# AI Governance

**Accelerate value with confidence.**

**October 2023**

# Agenda

**01** Survey results

**02** What are regulations telling us

**03** AI Governance

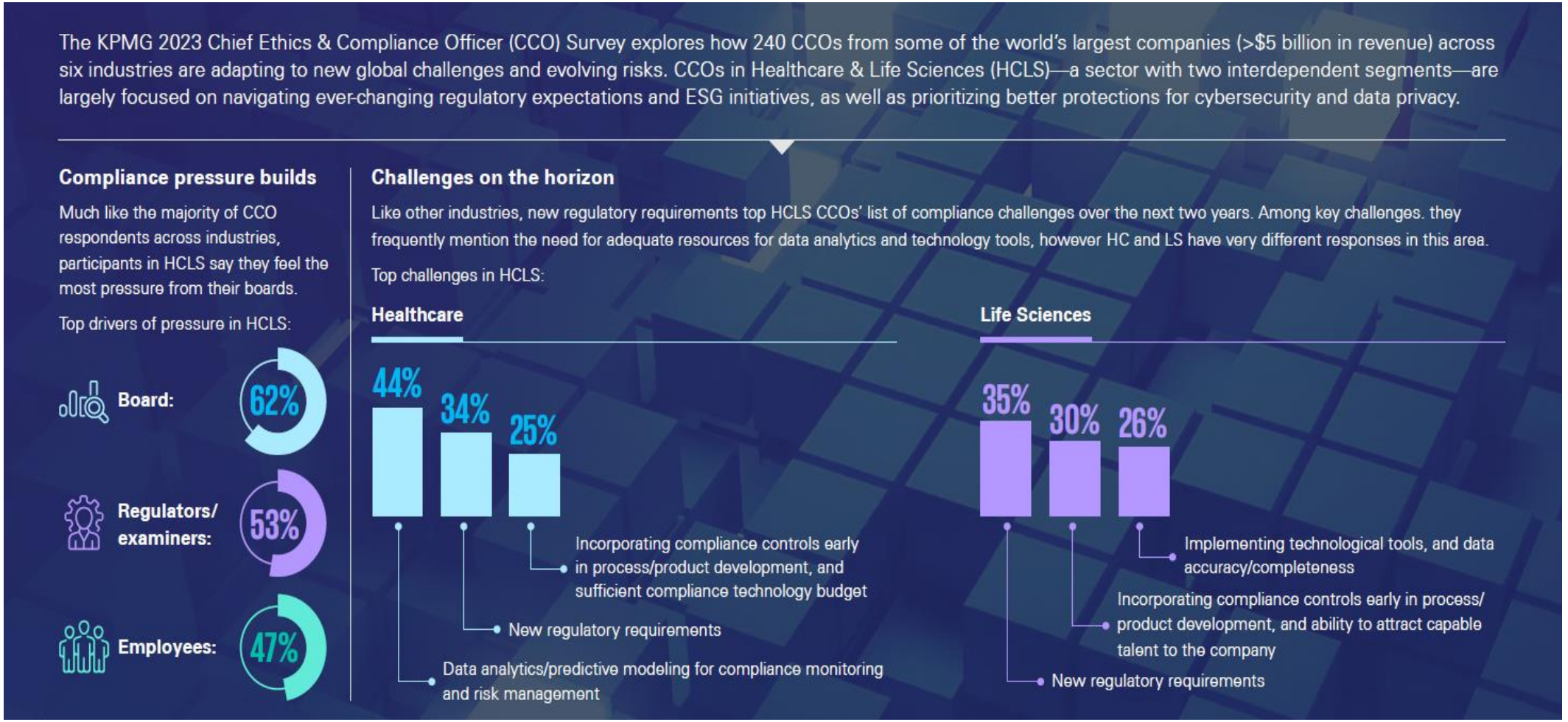
**04** Where do we go from here?

