

Generative AI enablement
Overview, risks, and
responsible activation
considerations

Discussion paper



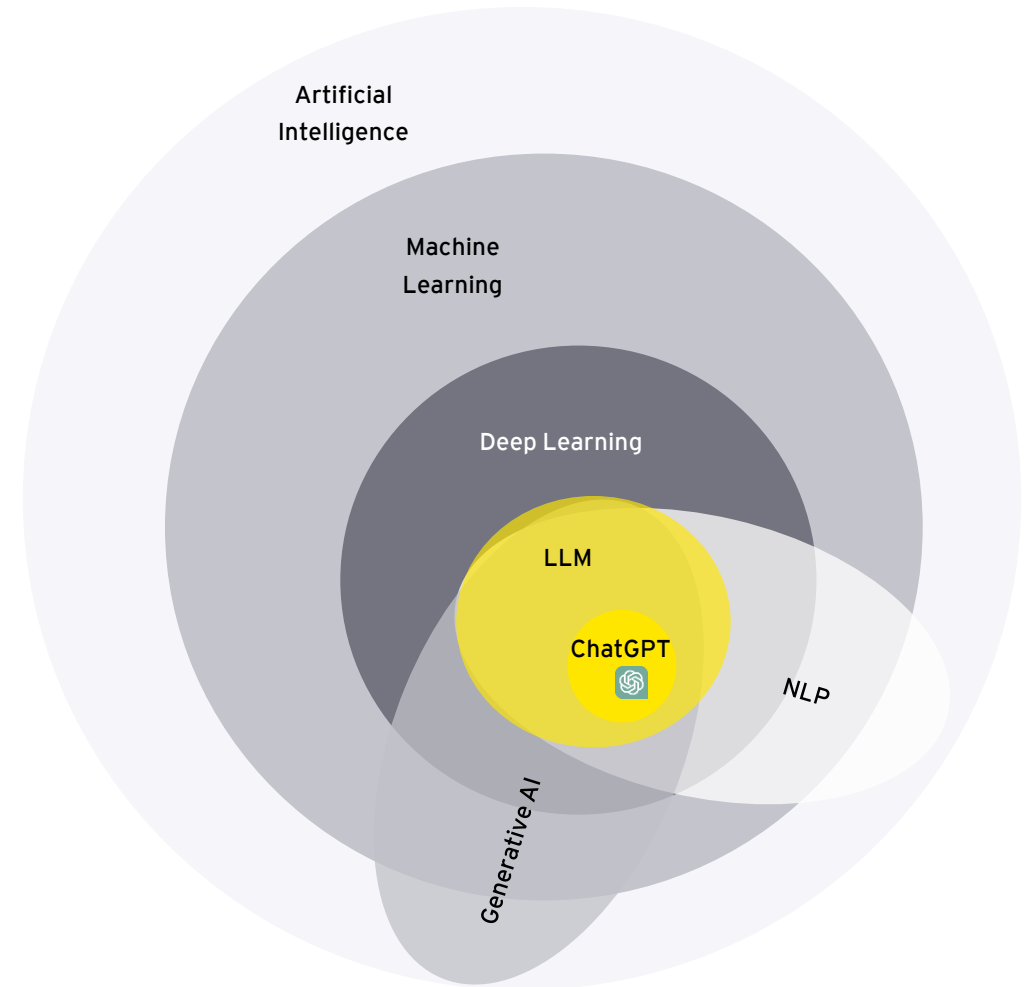
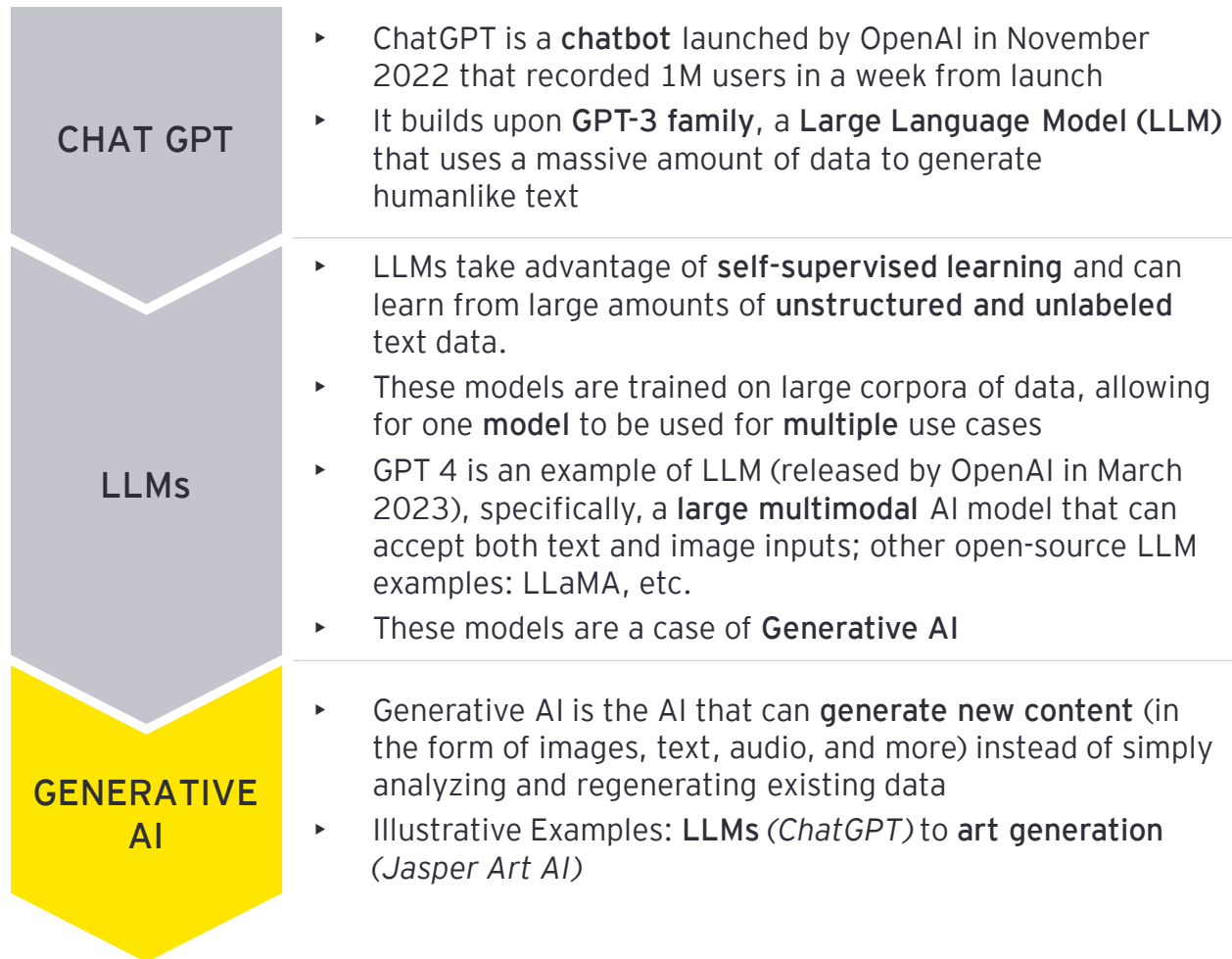
EY

