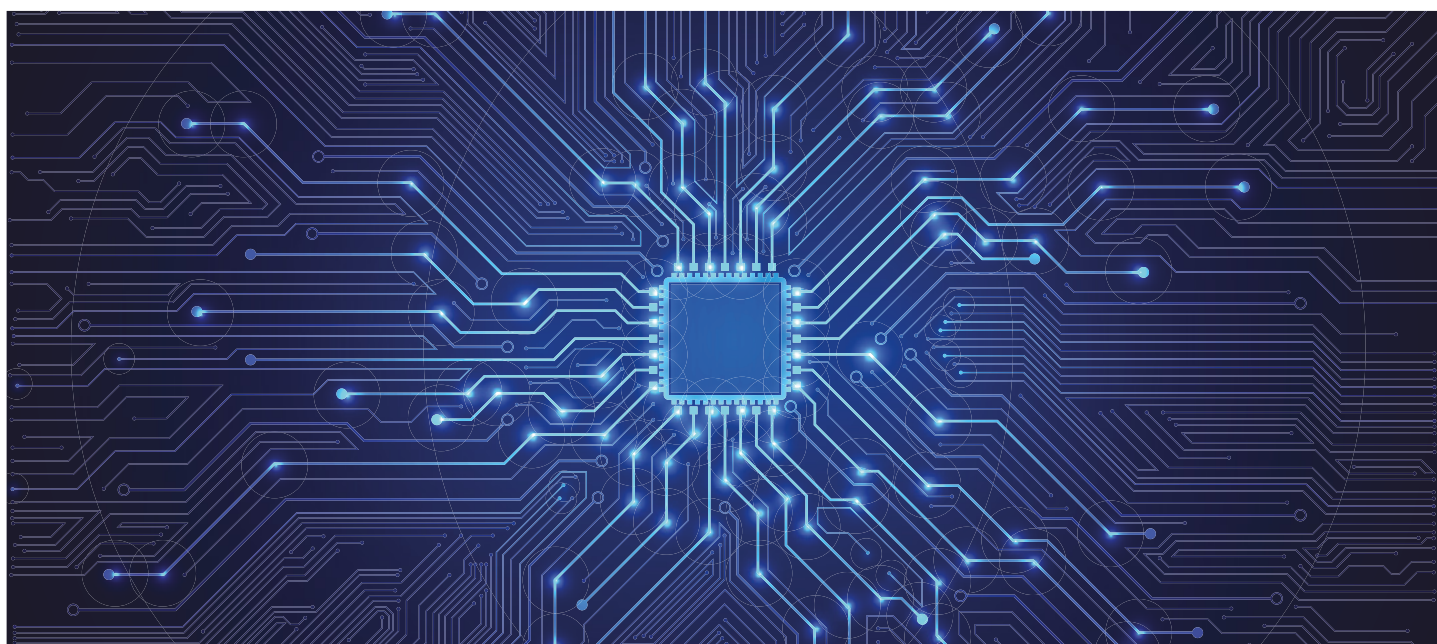
Identifying and evaluating risks

Notwithstanding these new opportunities, the risks relating to AI have been the subject of much discussion and scrutiny in the last year or two, as a result of the sudden acceleration in the availability of AI programmes using forms of “machine learning” functionality enabling the programme to teach itself and improve the reliability of its output over time. Various documents setting out draft legislation or a framework for regulation have been published by the UK Government, the EU, and by governments elsewhere in the world, and by individual regulators such as the FCA/PRA and Bank of England, as the race to successfully regulate AI gathers pace.

The resourcing challenge

The increasing adoption of AI requires businesses to plan ahead and step up their resources in order to manage adequately the introduction, preparation, use and scalability of AI to drive sustainable value for the business. This presents a greater challenge for smaller businesses that may have fewer specialists who are well-versed in AI. As a ubiquitous and disruptive technology, the alternative that is faced by professional services firms is to fall behind their competition and become side-lined as the client market gravitates towards the more extensive use of AI.

The profile-raising and headline grabbing nature of AI is driving extensive, yet polarised, attitudinal data. Whilst AI is developing at a rapid pace, embracing, and adopting digital transformation to drive value for business has been omnipresent over a number of decades due to the emergence of the internet, software solutions and myriad forms of social media. Accordingly, a firm’s decision to introduce AI in a particular field of business activity requires consideration of factors that are connected with adoption of any new technology, such as fitness for purpose, governance, cyber security, and future-proofing.



Cyber-security and Intellectual Property protection

One of the key business risks that is heightened by adoption of AI is cyber-security, in particular because AI tends to involve running programmes in relation to huge volumes of third-party input data which may be used as an entry point for a cyber-attack against a firm.

