Chinese Mainland and Hong Kong

pwc

A playbook for executives — beginning with governance

Managing the risks and opportunities of generative AI

October 2023

Trusted AI
Accelerate responsibly.

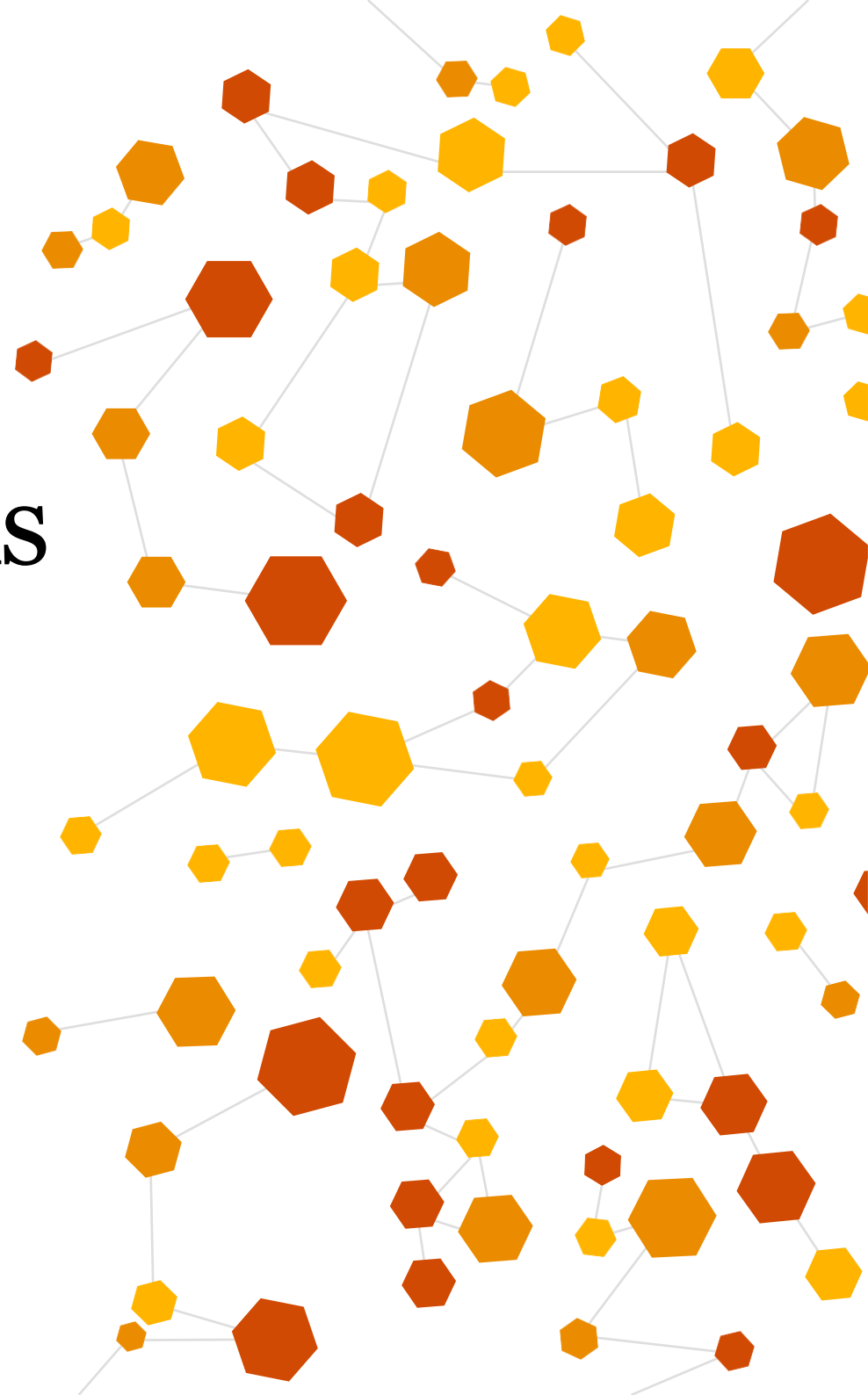


Table of contents

Introduction 2

What's at stake for business? 4

What generative AI means for your business 5

How to identify your Gen-AI Use Cases 6

The new and amplified risks to manage 8

What board members and directors can do 10

What the C-suite can do 11

Bottom line 13

How PwC Risk Assurance can help 14

Contact us to learn more 15

Introduction

Something truly revolutionary happened in November 2022. Suddenly, anyone with an internet connection, armed only with the ability to hold a conversation in a chat app, could wield the transformative power of artificial intelligence (AI).

