

Generative AI Risk in Healthcare

November 2023

1

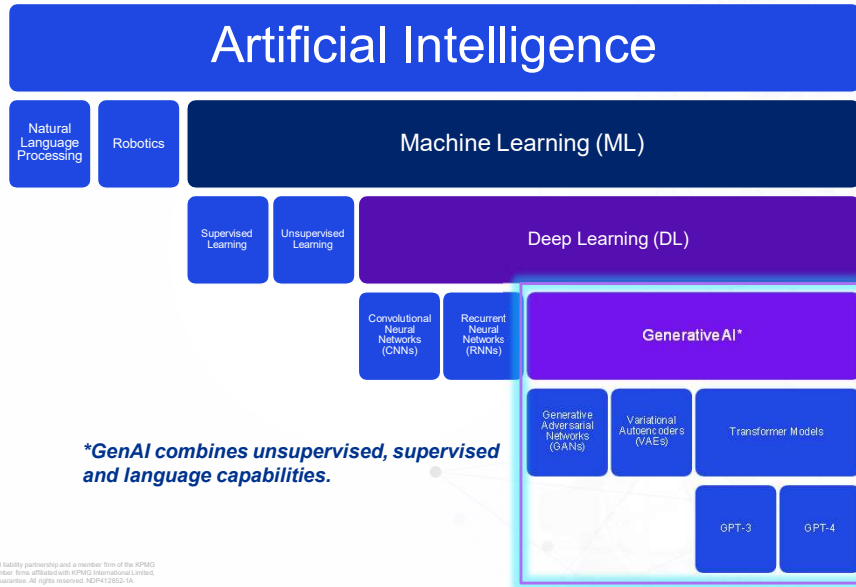
Real world examples of AI failures



2

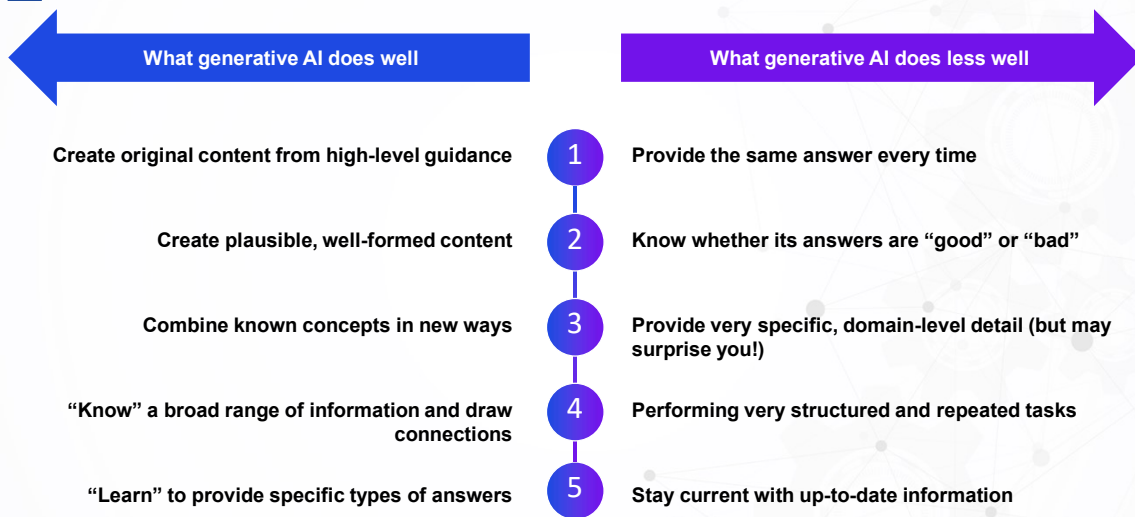
Level set on terminology before we go on

“AI” is an umbrella term that encompasses different techniques



© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. KPMG12852-1A

Generative AI strengths and trade-offs



© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. KPMG12852-1A

KPMG Advisory GPT: Live Demo

The screenshot displays the KPMG Advisory GPT interface. At the top, it identifies the chat model as GPT-3.5 Turbo. The user's input is: "I have a 48 year old male patient with blood pressure of 150/90 and chest pain- what could it be". The AI response lists several potential causes for chest pain and high blood pressure in a 48-year-old male patient:

- 1. Coronary artery disease (CAD): Chest pain is a common symptom of CAD, which occurs when the heart's blood vessels become narrowed or blocked due to plaque buildup.
- 2. Hypertension: High blood pressure can damage blood vessels and organs over time, leading to chest pain.
- 3. Aortic dissection: This is a medical emergency that occurs when the wall of the aorta tears, leading to a sudden onset of severe chest pain.
- 4. Pulmonary embolism: This is a condition in which a blood clot travels to the lung, causing chest pain and difficulty breathing.
- 5. Pneumonia or pleurisy: These respiratory infections can cause chest pain, particularly during deep breathing or coughing.
- 6. Gastroesophageal reflux disease (GERD): Acid reflux from the stomach can cause a burning sensation in the chest.