Building a better
working world



Generative AI introduction and risks overview

ChatGPT is a manifestation of Generative AI, which is the next generation of AI that will fundamentally change how we work



Powerful large language model (LLM) capabilities enable diverse applications across business functions

Risk & compliance

- ▶ Customer Interaction Insights - Complaints Identification, compliance monitoring
- ▶ Knowledge Management
- ▶ Documentation Automation
- ▶ Commercial borrower due diligence
- ▶ Underwriter assistance & training
- ▶ Fraud Monitoring

Customer & Growth

- ▶ Targeted marketing , Personalized / hyper-personalized campaigns and offers
- ▶ Market research
- ▶ Customer feedback and product insights

Finance

- ▶ Knowledge management: Financial document analysis, summarization, etc.
- ▶ Market movement and demand/sentiment shift
- ▶ Project portfolio and investment monitoring



Use Cases with predominant market interest

Technology

- ▶ Product Development, Engineering
- ▶ Code Generation, Code Translation, Analysis, Documentation
- ▶ Intelligent Tools - Auto content generation, virtual assistants

Servicing & Operations

- ▶ Call Center Insights / Customer Interaction Insights - Customer feedback and sentiment analysis, RCA
- ▶ Process Automation: Auto populate CRM, intelligent routing
- ▶ Virtual agents / Agent assist

HR & Peoples MGMT

- ▶ Workforce training - Performance Management insights, Internal resource training materials, Gamification of internal trainings
- ▶ Knowledge management - Policy Search

The tremendous promise of large language models is accompanied by heightened risks compared to classical AI models

Risk carried over from existing AI models

Data/Technology Risk

Data capability

Existing data capabilities (e.g., data modeling, storage, processing) and data governance (e.g., lineage and traceability) may not be sufficient for fine-tuning and business use of AI

Data/Technology Risk

Technology capability

AI adoption increases the computational needs and therefore potentially impacts the current use of infrastructure by other business use

Model Risk

Explainability

The higher complexity of AI models that are sometimes a black box decrease explainability

Conduct/Compliance Risk

Bias/fairness

Large volume of training data used in pre-training may introduce bias and unfairness. Complex model and training process make it hard to identify and control bias.

Operational Risk

Business continuity

Heavy reliance on third-party complex AI models, may aggravate the business continuity

Cyber Risk

Cyber attack and adversarial attack

Training data and trained AI model may be leaked out of the institution or vendor platform due to cyber attack or adversarial prompt engineering



Heightened risks of large language models (LLMs)

Data/Technology Risk

Data host, sharing, retention, and security

The nature that LLMs are all third-party based leads to concerns of data breach issue for all data used in fine-tuning and input data to the use cases and prompt

Data/Technology Risk

Data privacy and PII Data

Model fine-tuning may access internal confidential data and PII data for unintendedly. Trained LLM models may contain sensitive / confidential information. Lack of use control may cause data breaches

Model Risk

Hallucination

Pre-train LLMs can cause hallucination due to pre-training process and LLM's heavily reliance on transfer learning

Conduct/Compliance Risk

Toxic information

Similar to bias, toxic information can be introduced by training data used in pre-train, which is hard to avoid due to large training data volume and data sources

Legal Risk

Lawsuit and reg penalty

The risk in compliance, conduct, data potentially violate laws and regulations. Complex and heterogeneous jurisdictional differences aggravates risks

Third-party Risk

All LLMs are provided by third party

Pre-trained LLM models are all third-party based and institutional uses will heavily rely on the vendor provided LLM capabilities and update release

