

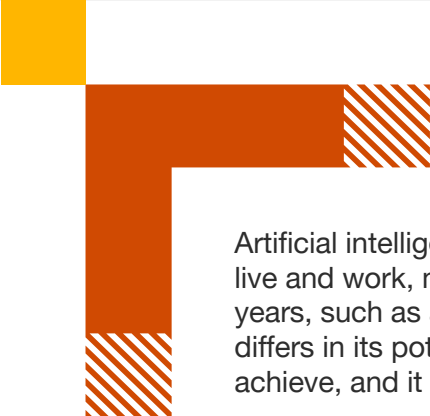


How to deploy AI at scale:

A PwC and Microsoft playbook that explores the critical role of cloud and cybersecurity



Introduction



Artificial intelligence (AI) stands poised to bring transformative changes to the way we live and work, much like the significant technological breakthroughs of the past 10,000 years, such as agriculture, the printing press, electricity, and the internet. However, AI differs in its potential to fundamentally enhance what individuals and businesses can achieve, and it promises to do so with unprecedented speed and impact

AI and Generative AI (GenAI) represent a truly transformational wave of technology that will reshape our world. AI will influence and change all areas of business and what we can accomplish in our working lives—for the better. AI is already starting to accelerate new innovations and automate processes in ways we would have thought unimaginable only a few years ago. It is improving our productivity and helping us reimagine the customer experience—and we are only at the very beginning of understanding what it can deliver.

There are multiple facets to what AI is and can do: machine learning, a subset of AI, enables algorithms to learn from data. Deep learning, another subset, also identifies patterns. GenAI, the most recent evolution, has garnered much interest of late because of its ability to generate novel content, such as text and images, which it is able to fulfil by using models trained on large datasets.

There are two underlying requirements that are essential for AI use within organisations: the adoption and use of cloud technology and security. Cloud infrastructure is the engine that helps to fully exploit AI's capabilities. This is needed to manage and grow with the vast sums of data that AI creates. But in consequence, it introduces new cybersecurity challenges. Strong cybersecurity provides fundamental protections for company data—including for AI models—and safeguards a business's intellectual property. Combining cloud with cybersecurity is what provides the essential building blocks that will truly help organisations to realise the full potential of AI.

This paper seeks to explain and outline all the necessary steps and considerations that organisations need to take to make the most of this exciting technology, one that will revolutionise the entire world.

1. Understand AI goals and ambitions by determining strategy

Momentum around AI has been building slowly and surely over the past decade, with a more recent surge in interest following the launch of GenAI tools. The tools' inherent ease of use has placed the technology in the reach of a much wider audience, and at the same time, highlighted the possibility for all businesses to transform operations.

We are now at the GenAI inflection point: businesses are moving beyond individual experimentation and are rolling out the technology in a concerted attempt to derive measurable gains across the organisation. Organisations are all at different stages with AI. Some are taking their first steps, some are at the early stages of exploring its strategic implications, while others are already into making development decisions.

Many of us have used AI without being aware of its existence: simple grammar and spelling checks and machine translations are both AI driven. We are now witnessing a significant leap in what AI and the latest generation of AI tools can do. We are seeing products such as the Microsoft Azure OpenAI Service, which can be customised to cater for specific use cases, but also off-the shelf GenAI tools, such as Microsoft Copilot¹, which are proving to be truly transformative for end users. Microsoft Copilot, for example, can help streamline a wide range of daily business activities, helping to cut down the production time needed for key deliverables from days to perhaps a single hour.

Business leaders are more than aware of GenAI's abilities and of its potential. Fully 70% of CEOs believe that GenAI will transform the way they create, deliver and capture value over the next three years, according to PwC's 27th Annual Global CEO Survey². But before businesses rush to start integrating GenAI into day-to-day operations, several factors need to be considered. The most important start point for every business leader is in understanding the organisation's AI maturity. This is crucial in determining readiness to adopt and scale AI use for any new initiative.

