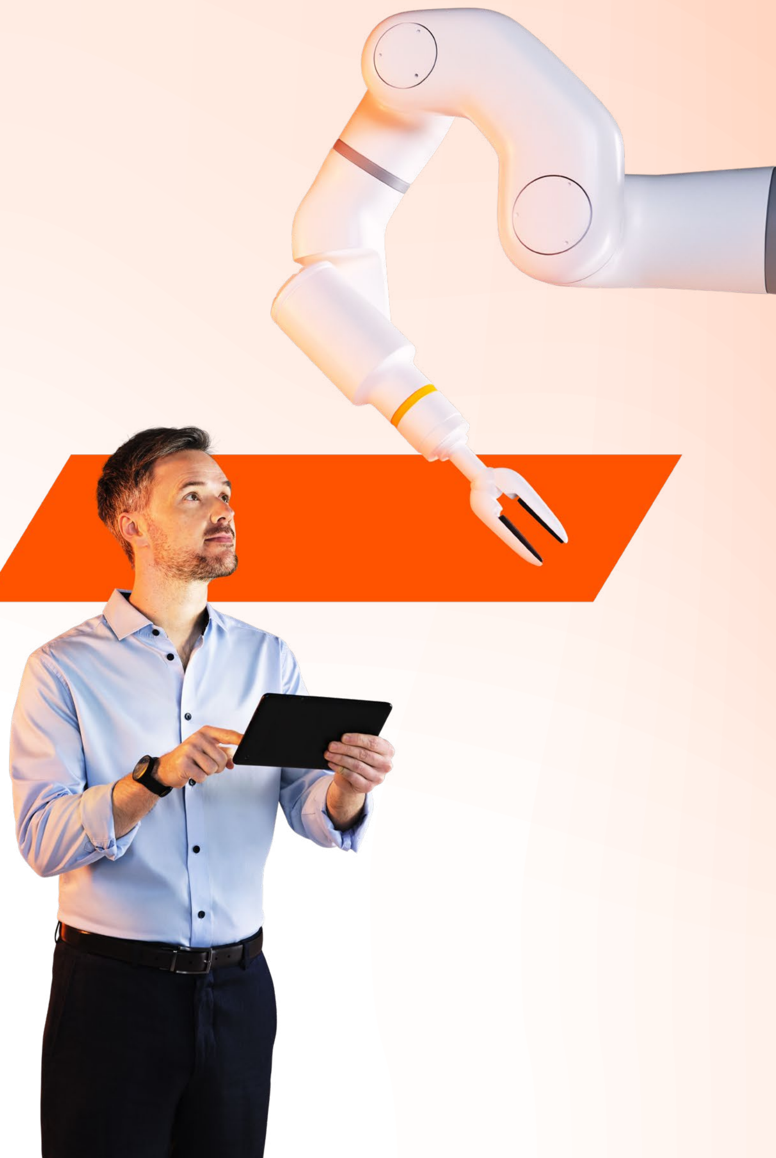
Driving trust and security in AI

Balancing innovation and risk



The time to act on AI is now

The maturity of AI brought us to a turning point where generative AI (GenAI) is complementing predictive AI and is going well beyond the hype in delivering superior value for organisations. However, organisations still need strong foundational capabilities to gain long-term competitive advantage.

Building trust in AI starts with securing the systems that make it possible

Your stakeholders, including board members, customers and regulators, will have many questions about your organisation's use of AI and data – from how it's developed to how it's governed. In addition to being ready to supply answers, you must demonstrate ongoing governance and regulatory compliance.