Legal Risk

Copyright

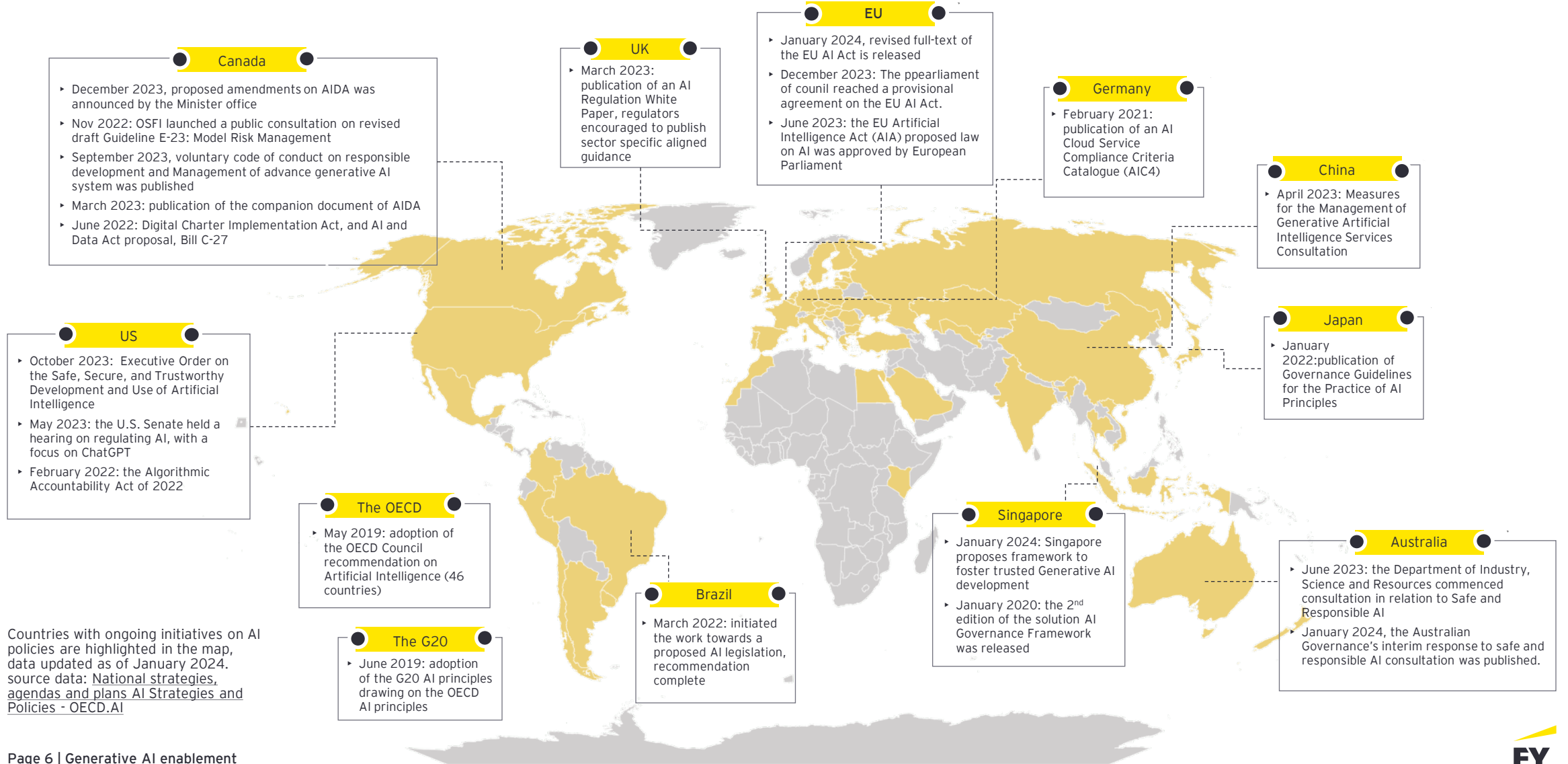
The ownership of products generated by LMM may be ambiguous given that generative AI has creative nature

Reputational Risk

Linked to all other risks

All the above risks may lead to reputational damages to the organization

There are initiatives across the globe to manage emerging risks as demonstrated by a fast-evolving regulatory landscape requiring organizations to adapt



Countries with ongoing initiatives on AI policies are highlighted in the map, data updated as of January 2024. source data: [National strategies, agendas and plans AI Strategies and Policies - OECD.AI](#)



Responsible Generative AI activation

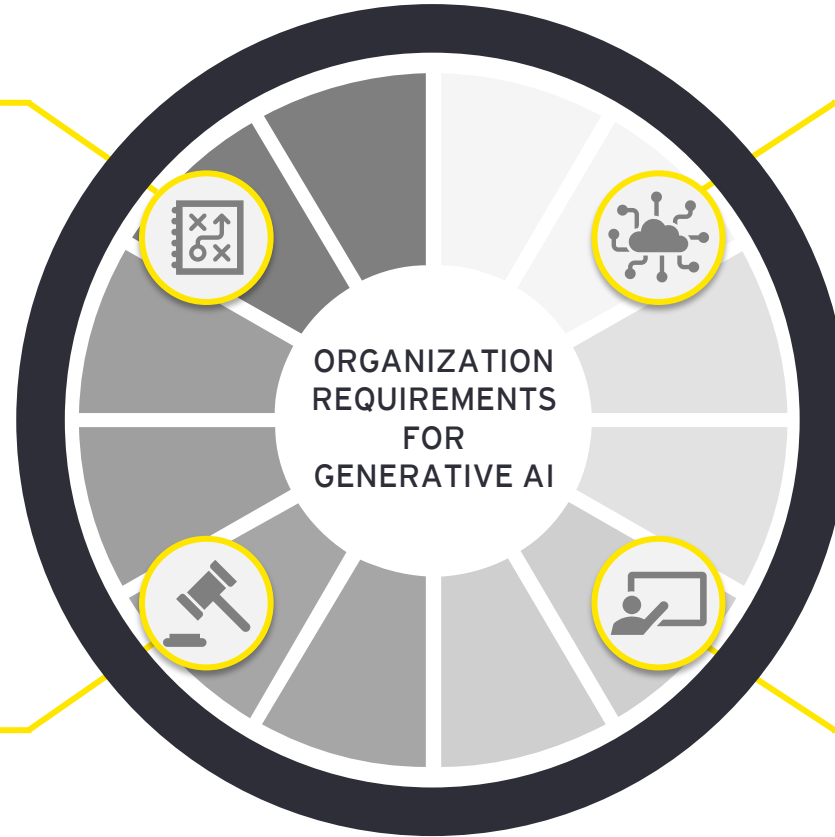
Responsible Generative AI Activation at the organization level relies on four core pillars: business, data & tech, people, risk

1. BUSINESS ENABLEMENT & OPS STRATEGY

- ▶ Harmonize organization's existing AI strategy to include Generative AI strategy
- ▶ Define and collect use cases across business units; define KPIs for measuring business impact, ROI and risk to support strategic activation and prioritization of Generative AI use cases
- ▶ Develop operating model, frameworks and playbooks to managing use cases progression from ideation to organization deployments
- ▶ Establish or enhance COEs to enable experimentation, innovation, and adoption of Generative AI

3. RISK & GOVERNANCE

- ▶ Establish/ update firm-wide AI-focused policies & disclosures and risk governance framework for heightened risks from Generative AI usage
- ▶ Reevaluate contracts, legal and compliance policies for protected IP usage, copyright infringements for potentially derived content and amplification of exiting model bias / discrimination (AI Ethics)
- ▶ Develop robust testing and monitoring frameworks to measure solution / model risks, and performance



2. DATA & TECHNOLOGY

- ▶ Establish data standards for protected PII use and new IP data creation while adhering to existing AI data governance requirements
- ▶ Invest in infrastructure/ tech patterns to scale capabilities, from Development to Production, along with ability to connect with organization Data Lake for structured/ unstructured data
- ▶ Establish adaptable architecture/orchestration to accommodate fit-for-purpose LLM models
- ▶ Examine existing vendor portfolio and align with current ecosystems for the selection of vendor LLMs
- ▶ LLM Ops: Enhance AI ModelOps process and frameworks to deploy/ monitor LLMs for the organization

4. PEOPLE & TRAINING

- ▶ Train employees on best practices, and business and security risks with usage of LLMs usage
- ▶ Upskill business users with focused training on using Gen AI organization applications (e.g., prompt creation)
- ▶ Develop talent with technical experience (e.g., - fine-tuning, chunking, prompt chaining/ classification) to develop organization GAI applications

Carefully balancing business value, enablement effort, and risk exposure involves strategic use case prioritization

This is key process where we collectively systematically evaluate and rank AI initiatives/uses cases based on strategic alignment, potential impact, and feasibility, and which will guide informed decision-making for resource allocation and implementation.