Another consideration that is more significant in the context of AI is intellectual property, whether regarding loss of control of IP belonging to the accountancy firm or its clients, or through using AI tools which infringe the IP rights of third parties by using protected materials as part of their training data.

Civil liability risks

The use of AI models in relation to the provision of services by accounting firms also presents a profile of civil claims risks that are specific to, or increased by, the use of AI. AI based on machine learning has certain characteristics that give rise to particular categories of risk, including that AI involves the collection and use of huge volumes of data, and has been developed with little or no regard for transparency of its mechanics, relying on algorithms to make predictions. Also, where there is use of third-party platforms, firms should consider ownership of outputs and the restrictions that there may be on the ability for firms to be able to use outputs in a specific way. These functions and dependencies trigger a host of risks of varying types and categories.

The principal risks are as follows:

- Risks arising from the loss of control over confidential client data (such as a claim for breach of confidence or a complaint to the Information Commissioner in connection with breaches of legislation, such as the General Data Protection Regulations (“GDPR”)), resulting from the fact that data has been inadvertently shared by using an AI platform;
- Risks arising from the use in an AI programme of data obtained by the programme supplier or developer from third parties (involving potential breach of the third party’s confidentiality, or interference with a third party’s intellectual property rights);
- Risks arising from the lack of transparency attaching to AI data inputs and the workings of AI software models (the so-called ‘black box’ problem), making it difficult to assess the reliability of output. This may give rise to a claim in negligence if inappropriate reliance is placed by the accountant on the AI output.
- Risks attaching to the limitations inherent in AI models that result in inaccurate output such as false data (known as data “hallucinations”). This is a particular difficulty associated with generative AI, and gives rise to the potential for claims in misrepresentation, negligent misstatement, and defamation.

Regulatory expectations and attendant risks

Now that the use of AI has become a matter of public discussion, involving a degree of controversy, and is becoming more extensive, it is beginning to receive more attention from regulators, and inevitably firms will become increasingly exposed to the risk of regulatory enforcement in relation to their handling of AI. Regulatory considerations might include:

- How firms justify the use of a specific machine learning tool in the deployment of an engagement (is the work suitable to be carried out by technologies such as AI or cognitive learning?);
- The ‘explainability’ of the tool itself and decisions made using it;
- The rights of individuals whose data will be processed using an AI tool;
- How the AI process is documented (and can it be reviewed by a knowledgeable individual);
- How the process is governed;
- How the platform or tool has been developed, including the use of test training data, corrections, and basis for improvement;
- The deployment of financial information bias detection tools; and
- The controls/human intervention capability to “stop it learning”.

Risk management and AI

In order to overcome the challenges presented by AI successfully, firms need to draw on their experience of handling risks for non-AI projects and avoid a mentality of abdicating responsibility to the AI software.

The UK Government’s regulatory framework contains material that will enable businesses to identify the various types of systems and procedures that they need to put in place to manage AI. Similar principles are enshrined in the EU’s draft AI Act which applies to UK businesses that provide AI models to EU clients or use AI models from which output is provided to EU clients. In time, more specific regulatory guidance for accountants and auditors may become available.

Effective governance, policies and procedures in relation to AI

The foundation for risk-averse adoption of AI lies with an effective governance system within the firm, drawing on specific relevant expertise and connecting it to those holding senior management responsibility to oversee the selection, training, testing, and implementation of AI.

The group responsible within a firm for introducing and overseeing AI should develop, disseminate and enforce internal policies and procedures to govern the use and handling of AI. This should include the development of policy relating to the safe and authorised use of AI by staff (such as the use of generative AI, like ChatGPT), in creating material for inclusion in professional reports and work products. Many high-profile businesses have for the time being banned the use of ChatGPT and similar programmes or are training staff on the risks of using ChatGPT/AI in the course of work and the potential risks and liabilities that may arise in doing so.

Due diligence and risk assessment

Accountancy firms should establish due diligence, quality assurance, and risk assessment procedures in connection with selecting and introducing new AI programmes, with clear requirements for:

- Assessing and ensuring the suitability and effectiveness of the AI programme, and the suitability of the developers/publishers with whom the firm will be contracting;
- Identifying input data sources;
- Evaluating the reliability and relevance of the AI programme;
- Evaluating the explainability of the AI model;
- Establishing the level of data security and the potential for data to be made available/accessible to third parties;
- Establishing a process for incident reporting;
- Considering the risk that input data may give rise to bias in data output (which may for example give rise to reputational and legal risks if the effect of the bias is to risk perpetuation of direct or indirect discrimination);
- Considering the potential for intellectual property being created or shared without authorisation or protection.