# Survey Results

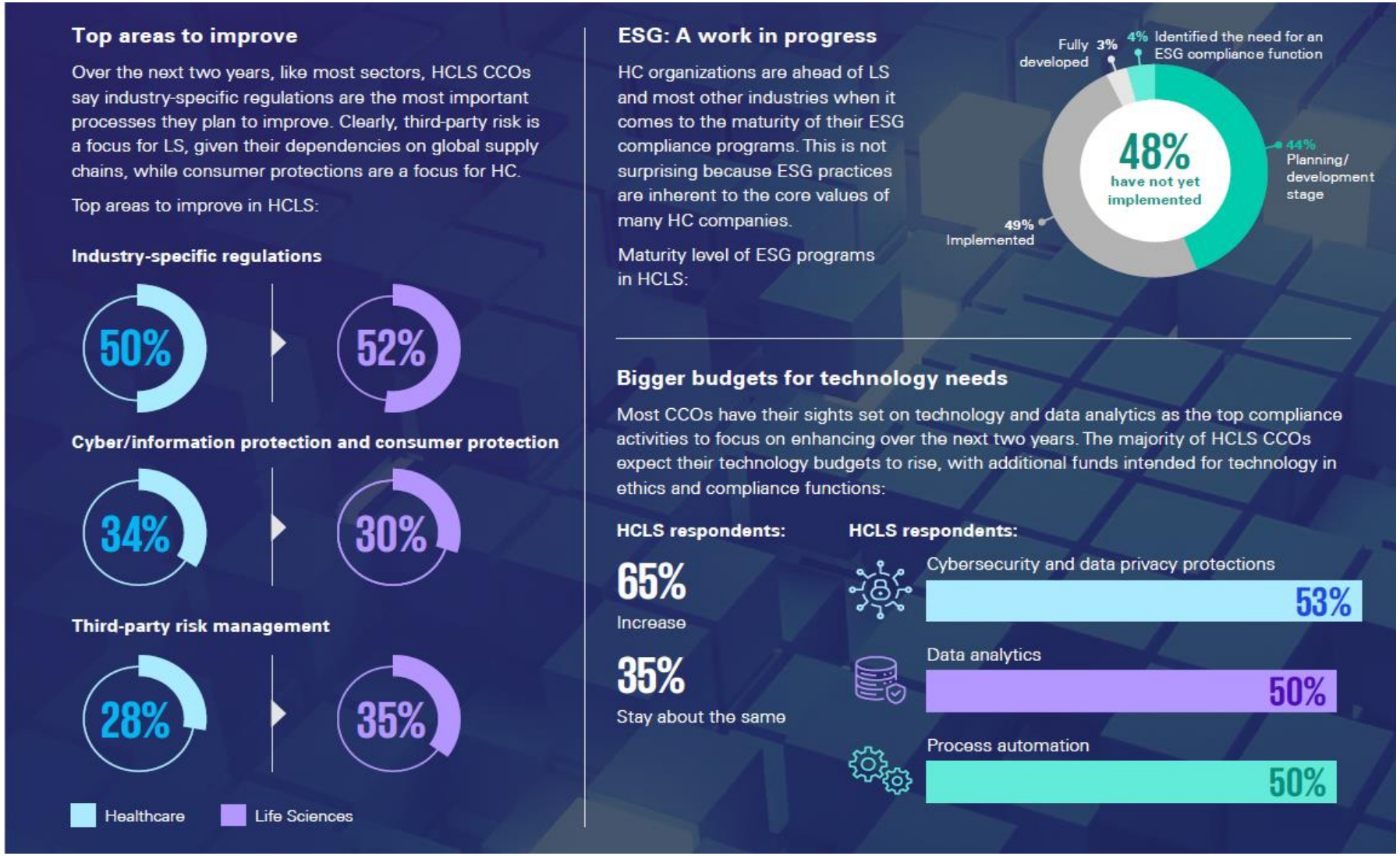
# KPMG CEO Outlook survey findings – AI data points

- 62% of life sciences CEOs agree or strongly agree that generative AI is a top investment priority for their organization, despite ongoing economic uncertainty.
- 21% of life sciences 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 life sciences CEOs said very or mostly challenging.
- 69% of life sciences 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 life sciences CEOs anticipate that it will take 3-5 years to see a return on their investment in the implementation of generative AI.
- 76% of life sciences 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.