The AI concludes by stating: "It is important for the patient to seek immediate medical attention to determine the cause of their symptoms and receive appropriate treatment." The user then adds: "he also has swollen fingers". The AI response indicates: "Swollen fingers along with chest pain and high blood pressure in a middle-aged man could be a sign of several underlying medical conditions, including:". Below the response is a "Regenerate Response" button and an input field labeled "Ask Advisory GPT*". A disclaimer at the bottom reads: "Please use your skepticism and professional judgement when using results from this tool in any deliverable." The interface includes a sidebar with "Support", "Settings", and "Submit Feedback" options, and a Windows taskbar at the bottom.

5



6

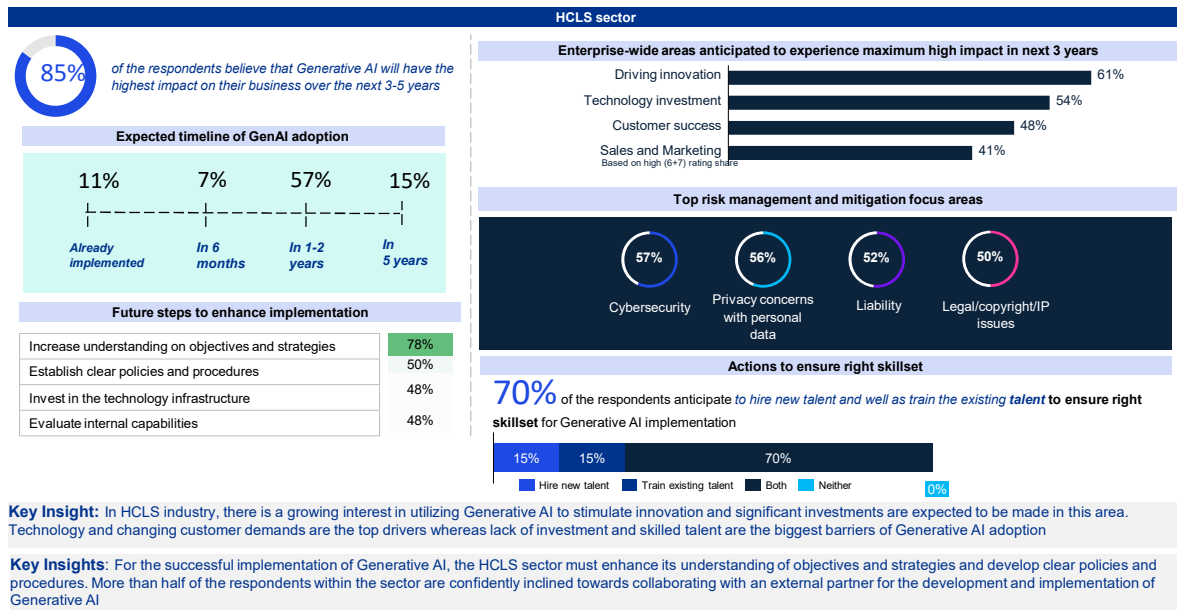
Perceptions on Generative AI are Evolving



