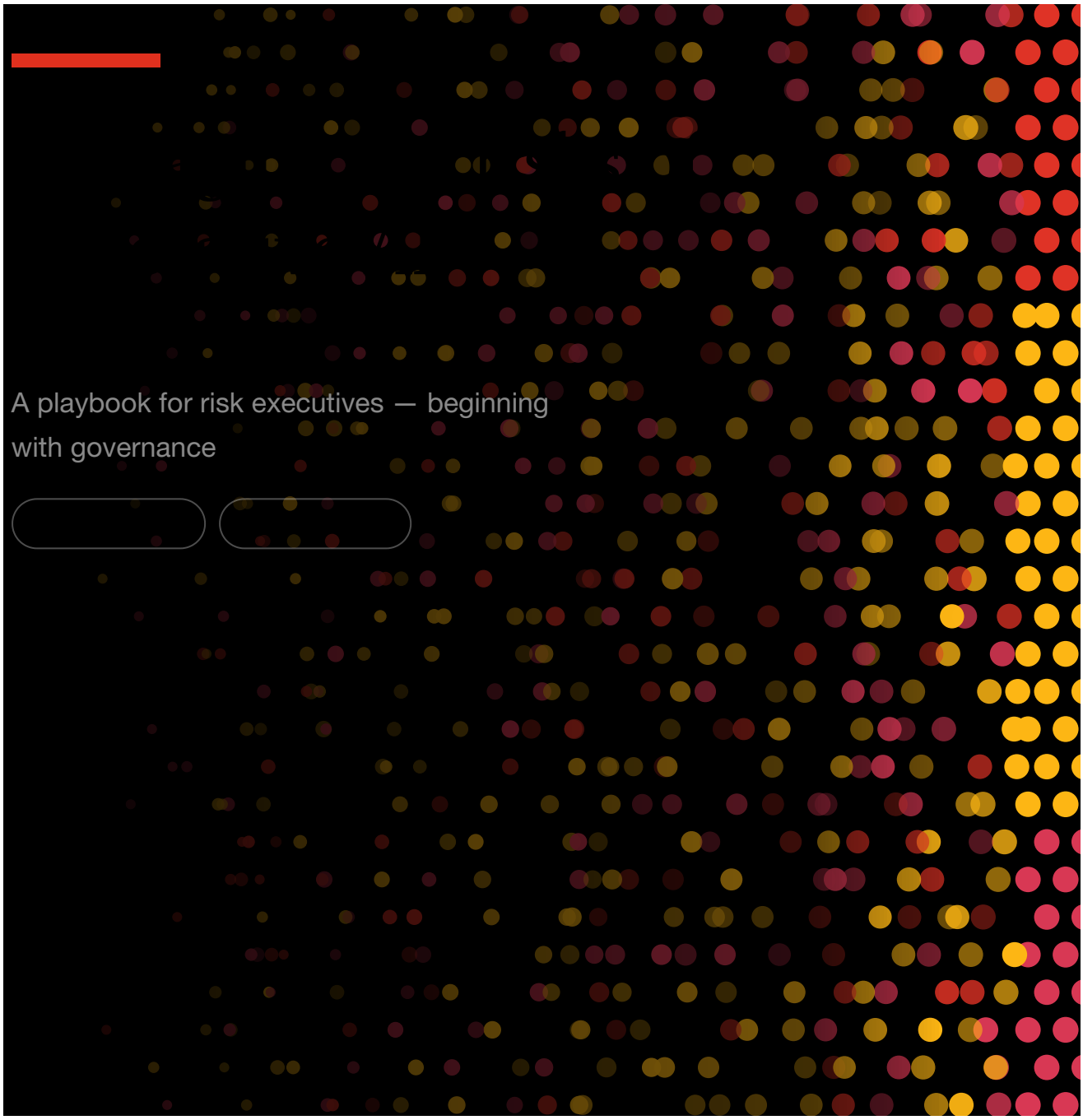


Using generative artificial intelligence (GenAI) requires constant, swift changes and adaptations — for AI developers, business users, investors, policymakers and citizens.

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. Risks to privacy, cybersecurity, regulatory compliance, third-party relationships, legal obligations and intellectual property have already emerged.

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.

Your risk professionals can help your company use generative AI safely, securely and resiliently. 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.

While every executive and user plays an important role, these key C-suite leaders will activate **responsible AI**, so that trust-by-design, not speed alone, is your value proposition to your customers, investors, business partners, employees and society.