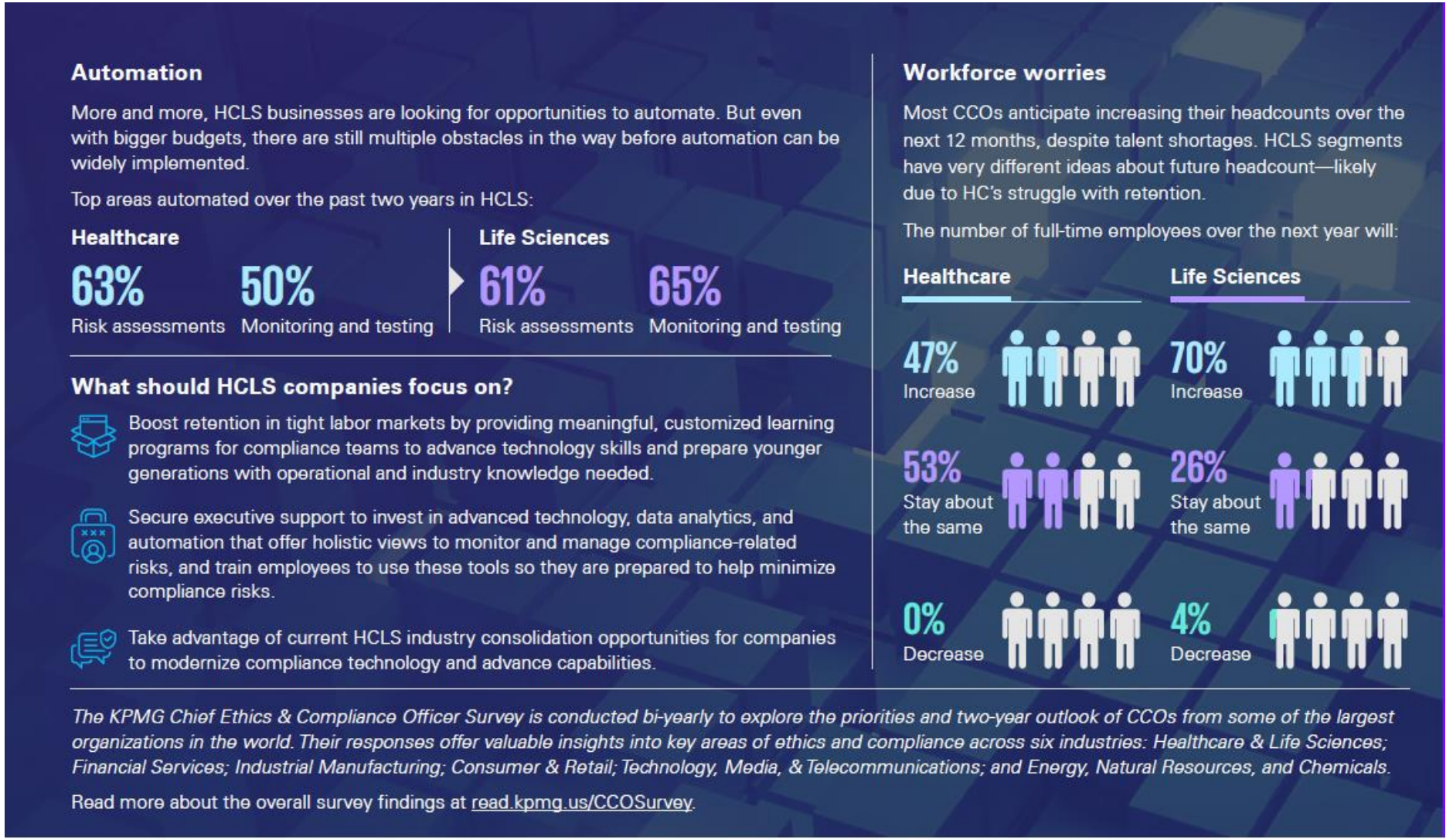
# KPMG 2023 CCO Survey – HCLS Segment



# KPMG 2023 CCO Survey – HCLS Segment

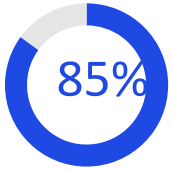


# KPMG 2023 CCO Survey – HCLS Segment



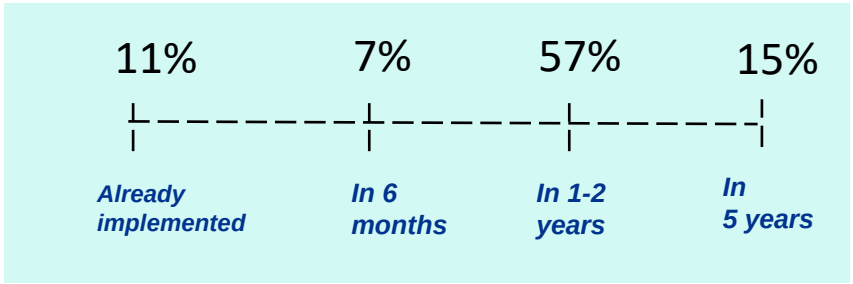
# AI survey – Focused Executive Summary

## HCLS sector




*of the respondents believe that Generative AI will have the highest impact on their business over the next 3-5 years*

### Expected timeline of GenAI adoption




### Future steps to enhance implementation

| | |
|---|---|
| Increase understanding on objectives and strategies | 78% |
| Establish clear policies and procedures | 50% |
| Invest in the technology infrastructure | 48% |
| Evaluate internal capabilities | 48% |

### Enterprise-wide areas anticipated to experience maximum high impact in next 3 years


### Top risk management and mitigation focus areas


### Actions to ensure right skillset

**70%** of the respondents anticipate *to hire new talent and well as train the existing **talent*** **to ensure right skillset** for Generative AI implementation


**Key Insight:** In HCLS industry, there is a growing interest in utilizing Generative AI to stimulate innovation and significant investments are expected to be made in this area. Technology and changing customer demands are the top drivers whereas lack of investment and skilled talent are the biggest barriers of Generative AI adoption

**Key Insights**: For the successful implementation of Generative AI, the HCLS sector must enhance its understanding of objectives and strategies and develop clear policies and procedures. More than half of the respondents within the sector are confidently inclined towards collaborating with an external partner for the development and implementation of Generative AI