Within a single week, more than a million users, with ChatGPT's help, produced short-form articles, wrote computer code, made art and summarised long sources into pieces perhaps better and more concise than the originals.

Meanwhile, malicious threat actors test-drove generative AI (Gen-AI) to write malware, more believable phishing emails and more convincing fake identities, rapidly and for widespread dissemination – potential harbingers of large-scale fraud, privacy violations, disinformation and cyber attacks.

Mere months after the debut of ChatGPT, generative AI continues to become ever more deeply intertwined into our lives and businesses. We've seen the fastest ramp-up in active consumer users ever. We've seen a leap in capabilities from OpenAI's GPT3 to GPT4 – achievements recorded in coding and mid-level professional writing. In quick succession, tech companies have launched/re-launched competing products; start-ups have released models for bespoke applications; and companies, including PwC, have announced massive investments to create their own "CompanyGPT" for internal use and new service offerings.

But generative AI comes with a warning label. "AI systems with human-competitive intelligence can pose profound risks to society and humanity," concerned citizens, including experts, caution. Even top providers of this technology acknowledge these risks.

Managing them is key to success. If your company wants to launch successful generative AI initiatives and gain a competitive edge, you will need to assess the risks the technology might pose enterprise-wide. For that, you will need a risk management framework that also allows you to embrace opportunity.

A risk-based approach to generative AI will start you on the right digital foot with regulators, consumers and other stakeholders. Earning trust as you deploy generative AI will position you to take full advantage, quickly, of the benefits this game-changing technology offers.

Are companies at risk of trading off trust for speed?

46% China vs 68% HK

respondents are investing in new and emerging technologies, including AI. (Source: PwC, 2023)

78%

Chinese respondents feel that products and services using AI have more benefits than drawbacks (Source: IPSOS, 2022)

Only 48%

employees feel that the increased use of artificial intelligence will make their career better (Source: IPSOS, 2022)

What's at stake for business?

Generative AI, a powerful subset of Artificial Intelligence (AI), is having a truly transformative impact on business. It can automate and enhance aspects of nearly all business operations, including customer service, software development and data analytics.

It might improve how you engage with your customers by personalising interactions with them. It could automate high-volume tasks, such as processing insurance claims and communications or performing certain software development tasks.

It may make it easier for your teams to understand unstructured data including contracts, invoices, customer feedback, policies, insurance adjuster notes, performance reviews, medical records and more.

Employee productivity could soar. By OpenAI's estimate, approximately 8 of every 10* workers could use generative AI to automate at least 10% of their work tasks, and this is just the beginning. By automating routine tasks, generative AI tools could free employees to work creatively, innovate and gain a fuller understanding of complex topics and tasks for more advanced critical thinking.

As the demand for this technology continues to grow, so do its capabilities. In four months alone, AI language systems advanced significantly in sophistication and use, and they aren't likely to stop anytime soon.

The key to sustainably riding this growth will be to enlist your risk professionals from the earliest stages. Doing so can help you build confidence in your generative AI projects.

Your risk managers will have to manage new and amplified risks as well as a slew of business, legal and regulatory challenges. One after another, the White House, US Congress, Federal Trade Commission, Cyberspace Administration of China and the European Union (EU) have moved to regulate generative AI. Meanwhile, several nations (Italy, Canada, Spain, France, Germany) started investigations in response to complaints or concerns about generative AI's collection, use and disclosure of personal information without consent, in violation of data protection laws.

Targeting a broader scope of generative AI technologies, Cyberspace Administration of China (CAC), the National Development and Reform Commission (NDRC), the Ministry of Education (MOE), the Ministry of Science and Technology (MST), the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security (MPS), and the National Radio and Television Administration (NRTA) jointly published the Generative AI Regulation on 10 July 2023, which went into effect on 15 August 2023. The CAC further published a Global AI Governance initiative on 18 October 2023.

President Xi has also stated that "It is crucial to priorities the development of general artificial intelligence, establish an innovative ecosystem, and focus on risk prevention" during a meeting of the Political Bureau of the Central Committee of the Communist Party of China.

*Based on a US study

What generative AI means for your business

Here are key focus areas to consider as your company begins harnessing Gen-AI.

Functional transformation: Reimagining operations.

