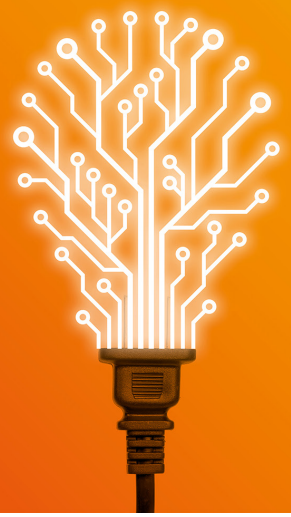
EVERSHEDS SUTHERLAND

AI unplugged

Are you prepared for the wave that is coming?



AI is transforming industries, reshaping the way businesses operate and driving innovation at an unprecedented pace.

Association of Corporate Counsel CHICAGO

AGENDA | Chicago

Tuesday, April 7

11:30 a.m.–12:00 p.m	Arrivals, registration and lunch
12:00–12:45 p.m.	AI overview
12:45–1:00 p.m.	*Break*
1:00–2:30 p.m.	Current US legal landscape AI governance and board oversight
2:30–2:45 p.m.	*Break*
2:45–4:00 p.m.	Third-party risk management and contracting
4:00–4:15 p.m.	*Break*
4:15–5:00 p.m.	Demonstration: How attorneys are using generative AI
5:00–5:15 p.m.	*Break*
5:15–6:30 p.m.	Fireside chat and networking reception

Program faculty

Neal Higgins, *Eversheds Sutherland*

As a leader in the firm's Cybersecurity and Data Privacy team and National Security team, **Neal** represents clients before the US Congress, particularly on cybersecurity, national security and issues of advanced technologies. He also advises clients on cyber incident response and prevention, as well on Artificial Intelligence, quantum computing and other innovative technologies. Neal has served in senior leadership positions at the White House, the Central Intelligence Agency and the US Senate. Prior to joining Eversheds Sutherland, Neal served at the White House as the first Deputy National Cyber Director for National Cybersecurity from 2021 to 2023.

Rachel Reid, *Eversheds Sutherland*

Rachel has more than 20 years of experience advising financial services and technology companies on a wide range of legal and regulatory matters, including data privacy and security, artificial intelligence, risk management, operations, corporate governance, complex commercial transactions, technology transactions and outsourcing. Prior to joining Eversheds Sutherland, Rachel was SVP, Deputy General Counsel, Corporate Secretary and Chief Privacy Officer at a leading health, wealth and investment company.

Mary Jane Wilson-Bilik, *Eversheds Sutherland*

Mary Jane (MJ) has advised financial services and technology clients on privacy and innovation issues for more than 25 years. Her recent focus has been to assist clients perform AI impact assessments and develop robust risk management, governance and vendor management policies for their AI efforts, including generative AI. She counsels clients on assessing AI risks on a cross-sector basis, monitoring for bias, privacy, cybersecurity, intellectual property and specialized regulatory risks, and implementing effective governance measures and guardrails.