Organisations should then define all the outcomes they wish to achieve with GenAI and set out clear

goals to get there, aligning them with business strategy. Developing a clear roadmap can help businesses navigate through the transformative process of AI adoption. For those just starting, the focus should be on building foundational knowledge and exploring pilot AI projects that align with key business objectives. Mid-level adopters should work on scaling these initiatives by refining their AI infrastructure and aligning AI strategies with broader business goals. Advanced users can focus on optimisation, leveraging AI to innovate and gain a competitive edge. A clear understanding of the outcomes that the organisation wants to achieve, and its level of maturity is crucial. By providing organisations with clear steps to follow, a solid roadmap can ensure smoother transitions and better integration of AI technologies into operations.

Responsible AI practices help to design trust in from the start and ensure that the impact of the technology is broadly positive. This requires developing a code of conduct that supports the transparent, accountable and fair use of AI. We will cover this topic in more depth later in this paper.

Once AI goals have been aligned with business strategy, you need to achieve a thorough understanding of your organisation's capabilities, assess your IT infrastructure and build in trust measures. Then the next step is to ensure the use of generative AI can be deployed effectively across the organisation. The key: a robust and supportive cloud architecture.



¹ PwC and Microsoft Copilot for Microsoft 365 | ² PwC's 27th Annual Global CEO Survey

2. Assess your cloud infrastructure

Adopt an effective cloud strategy

Cloud is the fuel of AI. Cloud offers scalability to harness vast computing resources and helps businesses be more agile and flexible, qualities which are essential to the effectiveness of all AI roll outs. Organisations should assess where they are on their cloud journey and consider what steps they need to take to support and enable their use of AI.

PwC's recent Cloud and AI Business survey³ identified a small number (12%) of businesses—named “Top Performers”—that have already begun to reap the rewards of their investment in AI and the cloud. The report notes that 72% of these Top Performers are far more likely to have achieved “all-in cloud adoption” when it comes to modernising data, versus 33% of other companies. By moving their data to the cloud and making it more easily ingestible by large language models (LLMs), Top Performers are more readily able to unlock new value from their data as they integrate new AI capabilities.

The use of cloud also requires a strategy that suits an organisation's individual needs. There are several options and each company must decide what works best for them. The public cloud is perhaps the best known. A simple internet connection allows any business to run all or parts of their IT infrastructure in the cloud, rent storage and servers and use a variety of services. Public cloud offers unlimited access to IT resources giving businesses a flexible IT usage model, one that is ideal for training LLMs.

Hybrid cloud combines public cloud services with existing on-premises data centres and private cloud infrastructures. This enables the seamless movement of workloads between the two environments without compromises to performance.

“There are many reasons why hybrid cloud makes good sense for businesses getting started with AI. It offers the best of both worlds by protecting existing investment but adding cloud scalability and flexibility. We've also pioneered the ability to manage both on-premises and cloud assets with cloud tools, which makes hybrid more attractive and simpler to adopt for many organisations.”

Joao Couto, EMEA VP and COO Cloud Commercial Solutions, Microsoft

The set-up is also useful to support the regulatory compliance and data sovereignty needs of highly regulated industries where sensitive data must be processed within a country's borders.

A multi-cloud approach refers to the simultaneous use of multiple cloud service providers (CSPs). As Couto points out, when organisations opt for this model, it is mostly because they perceive a risk of being reliant on one vendor: “Some customers want the option of using multiple cloud providers. What we find is that they eventually choose one of two models: either the use of a sole provider or a main cloud provider with another one as back-up.”

72%
of “Top Performers”

have achieved “all-in cloud adoption” when it comes to modernising data, versus 33% of other companies.

³ PwC US report: [2024 Cloud and AI Business Survey](#)

Use cloud to provide the necessary infrastructure for AI

Making the wheels of AI turn productively will require a robust cloud architecture. Building and maintaining a wholly owned IT infrastructure is expensive and can invariably place limits on a company's ability to scale.

“AI systems involve lots of data and that data needs to be accessible. The cloud is a scalable resource and it's reliable—you need that if you are serious about bringing AI into your business.”

Sebastian Paas, Partner, EMEA Cloud Leader, PwC Germany.