# Gen AI Use- Case Prioritization and Pr

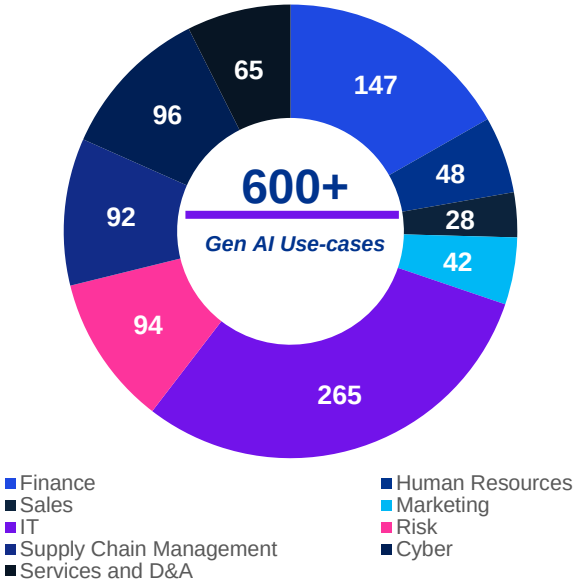
**Total Aggregate Industry Gen AI Opportunity: $5B**

## Key Takeaways

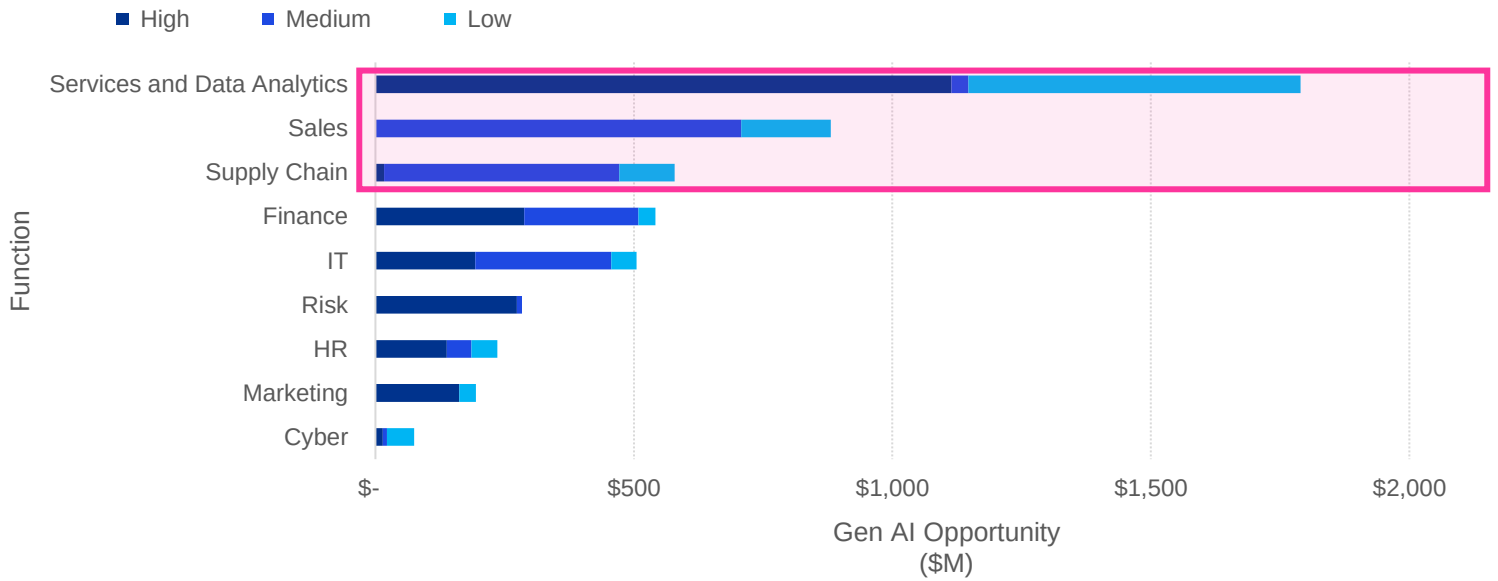
- KPMG has built a proprietary registry of 600+ Gen AI specific use-cases, that can be categorized into 9 functions. . Thus, enabling more efficient and effective development, implementation, and evaluation of AI-based applications.
- Investments in Gen AI enabling technology have the potential to unlock approximately $5B in obtainable Gen AI value. Service and data analytics, sales, and supply chain are the key functions with the highest potential to leverage Gen AI for value generation. These key functions feature a mix of high, moderate, and low-impact use cases, resulting in an estimated opportunity growth of around $3B for the Life Science industry

## Analytics

Total Use Cases




Use-case Prioritization & Opportunity Value by Function




- ***Value Levers Definition:*** *Growth refers to increases in the organizations ability to increase market opportunity using generative AI, Productivity refers to opportunities for the organization to do more with less, often thought of as cost takeout*
- *All peers chosen can be found on slide 10 in more detail*

# Service and Data Analytics Gen AI Functional Use Cases

## High Impact Use-case Examples

### Regulatory Compliance Risk Analysis

Generate insights into potential regulatory compliance risks and recommend mitigation strategies

### Training Material Generation

Generate personalized training materials based on employee roles and learning needs

### Data Visualization

Generate interactive and visually appealing data visualizations for effective data exploration and analysis

### Data Compression

Generate algorithms and methods to compress and optimize data storage, transmission, or processing

### Data Analysis

Large language models can be used to analyze large datasets related to Quote to Cash processes and identify patterns and trends, providing valuable insights that can be used to optimize financial operations

### Customer Sentiment Analysis

Generate synthetic data to analyze customer feedback and sentiment, allowing retailers to improve product offerings and customer experience.