KPMG CEO Outlook survey findings – AI data points

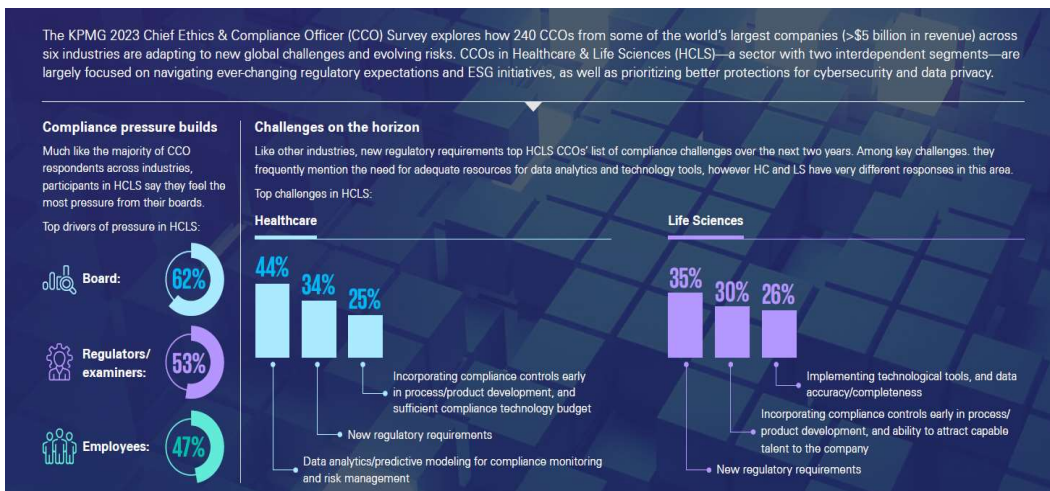
- 62% of HCLS CEOs agree or strongly agree that generative AI is a top investment priority for their organization, despite ongoing economic uncertainty.
- 21% of HCLS CEOs consider increased profitability as the top benefit of implementing generative AI in their organization, while 19% said it would increase efficiency and productivity by automating routine operations.
- When asked to indicate the degree in which technical capability presents a challenge when it comes to implementing the use of generative AI in their organization, 48% of HCLS CEOs said very or mostly challenging.
- 69% of HCLS CEOs agree that the lack of current regulations and direction for generative AI within their industry will be a barrier to their organization's success.
- 46% of HCLS CEOs anticipate that it will take 3-5 years to see a return on their investment in the implementation of generative AI.
- 76% of HCLS CEOs agree that generative AI is a double-edged sword in that it may aid in the detection of cyber-attacks but also provide new attack strategies for adversaries.