The new and amplified risks to manage

Here's an overview of the risks that each will focus on. For a more comprehensive discussion, see the complete **GenAI risk playbook**.

Chief information security officer

Generative AI can reduce barriers of entry for threat actors. The most immediate risk to worry about? More sophisticated phishing. More compelling, custom lures used in chats, videos, or live generated "deep fake" video or audio, impersonating someone familiar or in a position of authority.

For the CISO, GenAI adds a valuable asset for threat actors to target — and for your organization to manage. They could manipulate AI systems to make incorrect predictions or deny service to customers. Your proprietary language and foundational models, data and new content will need stronger cyberdefense protections.

Chief data officer and chief privacy officer

GenAI applications could exacerbate data and privacy risks; after all, the promise of large language models is that they use a massive amount of data and create even more new data, which are vulnerable to bias, poor quality, unauthorized access and loss.

Employees entering sensitive data into public generative AI models is already a significant problem for some companies. GenAI, which may store input information indefinitely and use it to train other models, could contravene privacy regulations that restrict secondary uses of personal data.

Chief compliance officer

A nimble, collaborative, regulatory-and-response approach is emerging with generative AI, requiring, perhaps, a major adjustment for compliance officers. Keep up with new regulations and stronger enforcement of existing regulations that apply to generative AI.

Chief legal officer and general counsel

Without proper governance and supervision, a company's use of generative AI can create or exacerbate legal risks. Lax data security measures, for example, can publicly expose the company's trade secrets and other proprietary information, as well as customer data. And not thoroughly reviewing your

generative AI outputs can result in inaccuracies, compliance violations, breach of contract, copyright infringement, erroneous fraud alerts, faulty internal investigations, harmful communications with customers and reputational damage. To challenge and defend GenAI-related issues, your legal teams will need deeper technical understanding that lawyers typically don't have.

Internal audit leaders

Auditing will be a key governance mechanism to confirm that AI systems are designed and deployed in line with a company's goals. But to create a risk-based audit plan specific to generative AI, Internal Audit must design and adopt new audit methodologies, new forms of supervision and new skill sets. It's difficult and ineffectual to assess the risks that generative AI systems pose independent of the context in which they are deployed. Understanding the problem the company is trying to solve using GenAI is an important starting point.