Prioritization lens for GenAI use cases

Business value

Alignment to strategy/chosen archetypes
Evaluate the viability and impact of the use case on overall strategy and journey towards chosen archetype

organization usability
Prioritize organization-wide clusters of value, that can provide wide value-reach and realize cross-business unit synergies

Probability of achieving predicted value
Success probability and predicted value are crucial guideposts for AI use case prioritization.

Cost to build


Financial impact and value to customer
Evaluate the cost to build in the context of the value provided to the customer and impact on top line metrics


AI solution risk
At maturing AI organizations, low-risk models should be prioritized until comprehensive evaluation frameworks are put in place

Data maturity and implementation complexity
Factors such as data availability/maturity, model type, and intricacies of the business problem can raise development costs


 Alignment to strategy/chosen archetypes

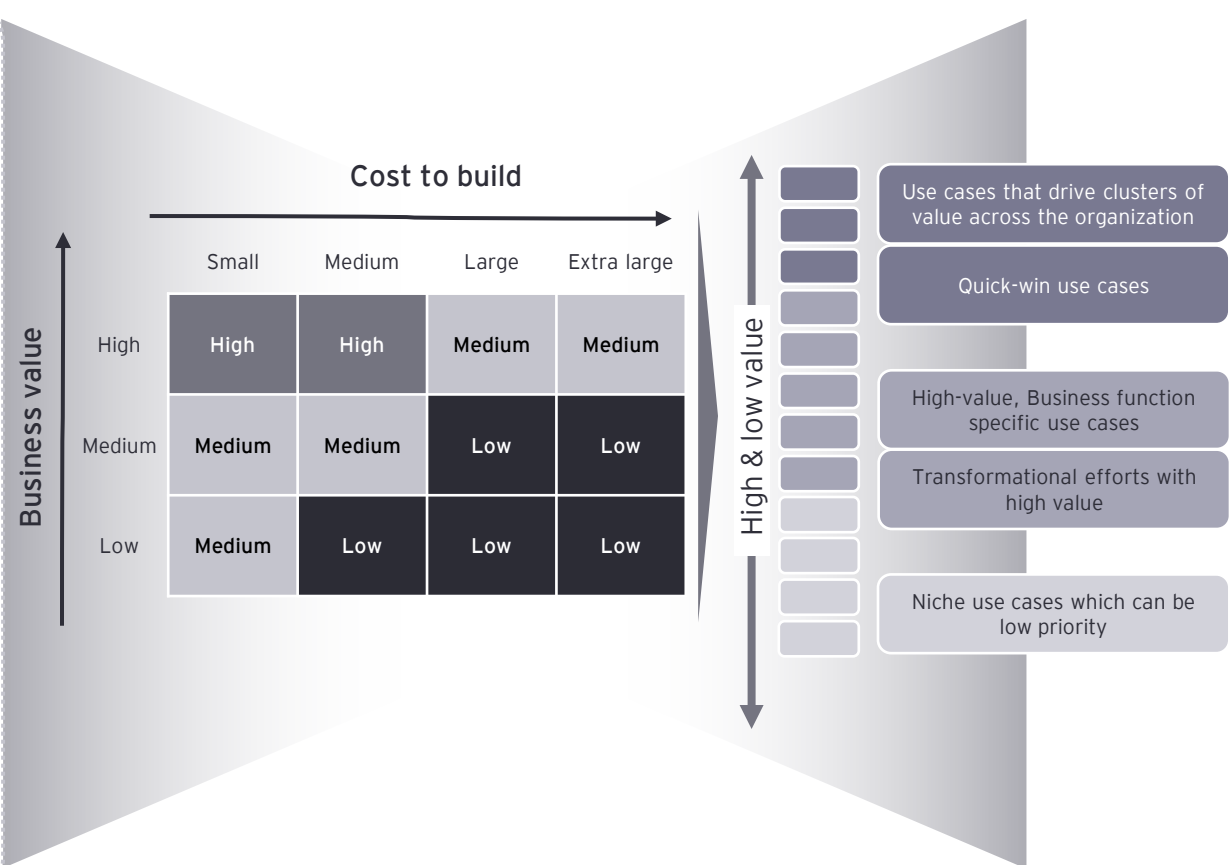
 Probability of achieving predicted value

 organization usability

Financial impact and value to customer


 AI solution risk

Implementation complexity




Type of prioritized GenAI use cases

- Use cases that drive clusters of value across the organization
- Quick-win use cases
- High-value, Business function specific use cases
- Transformational efforts with high value
- Niche use cases which can be low priority

Setting up the appropriate Generative AI technology involves reassessing existing organizational technology strategy and carefully considering available Generative AI enablement options

1 Foundational large language model (LLM) providers



Vendor supported: Offer out-of-the-box fully managed LLM solutions, taking care of infrastructure setup and maintenance. (e.g. GPT3.5/4)



Open source: Provide a more flexible approach, granting users access to the model's source code and architecture. (e.g. Llama-v2)

2 Technology platform providers



Offer a comprehensive cloud-based solution for deploying and running LLMs



Security layers and data management features offered is critical for cases involving sensitive data



Swift activation timeframes enabling rapid prototyping and smooth integration

3 Niche point solution providers



Specialize in a particular sector and focus their solutions to domain-specific use cases



Growing interest from a multitude of new start-ups, venture capital and private equity investments.