AI survey – Focused Executive Summary



9

KPMG 2023 CCO Survey – HCLS Segment

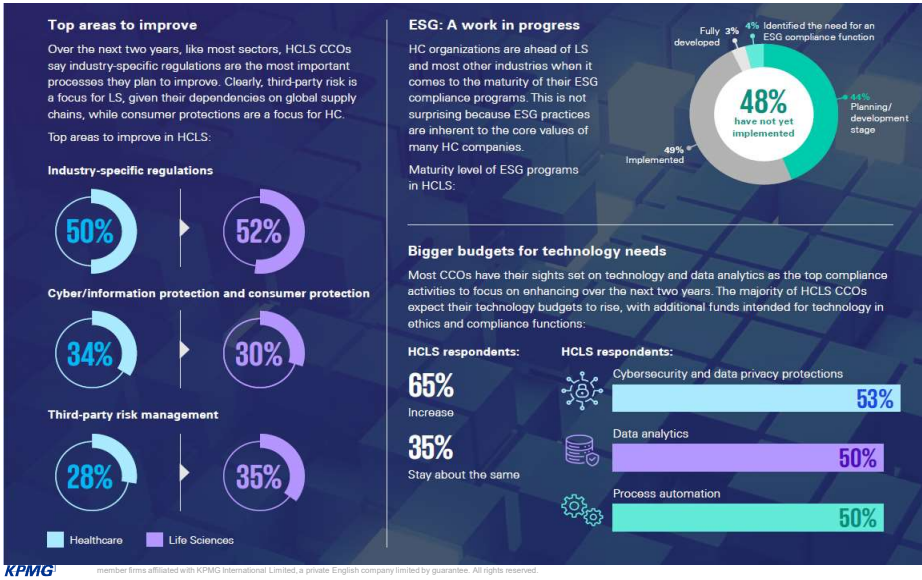


© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

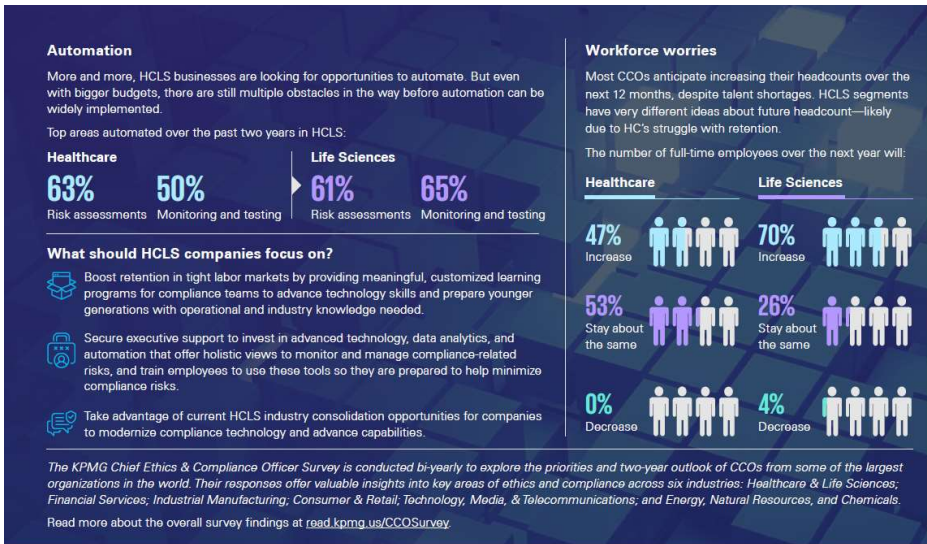
10

10

KPMG 2023 CCO Survey – HCLS Segment



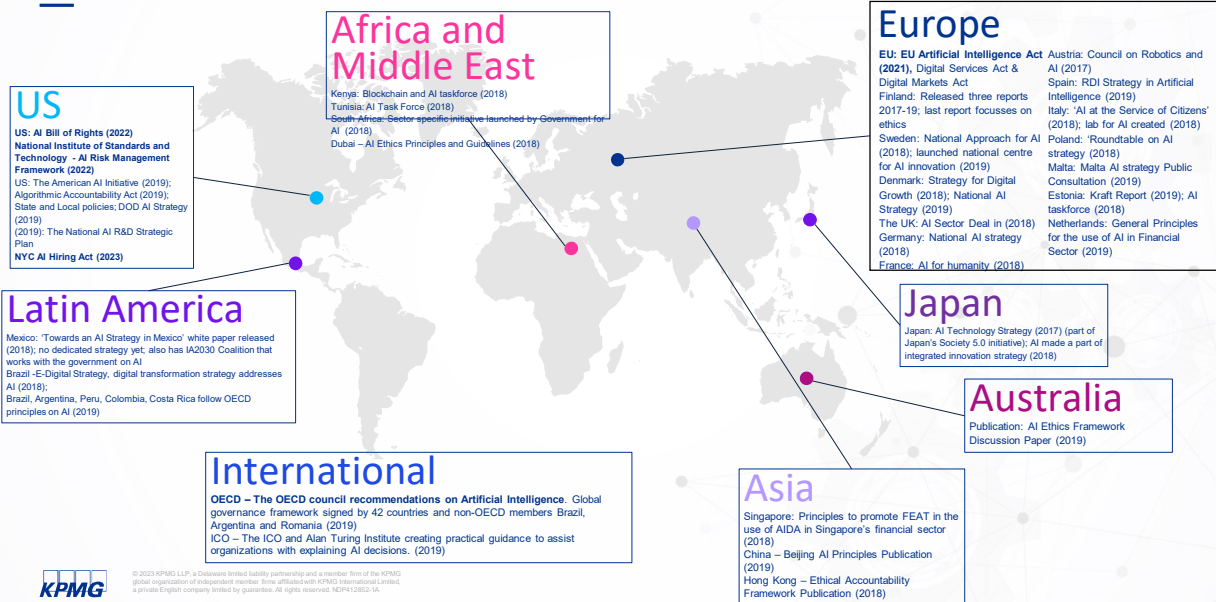
KPMG 2023 CCO Survey – HCLS Segment



Trusted AI Framework

13

Rising global regulatory guidelines for AI



14

Available AI frameworks

ISO



ISO/IEC DIS 42001
 Source: International Organization for Standardization⁴
 Release: November 2022
42001 provides requirements for establishing, implementing, maintaining and continuously improving an AI risk management system within the context of an organization.

ENISA



ENISA: Secure ML Guidelines
 Source: European Union Agency for Cybersecurity⁵
 Release: December 2021
 Based on a systematic review of relevant literature on machine learning, **ENISA provides a taxonomy for machine learning algorithms**, which highlights core functionalities across critical stages.
 ENISA then analyzes threats targeting machine learning systems, and present mainstream **security controls** that can effectively **detect, deter and mitigate harms** from identified threats.

NIST



NIST: AI RMF
 Source: National Institute of Standards and Technology⁶
 Release: January 2023
 The Core of the NIST RMF comprises four functions: **GOVERN, MAP, MEASURE, and MANAGE**. These functions can be applied in different contexts and at different stages of the AI lifecycle.

OECD



OECD: AI System Classification
 Source: Organization for Economic Co-operation and Development⁷
 Release: February 2022
 OECD allows users to zoom in on specific risks associated with AI and facilitates nuanced and precise policy debate to identify features of AI systems that matter most, helping facilitate **global consistency and interoperability in incident reporting**.

