ASTER & TRUJILLO

LEGAL . TAX . ACCOUNTANCY

ASTER & TRUJILLO

3-7 Temple Avenue, Temple Chambers, London EC4Y 0HP
Tel: + 44 (0) 20 7190 9812 Fax: + 44 (0) 20 7190 9813
info@astertrujillo.co.uk www.**astertrujillo.co.uk**

Next-step technology: opportunities, risks and compliance

Keeping up with emerging technology is a major concern for more than half of business leaders, according to recent research.

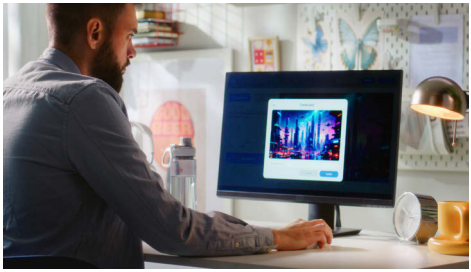
In this publication, we look at some key areas, as well as outlining risks, opportunities and tax compliance issues to be aware of.

Artificial Intelligence

The Organisation for Economic Cooperation and Development has described Artificial Intelligence (AI) as a 'transformative technology capable of tasks that typically require human-like intelligence, such as understanding language, recognising patterns and making decisions'. AI technology has been in use for some time. It powers pop-up chatbots offering help on websites, and the voice assistants, Siri and Alexa, for instance. And it's evolving rapidly.

Generative AI

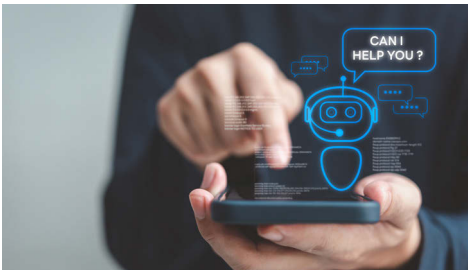
Generative AI is a revolutionary new element; and in the opinion of experts, it's as seismic a change as the development of the internet or the mobile phone. Very broadly, generative AI works using algorithms to decide the next likely thing to generate, based on training received from vast quantities of data. It's a type of 'deep learning' that generates new content - text, code, image, audio and video - in response to a prompt. OpenAI's ChatGPT fits into this space. It is a chatbot using what's called large language model technology to generate new content, such as articles, essays, even poetry and jokes, in response to a prompt in the form of a question. The government has been trialling its own AI chatbot, gov.uk Chat. This uses 700,000 pages of guidance on gov.uk to provide quick, personalised answers to questions on setting up a business.



Assessing potential and risk

So what should businesses do now? Firstly, there's a need for information. Though AI is so complex that even specialists can't fully explain it, it's important for business owners to have some idea of the technology involved, and to appreciate what generative AI can and can't do.

Generative AI can automate routine tasks, such as data entry or customer support. But it goes beyond automation; extracting information and re-presenting it in forms such as document or email trail summaries; financial reports; or budgets - and doing so with unparalleled speed. It can be used, for example, to refine job adverts; draft emails; craft content for social media marketing; or answer Excel queries.



Secondly, be aware of the risks. Generative AI is still in its infancy. Chatbots can hallucinate: that is, provide answers that sound plausible, but are wrong. As noted on gov.uk, industry-wide accuracy is improving, but no one has yet reached 100% accuracy. There is a risk of biased output where data used in AI training was incomplete or biased. This is something that could be a particular concern in recruitment, where the use of AI tools to review CVs could create inadvertent discrimination. Any use of AI will need human input to check the credibility and quality of what is produced.

Thirdly, assess what AI could do within your business, and draw up objectives. With a survey by the Federation of Small Businesses suggesting that one in five businesses had

already started to use AI, this will be a priority to retain competitive edge. In many cases, the best way to do so will be to start with small, non-critical projects. Using public AI tools will probably make sense in this trial stage, and will help inform any decision on whether to invest in private versions at a later point.

Fourthly, businesses will need to manage change and upskill staff. Businesses will need new policies to keep up with developments in AI. These must ensure that AI is used ethically, transparently, and in line with rules on data protection, data privacy and intellectual property. Internal procedures will need updating, to set out whether, for example, staff may use public AI tools in their work. Controls should be put in place so that staff don't use confidential data with such tools. Cyber security becomes even more critical. And with AI-powered services using much more energy than conventional applications, environmental impact is something else to consider.

In short, the implications of using AI are extensive and we have only been able to highlight a few of them here. Do please contact us for further discussion.

Cyber security: emerging areas of risk

Cyber crime is increasingly sophisticated, and embedding cyber security within your business is key. Once upon a time, poor grammar and spelling mistakes gave the game away, but phishing emails are now less likely to be conspicuous. Deepfake attacks, increasingly intense AI-powered hacks, and the use of files that might be bypassed by traditional monitoring are among some of the top risks.

Deep fake tactics, for example, can involve hackers using a video avatar to impersonate a key member of a business – so-called CEO fraud. The aim is to trick employees into transferring funds or providing sensitive information – and it's been described as 'terrifyingly easy'. Though the end results might not be 100% convincing, 'they only have to be good enough to fool someone for a few critical moments – enough to click a link, approve a transfer or obtain your login details', as one expert puts it.

Two-step phishing sees criminals taking control of a legitimate email account and using it to send emails with links to sites like SharePoint or Google Forms. The recipient clicks the link to input login details, or download a file that has been compromised. Frequently using Microsoft Visio.vsdx format files, which are not always scanned by security software, and featuring the command 'hold down the Ctrl key and click', attacks like these can, in some cases, side-step automated virus and malware scanning.