Preparing AI programmes for active use and monitoring their reliability

Once AI programmes have been approved for use, firms will need to ensure implementation of adequate mitigative measures against the legal risks associated with the usage of AI, including:

- Conforming data so that it is capable of being processed reliably by the AI model;
- Removing “bad” data that could distort the output and/or limit the effectiveness of the model in achieving the desired objective.
- Training of AI models using relevant data;
- Testing the output from the AI model in trials;
- Consistently monitoring the use of the AI model and testing its output for reliability from time to time;
- Training staff how to use the model as well as evaluate and interpret the output;
- Guardrails to identify and remediate machine hallucination or inaccuracies or to check outputs;
- Implementing safeguards including transitional arrangements that utilise existing systems alongside AI models to address the risk of placing undue reliance on output generated by AI.

Resourcing and documentation

The above activities call for a significant level of human involvement in setting up and monitoring the proper running of the AI model when using it in the course of the accountancy firm’s professional business. This is true not only of the central AI expertise (or external AI expertise) that will be required, but also applies to the role that engagement teams will be required to perform in ensuring that AI is used appropriately in any particular context, and that undue reliance is not placed on its output.

Similarly, those responsible for governance over the use of AI within the firm will need to develop and maintain the necessary skill sets and knowledge to perform their responsibilities. AI expertise will also need to be brought to bear in audit and assurance engagements when considering information produced by AI models.

An additional aspect of risk management relates to legal documentation, which may necessitate involving in-house counsel or external lawyers alongside internal AI experts:

- Contracts with AI developers/suppliers should be checked before being agreed. This is to assess the protection given to confidential data belonging to the firm or its clients, as well as the firm’s intellectual property. These contracts should also evaluate any rights of redress such as the reasonableness of liability limits and terms relating to allocation of responsibility for errors in output or defects in the AI model. Such evaluation should also consider the firm’s rights of access to the platform where its use and availability are critical to the firm, the ownership of outputs, rights for the firm to “audit” the AI model to ensure compliance, and security mechanisms to restrict access to the platform or prevent unauthorised access;
- Engagement terms with clients should include appropriate disclosure of the use of AI on any particular engagement, including any limits as to its reliability and explainability. Such terms should seek to include appropriate disclaimers of liability in respect of limitations in its explainability and regarding any reliance it places (whether in training or in data source) on third party data outside the control of the firm.

Legal and regulatory compliance

A further component of risk management relates to compliance with legal and regulatory requirements. This brings together many of the above aspects. The UK’s proposed Regulatory Framework for AI includes various principles relating to (among other things) governance, explainability of AI, fairness, data security, and redress. It is likely that professional regulators such as the FRC and in time the ICAEW will produce specific regulatory guidance or standards relating to the use of AI in engagements, which can be expected to reflect those principles.

Firms will need to draw on their risk management and compliance teams, and on their AI specialists, to ensure that they do not fall out of line with these requirements. Firms will also need to identify actions that may be needed in order to comply with the requirements of GDPR.