The “sweet spot” of deploying generative AI for achieving quick return on investment is evident: Deploy it to automate and improve various operational aspects such as marketing, finance, supply chain, and tax compliance. By leveraging Gen-AI, you can maximise the utilisation of your existing resources, enhance decision-making, and elevate both customer and employee experiences. Gen-AI can streamline the organisation of data and document sets, simplifying human research efforts. It can also generate initial versions of financial, risk, and compliance reports, craft personalised customer service responses, and identify irregularities in reports composed by humans. However, to ensure reliable outcomes, it is crucial to maintain robust oversight grounded in a responsible AI framework.

Responsible AI: Building trust and managing risk.

For Gen-AI to truly revolutionise your business, trustworthiness is paramount. This requires the adoption of responsible AI, a methodology specifically crafted to ensure the trustworthy and ethical application of AI. Through the incorporation of technologies, processes, and skills, responsible AI tackles the various risks associated with generative AI, such as cyber threats, privacy concerns, legal implications, performance issues, bias, and intellectual property risks. To implement responsible AI effectively, the ideal approach is trust-by-design, integrating it into your systems right from the start and continuously refining it based on the lessons learned.

Workforce: Building skills for a new way of working.

Gen-AI has the potential to empower knowledge workers, enabling them to achieve significantly more in a shorter timeframe compared to their current capabilities. However, to fully capitalise on this potential, it is essential to provide upskilling opportunities to your workforce, equipping them with the necessary skills to leverage new tools and adopt new ways of working. It is important not to be deceived by the perceived simplicity of Gen-AI, rather it is imperative to acquire the knowledge of how to utilise it responsibly. As your organisation embraces AI, new roles will emerge, such as prompt engineers and model mechanics, potentially forming an "AI factory" to support the implementation and maintenance of AI systems.

Cloud and data: Engineering the foundation for growth.

Gen-AI unlocks the potential of unstructured data, enabling better decision-making, revenue growth, and business expansion. It is vital for companies to plan their data and application modernisation with Gen-AI in mind, as it will fundamentally change how cloud based business applications are built and operate.

New business models: Monetising data and industry reinvention.

What if you could autonomously transform your unstructured data into actionable insights, or new software code, products, or services? Or what if you could provide each customer with a genuinely customised experience? Gen-AI offers this potential, which could both establish new business models and disrupt fundamental value chains. As you take advantage of the current operational efficiencies that Gen-AI provides, consider how it may transform your industry and business in the near future.

How to identify your Gen-AI Use Cases

Aspects of the vast majority of business operations, spanning from customer service to software development and data analytics, can be automated and enhanced by generative AI. Organisations can identify use cases using the following perspectives.

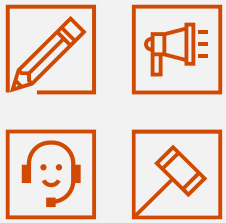
Top-Down

For my sector and functions, what Gen-AI fits?

Industry sector

Gen-AI technology has proven its worth in addressing sector-specific issues, such as those in healthcare, scientific research, and finance.

Which gen-AI technologies are available for your industry? How can generative capabilities increase your competitive advantage over rivals?



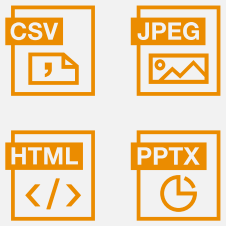
Business functions

Gen-AI technology can be integrated into R&D, marketing, sales, customer support, operations, legal, and back-office procedures.

How can a generative application best serve the greater good?

Bottom-Up

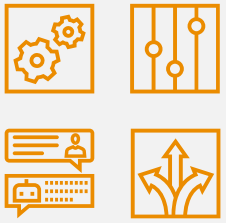
Gen-AI does this work well, how does that work serve me?



Task type

Certain categories of tasks, such as summarisation, transformation, and question answering, are best adapted to the technical mechanism of generative models.

How do these responsibilities work into your business process?



Output data modality

Generative tech involves net-new creation of text, code, image, audio, video, and more.

What types of content do teams and individual employees produce every day?

Your IT and risk professionals can help your company accelerate responsibly with Generative AI. They can help confirm that it's appropriately private, fair with harmful bias managed, valid and reliable, accountable and transparent, and explainable and interpretable.

In other words, that it's trusted.