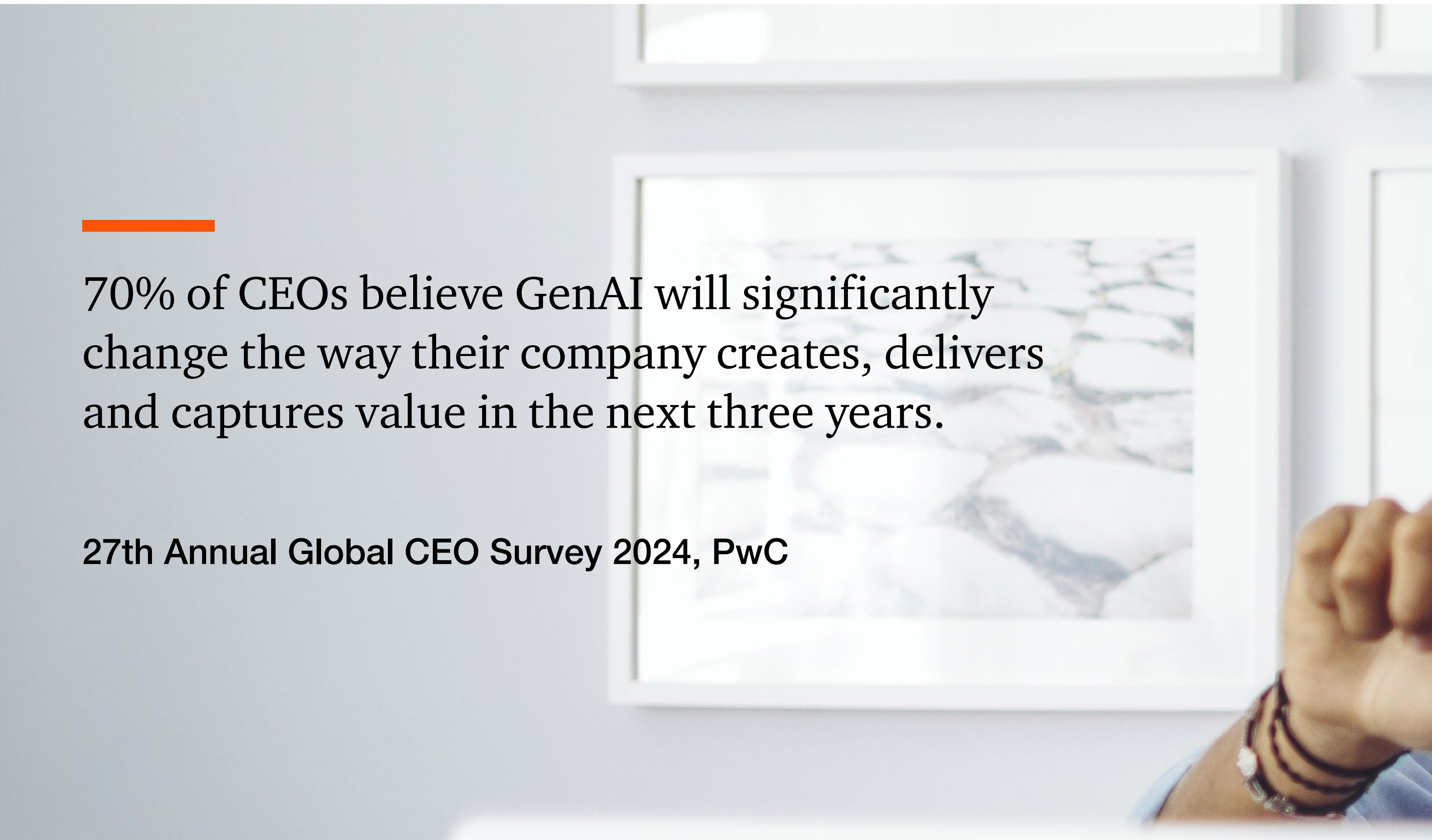
Security for AI and AI for security

1

Security for AI
Securing AI means defending models, data and systems from threats. We ensure AI remains trustworthy, resilient and compliant.

2

AI for security
This refers to leveraging AI to detect threats, automate responses and strengthen cyber defenses – making it faster, smarter and more adaptive than ever.



70% of CEOs believe GenAI will significantly change the way their company creates, delivers and captures value in the next three years.

27th Annual Global CEO Survey 2024, PwC

What you need to know

- **Where and how should we balance innovation with regulation to address compliance?**
- **How do I empower my C-suite to stay up to date with the rapidly evolving AI landscape?**
- **How must our roles, departments and operating model adapt to capture value from AI?**