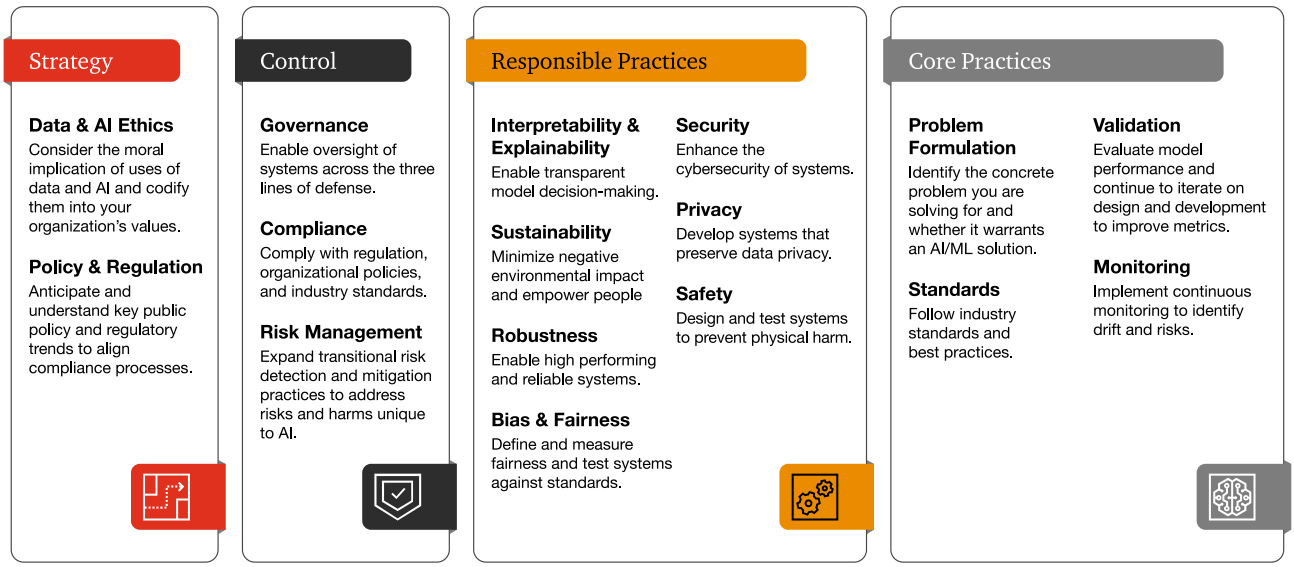
Chief financial officer and controller

Without proper governance and supervision, a company's use of GenAI can create or exacerbate financial risks. If not used properly, it opens the company to "hallucination" risk on financial facts, errors in reasoning and over-reliance on outputs requiring numerical computation. These are high-consequence risks that CFOs face in the course of their normal duties, often in a regulated environment. Highly-visible, unintended financial reporting errors result in loss of trust with customers, investors, regulators and other stakeholders and have resulted in severe reputational damage that is costly to recover from.

For trusted AI, start with governance

Having an effective AI governance strategy will be vital, and many people inside and outside of your organization can influence your ability to use generative AI responsibly. They include data scientists and engineers; data providers; specialists in the field of diversity, equity, inclusion and accessibility; user experience designers, functional leaders and product managers.

PwC's Responsible AI framework



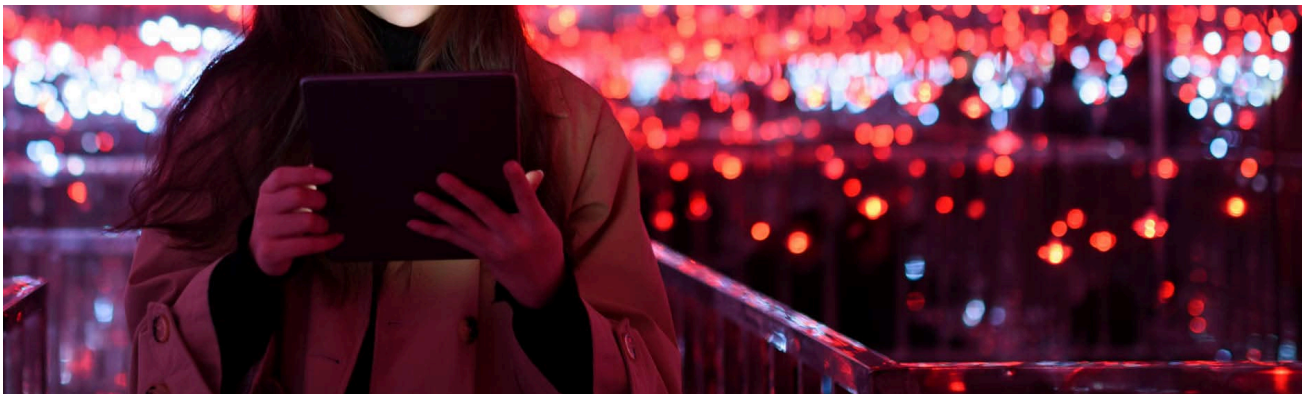
Stakeholders will need to come together to consider all the effects and issues of bringing on board each new generative AI solution.

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 realize its potential. Empower your people to apply their knowledge and 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.

Get the complete GenAI risk playbook

What security, privacy, internal audit, legal, finance and compliance leaders need to know now.

Learn more



Generative AI

Lead with trust to drive sustained outcomes and transform the future of your business.

Learn more

Subscribe here

Our insights. Your choices.

Sean Joyce

Global Cybersecurity & Privacy Leader, PwC US; Cyber, Risk & Regulatory Leader, PwC US

Mir Kashifuddin

Data Risk & Privacy Leader, PwC US

Jennifer Kosar

Trust and Transparency Solutions Leader, PwC US

Tim Persons

Principal, Digital Assurance and Transparency, PwC US

Vikas Agarwal

Financial Services Leader, Cyber, Risk & Regulatory, PwC US

Bret Greenstein

Data and Analytics Partner, PwC US

Related content

Generative AI

Manufacturers want to adopt generative AI. Where and how do they begin?

6 min. | Dec 11, 2023

Cybersecurity

Tech Translated: Cyberphysical systems

4 min. | Dec 7, 2023

Generative AI

Do you have an “early days” generative AI strategy?

16 min. | Dec 7, 2023

Cybersecurity · Generative AI

For gen-AI-enabled threats, fight fire with fire

6 min. | Nov 28, 2023