The new and amplified risks to manage

We see four broad risks inherent to the technology that organisations need to understand and manage:

Data risks

Error propagation, intellectual property (IP) or contractual issues (due to lack of approvals to use data for such purposes), or misleading and harmful content caused by low-quality data used to train generative AI models.

Model and bias risks

Breach of ethical and responsible AI principles in the language model development, leading to discriminatory or unfair outputs.

Prompt or input risks

Misleading, inaccurate or harmful responses due to unsophisticated prompts or questions being provided to the AI model.

User risks

Unintended consequences due to users becoming unwitting parties to the creation of misinformation and other harmful content. For instance, they might pass off AI-generated hallucinations – erroneous or nonsensical responses – as fact.

You may incur other risks, as well, depending on how your company uses generative AI – particularly if you plan to create proprietary models connected to the foundational models and add proprietary or third-party data.

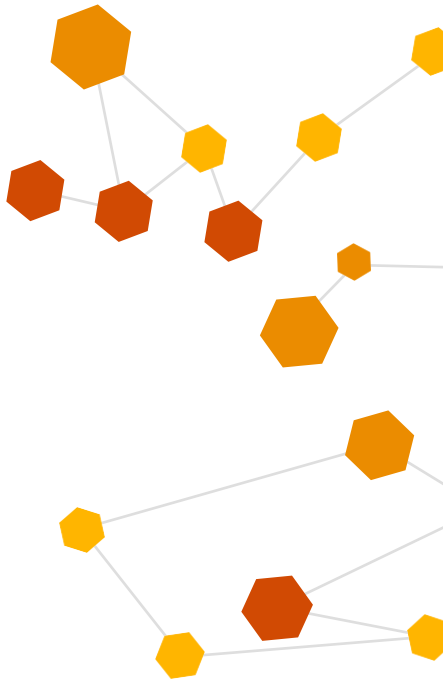
Your risk professionals are the ones who will activate generative AI toward trusted outcomes, so that trust-by-design, not speed alone, is your value proposition to your customers, investors, business partners, employees and society.

Risk domain specialists should consider the whole host of risks to privacy, cybersecurity, regulatory compliance, third-party management, legal obligations, intellectual property, and collaborate with one another to manage overall *enterprise* risk.

In parallel, you should work with your talent/HR leaders to develop training programs at all levels to familiarise everyone with the risks and rewards of generative AI. Put experienced humans in place to validate “rough draft” generative AI outputs.

Monitor human performance to guard against “skills atrophy,” complacency or drop in quality over time.

Established frameworks, such as the Ethical AI framework published by Hongkong Office of the Government Chief Information Officer (OGCIO), the Guidance on Ethical Development and Use of AI published by Hongkong Office of the Privacy Commissioner for Personal Data (PCPD), Guiding Opinions on the Digital Transformation of Banking and Insurance Industries, published by China Banking and Insurance Regulatory Commission. and the IS0/IEC 23053:2022 Framework for AI systems Using Machine Learning are a good start for designing and deploying trusted AI applications,



Having an effective AI governance strategy will be vital because beyond the risk professionals, many people inside and outside your organisation can influence your ability to use generative AI responsibly. They include data scientists, data engineers, data providers, domain experts, socio-cultural analysts, experts in the field of diversity, equity, inclusion and accessibility, affected communities, user experience designers, governance experts, system funders, product managers, third-party entities, evaluators and legal and privacy professionals.

Key AI Governance Considerations for Trusted AI

1. Model Design and Development

Key controls for planning, designing, procuring and/or developing AI models.

- Legal and regulatory compliance
- Impact analysis and risk assessment
- Strategic alignment and business care
- Model design, methods and assumption
- Defined scope and requirements
- Limits, guardrails and overrides
- Options analysis
- Training data

2. Model Verification

A risk-based testing approach with designed evaluation metrics and acceptance criteria.

- Safety
- Validity and Reliability
- Security and Resilience
- Transparency and Accountability
- Explainability and Interpretability
- Privacy
- Fairness (harmful bias managed)
- Performance and Business Value

3. Model Management

Key controls for deploying, operating and monitoring AI models in production.

- Performance monitoring (i.e. drift)
- Benefits management
- Change and release management
- Issue management
- Configuration and version management
- Human oversight
- Training and upskilling
- Feedback mechanisms

Key inputs and dependencies

- Clear roles and responsibilities
- Diverse and inclusive teams
- Engaged leadership
- Workforce and skills planning
- Defined policies and procedures
- Risk management framework
- Defined risk tolerances
- Third party risk management

Key risks that generative AI poses and actions that risk executives can take are in the following sections.

