KPMG Risk Insights Executive talk

AI in Governance, Risk and Compliance (GRC)

KPMG in Thailand
No. 3/2025 – 17 July 2025

KPMG presenters today

Supachate Kunaluckkul

CIA, CISA, CCSA, CPA

Head of Enterprise Risk
Consulting Partner
KPMG in Thailand

Saowanee Sethsathira

CISA, CRISC, CDPSE, ISO27001 LA

Head of Tech-Cyber
Tech-Cyber Partner
KPMG in Thailand

Woramon Sayalak

CISA, CPA, ISO27001 LA

Tech-Cyber Director
KPMG in Thailand

Peerawat Apiratitham

CIA, CPA, GRCA, GRCP, IAAP

Consulting Associate Director
KPMG in Thailand

Tienlert Leenanupun

CPA

Consulting Manager
KPMG in Thailand

Agenda

01

Evolving risk landscape in the AI era and AI governance

Embrace AI governance to stay ahead in a rapidly evolving risk landscape

02

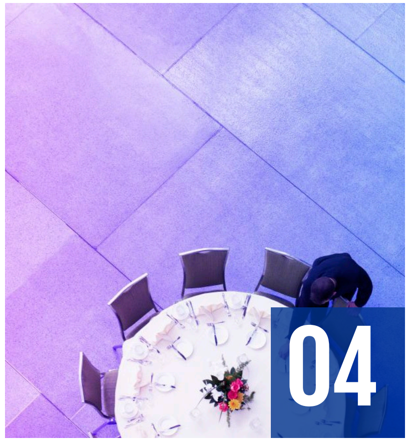
Exploring the potential of AI in GRC

Leverage AI to enhance Governance, Risk and Compliance (GRC)

03

Navigating AI assurance: building trust in your AI

Improve AI reliability and fairness with structured assurance


04

Q&A session

An exclusive conversation with KPMG Business Advisors

01

Evolving risk landscape in the AI era and AI governance

AI development and associated risks over time

1950s

Conceptual birth of AI (e.g. Turing Test, logic-based systems)

1990s

Renewed interest in neural networks and machine learning

2010s

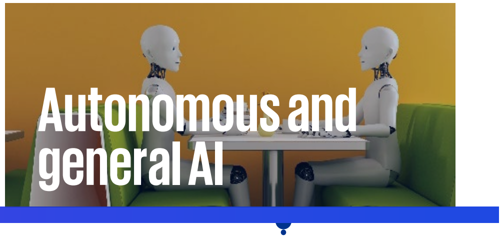
Revolution in deep learning fueled by breakthroughs in neural networks

2020s

Increasing application of generative AI in diverse sectors

2030s (Emerging)

AI that acts independently with human-like intelligence and flexibility



⚠ **Evolving risks**

- Unrealistic expectations
- Ethical concerns about autonomy
- Early fears of automation

- Data bias and overfitting
- Lack of explainability
- Misuse of AI due to insufficient regulation

- Discrimination and bias
- Black-box models
- Data privacy concerns

- Misinformation and deepfakes
- Hallucinations
- Intellectual Property Infringement

- Loss of human oversight
- Value misalignment
- Workforce displacement
- Non-compliance with rapidly evolving AI laws

Key findings on AI adoption survey

“AI Front and center as the urgency around adoption accelerates”

64% of Global CEOs indicated that they would invest in AI regardless of economic conditions in 2024.

76% of CEOs anticipated AI will not fundamentally reduce the number of jobs within their organizations over the next three years.

Global CEOs recognize the need to seize the challenges that lie ahead, considering AI as potentials to transform business.

Global CEOs recognize that their workforce will need to adapt and upskills to fully leverage the benefits of AI.

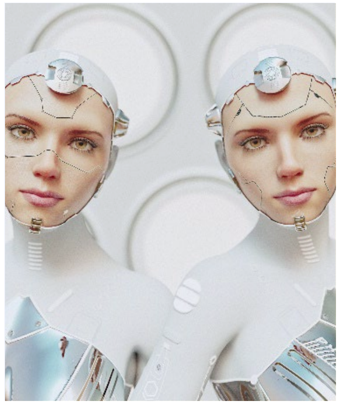
Global CEOs say that they plan to invest in AI in some form.

Global CEOs are increasing aware of the risks tied to the rapid AI adoption concerning the ethical use and implementation of AI.

Source: KPMG 2024 CEO Outlook

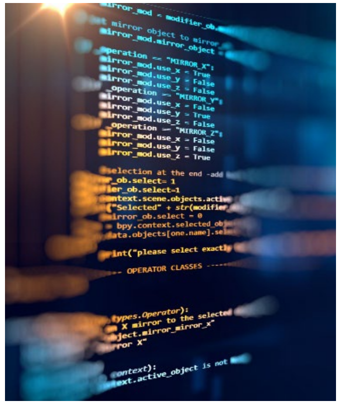
AI challenges and ethical dilemmas

AI recruiting tool favoring certain type of candidates due to historical data



Defrauding the public by generating realistic fake identities

Sensitive code leak from free version of generative AI



Chatbot giving a customer inaccurate information, resulting in the company being sued

AI firm sued for copyright infringement over its image generator

AI System used to identify targets for attacks during the war

AI ethical considerations

To build and sustain a responsible enterprise, AI must be developed, governed and deployed with clear ethical principles and meaningful oversight — this is the foundation of ethical AI.

"The rise of AI has introduced transformative capabilities into both business operations and daily life. With this power, however, come important questions about the trustworthiness, accountability, and governance of AI systems."

Trust and acceptance of AI

AI benefits and risks

AI use and understanding

AI literacy

Responsible AI

AI governance: building trust in AI

To proactively operationalize Trusted AI governance and establish accountability as the regulatory landscape and global standards continue to evolve, below are examples of questions the organizations can ask as they begin the process:

Trusted AI people 1 Do you have someone responsible for AI within your organization?

AI policy 2 Do you have guidelines and controls that govern the use of AI?

AI inventory 3 Do you know everywhere AI is being used across your company?

AI system 4 Do you have ongoing monitoring and reporting in place against your Trusted AI framework?

Trusted AI training 5 Are your professionals equipped to make responsible and ethical AI decisions?

02

Exploring the potential of AI in GRC

Why do we need GRC?

Rising cost of compliance

Growing digital risk

Stakeholder expectations

Greater reliance on third and fourth parties

It impacts how people work.

More pandemics and extreme weather

Increasing reputational risk

Strategic decision-making

Disconnected tools, systems and processes (data silos and inefficiency)

It impacts their bottom line.

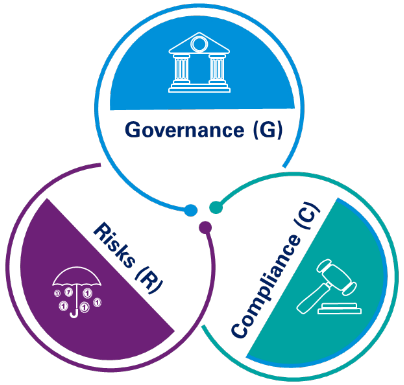
IT → Security → Legal → Finance → HR → Customer service → Lines of business

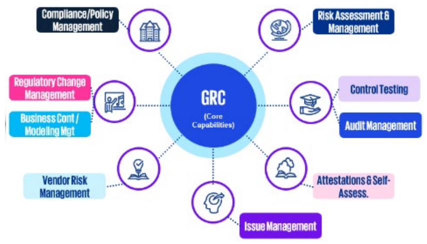
GRC ecosystem

Key challenges

- Data silo/ fragmentation
- Duplication of efforts
- Inconsistent GRC languages and terminology
- Unstandardized process of framework
- Evolving risk and compliance landscape

GRC ecosystem




GRC
(Core Capabilities)
Compliance/Policy Management
Risk Assessment & Management
Regulatory Change Management
Business Cont / Modeling Mgt
Control Testing
Audit Management
Vendor Risk Management
Attestations & Self-Assess.
Issue Management

Governance:

Oversight role and the process by which companies manage and mitigate business risks

Risk:

Enables an organization to evaluate all relevant business and regulatory risks and controls, and monitor mitigation actions in a structured manner

Compliance:

Ensures that an organization has the processes and internal controls to meet the requirements imposed by governmental bodies, regulators, industry mandates or internal policies

Expected benefits

- **Single source of data**
- **Streamlined/efficient operations**
- **Improved and data-enabled decision-making**
- **Strengthened governance/ assurance**
- **Collaboration and integrated information**
- **Enhanced stakeholders' trust**

Benefits and challenges of using AI for GRC

BENEFITS

Enhanced decision making

- Real-time insights and trends analysis
- Forecast of potential challenges, risks and opportunities

Cost savings

- Reducing likelihood of non-compliance
- Streamlined and efficient GRC processes

Automating monitoring process

- Routine compliance monitoring can be automated
- Reduce manual processing

Advanced risk assessment

- Ability to process vast amount of data
- Enhance service delivery, anticipating potential risks

CHALLENGES

Ethical consideration

- AI could can unintentionally embed bias, discriminate or make opaque decisions.