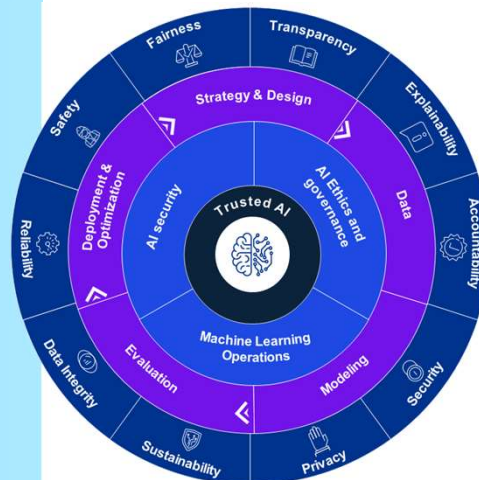


© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. KPMG LLP, CA.

Trusted AI is critical

We understand trustworthy & 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 Trusted AI program across the AI/ML lifecycle



- Fairness**
 Ensure models 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**
 Ensure AI solutions are understandable as to how and why recommendations are made or conclusions drawn.
- Accountability**
 Human oversight and responsibility embedded across the AI lifecycle to manage risk and ensure compliance with regulations and applicable laws.
- Security**
 Safeguard against unauthorized access, bad actors, misinformation, corruption, or attacks.
- Privacy**
 Ensure compliance with data privacy regulations and consumer data usage.
- Sustainability**
 Optimize AI solutions to limit negative environmental impact where possible.
- Data integrity**
 Ensure data quality, governance, and enrichment steps embed trust.
- Reliability**
 Ensure AI systems perform at the desired level of precision and consistency.
- Safety**
 Safeguard AI solutions against harm to humans and/or property.



© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Managing it all

Managing risk associated with the design, development, deployment and management of AI solutions will require an understanding of each AI deployment; adapting legacy risk frameworks to embrace and incorporate emerging AI tools and trends; and adapting risk mindset with a focus toward monitoring outcomes, identifying model risk threats, and overall model risk management. To do this, the following are four pillars and representative actions Risk organizations should be focused on today:



Establish Governance

- Establish AI governance framework
- Develop policies that govern the use of AI throughout the organization with clearly defined roles and responsibilities
- Educate stakeholders on the use of AI, emerging risks around AI, and appropriate use policies
- Establish transparency principles and policies
- Incorporate AI into model risk management (MRM) framework including areas such as approved use, ongoing monitoring, and risk ratings
- Establish protocols for AI modeling usage, including business decisions vs experimental (Internal deployments), that align to MRM standards



Compliance and Legal Risk

- Monitor AI regulatory developments
- Ensure appropriate stakeholder groups are implementing requirements and/or controls
- Align AI deployments and governance standards with appropriate regulatory guidelines and requirements
- Validate oversight of enterprise AI use and deployment standards
- Establish consistent contracting and AI deployment requirements for 3rd parties
- Ensure a mechanism has been established to identify, report, and manage AI vulnerabilities
- Assess ethical or societal impacts of planned AI usage
- Monitor legal considerations of external facing deployments



Understand AI Strategy and Roadmap

- Align current vision, strategy, and operating model for AI solutions
- Assess Board level oversight
- Inventory AI landscape within your organization, along with planned use cases, models, and tools.
- Ensure the use cases and vendor landscape for each AI solution are clearly understood
- Monitor 3rd party risks associated with data protection, storage of data, and access to confidential data
- Evaluate software tools that are being acquired to monitor ongoing data and AI pipeline security and privacy concerns (including poison and drift)
- Incorporate AI assessment into annual risk assessment process



Monitor Usage and Deployments

- Perform AI risk assessments around areas such as compliance, governance, security, fairness, bias, accuracy, and explainability
- Assess access, API/interface, data security, privacy and change management controls specific to AI deployments
- Evaluate AI testing, training and deployment standards
- Assess financial reporting impact
- Identify KPIs to monitor AI outcomes, as well as detect anomalies, fraud, data poisoning
- Assess AI solution resiliency and reliability



© 2023 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Viewpoint from Industry

Q&A with:
Mark Johnson, CISO
Hackensack Meridian Health



Thank you!

Contact us

Jaime Pego
Healthcare Risk Leader

T +1 908 416 1662
jpego@kpmg.com

Wontae Kim
Technology Risk

T +1 415 710 7179
wontaekim@kpmg.com



© 2020 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. [Printed in the US]. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.