What board members and directors can do

The first place to start is for boards to increase directors' knowledge of AI and generative AI, tapping both management and external resources to stay apprised of the technologies' growing capabilities, keep up with new use cases and how business models are changing, and risks and responsible use.

When addressing AI and generative AI, **directors need to think about the technology and its use from a business perspective.** As with the many other areas that the board oversees, its role is to ask management good questions — some examples to start with are shared in this report — and challenge management when appropriate. As the board addresses AI and generative AI, the board can consider whether additional skill sets are needed, or whether to rely on management's skills or those of third parties.

Review the costs and benefits of this technology

- Boards should discuss with management the overall benefits and costs to the company.
- For benefits, it's a matter of reimagining how you get things done — how employees work, how customers engage, and what you sell and how you compete.
- Costs for employees across the company to be trained and upskilled on AI and generative AI use may be needed, as management looks to build a culture that encourages employees to learn new skills — and one that incentivises speed and innovation to capture new opportunities.

Consider communications with stakeholders

- The board should also examine how the company communicates its AI story both internally and externally to stakeholders,
- Focus on the strategic changes management is making to remain relevant and competitive in today's rapidly changing business environment
- Ensure safeguards are employed to protect staff, customers, the organisation and other stakeholders.

Develop a governance model with accountability

- A governance model that drives accountability is critical, beginning with understanding who owns the responsibility for AI governance within the company.
- An effective governance model enables an organisation to evaluate the unique benefit and risk trade-offs associated with its particular technology and individual use cases.

Oversee a plan for AI oversight to measure success

- As companies decide their path forward with AI and the business use cases that management is prioritising, there may be a large digital transformation across the company and a substantial investment required.
- When a big investment is being made to transform the company, the board will want to understand the digital transformation strategy and plan around AI, and how it aligns with the business strategy.