AI and insurance cover

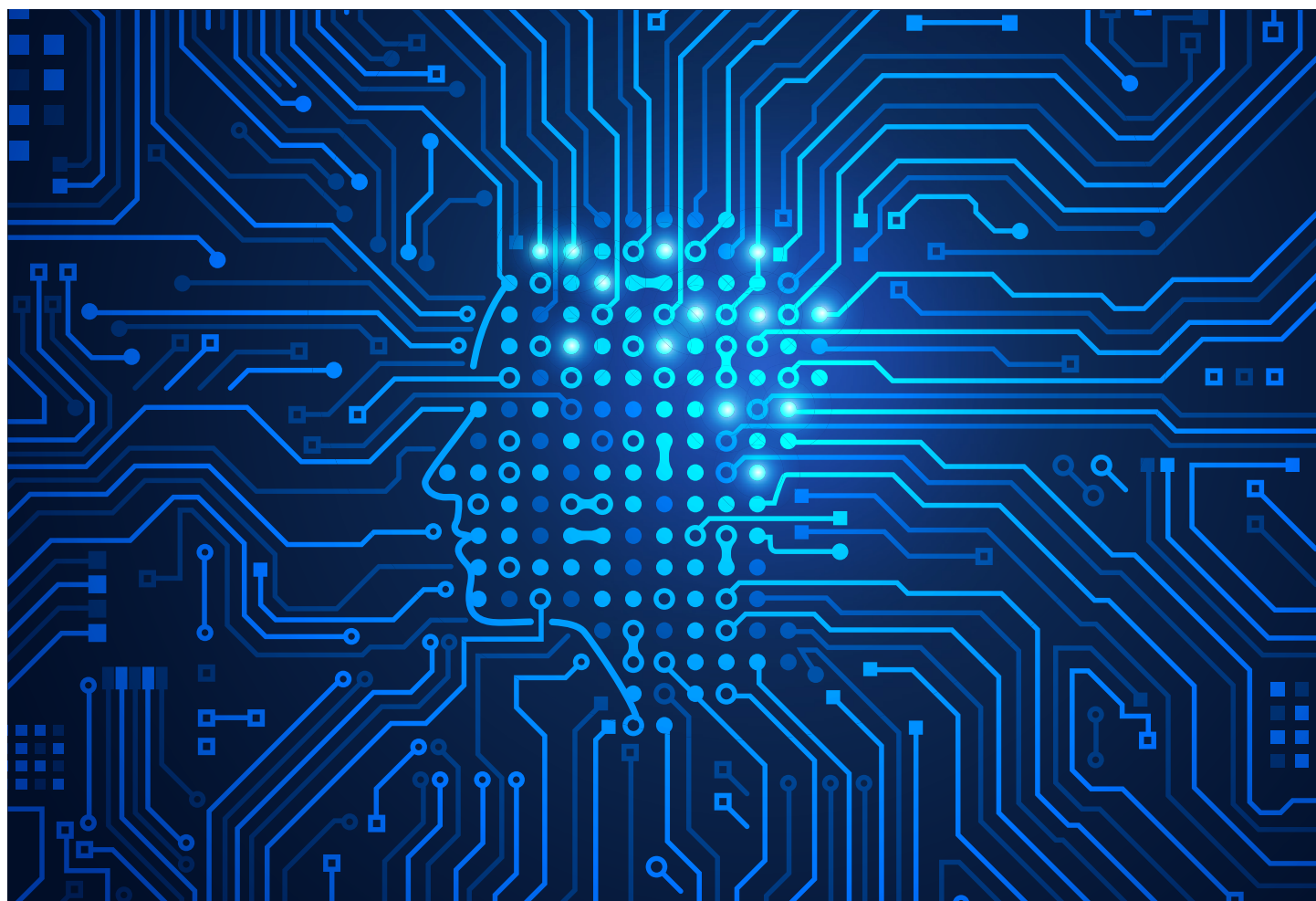
AI, in its advanced forms such as machine learning, remains a somewhat experimental development in relation to many aspects of an accountancy firm's business. Whilst AI remains very much in its early infancy, as there is no history of claims experience from which secure conclusions can be drawn, insurers are likely to take a conservative, risk selection, approach in providing cover for the use of AI, based on the scope and scale of AI applications. They may be also mindful of, or influenced by, recency bias derived from the lack of clarity for cyber-related incidents under non-cyber insurance policies, known as silent cyber.

Accountancy firms should not assume that use of AI will be treated by insurers with indifference. They should discuss with brokers whether any additional disclosure is required when firms intend to use AI. As insurers ask more questions and seek to learn more about the legal and regulatory risks, there will inevitably be greater focus on AI risk strategy, culture, risk taxonomy, monitoring and reporting, the nature and use of data and the level of AI expertise and human intervention, as part of these AI-related discussions. The unavailability of insurance cover, or limits and terms that might be applied, might be a factor for firms when considering whether to implement particular forms of AI in particular contexts.

Concluding comments

First-time adoption of machine-learning AI in a particular context will be a significant step for any firm, and a considerable investment of resource and time will be required in order to prepare the ground properly before committing to that step, and to maintain the AI once it comes into operation. It will be particularly important for firms to apply sound risk management principles, draw on appropriate expertise and keep on top of developments in a rapidly changing field.

We encourage and welcome your feedback and would value the opportunity to open a dialogue with you on any of these topics.



Clyde & Co LLP accepts no responsibility for loss occasioned to any person acting or refraining from acting as a result of material contained in this summary.

Please talk to us

The Lockton Global Professional & Financial Risks Group has focused on placing Professional Indemnity insurance for UK accountancy firms for more than 20 years. Our team offers expertise in risk identification, protection, and management, as well as analysing new or evolving risks. We value every client and use our market influence to ensure the right solution for your business.



Steve Claringbold

Strategic Consultant

E: steve.claringbold@lockton.com

T: +44 (0) 207 933 2418



Simon Mantell

Account Executive

E: simon.mantell@lockton.com

T: +44 (0) 207 933 1560



James Roberts

Partner

E: james.roberts@clydeco.com

T: +44 (0) 207 876 6550



Andrew Forsyth

Of Counsel

E: andrew.forsyth@clydeco.com

T: +44 (0) 207 876 6501



CLYDE&CO