Key Dimensions for Technology Provider Evaluation



Effectiveness:
Solution offerings and relevance



Cost:
Usage and deployment costs



Speed to activation:
Infrastructure and deployment time



Ongoing maintenance:
Application management cost



Performance:
Quality and scalability of solution



Customization:
Fine-tuning for niche applications



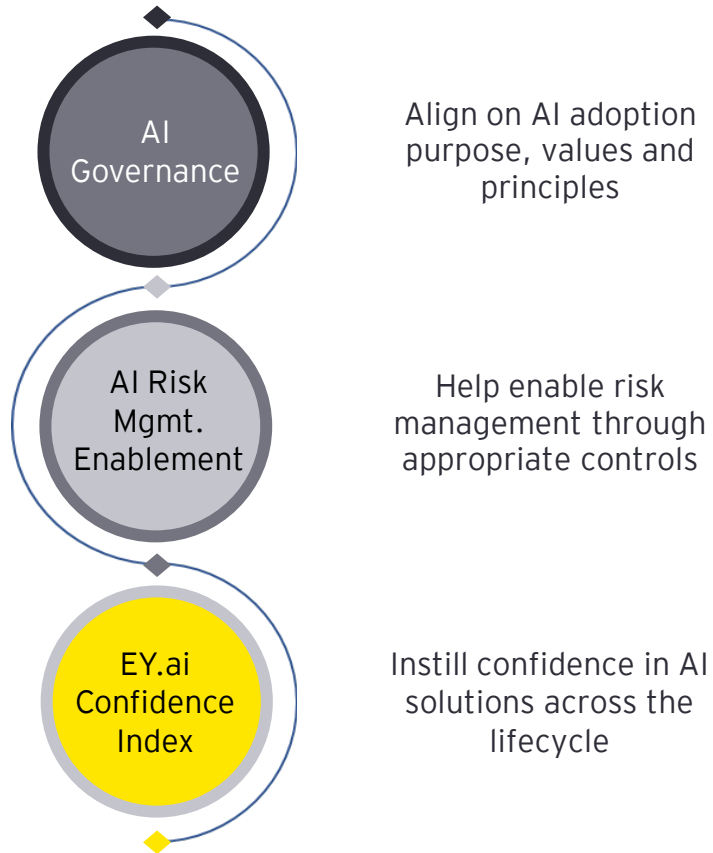
Risk and security:
Data protection, compliance, attacks/threat risk



Future proofing:
Upgrade ease for tech components

A Responsible AI Framework consists of a suite of organization-level and solution-level frameworks supporting AI governance, risk management enablement, and operationalization

The EY organization's Responsible AI Framework



Align on AI adoption purpose, values and principles

Help enable risk management through appropriate controls

Instill confidence in AI solutions across the lifecycle

Key Benefits



Alignment with current regulations- Updates / amendments of current internal regulations in line with AIDA AI Act , Law 25 and other guidelines.



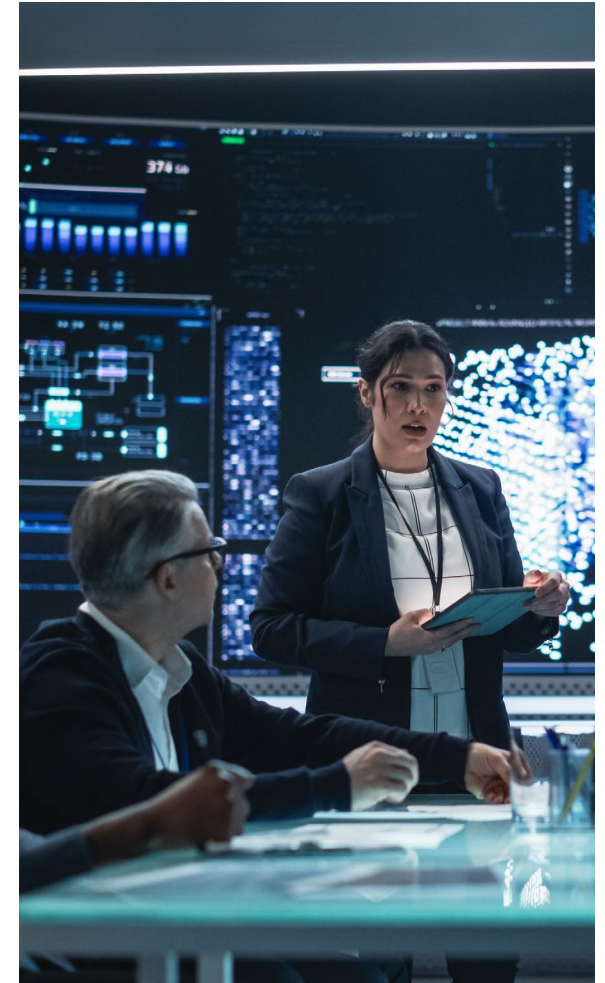
Establish effective AI Governance policies & procedures-provide guidance on the effective control & management of AI risk throughout AI lifecycle,



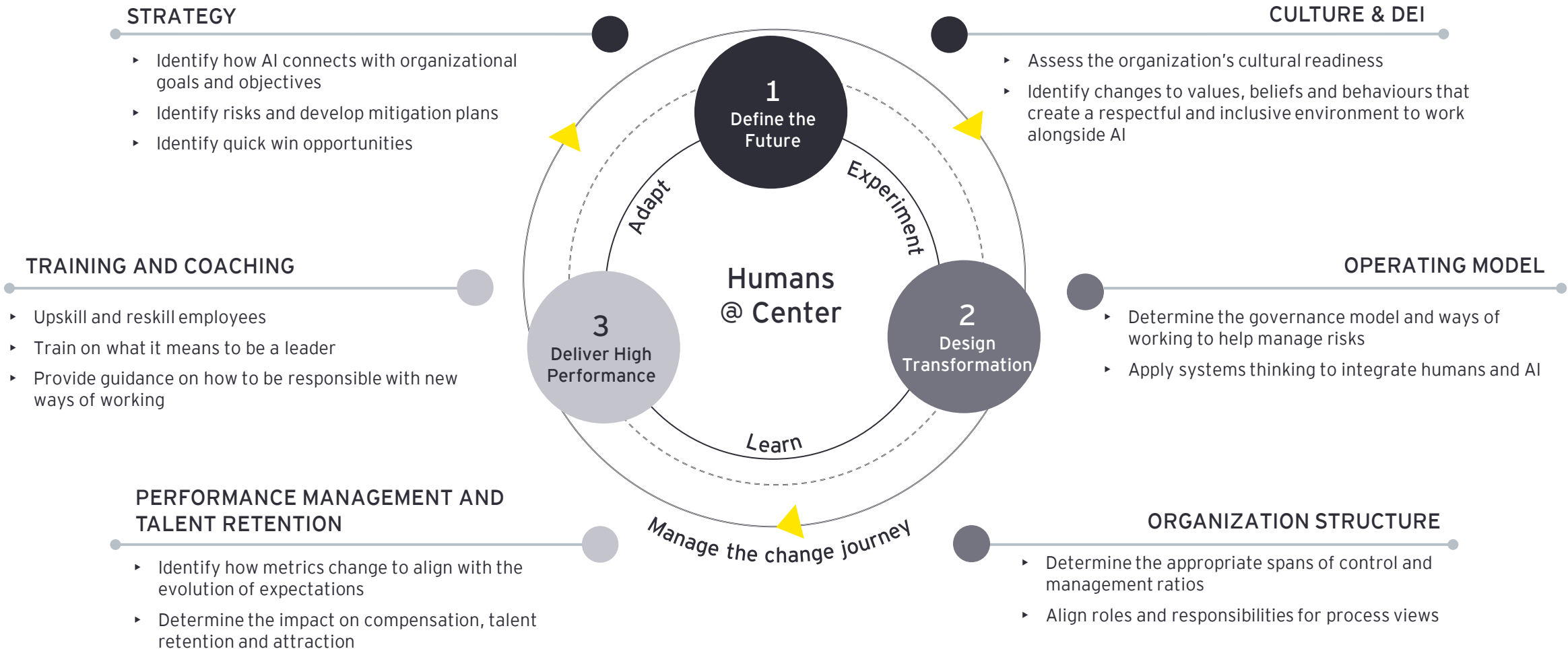
Provide an effective risk management framework by updating risk taxonomy, enhancing existing controls (privacy, ethics etc.), **helping establish new controls**, etc.