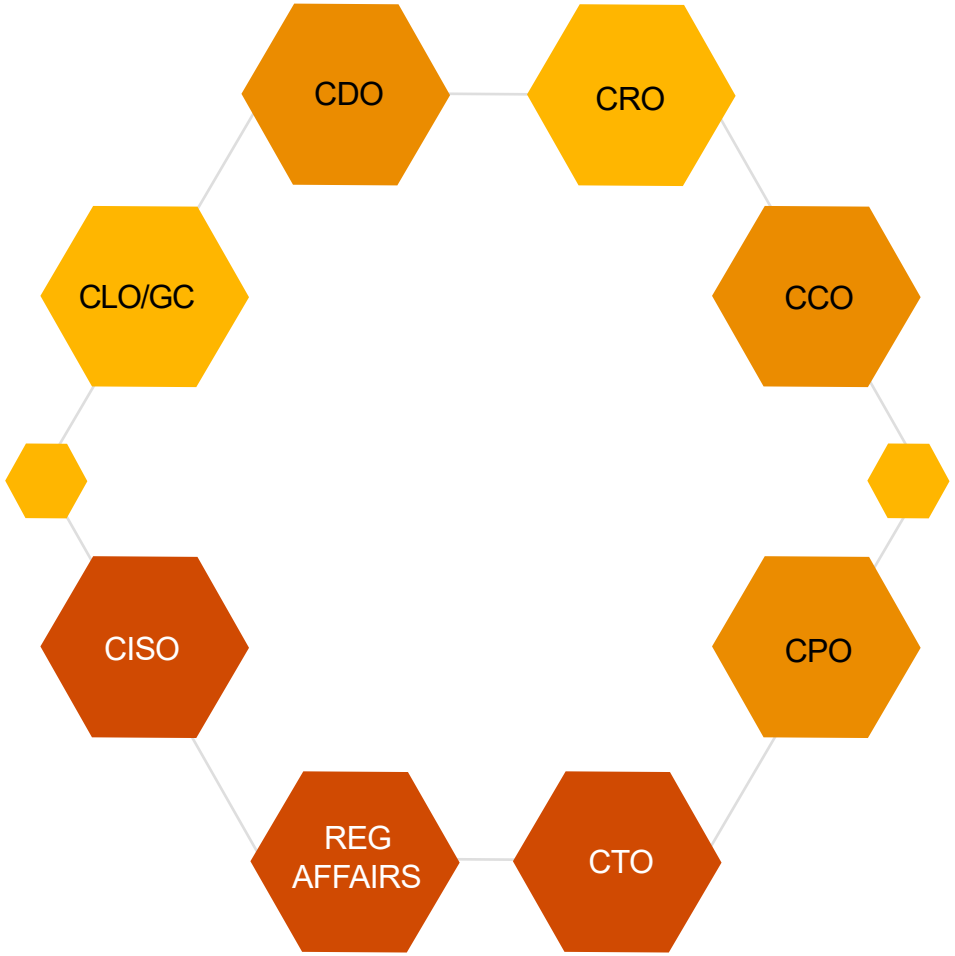
What the C-Suite can do

Let's look at two examples in which executives and their teams might collaborate to manage the risks, and how strong governance can help.

Example 1: The opportunities and risks of building a generative AI-powered medical consultation chatbot

A healthcare provider contemplates using generative AI to offer medical advice in place of tele-health sessions with clinical staff. The provider gathers years of patient data, symptoms, diagnoses and treatments to train the model.

- **CDO:** Make sure the data is accurate and clean with no overweighting of certain populations, age groups, etc.
- **CCO:** Determine whether the use of data meets compliance obligations under state-based health records legislation and The Commonwealth Privacy Act. i.e.: Health Insurance Act, My Health Records Act, Aged Care Act and state based non-health privacy laws for non health related PI if public.
- **CPO:** Collaborate to take a privacy-by-design approach and make it clear to users how their inputs will be used and which data will be retained.
- **CTO:** Design a dedicated instance for this use case so as to not inadvertently commingle the data with other operational generative AI tools.
- **Legal/GC:** Responsibly for compliance, particularity with health and data laws, potential legal analysis on IP and data, risks associated with negligent advice and negotiate contractual assurances with the generative AI platform that patient data will remain segregated from the AI model's public instance.



- **CISO:** Designate this application and data store as a “crown jewel” and provide adequate protections for it based on the most sensitive data classification.
- **Internal audit:** Develop an audit risk assessment and plan around the proposed system and model – including legal and compliance risks based on state-based health records legislation and The Commonwealth Privacy Act. i.e.: Health Insurance Act, My Health Records Act, Aged Care Act and state based non-health privacy laws for non health related PI if public – and assess reliability and performance of system and models.
- **CRO:** Coordinate with the CCO to establish policies, training, testing and controls to confirm that AI-generated medical advice is accurate and compliant with state medical board standards.

Example 2: Validating credit analysis efficiently and with awareness of the risks

A bank considers using generative AI to automate manual processes for performing annual credit checks on every counterparty documented in counterparty credit evaluations, as well as quarterly checks for high-risk customers based on market events and other triggers.

- **CDO:** Make sure the data is accurate and clean, and that there is no inherent bias weighting towards certain demographics. Set up dedicated sandbox instances to support the product.
- **CCO:** Update process maps and compliance artefacts to show how the technology is being used to reach decisions and to demonstrate evidence that it complies with Part IIIA of the Privacy Act, the Privacy (Credit Reporting) Code, The Competition and Consumer Act (CCA) and Discrimination laws.
- **Regulatory affairs:** Update reporting protocols.
- **CPO:** Call for a privacy-by-design approach, making it clear to end users how the data they provide will be used and what will be retained.
- **CLO/general counsel:** Negotiate contractual assurances from credit agencies and other data vendors to allow use of their data for generative AI, as well as assurances from the generative AI platform that customer data will not be commingled with or used to train other instances.
- **CFO/controller:** Ensure that the internal controls environment and relevant risk and controls frameworks is adequate in addressing the potential implications of AI adoption, by having the confidence on the effectiveness of the design and operation of the controls on the integrity of financial reporting process and meeting regulatory and legislative requirements such as IFRS or SOX 404.
- **CISO:** Designate this application and data store a “crown jewel” and protect it based on the most sensitive data classification.

Bottom line

For the organisations that apply it wisely, generative AI has the potential to save time and money, improve products and services and even strengthen reputations. But the approach should be human-led and tech-powered, rather than the other way around.

To truly get the most benefits from this groundbreaking technology, you need to manage the wide array of risks it poses in a way that considers the business as a whole. Stakeholders will need to come together as never before to consider all the effects and issues of bringing on board each new generative AI solution. Demonstrating that you're balancing the risks with the rewards of innovation will go a long way toward gaining trust in your company – and in getting a leg up on the competition.