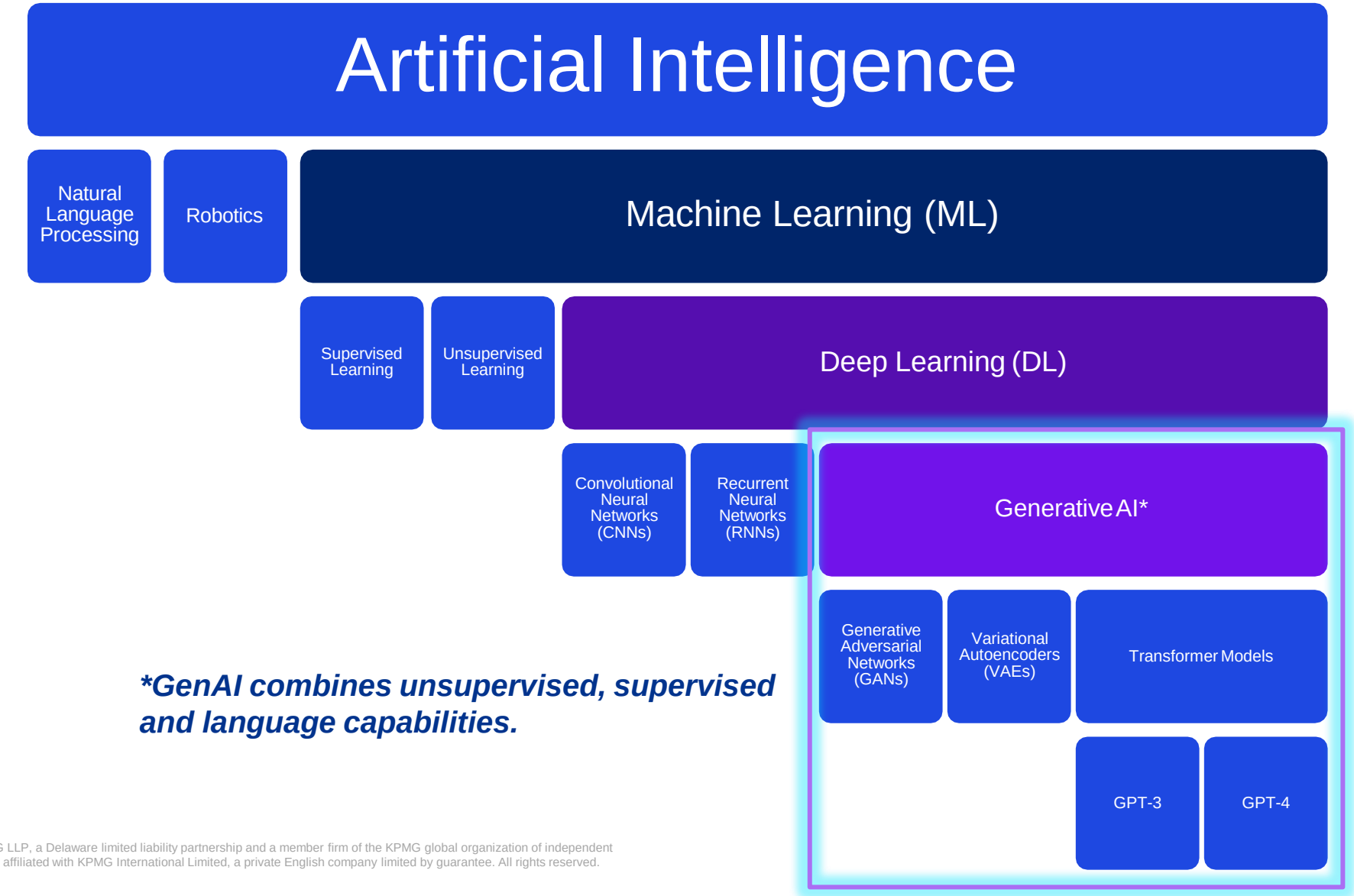
### Predictive Customer Service

Generate predictions on customer service needs and issues, allowing proactive resolution and support