Cyber security action points

- Train staff. They need to know what the latest risks are and what to do about them; how to spot obvious signs of phishing; and how to report concerns.
- Resist pressure. Cyber crime, especially deepfake crime, is often about pushing someone into action under time pressure. Encourage staff to ask questions; to confirm that the person on the other end is who they say they are, for example by phoning them back or making contact by another channel.
- Protect identity. Reduce the risk of deepfakes and targeted phishing by caution over the type and amount of information shared

online. Help staff understand how sharing their personal information can affect them and your business. Work with them to minimise online security risks.

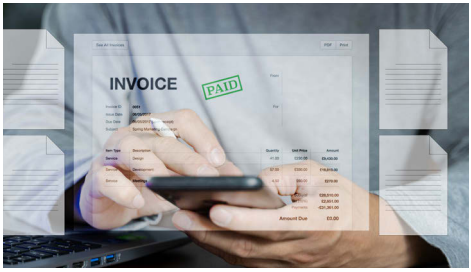
- Make sure basic, but critical controls are in place. They remain a key line of defence. Two-factor authentication should be enabled for important accounts such as email, or logging into platforms. Access controls for users should be limited so they only access information/systems required for their job. Administrator accounts should not be used to browse the web or check email.
- Government-provided resources to help businesses of any size improve their cyber resilience can be accessed via gov.uk and the National Cyber Security Centre. Most are free, and need no expertise to implement. They include, for example, Exercise in a Box, designed to help an organisation test and practise how to respond to a cyber attack.

Digital tax compliance

As the government looks to close the tax gap and drive up compliance, there is a corresponding push for businesses to interact digitally with HMRC.

Electronic invoicing: what it is

Electronic invoicing (e-invoicing) involves the exchange of an electronic invoice document between a supplier and customer in a structured data format: a machine-readable format that's automatically imported into the customer's system, without the need for manual entry.



The advantages from the business point of view are increased efficiency; reduced errors in invoice processing; faster processing time and potential for improved cash flow. It can also enhance security, as invoices cannot be manually tampered with to alter bank details.

Why you need to know

Globally, use of e-invoicing is increasing. It is in use in more than 80 countries already. In the UK, it is already mandatory for payments to and from public bodies like the NHS.

E-invoicing has a particular role in the reduction of tax fraud. It can be used alongside mandatory digital reporting, meaning businesses are required to submit data to the tax authorities to deadlines very much closer to real time. Some European countries already use combinations of live reporting and e-invoicing, and others are following suit. Developments like these will fundamentally change tax compliance for businesses.

EU VAT

E-invoicing plays a key part in the EU's VAT in the Digital Age (ViDA) proposals, a package of measures intended to reduce VAT fraud by up to 11 billion euros a year. Starting in 2030, they introduce a new real-time digital reporting system for cross-border trade, based on e-invoicing.

Businesses will issue e-invoices for cross-border transactions, and automatically submit data to their tax administration at the same time. National tax administrations will then share data through a new IT system which will analyse potentially suspicious activities.

Changing position in UK

The government has announced that it intends to consult on e-invoicing shortly, with the aim of establishing standards and increasing take-up.

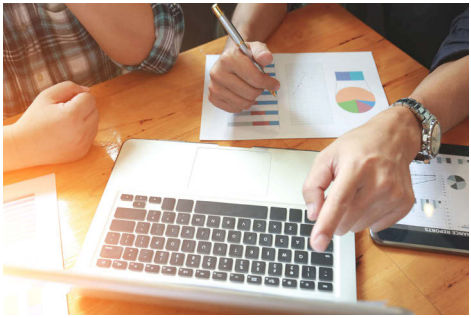
Introducing e-invoicing into a business is a significant change, and preparation is key. Though any move towards mandation in the UK may yet be some way off, businesses should be aware of why e-invoicing is on the government's agenda, and that a push in this direction is possible. We should be happy to discuss the potential of e-invoicing for your business at this stage, and advise on how to proceed.

Making Tax Digital for Income Tax

The Making Tax Digital (MTD) initiative is expected to reduce the tax gap attributable to error and carelessness, and the Autumn Budget 2024 set out the timetable for Income Tax (MTD IT). MTD is also expected to apply to Corporation Tax in due course, but not before April 2026 at the earliest.

Requirements and timescale

MTD is a major change. It's all about how accounting records are kept, and how businesses interact with HMRC. Specific accounting records must be kept in digital format, using MTD compatible software.



Perhaps the most significant change, however, is how often businesses interact with HMRC. MTD IT requires a filing every quarter, with an update summarising income and expenditure, sent to HMRC from the digital records kept by the business. This has to be an uninterrupted digital process with no manual input. Separate quarterly updates are required for each business: a self-employed person who also has a UK property business, for example, will provide eight quarterly updates each year. At the end of the year, there is then a process to finalise the tax position and make any tax and accounting adjustments necessary. There is no change to the timing of tax payments.

MTD IT will be mandatory for the self-employed and landlords with annual turnover over a particular level. Note that partnerships are currently outside the scope of MTD IT. MTD IT applies:

- from 6 April 2026 where qualifying income is more than £50,000
- from 6 April 2027 where qualifying income is more than £30,000
- at a date as yet unspecified, but expected to be before the end of the current parliament, where qualifying income is more than £20,000.

Appropriate digital record keeping will be needed in advance of sign up to MTD. As well as advising on how best to prepare your business, we can also advise whether change to record keeping will be necessary.

We can help

The pace of digital change is unprecedented. Please do contact us to discuss in more detail any of the areas described here.