Help Establish an AI confidence Index framework based on the organization requirement. Provide AI confidence Playbook



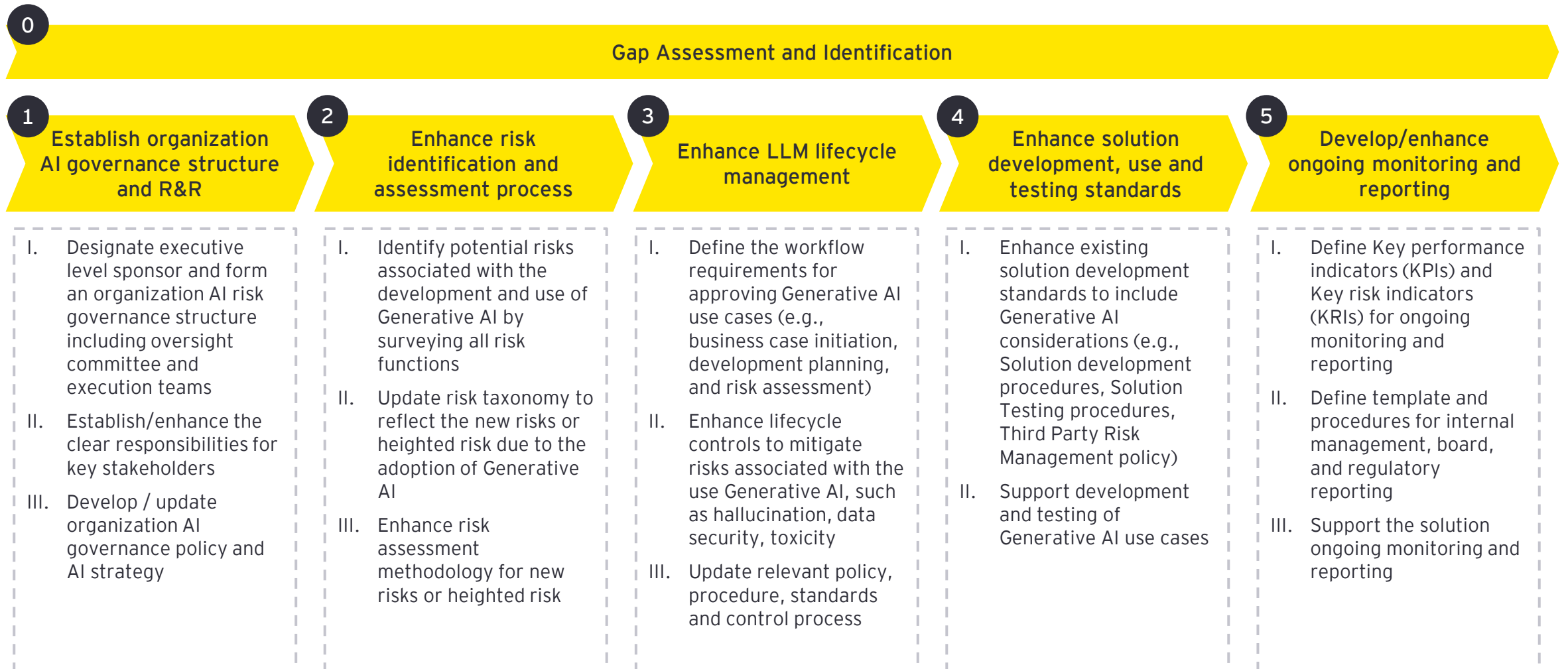
Keeping Humans@Center promotes a sustainable Generative AI implementation and adoption