# What are we learning from regulations

# Level set on terminology before we go on

"AI" is an umbrella term that encompasses different techniques




***GenAI combines unsupervised, supervised and language capabilities.***

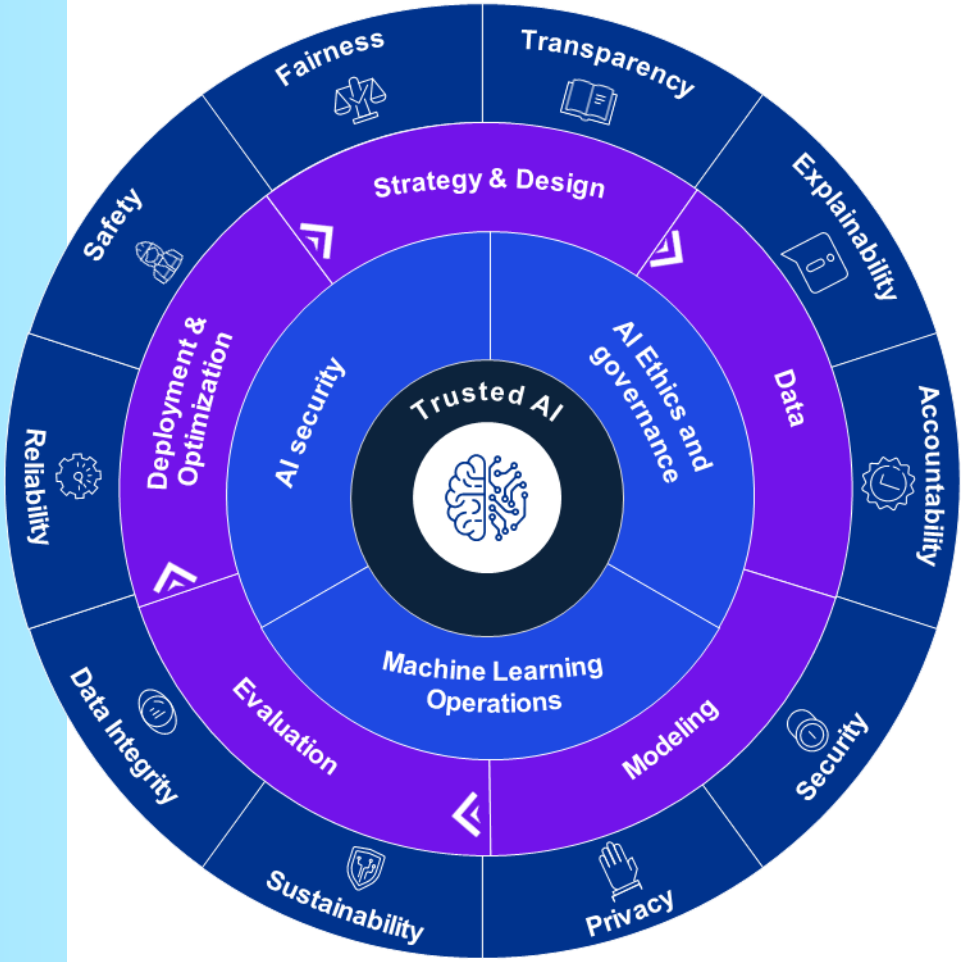
# Leading global regulation on AI and what it tells us to focus on

| Core Governance Principle | Fairness | Explainability | Integrity of Data | Security & Resiliency | Accountability | Privacy | Risk Approach |
|---|---|---|---|---|---|---|---|
| Description of Principle | Fair and equitable outcomes across different groups | Ability to explain how AI outcomes were achieved | Leverage high-quality, appropriate data with lineage | Design AI to operate as intended with security | Human responsibility for AI decisions outcomes | Respect and protect privacy rights of consumer data | Targeted risk identification and assessment |
| **Global Regulatory Guidance** | | | | | | | |
| United States — National AI Initiative Act | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| United States — AI in Government | ✓ | | ✓ | ✓ | ✓ | | |
| United States — The National AI Research Resource Task Force | | | | ✓ | ✓ | ✓ | |
| United States — NIST AI Risk Framework | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| United States — FHFA AB 2020-02 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| United States — NAIC Principles on AI | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| United States — Federal Trade Commission | ✓ | | ✓ | | ✓ | | |
| EU — EU Artificial Intelligence Act | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| EU — EU Digital Services Act | ✓ | | | ✓ | ✓ | ✓ | ✓ |
| EU — OECD Principles | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| Japan — Social Principles of Human Centric AI | ✓ | ✓ | | ✓ | | ✓ | |
| Japan — AIST ML Quality Management Guideline | ✓ | ✓ | | ✓ | | ✓ | |
| LATAM — Brazilian AI Strategy | ✓ | ✓ | | | | ✓ | |
| LATAM — Brazilian AI Bill | | ✓ | | | | | |
| LATAM — AI National Policy (Chile) | | ✓ | | ✓ | | ✓ | |
| LATAM — AI National Plan (Argentina) | ✓ | | | ✓ | | ✓ | |