Cloud service providers, such as Microsoft Azure⁴, offer scalable resources that help control and minimise the cost of AI development and deployment. Cloud resources also facilitate collaboration across a company and among individual teams helping users to seamlessly share real-time insights and resources.

PwC's 2024 Cloud Business and AI Survey⁵ showed that while most companies rather their CSPs favourably, there are opportunities to get even more value out of cloud by evolving their relationships. At the top of the list: monitoring and managing security and compliance, where more than half of companies are looking to change their relationships with their CSPs. More than two-fifths of companies are also evaluating the types of services provided and looking to collaborate on future-state capabilities.

Streamline access to data while making AI and machine learning more accessible

Cloud's operational agility is essential in supporting AI systems and is also providing access to specialised tools and services that are designed for developing, deploying and enhancing GenAI applications. One notable example is the Microsoft Azure OpenAI Service, which delivers access to powerful language models, such as GPT-4 and DALL-E. Furthermore, Microsoft also provides data management tools that help clean, organise and prepare unstructured and structured data, to increase its usability for those applications.

Address data privacy issues

Whether a business is at the starting gate or has already begun to use AI, it is essential to assess the organisation's processes and policies and adapt these to govern the use of the technology. Cloud helps classify data access, for example, providing permissions for employees to access data at the right time, when they need it, and only if they need it. With stringent access controls, organisations can more easily meet data protection regulation compliance and overcome data privacy issues.

Security is essential to AI because of the huge data volumes involved. A strong security posture helps ensure that all data used within AI systems are not misused. Cybersecurity is foundational to successful AI implementation.



⁴ PwC and Microsoft generative AI | ⁵ PwC US report: 2024 Cloud and AI Business Survey

3. Secure your data to power AI solutions

Like any technology system, artificial intelligence systems need to be protected from potential threats and vulnerabilities. AI systems handle huge amounts of data that include both personal and proprietary information, making them appealing cyberattack targets.

When designing a new AI system, organisations should take care to build in strong security measures from the start to counter the rising number of attacks, which are continually growing in their levels of sophistication. Unsurprisingly, organisations believe cyber risk to be only second in importance for businesses after inflation, according to PwC's 2023 Global Risk Survey⁶, with many respondents feeling they are "highly or extremely exposed" to them. The same survey notes that digital and technology risks are also of high concern.

CSPs offer the most highly advanced security controls with continuous monitoring and encryption. A 'zero trust' security architecture adds additional protection with superior access controls, ensuring that every access request is verified regardless of its origin. This helps to maintain AI system integrity and data confidentiality. These measures also work to prevent unauthorised access and malicious actors from compromising the AI system, so it remains available to users.

LLMs are complex pieces of software, which are open to multiple security risks that threaten their integrity. The way LLM data is trained can lead to biased or erroneous outputs that raise either legal and ethical concerns or erode trust in AI systems, so it's vital to include human oversight throughout the training process and beyond. Continuous model training and bias mitigation measures help identify and eliminate problematic output.

Fine tuning models through continued validation of inputs and outputs, along with anomaly detection processes, help to achieve fair and reliable results, too.

"Organisations need to ensure they have policies and processes in place to mitigate high levels of risk in their AI systems, such as anything that is harmful to an individual. Not only do companies need to implement strong cybersecurity, but they also need to ensure AI outputs are monitored and managed."

Neil Redmond, Director, Cybersecurity and Privacy, Competency Lead, PwC Ireland

A secure cloud platform, such as Microsoft Azure, helps protect AI data from the additional risk of cloud vulnerabilities because of the greater visibility it offers in security monitoring. This also helps minimise data breaches and unintentional user input. Implementing robust governance structures supports data integrity further by ensuring data is validated and monitored, along with processes that can quickly detect and correct any additional errors in the AI data.

Authorised GenAI business tools also reinforce security, avoiding what is termed 'shadow GenAI'. In the absence of a company-authorized chatbot tool and associated policy, employees are likely to use unauthorised tools, which increases the risk of data breaches. When companies block GenAI tools, they can also inadvertently push staff to transfer sensitive data to less-secure personal devices. Having an approved tool used in the cloud environment and blocking access to browser-based or consumer GenAI tools helps to reduce the risk of shadow GenAI practices.