Data privacy concerns

- As AI processes and involves large volume of data, it presents significant privacy risks.

Over-reliance on automation

- Excessive dependence on AI tools may lead to reduced human oversight and missed anomalies.

Evolving regulatory landscape

- The challenge of staying ahead of shifting legal and compliance requirements to ensure AI governance and compliance.

Example of AI in GRC

Corporate governance

Use cases	How ?	Outcomes
1 Ai-enabled regulatory scanning and policy update automation	• **Regulation scanning and policy impact:** Use AI to scan new or updated regulations, identify affected policy areas and suggest edits • **Automated compliance workflow:** Generate workflow tasks to ensure timely policy updates and adherence	• Reduce manual effort through automated policy review and edit suggestions • Reduce regulatory response time • Improve workflow efficiency by generating timely tasks for policy updates
2 AI board observer elevates corporate strategy with real-time insights	• **Real-time insights:** Provide live data analysis and strategic recommendations during board meetings • **Meeting automation:** Automate routine tasks and report generation for efficient board management	• Improve decision-making • Save time by automating routine tasks • Enhance strategic planning through comprehensive performance analysis
3 Fraud prevention with AI transaction analysis	• **Machine learning for patterns**: Train AI on historical data to identify fraud patterns • **Behavioral analysis:** Detect unusual behavior • **Real-time monitoring:** Monitor transactions in real time and trigger immediate alerts for potential fraud	• Reduce potential financial losses • Increase response time • Enhance trust from stakeholders

Source: OCEG, KPMG

Example of AI in GRC

Risk management

Use cases	How ?	Outcomes
1 AI-driven emerging risk detection from multi-source data	• **Analyzing data sources:** Leverage NLP, and ML to analyze emerging risks from diverse sources • **Identifying new data sources:** Explore and experiment with new data sources	• Early identification of potential risks • Enhance comprehensive risk view • Improve decision-making with real-time insights
2 Leveraging AI to identify threats through patterns and trends	• **Time-series analysis:** Utilize time-series analysis to identify trends and detect anomalies over time • **NLP analysis:** Extract risk signals from textual data • **Predictive analytics:** Predict potential risks by analyzing historical patterns and behavior	• Detect hidden risks early • Reveal key patterns in complex data • Enable timely, predictive decisions
3 Real-time risk monitoring with AI-powered alerts	• **Data integration:** Integrate insights from financial documents, industry trends and online sentiment • **Real-time risk monitoring:** Monitor, detect and alert when risk indicators reach defined thresholds	• Enhance awareness through integrated data sources • Respond quickly to emerging risks • Offer continuous risk monitoring

Source: OCEG, KPMG

Example of AI in GRC

Compliance management

Use cases	How ?	Outcomes
1 AI for dynamic monitoring of laws and regulations	• **Automated monitoring:** Monitor updates from government websites, legal databases and news sources • **Predictive insights:** Predict regulatory developments from trends and historical data	• Effectively track legal changes to save time and reduce manual effort • Gain forward-looking insights to anticipate and prepare for future developments
2 Smart monitoring for compliance violations	• **Anomaly detection**: Identify and detect patterns of anomalies that signal potential non-compliance • **Real-time monitoring:** Continuous real-time compliance check with instant violation alert	• Spot potential violations early • Respond rapidly to non-compliance • Reduce regulatory risks proactively • Strengthen trust through consistent compliance
3 Behavioral monitoring for policy compliance	• **Behavioral analytics**: Apply AI to analyze behavior and spot potential policy violations • **Social network analysis**: Analyze networks to detect collusion or unethical ties	• Detect unusual behaviors or interactions early • Enable faster, data-driven investigations and interventions

Source: OCEG, KPMG

Example of AI in GRC

Internal audit

Use cases	How ?	Outcomes
1 Automated document review for risk-based audit planning	• **NLP :** Extract key topics and potential risk signals from meeting minutes and reports • **Machine learning:** Classify, prioritize and flag emerging risks based on historical risk patterns	• Enhance audit plan quality by identifying key risks early from unstructured data • Automate document review to save time • Align audit scope with emerging issues
2 Data-enabled audit execution	• **Machine learning:** Learn normal transaction patterns from large datasets • **Anomaly detection:** Spot unusual or suspicious activities • **Risk prioritization:** Highlight high-risk items for focused audit testing	• Reduces manual effort data analysis by automating • Improves accuracy by finding hidden anomalies • Boosts efficiency by targeting high-risk areas
3 Intelligent audit documentation support	• **NLP:** Automatically summarize key information from workpapers and audit documents • **Conversational AI:** Let auditors ask questions and get context-aware answers • **Content Analysis:** Identify documentation gaps or issues and suggest improvements	• Speeds up reviews with automated summaries • Enhances quality with AI suggestions • Supports auditor decisions with contextual guidance

Source: KPMG

Reshaping AI-driven GRC professionals

“AI is revolutionizing businesses, redefining roles and unlocking new opportunities for growth. To thrive in this evolving landscape, all staff should enhance their skills, especially AI-specific skills, while continuing to build on their existing competencies.”

AI transforming job roles

AI not tech-industry specific

Human collaboration with AI tools

Continuous learnings is key

“AI-driven workforce strategy to involve AI skills required for the changing landscape”

Examples of AI business skills

- Adaptability
- Ai-driven strategy
- Business foresight
- Communication
- Critical thinking
- Data governance
- Ethical AI
- Project management

Examples of AI technical skills

- AI quality assurance
- AI systems security
- Algorithm design and analysis
- Data engineering
- Large language models
- Machine learning
- Natural language processing
- Prompt engineering

03

Navigating AI assurance: building trust in your AI

01

What are the market drivers ?

Common challenges the C-suite are facing

How do organizations safely and responsibly unlock value from AI - and achieve the business ambitions?

C-suite need to

Secure our models from adversarial attacks

Maintain compliance with global AI regulations

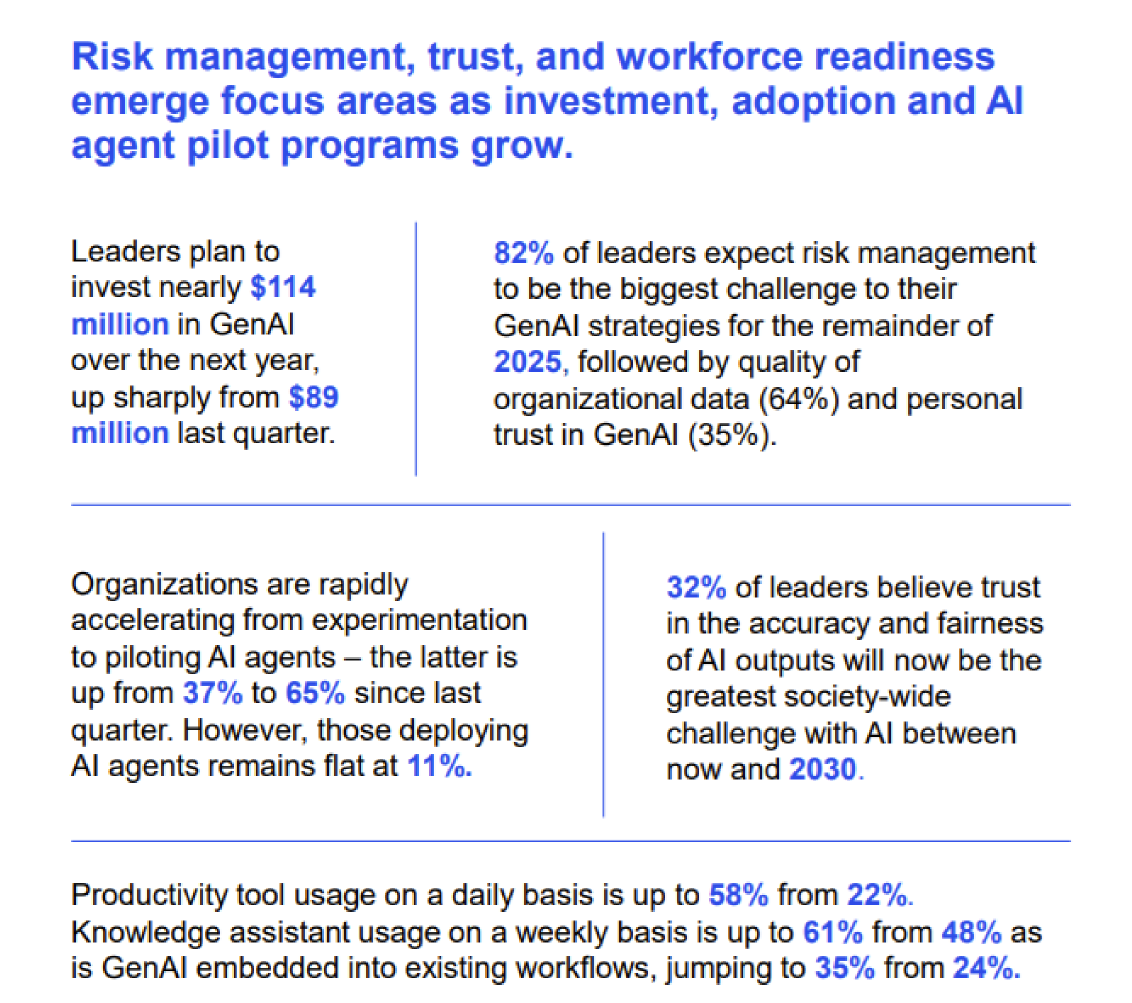
Harness the value of our AI at scale and responsibly

Protect ourselves from financial and reputational risks

Enhance the trust of our consumers (internal, external)

Drive accountability and transparency

Key stats from KPMG Q1 2025 AI Pulse Survey



Risk management, trust, and workforce readiness emerge focus areas as investment, adoption and AI agent pilot programs grow.