# 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.

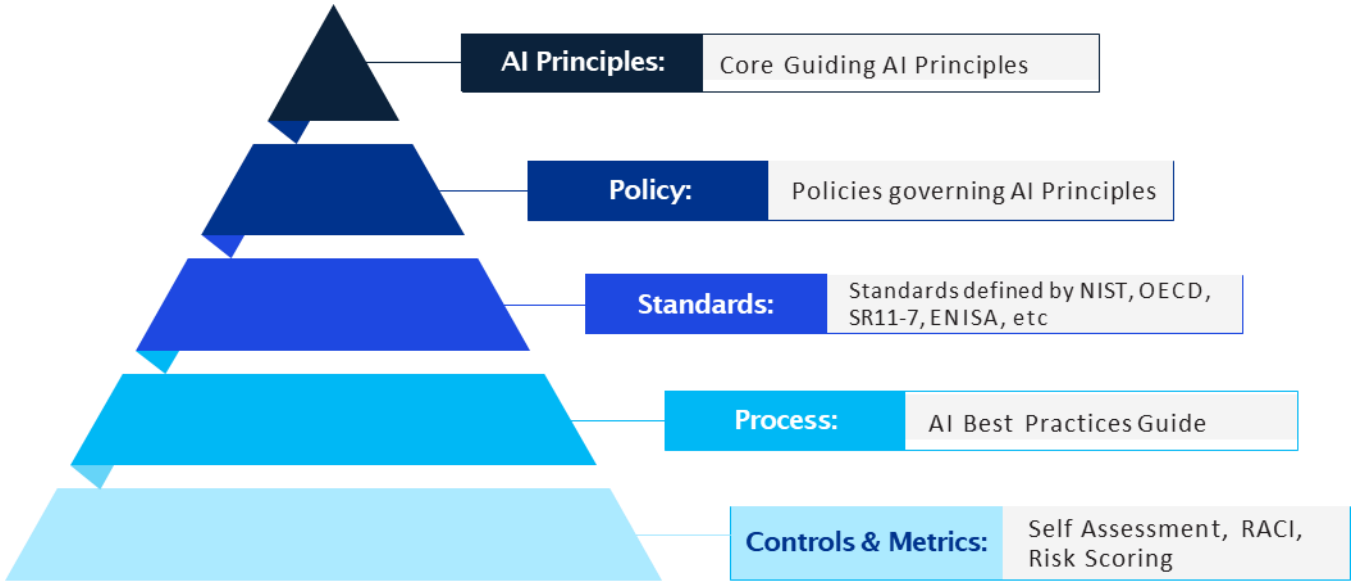
**Data integrity**
Ensure data quality, governance, and enrichment steps embed trust.

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

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

# AI Governance

# AI Governance Considerations




- **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
- Ensure that your AI office is inclusive **diverse** group of **stakeholders** across Business, Technology, HR, Diversity amongst 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.

# Lessons learned from building AI Governance models

01 Maintain security and privacy as core components of any governance model

02 Define a risk tiered governance approach

03 Develop and publicize a company wide Responsible Artificial Intelligence Charter

04 Help ensure that a diverse and representative group of stakeholders are involved in governance and model development

05 Re-evaluate your third-party risk management process

06 Reimagine your AI intake process

07 Build appropriate safeguards and measures to manage risks across the entire AI lifecycle, including ongoing monitoring

08 Align existing policies for AI

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

## Internal risks & considerations

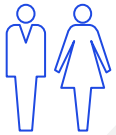
1. Breaking Confidentiality and Intellectual Property
2. Employee misuse and inaccuracies
3. Generative AI evolves
4. Talent Implications

## External risks & 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 is difficult to answer.

### Cybersecurity

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

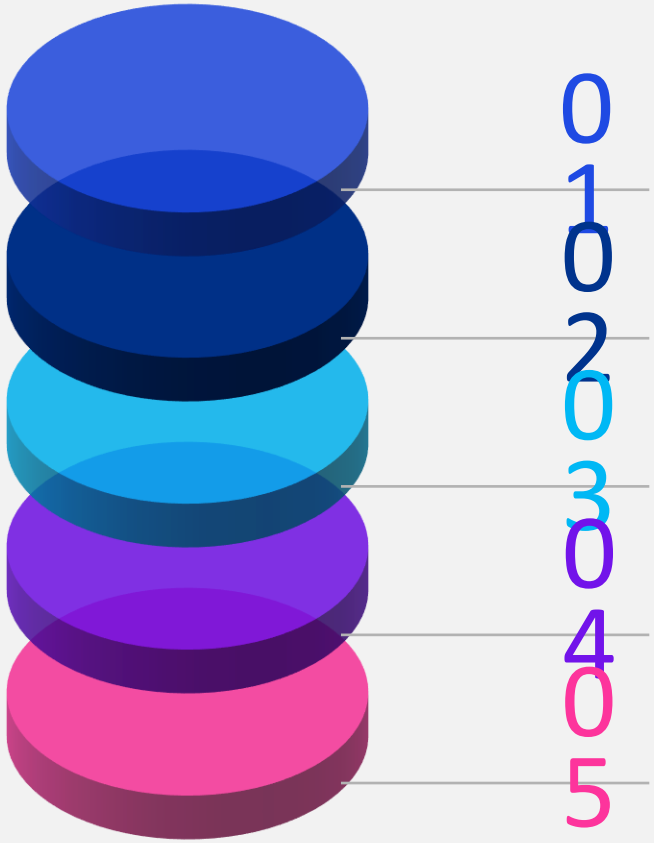
### Adversarial Attack

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.