Building trust in AI system accuracy is vital in protecting organisational reputation and credibility. Customers feel more assured and users more confident in AI outputs when robust security measures and governance frameworks⁷ are in place.

⁶ PwC Global Risk Survey 2023 | ⁷ PwC report: [GenAI is here to stay: What it means for cyber security](#)

4. Streamline cyber defences

Security teams, under constant pressure from attacks and hackers, can strengthen and streamline their cybersecurity using GenAI⁸. The three principal ways organisations are prioritising the use of GenAI for cyber defences, according to PwC's latest Global Digital Trust Insights report⁹, are:

1. Threat detection and response
2. Threat intelligence
3. Malware/phishing detection

Automating security using GenAI protects AI systems because of the ability to constantly monitor for vulnerabilities in networks, applications, platforms, systems and cloud.

A good example of automation is in the use of Microsoft Copilot for Security for continuous monitoring of network traffic and threat identification in real time. Not only does this mean that threats can be mitigated expeditiously, but also the burden of repetitive and time-consuming tasks is greatly reduced.

This not only increases productivity, but it can also help companies retain skilled employees who appreciate a more varied and challenging workload.

While Security Copilot significantly boosts cybersecurity defences, organisations can improve its use further with expert help.

“AI can be extremely helpful in maintaining security costs, while increasing cybersecurity protections and managing the constantly changing security threat landscape. GenAI tools help organisations execute routine monitoring more efficiently, freeing up analyst time to focus on more complex tasks.”

Aleksei Resetko, Partner, Cybersecurity & Privacy, PwC Germany

Because PwC works closely with Microsoft, its security experts are well placed to tailor the tools to meet specific organisational needs. PwC's global reach provides an additional layer of understanding in addressing complex security challenges across different regions and sectors.

GenAI can also be employed to review code for security flaws or for penetration testing to identify IT system vulnerabilities. In addition to making these processes faster, GenAI can also provide much more precise analyses and support lower-level work, such as recognising threat patterns, drafting incident reports and general management reporting. While GenAI tools won't replace human analysts, the tech can significantly boost efficiency for security teams, enabling them to more easily monitor, report and respond rapidly to incidents.

⁸ PwC report: [GenAI is here to stay: What it means for cyber security](#) | ⁹ PwC 2025 Global Digital Trust Insights: [Bridging the gaps to cyber resilience: The C-suite playbook](#)

5. Keep up with changing regulatory environments

Regulatory compliance is an important consideration, as regulators are responding to the rapid development of GenAI and the growing use of other forms of AI and organisations must comply with an increasing number of regulatory requirements. While CEOs have a higher level of confidence in the ability of their organisation to comply with regulations, CISOs, at the front line of cybersecurity are less optimistic. For example, while 67% of CEOs in a recent survey reported a high level of confidence in their organisation's ability to be in compliance with AI regulations, just 54% of CISO/CSOs were equally confident¹⁰. The recent enactment of the EU AI Act¹¹ in Europe—which came into force in August 2024—is the first legislation to govern AI use. It is aimed at ensuring the safe and ethical development and deployment of AI within the European Union.

involved for all AI-driven activity. Under the Act, AI systems that pose an unacceptable risk to the safety, livelihood or rights of individuals, or that are seen to manipulate the behaviour of humans or exploit their vulnerabilities are not permissible.

GenAI can be employed to achieve compliance with the Act. For example, PwC has developed its own AI-based processes to test and validate use cases against the EU legislation. This helps to determine what is acceptable, what is prohibited under the Act, and how a particular use case aligns with an organisation's responsibilities and compliance obligations. AI can also help address other types of regulatory compliance, for example by using GenAI to help achieve compliance on data protection rules or other types of legislation.

“The Act represents a vital first step in creating safe digital markets. It is expected to be the first of many and similar legislations are already in development in other global regions.”