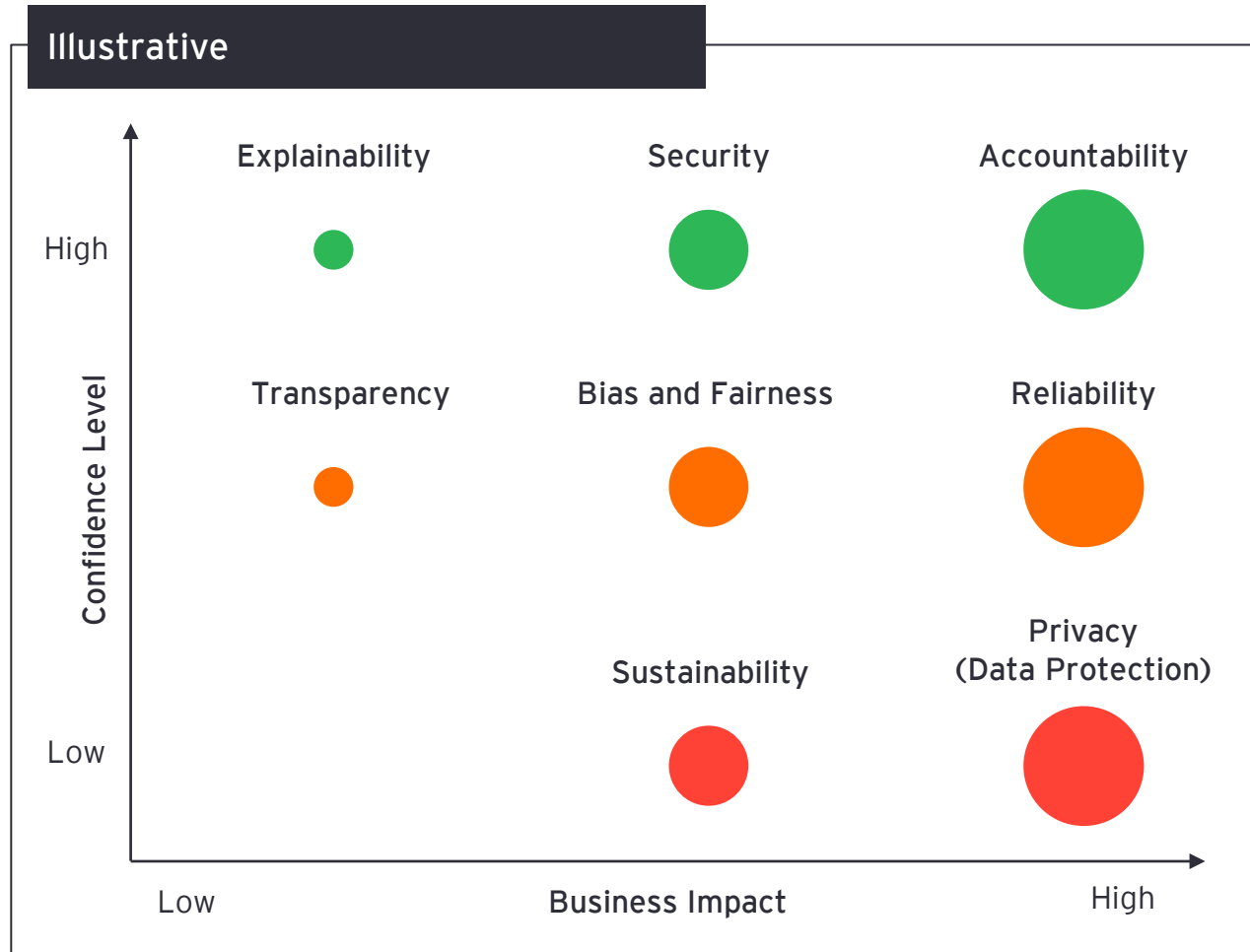


Risk and governance deep dive

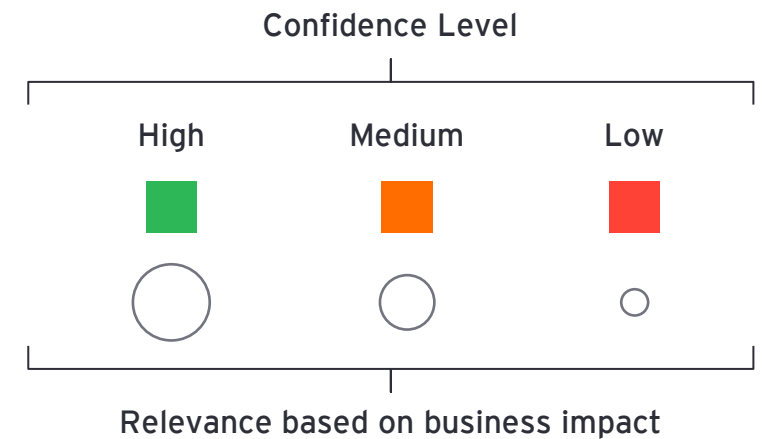
Governance and control enhancement at the organization and solution level enables responsible innovation



The EY.ai confidence index helps organizations reap the benefits of responsible AI/Generative AI adoption, at a solution level



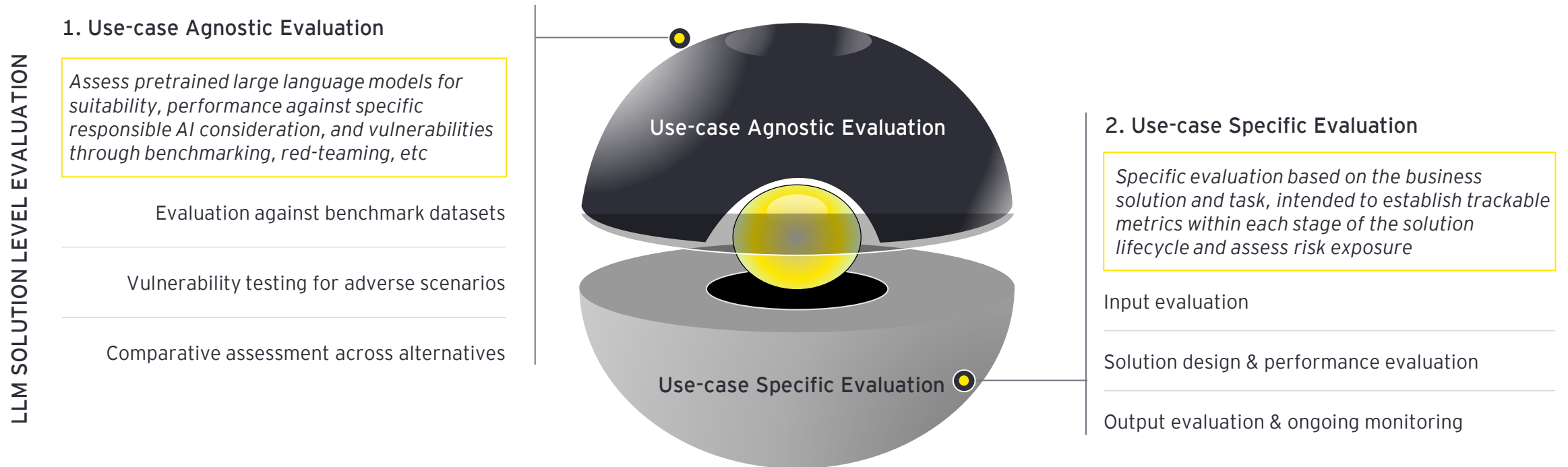
Quantifying our understanding of risk in the AI solutions with continuous monitoring across its lifecycle, based on our Responsible AI dimensions weighted by their business impact



The ninth principle, compliance, is considered as part of Relevance, along with financial and non-financial impact