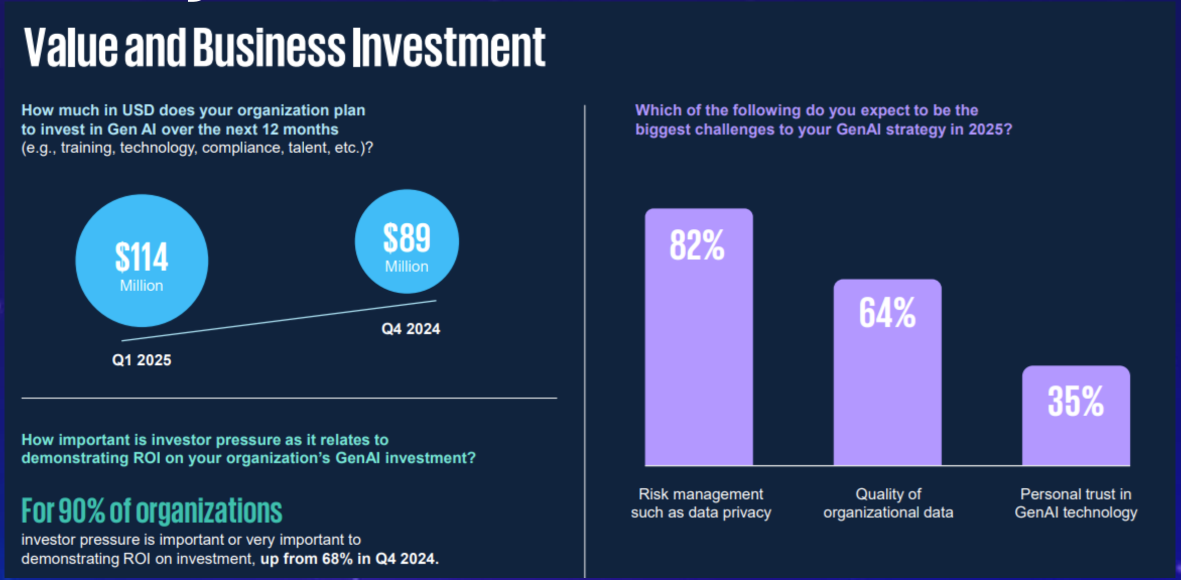
Leaders plan to invest nearly **$114 million** in GenAI over the next year, up sharply from **$89 million** last quarter.

82% of leaders expect risk management to be the biggest challenge to their GenAI strategies for the remainder of **2025**, followed by quality of organizational data (64%) and personal trust in GenAI (35%).

Organizations are rapidly accelerating from experimentation to piloting AI agents – the latter is up from **37%** to **65%** since last quarter. However, those deploying AI agents remains flat at **11%.**

32% of leaders believe trust in the accuracy and fairness of AI outputs will now be the greatest society-wide challenge with AI between now and **2030**.

Productivity tool usage on a daily basis is up to **58%** from **22%.** Knowledge assistant usage on a weekly basis is up to **61%** from **48%** as is GenAI embedded into existing workflows, jumping to **35%** from **24%.**



Value and Business Investment

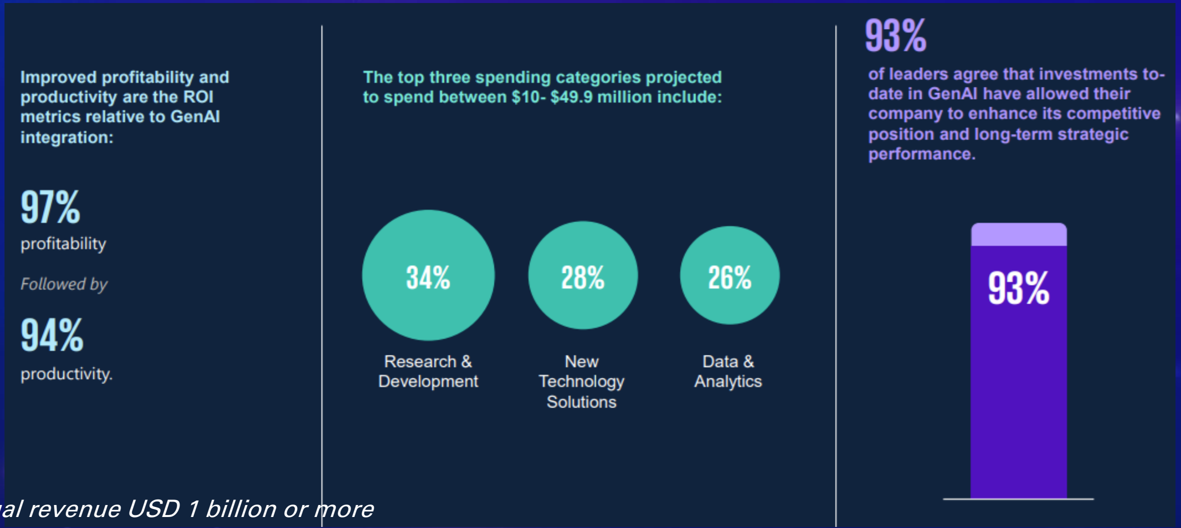
How much in USD does your organization plan to invest in Gen AI over the next 12 months
(e.g., training, technology, compliance, talent, etc.)?

How important is investor pressure as it relates to demonstrating ROI on your organization's GenAI investment?

For 90% of organizations

investor pressure is important or very important to demonstrating ROI on investment, **up from 68% in Q4 2024.**

Which of the following do you expect to be the biggest challenges to your GenAI strategy in 2025?



Improved profitability and productivity are the ROI metrics relative to GenAI integration:

97%
profitability

Followed by

94%
productivity.

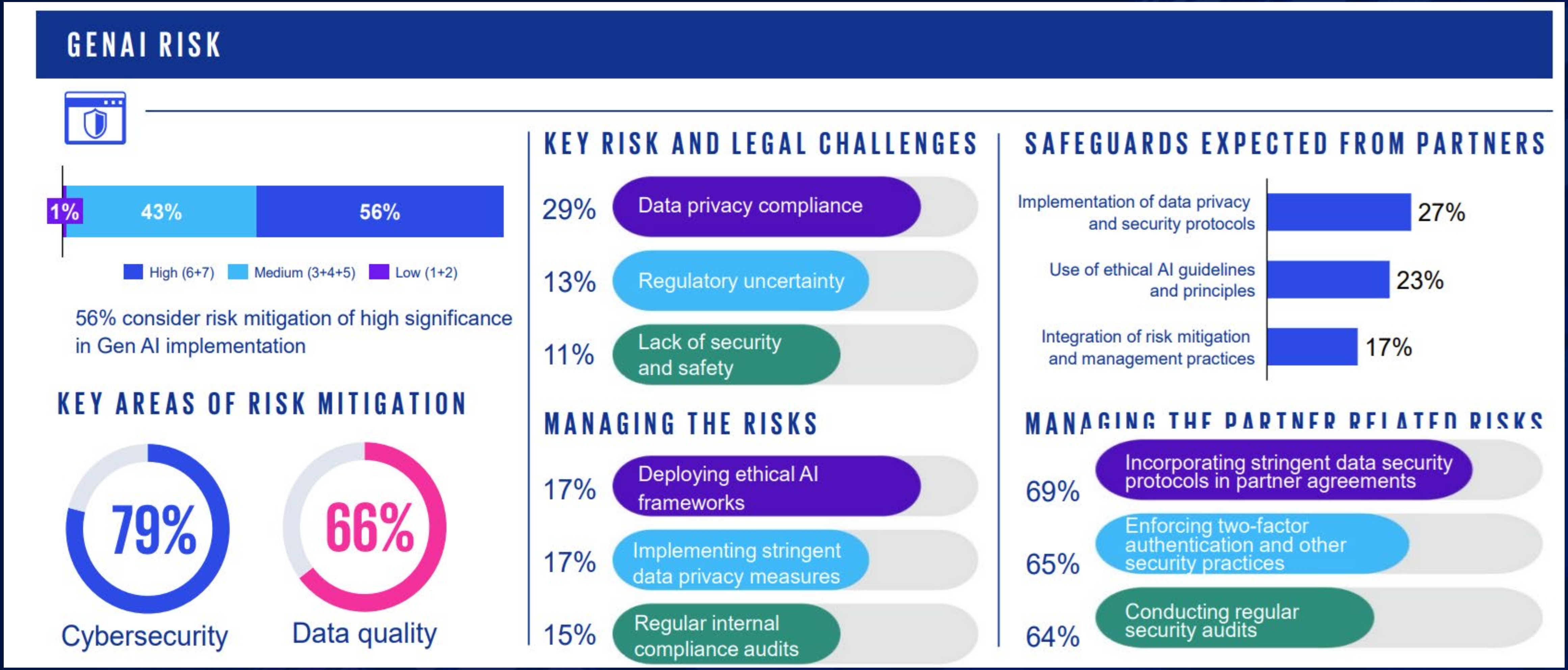
The top three spending categories projected to spend between $10- $49.9 million include:

93%

of leaders agree that investments to-date in GenAI have allowed their company to enhance its competitive position and long-term strategic performance.

Insights collected from 130 U.S.-based C-suite and business leaders in public and private organizations, annual revenue USD 1 billion or more

Gen AI risks



GENAI RISK

1% 43% 56%

High (6+7) Medium (3+4+5) Low (1+2)

56% consider risk mitigation of high significance in Gen AI implementation

KEY AREAS OF RISK MITIGATION

79% Cybersecurity

66% Data quality

KEY RISK AND LEGAL CHALLENGES

29% Data privacy compliance

13% Regulatory uncertainty

11% Lack of security and safety

MANAGING THE RISKS

17% Deploying ethical AI frameworks

17% Implementing stringent data privacy measures

15% Regular internal compliance audits

SAFEGUARDS EXPECTED FROM PARTNERS

Implementation of data privacy and security protocols 27%

Use of ethical AI guidelines and principles 23%

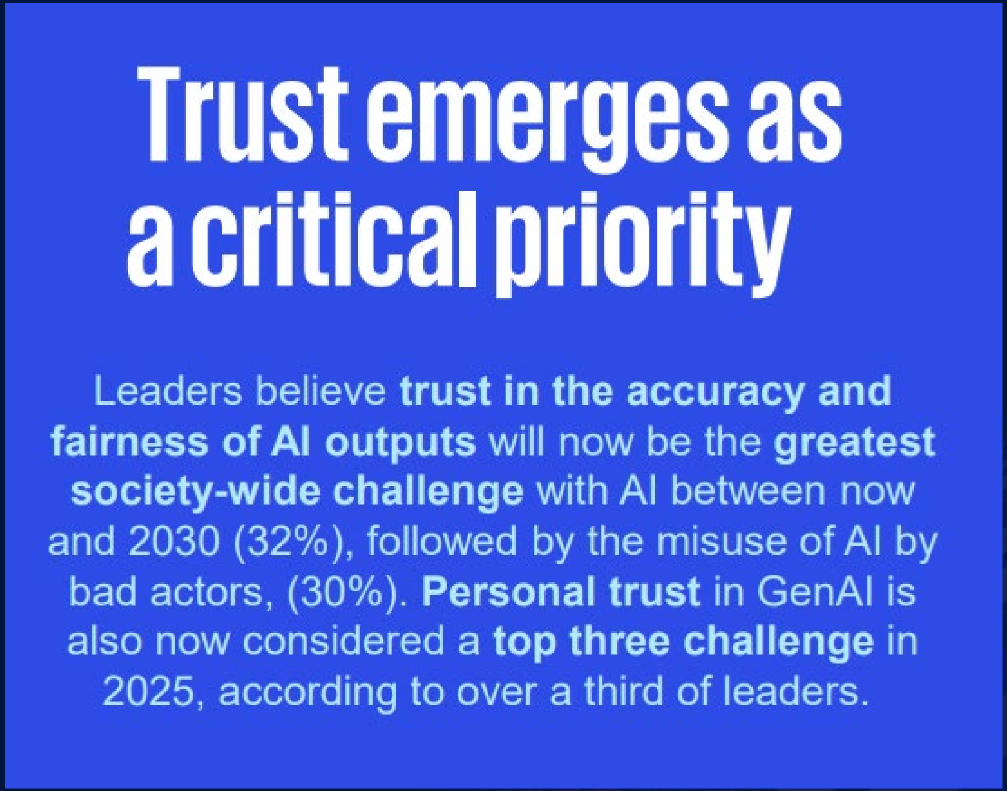
Integration of risk mitigation and management practices 17%

MANAGING THE PARTNER RELATED RISKS

69% Incorporating stringent data security protocols in partner agreements

65% Enforcing two-factor authentication and other security practices

64% Conducting regular security audits



Trust emerges as a critical priority

Leaders believe **trust in the accuracy and fairness of AI outputs** will now be the **greatest society-wide challenge** with AI between now and 2030 (32%), followed by the misuse of AI by bad actors, (30%). **Personal trust** in GenAI is also now considered a **top three challenge** in 2025, according to over a third of leaders.

Source: KPMG Q1 2025 Pulse Survey

Scaling AI has also introduced a growing number of challenges

Security and privacy

The use of generative AI poses security and privacy risks, which could result in data breaches, reputational damage or privacy regulation violations, increasing sophistication from threat actors and velocity of malware and cyber attacks.

Data quality, integrity and bias

Generative AI presents potential risks to data quality, integrity and bias. If not managed properly, it could result in inaccurate or biased outcomes, leading to legal liabilities, loss of client trust and reputational damage.

Intellectual property

Lack of legislation defining ownership of AI generated content may result in the inability to obtain copyright of content produced. Additionally, unclear terms of use may result in unintended violation of intellectual property rules.

Regulatory and professional standards

Regulators have not provided clear guidance on the use of generative AI. Navigating regulatory requirements and adhering to our professional standards may pose challenges due to unclear guidance.

Policy

Organizations must amend existing IT policies by identifying scenarios for use, aligning with data governance and ethical standards, and provide adequate training to users. Failure to do so may result in policy violations, legal liabilities and ethical concerns.

Brand and marketing

Generative AI may perpetuate or amplify existing biases in the marketing and branding, which can result in negative impact on brand image and market share. An overreliance on AI generated content may lead to a lack of creativity and originality in marketing campaigns.

Key risks and considerations presented by gen AI

Generative AI falls under the larger umbrella of AI, and therefore also inherits the risks of AI platforms that are not new to the enterprise. However, generative AI is unique in that it generates new content in forms such as text, images, audio and video. This creation of content – which can also be difficult to distinguish from human-created content – also reveals new risks and challenges.

Internal risks & considerations

Intellectual property

#Exposing IP

#Misuse of proprietary info

#Unintended leaks

Talent implications

#Talent masking

#Imposter syndrome

Inaccuracies

#False responses

#Shallow trained models

#Lack of model cards

Data quality

#Ground truth management

#Accuracy of output

#Data irrelevance

#Data sparsity

#data drift

#Data loss

#Data toxicity

#transfer learning errors

#Data governance

#Measuring inception scores

Sustainability

#Computational costs

#Energy intensiveness

#carbon reporting impacts

Data privacy

#Data breaches

#Manipulation

#Unauthroized access

#Data repurposing

#Discrimination and bias

#Unauthroized use

External risks & considerations

Misinformation & discrimination

#Harmful outputs

#Loss of control

#Hallucinations

#Bias in output

#FID scores

Infringement

#Copyright claims

#Privacy infringement

#Liability infringement

Brand reputation

#Lack of creativity

#Job displacement

#Output transparency

Cyber & adversarial threats

#Phishing scams

#Loss of control

#Deliberate manipulations

#Prompt injection

A thoughtful roll-out of generative AI will allow you to simply address the associated risks

Internal risks and considerations

1. Breaking confidentiality and intellectual property
2. Employee misuse and inaccuracies
3. Generative AI evolves
4. Talent implications

External risks and considerations

1. Misinformation, bias and discrimination
2. Copyright
3. Financial, brand and reputational risk
4. Cybersecurity
5. Adversarial attack

Breaking confidentiality and intellectual property

Many generative AI models are built to absorb user-inputted data to improve the model over time, and that could be used to **expose private or proprietary info**.