Mona de Boer, Partner, Data and Artificial Intelligence, PwC Netherlands

The EU Act will require developers of GenAI foundation models to be transparent about the data they use for model training and demonstrate how models are developed to highlight the levels of risk

67%
of CEOs

reported a high level of confidence in their organisation's ability to be in compliance with AI regulations

10 PwC 2025 Global Digital Trust Insights: [Bridging the gaps to cyber resilience: The C-suite playbook](#) | 11 European Parliament: [EU AI Act](#)

6. Operationalise responsible AI practices

AI systems need to be implemented responsibly to ensure their lawful, ethical and robust use. PwC's Responsible AI methodology¹² helps support the development of robust governance frameworks to ensure AI use is transparent, fair and accountable. This helps to manage AI risks effectively through the institution of comprehensive policies and procedures, meaning organisations can overcome potential ethical violations and mitigate legal risks. To operationalise responsible AI, businesses should implement governance frameworks that monitor AI's use in real time, ensuring continuous oversight and immediate response to any issues that may arise. Conducting regular audits to prevent biases or unintended consequences should also be an integral part of the process. "When approaching AI for the first time, risk is often a key client concern," adds Mona de Boer. "It's essential to show how a high-level responsible AI strategy translates to an operational procedure level so they can see how risks are managed."

Responsible AI deployment also means aligning AI investment with clearly defined ethical standards that cover items such as privacy and bias prevention, to maintain stakeholder trust. With GenAI and

AI still nascent and growing in its use in organisations, trust is critical to engender acceptance of AI use and the overall success of AI projects.

"There are still challenges in getting people to use available AI tools in organisations. 'Employees' tolerance levels will diminish if AI tools don't work or are perceived to be biased. We have to acknowledge that especially in regulated industries such as financial services, accuracy is key and it's absolutely critical to ensure that client data is well-protected."

Prafull Sharma, Partner, Technology and Data Leader, PwC Switzerland

While responsible AI practices provide the backbone for GenAI use, it is critical to design trust in from the outset, not only for AI applications in use, but also for supporting infrastructure such as with the cloud platform.

¹² PwC: [The responsible AI framework](#)

7. Build strategic partnerships

For organisations wanting to successfully develop secure AI solutions, it is imperative to bring in a strong technology partner with the right capabilities, industry knowledge and functional expertise. It is equally essential to tap into proven industry expertise and knowledge to overcome barriers to implementation. This helps to smooth the journey to AI and jump-start its adoption.

PwC has taken a 360-degree approach to AI. First, we embarked on our own AI journey by adopting and using GenAI across the entire PwC organisation. This is helping us thoroughly test and refine the technology and ensure that any GenAI offering could deliver the most client value. Our significant investment in deploying these solutions internally, for example through our strategic partnership with Microsoft, is also helping us to deliver more tailored AI solutions.

“Our partnership with Microsoft enables pilot projects that help us to demonstrate the impact and potential of AI. Because we can rely on a full range of AI, GenAI, machine learning and deep learning solutions from Microsoft, we believe we can quickly help our clients gain that all-important first mover advantage.”

Mauro Xavier, Partner, EMEA Microsoft Alliance Leader, PwC Spain

PwC now has one of the largest implementations of Azure OpenAI in the world, and our AI Factory¹³ operating model supports the rapid scaling of models for use in other areas of a client’s business. A good illustration of this is an automated invoice processing solution we developed using a Microsoft GenAI model for a global manufacturing client. This solution can automatically approve, deny or send invoices for human review and greatly reduces tedious and repetitive work. The AI Factory model is helping to scale the model for document review and analysis across the entire finance function. “PwC is a pioneer in our entire partner ecosystem and is leading by example,” adds Joao Couto. “Because PwC adopted Microsoft GenAI tools across its business, it can quickly and reliably demonstrate the business impact to customers based on its own experiences. It’s a unique position to be in.”

Microsoft is a leader in secure generative AI technology with more than 60,000¹⁴ customers using Azure AI today. And this sophisticated technology is backed by the stringent security tools and controls of the Azure Cloud Platform. By tapping into the PwC and Microsoft relationship, companies can use AI to drive growth. The Microsoft OpenAI Service integrates several powerful foundation models into its products. It also offers an Application Programming Interface (API) service for developers to integrate the models it uses into their own applications.