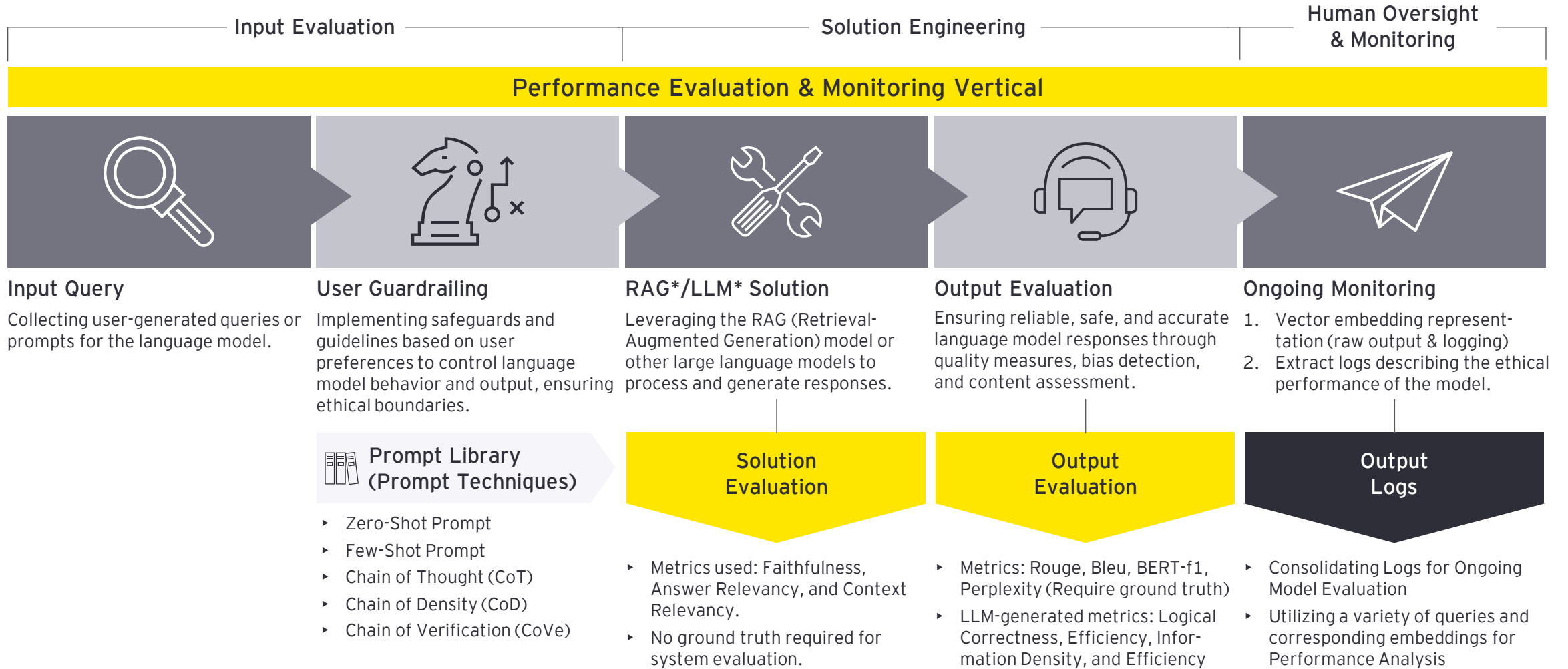
The EY.ai confidence Index hosts a Generative evaluation toolkit to identify & mitigate risks, and help ensure responsible enablement of Generative AI

OVERALL SOLUTION EVALUATION



- Data Quality Testing
- Unit Testing
- Functional Testing
- Security Testing
- Integration Testing
- User Acceptance Testing
- Usability Testing
- Continuous Monitoring
- Maintenance Planning

Application specific LLM model and solution evaluation consideration across the lifecycle for an Illustrative Retrieval Augmented Generation (RAG) use case



*RAG: Retrieval Augmented Generation

**LLM: Large Language Model

Our tested frameworks, models and methods can help your organization accelerate value creation

Frameworks, models and methods

Extensive GenAI Use case catalogues

The catalogue can be used to supplement those already active and under consideration or to provide a portfolio of AI use case options that can deliver quick wins and long-term value.

GenAI use case value prioritisation framework

A matrix, and qualification framework which assesses complexity, business value, time to value and other dimensions for clarity on adoption approach for organizational use cases

GenAI evaluation toolkit

This framework helps assess, quantify, and mitigate risks associated with Generative AI solutions. Applicable for a development, validation and governance personas

AI Confidence Index

The EY.ai confidence index builds and executes an AI confidence framework based on risk appetite to promote AI adoption and innovation

AI/GenAI Process Flows

E2E lifecycle (tollgate view, decision/validation requirements, etc) for GenAI solution enablement across stakeholder groups

AI governance frameworks

EY AI governance framework showing policies, procedures, and standards, governance rollout procedures, etc.

AI Standards & Execution Playbooks

GenAI specific playbooks and standards for responsible development and deployment

Use Case Accelerators

Code modules and prompt libraries to expedite and help the delivery of specific use cases

Authors



Mario Schlener

Partner, Lead Financial Services Risk Management Practice and Enterprise Risk Strategy, EY Canada

EY Global FS Risk Technology, Alliance, Innovation Lead

mario.schlener@ca.ey.com



Kiranjot Dhillon

Senior Manager, AI Risk, Financial Services Risk Management, EY Canada

kiranjot.dhillon1@ca.ey.com



Yara Elias, Ph.D.

Senior Manager, AI Risk Lead, Financial Services Risk Management, EY Canada

yara.elias@ca.ey.com



Vishaal Venkatesh

Senior, AI Risk, Financial Services Risk Management, EY Canada

vishaal.venkatesh@ca.ey.com



Liang Hu, Ph.D.

Manager, Responsible AI and AI Risk, Financial Service Risk Management, EY Canada

liang.Hu@ca.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2024 Ernst & Young LLP. All Rights Reserved.
A member firm of Ernst & Young Global Limited.

4261712

This publication contains information in summary form, current as of the date of publication, and is intended for general guidance only. It should not be regarded as comprehensive or a substitute for professional advice. Before taking any particular course of action, contact Ernst & Young or another professional advisor to discuss these matters in the context of your particular circumstances. We accept no responsibility for any loss or damage occasioned by your reliance on information contained in this publication.

ey.com/ca