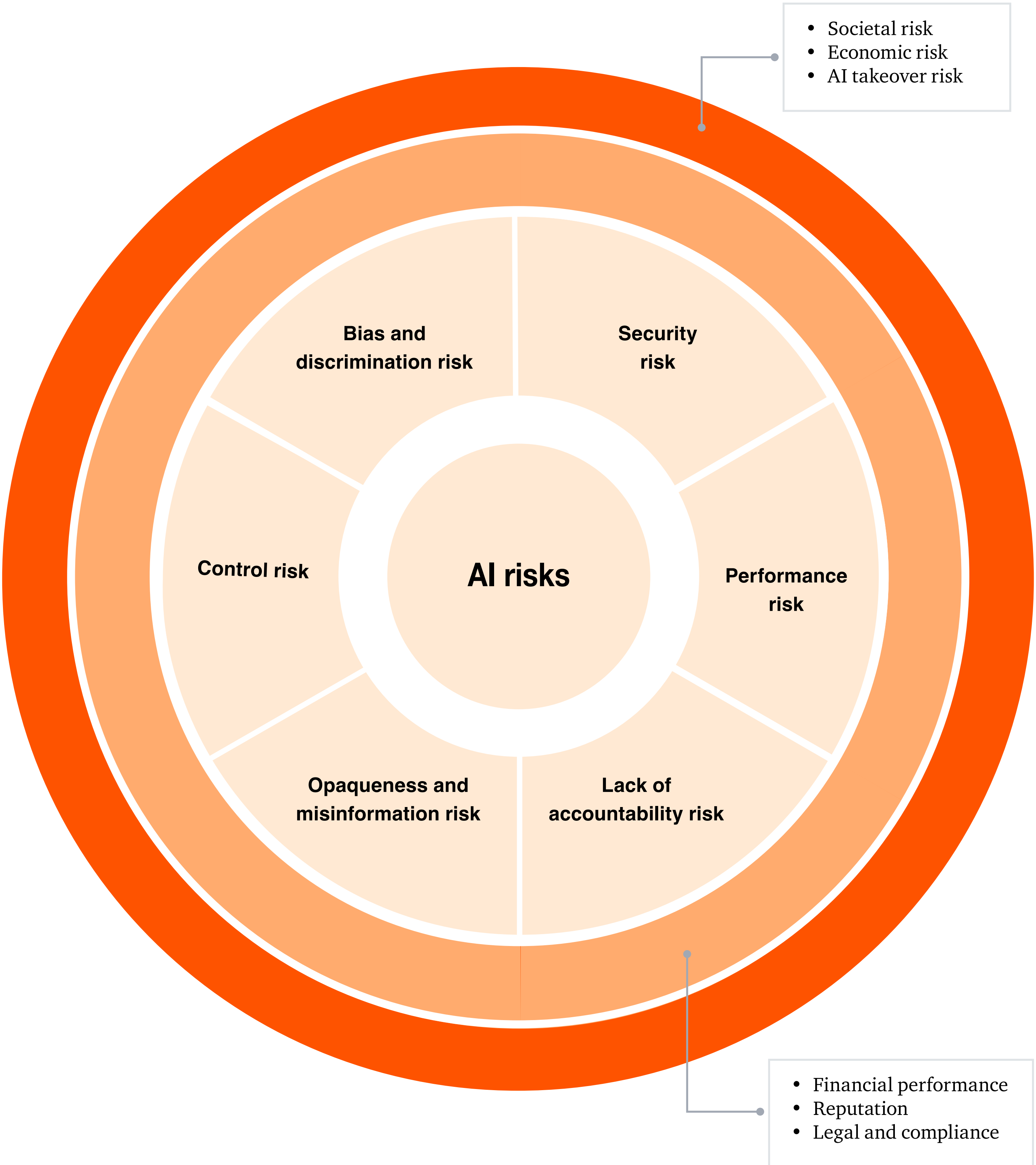
Six-step process to gain effective oversight of AI

1. AI awareness and adoption
2. Reimagine AI use case evaluation and development
3. Regulatory and compliance obligations
4. Responsible AI guardrails
5. Operating model and workforce of the future
6. Continuous AI risk management

AI risks

With great potential comes great risk. Are your algorithms making decisions that align with your values? Do customers trust you with their data? How is your brand affected if you can't explain how AI systems work? It's critical to anticipate problems and future-proof your systems so that you can fully realise AI's potential.

Risks posed by GenAI		
AI system risks	Enterprise-level	Nation/country/global risks



From a responsible AI strategy...

AI strategy

- **Adoption, readiness and maturity assessment –** Whether you have already started on your AI journey or are trying to decide the approach, we can help you to understand your readiness or maturity and course correct.

AI governance

- **AI security framework –** We empower organisations to build customised AI security frameworks by leveraging globally recognised standards such as NIST AI RMF and ISO 42001, while ensuring alignment with key regulations, including – but not limited to – the EU AI Act.

...to trusted AI implementation.

AI testing and enablement

- **RAI framework and assessments (including regulations) –** Guiding ethical AI through structured evaluations and regulatory alignment to ensure responsible, transparent and compliant systems
- **Red teaming and adversarial testing –** Simulating real-world attacks to uncover vulnerabilities in AI systems, thereby ensuring resilience, robustness and readiness against evolving threats

AI sustenance and growth

- **Awareness and cultural adaptations –** Fostering AI understanding and aligning practices with diverse cultural values to drive responsible adoption and inclusive innovation
- **Co-creation and alignment with hyper-scalers and alliances –** Collaborating with leading cloud providers and strategic alliances to accelerate innovation, ensure interoperability and scale AI responsibly

Partnering with hyper-scalers and alliances, we integrate cutting-edge technology to drive innovation, align with business goals and fast-track digital transformation.

Strategic alliances*

Academia and research organisations

Service provider alliances

Startups and emerging technologies*

*Alliances and tie-ups with partners/vendors continue to evolve.

1. Direct access to LLMs via APIs to build custom use cases
2. Platforms to build generalised AI/GenAI use cases
3. Research groups for advancing ethical and responsible AI

Why PwC

At PwC, our reputation is defined by building trust and achieving quality and sustainable value. We believe in winning work on the merits of the quality and the value we deliver to our clients. We are committed to delivering sustained outcomes leveraging our expertise, dedication and unwavering focus.

Professionals with deep expertise in AI practices and governance standards

Strategic alignment with businesses

Holistic risk management

Responsible adoption practices

Client-centric approach

AI domain knowledge

About PwC

We help you build trust so you can boldly reinvent

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 370,000 people in 149 countries. Across assurance, tax and legal, deals and consulting we help build, accelerate and sustain momentum. Find out more at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Sundareshwar Krishnamurthy
Partner and Leader - Cybersecurity
PwC India
sundareshwar.krishnamurthy@pwc.com

Venkat Iyer
Partner – Cybersecurity
PwC India
iyer.venkat@pwc.com

pwc.in

KS/August2025 - M&C 47814