13 Why you need an AI factory: A CIO’s guide to generative AI | 14 Press Release Webcast - FY 2024 Q4



8. Empower and upskill your people on AI

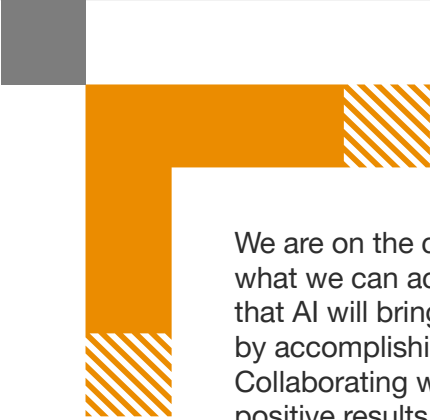
As AI continues to evolve, its impact on the workforce will be increasingly far-reaching. Using AI has the potential to help the workforce be far more productive. PwC's 2024 AI Jobs Barometer notes an almost five-fold increase in labour productivity in business sectors exposed to AI¹⁵.

To achieve this impressive level of impact, organisations need to proactively prepare their employees for the AI revolution by providing training opportunities and a safe space for employees to experiment with the technology.

Both will contribute significantly to gaining more confidence and adopting AI in the organisation. If this succeeds, it can both increase employee productivity and help employers retain talent within the company. PwC's 2024 AI Jobs Barometer shows that these capabilities are already highly valued; employers in the countries surveyed are willing to pay a 14% wage premium for people skilled in the technology¹⁶. PwC will explore this topic in greater depth in one of a series of forthcoming AI whitepapers.

15, 16 PwC's 2024 AI Jobs Barometer

Closing: monitor and adapt to new business issues



We are on the cusp of great change. AI and GenAI are showing how we can transform what we can achieve. And we are only at the very beginning of the seismic effect that AI will bring to the efficiency of businesses and their ability to compete and grow by accomplishing goals much faster¹⁷. Starting the AI journey correctly is crucial. Collaborating with experienced business and technology partners yields better, more positive results and motivates organisations to keep progressing.

A strong cloud partner is of equal importance. As we have stated: for AI projects to be successful, they need the scalability of a robust cloud infrastructure. This removes the brakes that traditional wholly-owned IT infrastructures can place on development and enables AI applications to be deployed rapidly.

Those organisations that don't adopt AI now may find themselves pushed out of their markets very quickly. And once the technology has been adopted, organisations should keep an eye on the future. The possibilities of AI are constantly evolving and growing. To maintain the competitive edge that AI and GenAI can deliver, it is essential for every business to focus on continually improving its AI capabilities and keep pace with industry trends.

We believe that AI has the potential to help organisations fuel innovation, make great advances in productivity and reinvent how they operate. A new dawn of possibilities is emerging—one that helps businesses solve their most important challenges and build the trust they need to achieve a better tomorrow.

¹⁷ PwC The Leadership Agenda: [Gen AI is a tool for growth, not just efficiency](#)

Contacts



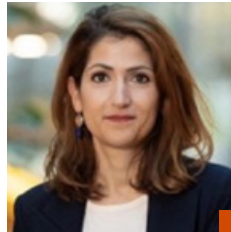
Joao Couto

**EMEA VP & COO
Cloud Commercial
Solutions**
Microsoft



Mauro Xavier

**Partner,
EMEA Microsoft
Alliance Leader**
PwC Spain



Mona de Boer

**Partner, Data
& Artificial
Intelligence**
PwC Netherlands



Sebastian Paas

**Partner,
EMEA Cloud
Transformation
Leader**
PwC Germany



Aleksei Resetko

**Partner,
Cybersecurity
& Privacy**
PwC Germany



Prafull Sharma

**Partner,
Technology &
Data Leader**
PwC Switzerland



Neil Redmond

**Director,
Cybersecurity
and Privacy,
Competency Lead**
PwC Ireland



© 2024 PwC. All rights reserved. Not for further distribution without the permission of PwC. ‘PwC’ refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.