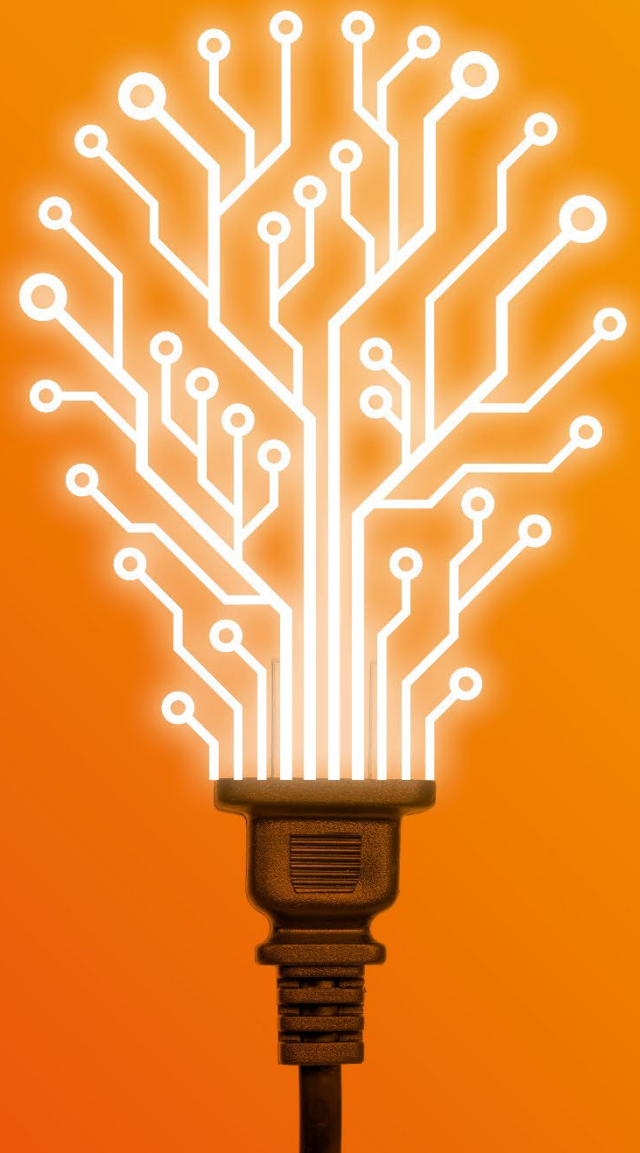
eversheds-sutherland.com

EVERSHEDS SUTHERLAND

AI unplugged

Are you prepared for the wave that is coming?

AI is transforming industries, reshaping the way businesses operate and driving innovation at an unprecedented pace.



ACC Association of Corporate Counsel CHICAGO

ACC Association of Corporate Counsel CHICAGO

Welcome and Some Housekeeping Items

- Be sure to sign-in for MCLE Credit at the registration desk.
- Ask questions! Our panelists are happy to engage with you.
- If your attendance time meets the rules set by the Illinois MCLE Board, ACC Chicago will send your certificate by email next week.
- Watch for the survey/feedback link sent to your email after the program.

A reminder about the benefits of ACC membership…

- Free CLE, Roundtables, DEI & Professional Development Programs
- Socials, Special Networking Groups, Annual Celebration Event
- Community Outreach, Diversity Initiatives & Pro Bono Offerings
- Leadership and Speaking Opportunities, Chicago Lawyer Subscription
- Access to ACC Global Resources, including:
    - ACC Docket Magazine & Newsstand (searchable legal news feed)
    - ACC Survey Portal, Resource Library, Contracts Portal & Legal Ops Section
    - E-Groups and Committees on Substantive Practice Areas

Agenda

12:00 p.m. – 12:45 p.m.	AI overview
12:45 p.m. – 1:00 p.m.	Break
1:00 p.m. – 2:30 p.m.	Current US legal landscape AI governance and board oversight
2:30 p.m. – 2:45 p.m.	Break
2:45 p.m. – 4:00 p.m.	Third-party risk management and contracting
4:00 p.m. – 4:15 p.m.	Break
4:15 p.m. – 5:00 p.m.	Demonstration: How attorneys are using generative AI
5:00 p.m. – 5:15 p.m.	Break
5:15 p.m. – 6:30 p.m.	Fireside chat and networking reception