# AI Privacy Considerations




## Privacy by design

Are privacy professionals involved throughout the development lifecycle to help ensure the privacy rights of data subjects are respected?

## Data minimization vs. Statistical accuracy

How can the organization balance regulations requiring data minimization while also achieving their desired level of statistical accuracy?

## Notice & consent

Have individuals explicitly consented to the use of their personal data – or is there a way for the individual to request to “opt-out”?

## Data retention

Once a model has been trained, is the underlying training data still required (i.e., Continuous Learning Models) or can it be deleted?

## Data deletion (‘Right to be forgotten’)

Is the organization able to (1) identify an individual’s data after it has been ingested into a model, and (2) validate that both the original data – as well as any resulting impact or contribution derived from that data – are able to be deleted?

# Where do we go from here?

# Next steps with Generative AI

There are numerous considerations to developing sustainable use cases with generative AI.

## 01 Problem statement

- What problem is generative AI being used to solve?
- Does the use case address a real problem that users are facing?

## 02 Data

- What data will be used to train/fine-tune/adapt the generative AI model?
- Data types, sources, quality, and formats?

## 03 Metrics

- Criteria and success metrics used to measure the performance of the generative AI algorithm or model.

## 04 Risks

- Potential risks and challenges associated with implementing and deploying the solution, such as ethical, regulatory compliance, IP or user adoption.

## 05 Goals

- What is the desired outcome of using generative AI?
- Who are personas/segments you are solving for?
- Expected business benefits and value.

## 06 Models

- What type of generative AI model(s) will be used?
- Performance considerations.
- Build vs. buy considerations.

## 07 Evaluation

- What type of output will the generative AI model produce?
- Ground truth to evaluate the model for accuracy, consistency, hallucinations, and veracity.

## 08 People

- Do we have the talent and skills in-house?

## 09 Solution

- Description of the proposed solution including non-generative AI capabilities that will be required to realize the solution.

## 10 Output

- What type of output will the generative AI model(s) produce?

## 11 Limitations

- Potential limitations or constraints that could affect the performance or scalability of the solution.

## 12 Operations

- Long-term operations and maintenance of the models.

# Questions to begin crucial conversations

## How can I use AI effectively, at scale, and responsibly to achieve tangible business outcomes?

**DIVERSE MIX OF STAKEHOLDERS**

AI/ML Executives | CTO/CIO/CDO | Finance | CISO | Risk/Compliance | Legal | Human Resources | Internal Audit

**CRITICAL QUESTIONS AND CONCERNS**

### 01 We need to **protect ourselves from financial and reputational risks**

- How can I ensure my models are managed effectively to mitigate any financial penalties from non-compliance with regulations?
- How do I proactively manage my AI models to ensure it doesn't violate social norms & values

### 02 We need to **enhance the trust of our consumers** (internal, external)

- Can we trust our AI models?
- Am I at risk of approving/rejecting the wrong decision?
- Is this in line with our ethics, values, and brand?

### 03 We need to **drive accountability and transparency**

- Who is responsible for the decision made?
- What are the consequences for bad decisions?
- How does our operational model, training and change management practices need to evolve in support of Responsible AI?

### 04 We need to **secure our models** from adversarial attacks

- How secure are my AI models against cyber attacks, bad actors and insider threat?
- Are my security controls working? What are some opportunities for improvement?
- Are my AI models violating anyone's privacy?

### 05 We need to **ensure compliance** with global AI regulations

- How can we effectively ensure our AI models are compliant with the rapidly growing list of global regulations?
- How can we automate the review, insights and management of compliance policies?
- How do I to explain this to the customer (or regulator) so that they understand?

### 06 We need to **harness the value of** our AI at scale and responsibly.

- How can I effectively manage the growing number of AI models in my environment?
- What tools can I use to scale, drive automation, and also balance responsibility

# No regrets: Actions to consider

**Organizations have had creative approaches to mitigate risks while still harnessing the power of AI**

### Establishing Chief Trust Off...

An emerging c-suite role with the purpose of retaining customer trust.

### AI Data Policy

Maintaining records of what is ingested and created by Generative AI.

### Labelling Materials

Clearly labeling any content that has been created by generative AI for both internal and external use.

### Use Case Prioritization

Analyze actual data about employee and customer preferences and intentions to identify the best use cases for AI tools.

### Warnings and Trainings

Having specific AI and Generative AI trainings for employees to use responsibly and mitigate risk.

### Internal Tool Development

Developing AI tools so that confidential data does not leave the enterprise environment as input, output, or training data.

### Upskilling

Developing key skills to manage and maintain AI solutions, including technical, analytical and innovative skills.

### Ongoing Monitoring

Regular audits to determine whether information created by AI tools was in violation of company policy.

# 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

Bryan McGowan
Advisory Principal
314.458.8898
bmcgowan@kpmg.com

John Gitas
HCLS Advisory, Principal
917.539.2922
johngitas@kpmg.com

**kpmg.com/socialmedia**

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.