Talent implications

High-quality, **expert output can only be achieved with high-quality, expert queries**. Professionals need to be made aware that they're not just using a solution; they're training and evolving it.

Employee misuse and inaccuracies

The models generate responses based on input received, meaning there's a **risk they may provide false or malicious content**.

Generative AI evolves

As the world's understanding of AI evolve, we are already seeing a **rising number of global regulations**. It will continue to be integrated into many common applications.

Misinformation, bias and discrimination

Generative AI can be used to create **deepfake images and videos**. These images and videos often look extremely realistic and lack forensic traces left behind in edited digital media.

Copyright

Questions abound around **who owns content** once it's run through generative AI are difficult to answer.

Cybersecurity

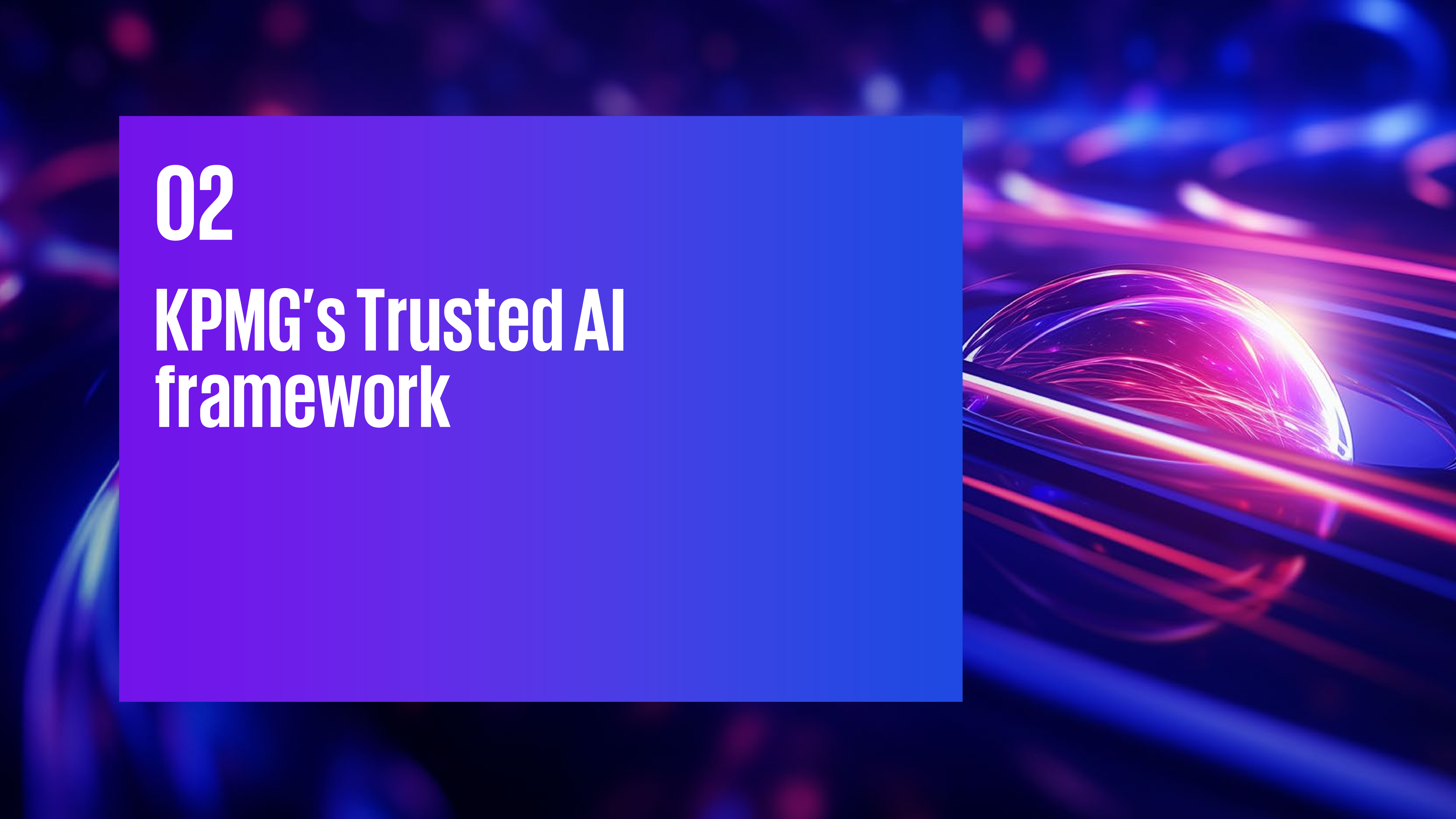
Cybercriminals can use gen AI to create more **realistic and sophisticated phishing scams** or credentials to hack into systems.

Adversarial attack

Even when trained to work within acceptable boundaries, gen AI models have proven to be vulnerable to **deliberate manipulation by sophisticated users**.

Financial, brand and reputational risk

If AI produced information were to be used into any deliverable, it **may constitute copyright or intellectual property infringement**. This could potentially cause your organization legal and reputational harm.



02

KPMG's Trusted AI framework

Trusted AI is critical

We understand trustworthy and ethical AI is a complex business, regulatory, and technical challenge, and we are committed to helping clients put it into practice. We help develop and deploy an end-to-end responsible AI program across the AI/GenAI lifecycle leveraging our Trusted AI framework.

Fairness
Design models to reduce or eliminate bias against individuals, communities or groups

Transparency
Include responsible disclosure to provide stakeholders a clear understanding as to what is happening within the AI solution and across the AI lifecycle

Explainability
Develop and deliver AI solutions in a way that answers the questions of how and why recommendations are made or conclusions drawn

Accountability
Human oversight and responsibility embedded across the AI lifecycle to manage risk and comply with regulations and applicable laws

Security
Safeguard against unauthorized access, bad actors, misinformation, corruption, or attacks

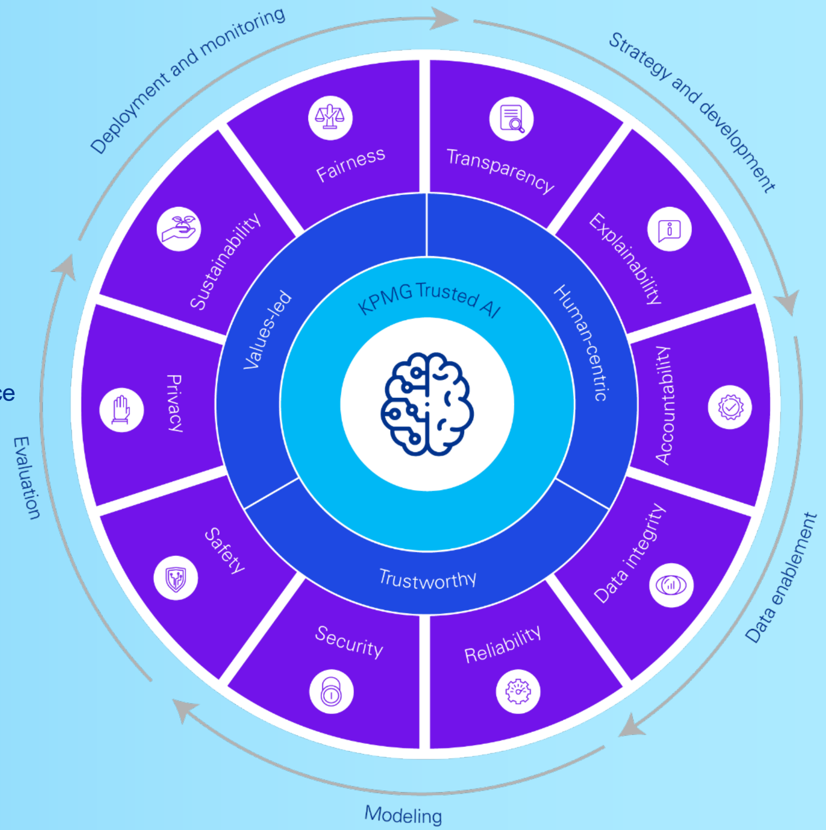
Privacy
Design AI solutions that comply with data privacy regulations and consumer data usage

Sustainability
Design AI solutions to limit negative environmental impact where possible

Data integrity
Data used in AI solutions is acquired in compliance with regulations and are assessed for accuracy, completeness and quality