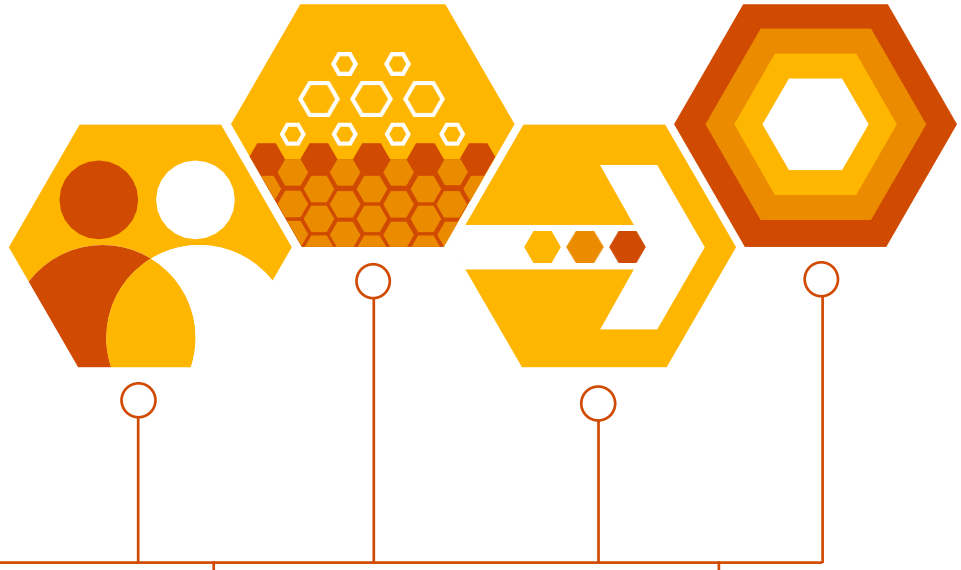
Ultimately, the promise of generative AI rests with your people. Invest in them to know the limits of using the technology as assistant, co-pilot, or tutor, even as they exploit and realise its potential. Empower your people to apply their experience to critically evaluate the outputs of generative AI models – after building your enterprise risk guardrails. Every savvy user can be a steward of trust.

The organisations that have a strong understanding of generative AI risks and how trustworthy AI systems can be designed, measured and managed can afford to move faster on AI transformation and are more ready to unlock high value use cases than those who don't.

How PwC Risk Assurance Can Help

Our Risk Assurance practice brings together a team of experts in data science, engineering, data ethics, digital law, risk and governance - along with experts in your industry - to help you accelerate responsibly and take the next step on your organisation's journey towards Trusted AI.

Understand, Establish, Accelerate and Assure are our formula for AI in the enterprise, and it is underpinned by 25 years of experience as a leader in technology and data governance, our award-winning AI consulting services and our global ecosystem of technology alliances.



Understand

Understanding your baseline and readiness to respond to the opportunities and risks of artificial intelligence.

- Ideation and strategy creation
- Use case exploration and selection

Establish

Establishing the foundations that organisations should have in place for embracing AI swiftly yet safely.

- Data maturity review
- Risk and controls review
- AI governance model
- Responsible AI

Accelerate

Accelerating your ideation, exploration and prototyping. Scaling successful ideas and monitoring their efficacy and safety.

- Data platform implementation
- Gen AI PoC deployment

Assure

Reviewing your existing AI frameworks, platforms, models and implementations to help build and maintain trust with your stakeholders.

- Controls implementation
- Data observability managed service

Contact us to learn more

Jennifer Ho
Asia Pacific Risk Services Leader
Mainland China and Hong Kong Digital Trust & Risk Leader
PwC Hong Kong
jennifer.cw.ho@hk.pwc.com

Jasper Xu
Mainland China and Hong Kong Digital Trust & Risk Markets Leader
China Central Digital Trust & Risk Leader
PwC China
jasper.xu@cn.pwc.com

Rachel Pan
Digital Trust & Risk Partner
PwC China
rachel.pan@cn.pwc.com

George Lu
Mainland China and Hong Kong Digital Trust & Risk - Digital Trust and Analytics Leader, Digital Intelligence Centre of Excellence co-lead
PwC China
george.l.lu@cn.pwc.com

Chris Mo
Digital Trust & Risk Partner
PwC Hong Kong
chris.yw.mo@hk.pwc.com

Chun Yin Cheung
Cyber and Tech Risk Partner
PwC China
chun.yin.cheung@cn.pwc.com