Reliability
AI systems perform at the desired level of precision and consistency

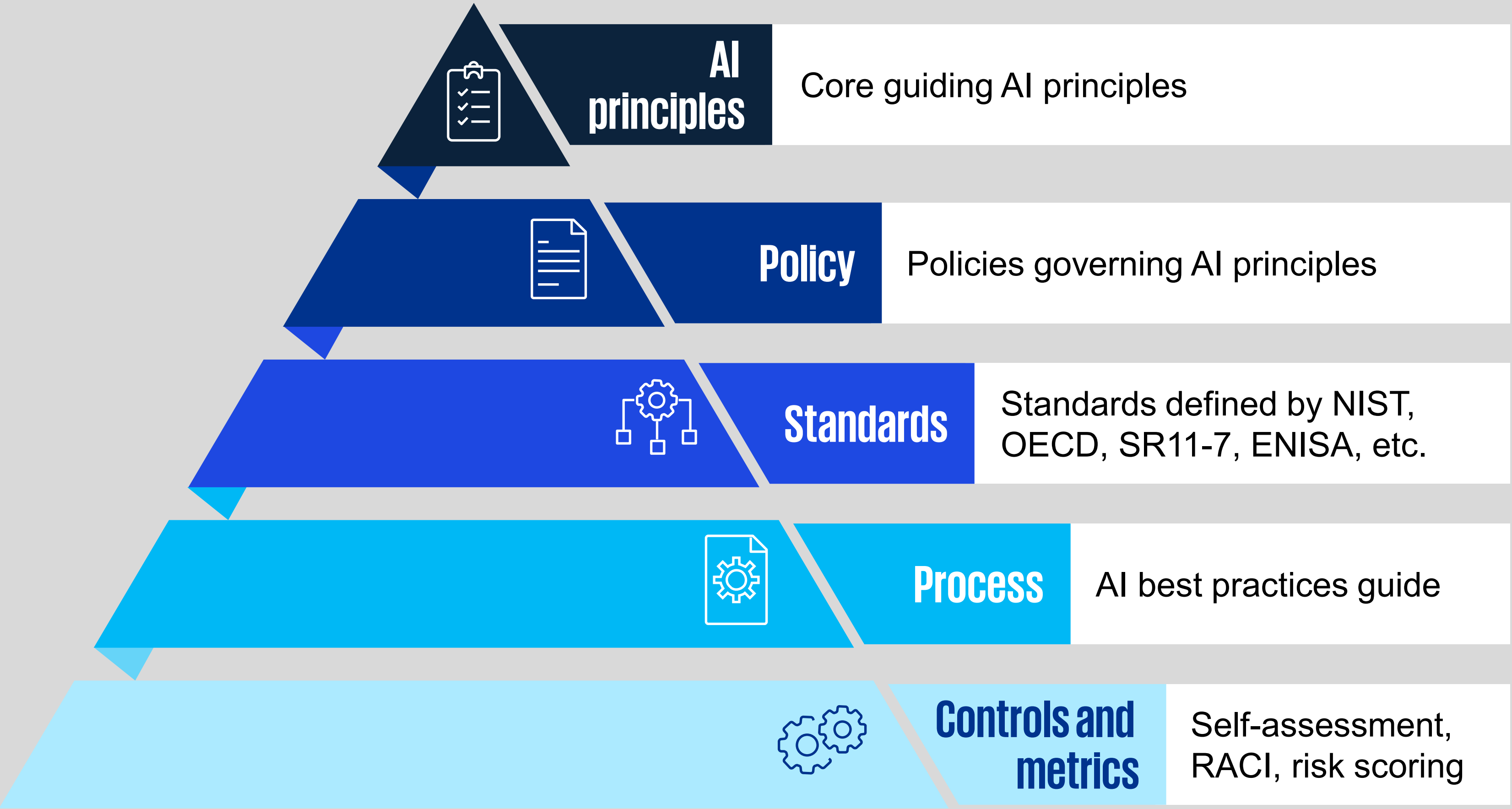
Safety
Safeguard AI solutions against harm to humans and/or property



03

Establishing effective AI governance

AI governance considerations



AI principles — Core guiding AI principles

Policy — Policies governing AI principles

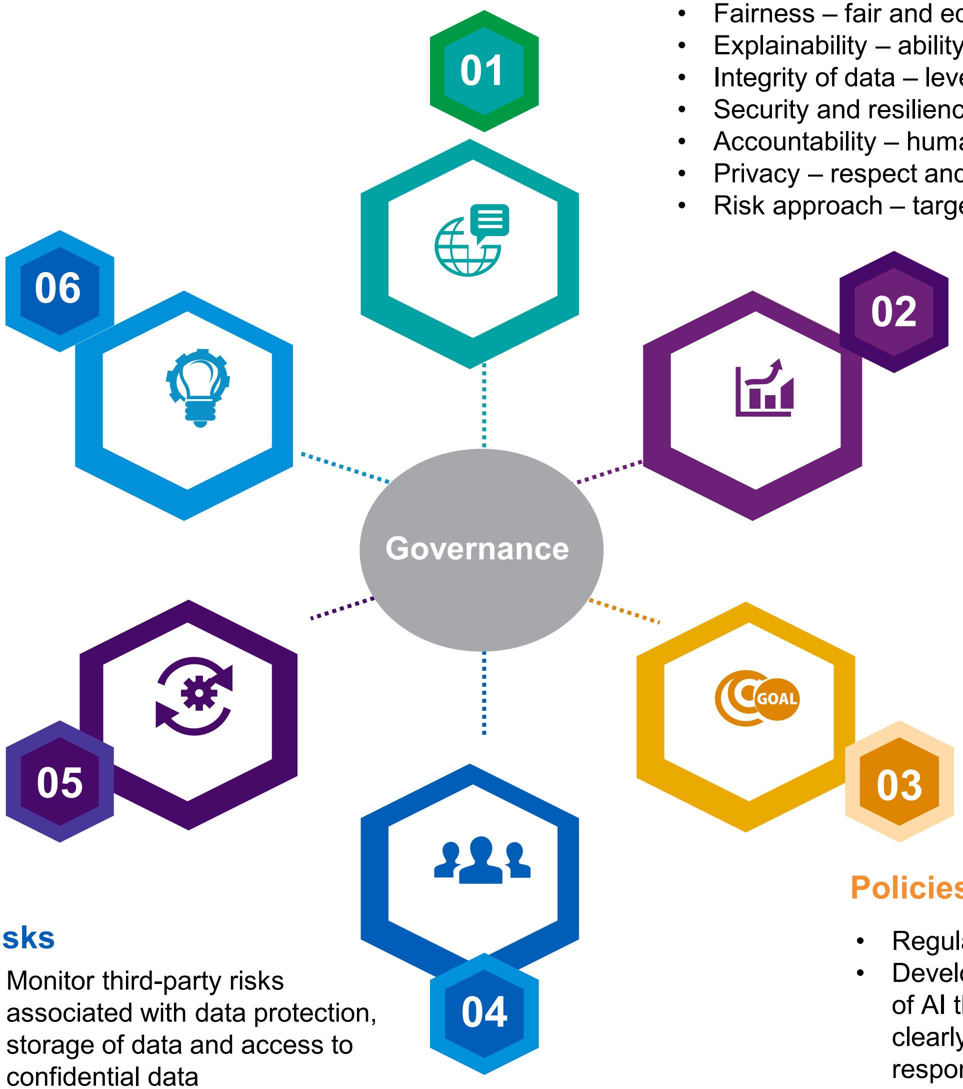
Standards — Standards defined by NIST, OECD, SR11-7, ENISA, etc.

Process — AI best practices guide

Controls and metrics — Self-assessment, RACI, risk scoring

- **Establish** your principles for AI that will guide your process in building the governance model and consider an enterprise-wide AI mission statement.
- **Reimagine** your existing governance model including your risk assessment process to uncover the risks of AI.
- Support your AI office in gathering a **diverse** group of **stakeholders** from business, technology, HR, diversity, among others.
- **Align** your AI deployments against appropriate standards and regulatory guidelines.
- **Monitor** your existing third and fourth parties to determine compliance against your responsible AI principles including existing low-risk approved vendors.

Governance



Principles

- Fairness – fair and equitable outcomes
- Explainability – ability to explain how AI outcomes were achieved
- Integrity of data – leverage high-quality, appropriate data
- Security and resiliency – design AI to operate as intended with security
- Accountability – human responsibility for AI decisions outcomes
- Privacy – respect and protect privacy rights of consumer data
- Risk approach – targeted risk identification and assessment

Strategy

- Align current vision, strategy and operating models for AI solutions

Policies/standards

- Regulatory compliance
- Develop policies that govern the use of AI throughout the organization with clearly defined roles and responsibilities
- Standards defined by NIST, ISO, OECD SR11-7

Risks

- Monitor third-party risks associated with data protection, storage of data and access to confidential data

Controls

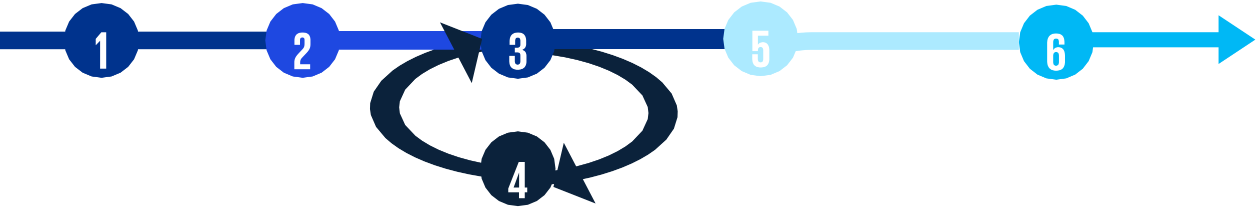
- Self-assessment, RACI, risk scoring

Training

- Enterprise-wide training – Deploy a comprehensive training program to baseline professionals across the organization on AI risks and responsible AI.
- Key skills include technical skills, analytical skills, creativity and innovation, critical thinking, interpersonal skills, and lifelong learning.

Using the AI lifecycle to responsibly control AI

By understanding what risks are relative to phases in the AI lifecycle, we can successfully mitigate AI risk by identifying the right risks at the right time. Additional factors that will influence risks include the goal and use of the AI system, learning types used, and the data that is being used.



	1. Strategy and design	2. Data gathering and exploration	3. Modeling	4. Evaluation	5. Deployment	6. Optimization
Data integrity	x	x	x	x		
Statistical validity	x	x				
Resiliency and reliability					x	x
Fairness	x	x	x	x	x	x
Model accuracy				x	x	x
Transparency	x	x	x	x	x	x
Explainability	x	x	x	x	x	x
Regulatory compliance	x	x	x	x	x	x

04

Navigating AI assurance

Technology risk universe

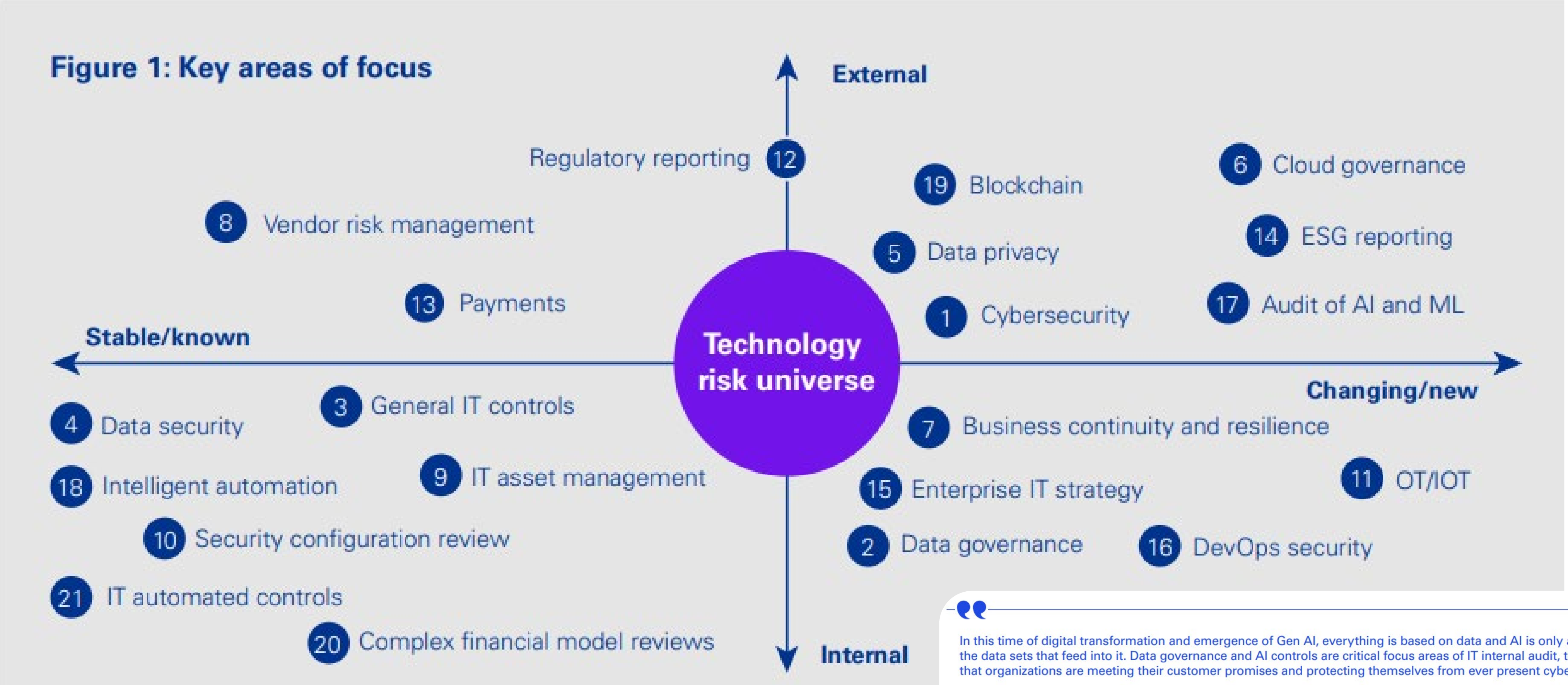


Figure 1: Key areas of focus

External

Internal

Stable/known

Changing/new

Technology risk universe

12 Regulatory reporting

8 Vendor risk management

13 Payments

19 Blockchain

5 Data privacy

1 Cybersecurity

6 Cloud governance

14 ESG reporting

17 Audit of AI and ML

4 Data security

3 General IT controls

18 Intelligent automation

9 IT asset management

10 Security configuration review

21 IT automated controls

20 Complex financial model reviews

7 Business continuity and resilience

15 Enterprise IT strategy

11 OT/IOT

2 Data governance

16 DevOps security

> In this time of digital transformation and emergence of Gen AI, everything is based on data and AI is only as good as the data sets that feed into it. Data governance and AI controls are critical focus areas of IT internal audit, to confirm that organizations are meeting their customer promises and protecting themselves from ever present cyber threats.

James Buchanan
ASPAC Head of Tech Governance and
IT Internal Audit and Partner
KPMG Australia

Ref: Trailblazing digital frontiers

How do we get started with AI auditing?

Overall strategy for AI

1. Internal auditors should begin by researching and gathering relevant information regarding **the potential use of AI** under review from multiple internal and external sources.

2. Collaborate with management in reviewing an inventory to **capture which AI is being utilized** (or planned for future use).

3. Start the process of understanding what **AI governance is in place**.

How is AI being used?

1. Internal auditors should have a discussion with the AI/data science/IT/Risk team. That discussion should include asking them to explain which **AI/algorithms have been deployed, including their function, sources of data used, use, limitations, risks and ethical implications.**

2. Internal auditors should also begin to understand what **existing controls are in place to help manage the risks posed by AI.**

3. Gaining a preliminary **understanding of the design of the controls** used to manage AI-related risk is an important step that can be performed in concert with these initial discussions.

Data and cybersecurity

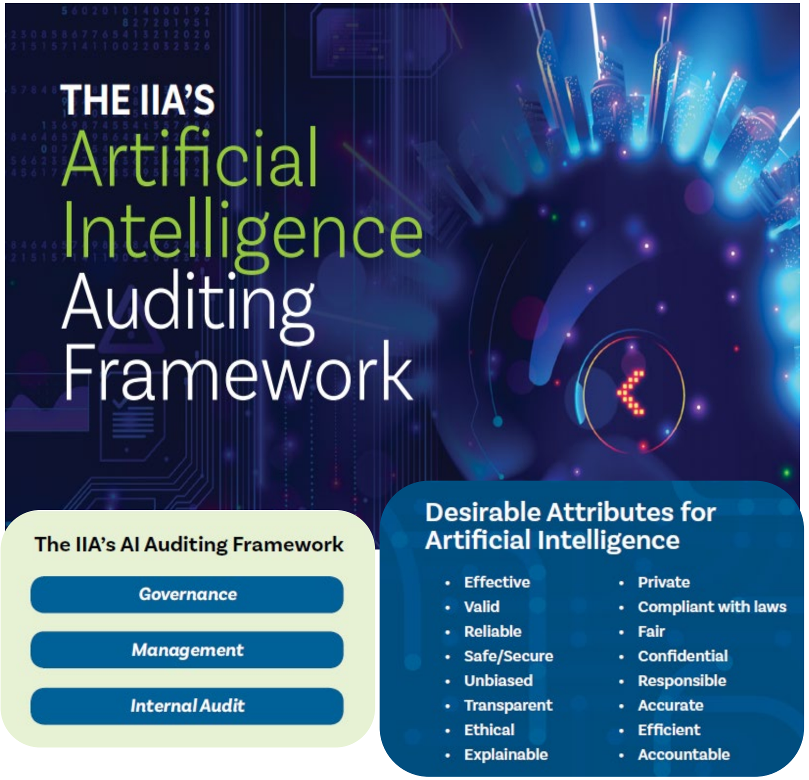
1. Internal auditors should determine **what organizational data is being used** within any given AI application and **how that data is managed.**

2. Understand **user access and who can edit or make changes to data.** Manipulating data sets from an input standpoint can impact the downstream output of AI.

3. Internal auditors need to determine where AI-reliant data is stored (internally, externally, or both) and **consider what cybersecurity controls are in place.**

4. Internal auditors must always **consider the risks related to third (and fourth) party** transactions.

AI auditing



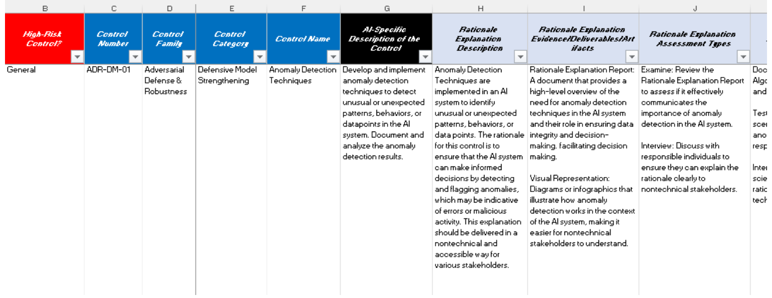
The IIA's AI Auditing Framework

- Governance
- Management
- Internal Audit

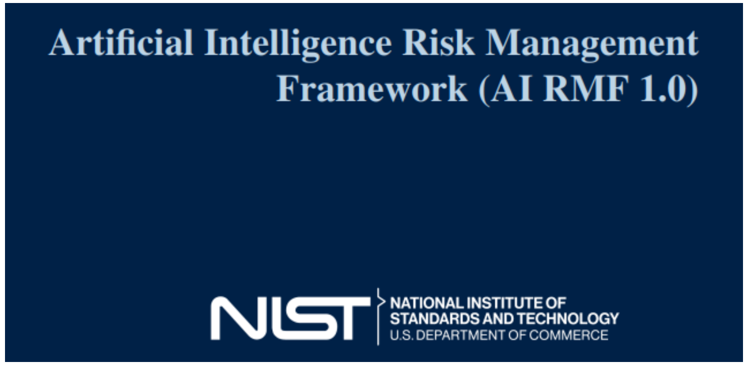
Desirable Attributes for Artificial Intelligence

- Effective
- Valid
- Reliable
- Safe/Secure
- Unbiased
- Transparent
- Ethical
- Explainable
- Private
- Compliant with laws
- Fair
- Confidential
- Responsible
- Accurate
- Efficient
- Accountable

Artificial Intelligence Audit Toolkit



B	C	D	E	F	G	H	I	J	
High-Risk Control?	Control Number	Control Family	Control Category	Control Name	AI-Specific Description of the Control	Rationale Explanation Description	Rationale Explanation Evidence/Deliverables/Artifacts	Rationale Explanation Assessment Types	
General	ADR-DM-01	Adversarial Defense & Robustness	Defensive Model Strengthening	Anomaly Detection Techniques	Develop and implement anomaly detection techniques to detect unusual or unexpected patterns, behaviors, or datapoints in the AI system. Document and analyze the anomaly detection results.	Anomaly Detection Techniques are implemented in an AI system to identify unusual or unexpected patterns, behaviors, or data points. The rationale for this control is to ensure that the AI system can make informed decisions by detecting and flagging anomalies, which may be indicative of errors or malicious activity. This explanation should be delivered in a nontechnical and accessible way for various stakeholders.	Rationale Explanation Report: A document that provides a high-level overview of the need for anomaly detection techniques in the AI system and their role in ensuring data integrity and decision-making. facilitating decision making. Visual Representation: Diagrams or infographics that illustrate how anomaly detection works in the context of the AI system, making it easier for nontechnical stakeholders to understand.	Examine: Review the Rationale Explanation Report to assess if it effectively communicates the importance of anomaly detection in the AI system. Interview: Discuss with responsible individuals to ensure they can explain the rationale clearly to nontechnical stakeholders.	Doc Algo and Test scen ano resp Inter scie ratic tech


Artificial Intelligence Risk Management Framework (AI RMF 1.0)
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

AI auditing to support Trusted AI

	Governance	Management			
		Risk management	Data	AI management	Cybersecurity
	• evaluating **how well the organization is managing AI operations** (direct, manage, and monitor), and • whether the organization's **AI strategic goals and objectives are being achieved** in a manner that is consistent with established values.	The importance of identifying **AI risks related to security, integrity, privacy and confidentiality of data**, and addressing these concerns should be a focus as the organization executes AI projects.	Determining what organizational data is being used within any given AI application and **how that data is managed is critical.**	Involves **comprehensive and responsible management of AI systems throughout their entire life cycle** — from development to deployment, operation and maintenance.	Cybersecurity must also be considered as it relates to **restricting unauthorized users from accessing data and safeguarding privacy, confidentiality, and protection of data.**
Internal audit	• Governance and strategy • Ethical AI governance and accountability	• Asset management • Risk management	• AI data privacy and rights • Data protection • User privacy, engagement and protection	• AI life cycle management • AI model governance • AI bias mitigation & fairness • AI operations • Legal, regulatory and AI-prohibited use cases • External components and supply chain governance • Human-AI interaction and experience • Training and awareness	• AI ecosystem security • Identity and access management • Secure systems design and development • Adversarial defense and robustness • Incident management • Business continuity

Our Trusted AI thought leadership

Staying up-to-date on all things Trusted AI is no small feat, that is why we've collected some of our top global thought leadership pieces around AI for you.

KPMG | Reality Defender

Deepfakes:
Real threat

As artificial intelligence grows ever more powerful and sophisticated, it has become easier to create fake content than detect it.

KPMG

Governing
AI responsibly

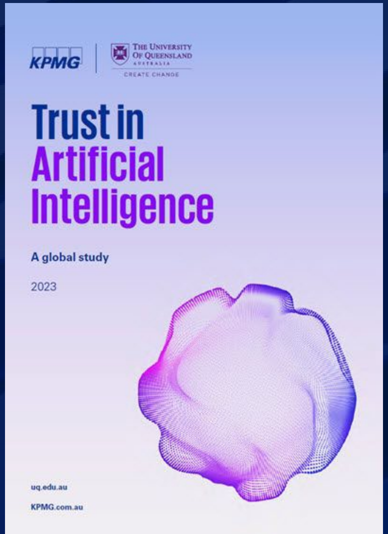
Building an integrated AI governance model

KPMG

Privacy in the
new world of AI

How to build trust in AI through privacy.

KPMG International | kpmg.com/privacyservices


KPMG | The University Of Queensland Australia Create Change

Trust in
Artificial
Intelligence

A global study

2023

uq.edu.au

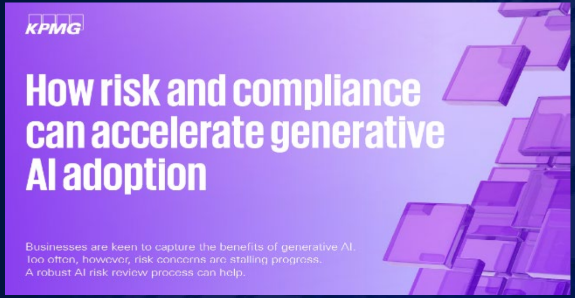
KPMG.com.au

KPMG

Responsible AI and the
challenge of AI risk

Insights from the 2023 KPMG US AI Risk Survey Report

Learn more >


KPMG

How risk and compliance
can accelerate generative
AI adoption

Businesses are keen to capture the benefits of generative AI.
Too often, however, risk concerns are stalling progress.
A robust AI risk review process can help.

KPMG

The impact of
the Artificial
Intelligence Act

A deep dive into the world's first harmonized legal framework for trustworthy AI

KPMG

Where will AI/GenAI
regulations go?

Demonstrating 'trusted AI systems'

November 2023

KPMG

Game
changer:

The startling power generative AI is bringing to software development

KPMG

Generative AI
Adoption Index
Executive Summary

Additional resources:
KPMG Trusted AI

Key takeaways

As AI continues to evolve rapidly, organizations have a responsibility to design, develop, and deploy it in a responsible and ethical manner, ensuring its use inspires trust and confidence.

As the GRC landscape continues to evolve, AI is emerging as a key driver in transforming how organizations manage risk, ensure compliance, and uphold governance standards with skilled professionals empowered to use AI responsibly and ethically.

Building trust in AI requires effective governance, which includes clear accountability and ongoing monitoring.

AI auditing ensures trusted AI by reviewing the overall AI strategy, understanding its usage, and assessing data integrity and cybersecurity risks using established best practices.

KPMG in Thailand
48th-50th Floor, Empire Tower
1 South Sathorn Road
Bangkok 10120
T: +66 2677 2000

KPMG in Thailand

kpmg.com/th

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Document Classification: KPMG Public