Speakers

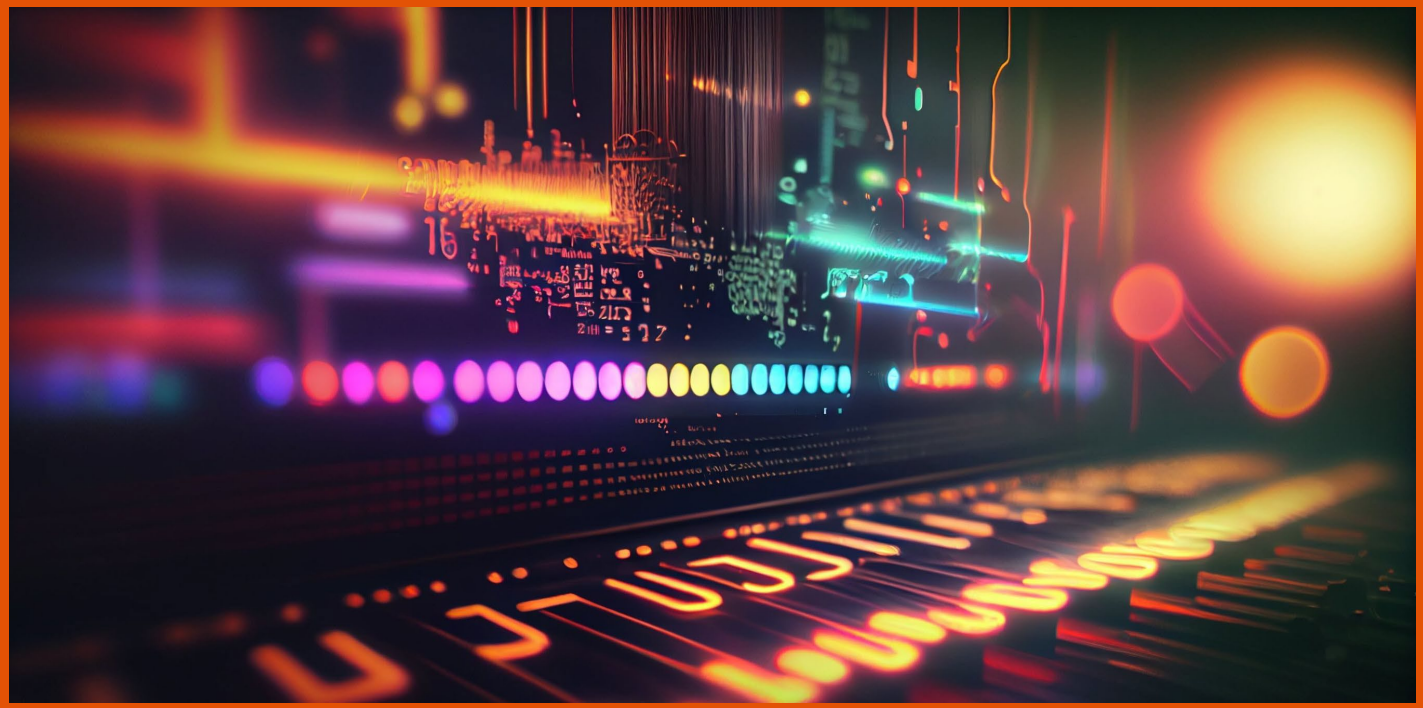
Eversheds Sutherland presenters:

Rachel Reid

Neal Higgins

Mary Jane Wilson-Bilik

AI overview



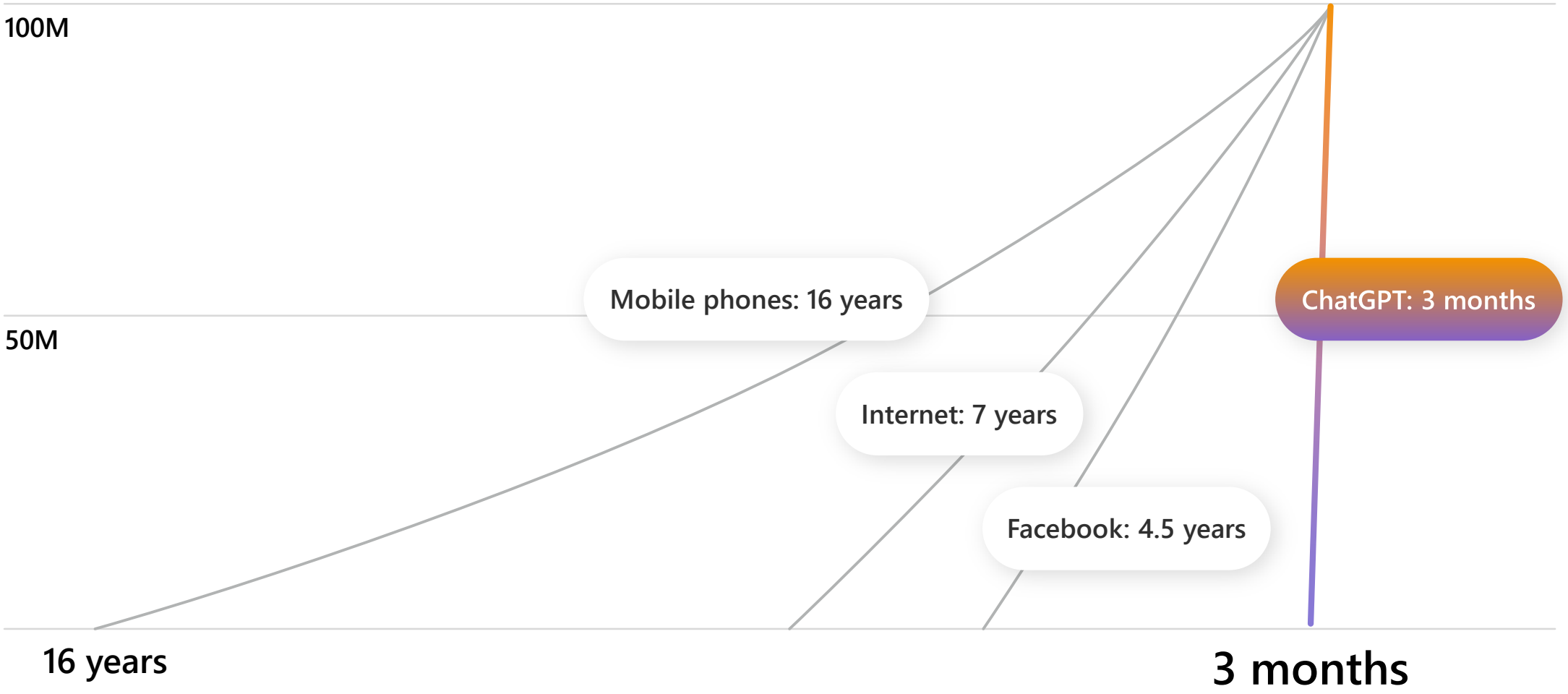
Why the focus on AI now?

"Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society."

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023.

Generative AI technology is here

Time to reach **100M** users



Predictions (Gartner)

2026	– More than 80% of enterprises will have used generative AI application programming interfaces (APIs) or models and/or deployed GenAI-enabled applications in production environments, up from less than 5% in 2023 – Organizations that operationalize AI transparency, trust and security will see their models achieve a 50% improvement in terms of adoption, business goals and user acceptance – 75% of business will use generative AI to create synthetic customer data, up from less than 5% in 2023
2027	– Foundational models will underpin 60% or natural language processing (NLP) use cases, up from fewer than 5% in 2021. – More than 50% of the GenAI models used by enterprises will be specific to either an industry or business function – up from approx. 1% in 2023
2028	– 30% of GenAI implementations will be optimized using energy-conserving computational methods, driven by sustainability initiatives

Artificial intelligence defined

Executive Order

- **Artificial intelligence (AI)** means an engineered or machine-based system that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations or decisions influencing real or virtual environments.

National Institute of Standards and Technology (NIST)
AI Risk Management Framework

- **AI system** means an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.

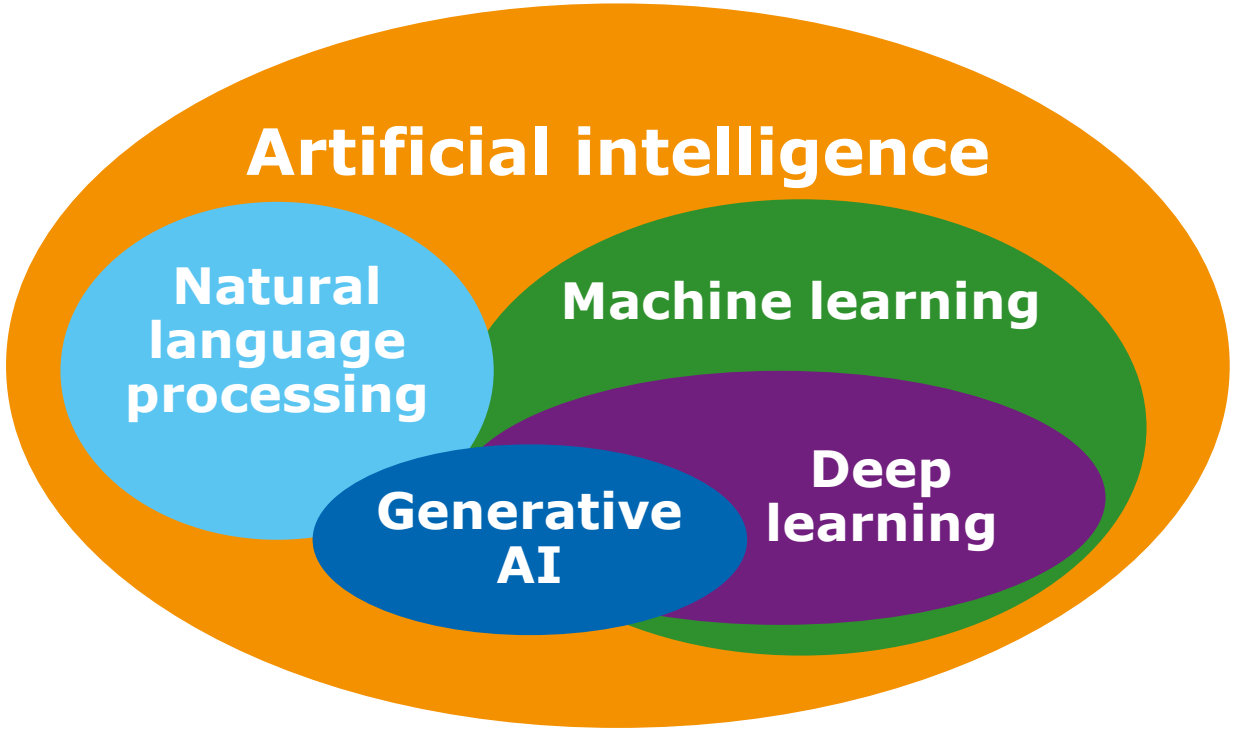
Generative AI

- Generative artificial intelligence (GenAI) is a category of AI that uses large language models (LLMs) that emulate the structure and characteristics of training data in order to generate derived synthetic content as outputs. This can include images, videos, audio, text, computer code and other digital content.
- **Can be public or private. Can involve more than one vendor in the production of the outputs, which are connected to the LLM via application programming interfaces (APIs).**

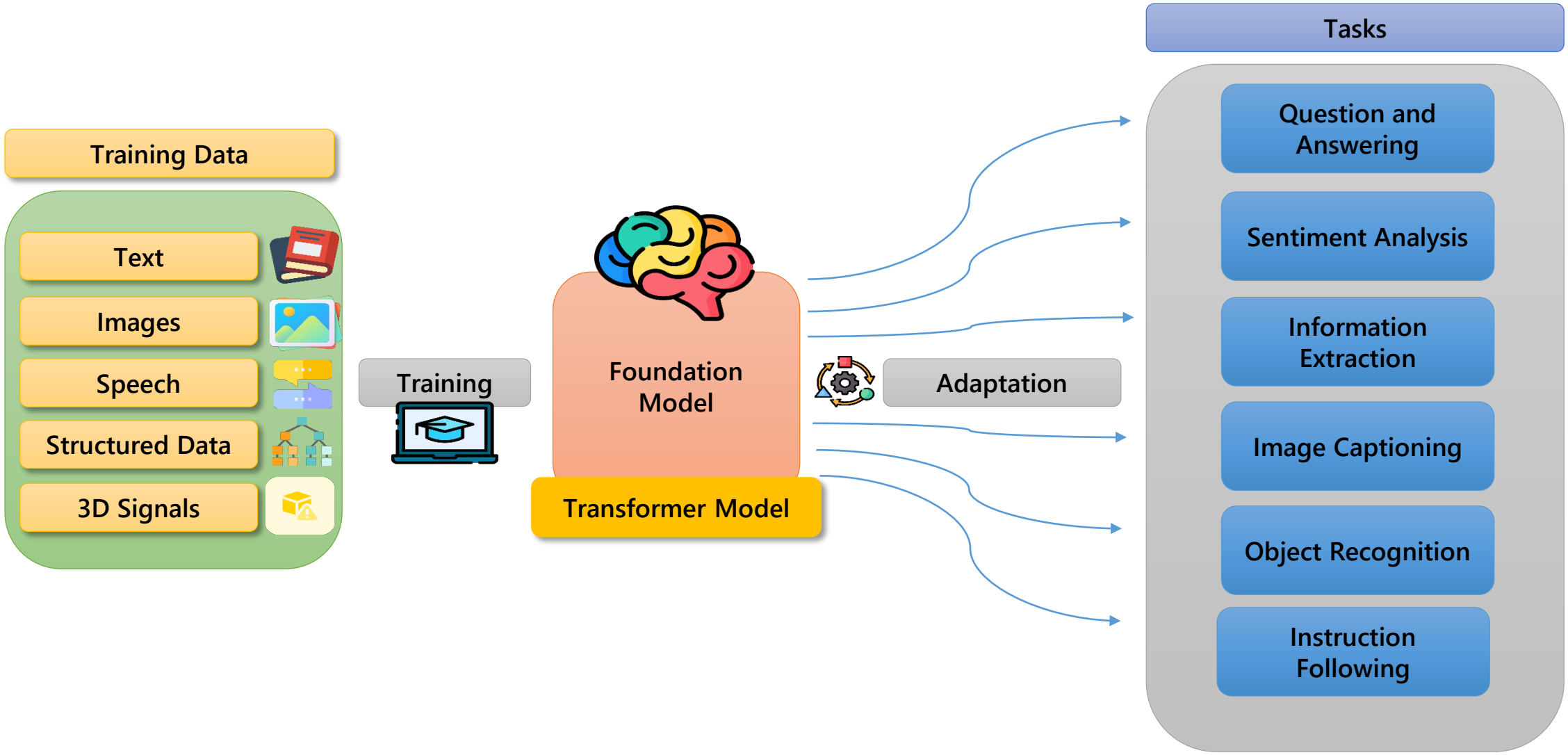
Generative AI tech:

- ChatGPT*
- DALL-E
- Gemini (formerly Bard)
- Copilot (formerly Bing Chat)
- Codex
- LexisNexis and Thomson Reuters

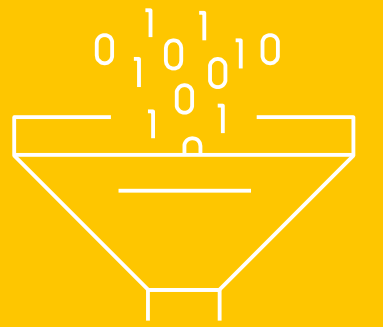
**GPT = Generative Pre-trained Transformer*



Generative AI at a glance

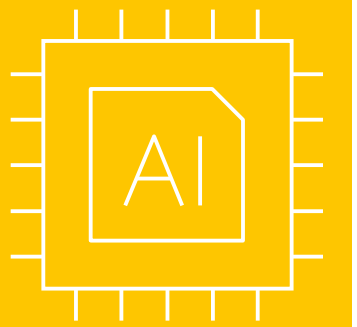


Technology stack for AI foundation models



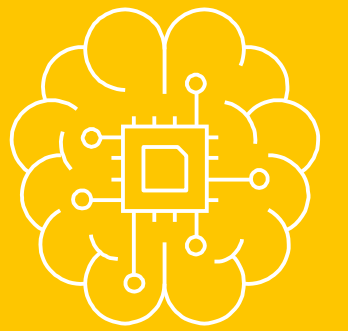
Applications

Software programs where the output of an AI model is put to work



API Services

APIs, or endpoints, through which applications access pre-trained models

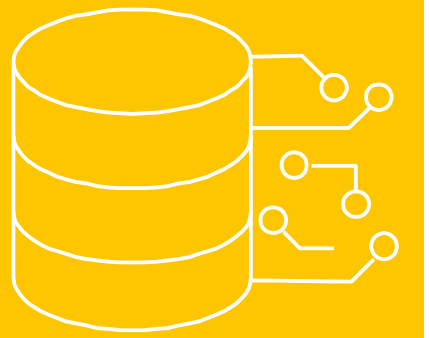


Powerful Pre-trained AI Models

Pre-trained models like GPT-4 that can be used to solve similar problems without starting from scratch

Machine Learning Acceleration Software

Software that speeds up the process of developing and deploying large AI models



AI Datacenter Infrastructure

Advanced supercomputing infrastructure, including clusters of advanced graphics processing units (GPUs) with high-bandwidth network connections

Generative AI risks

Compared to traditional software, new AI-specific risks include the following:

- The **data used for training** an AI system may not be true or appropriate for the intended use of the AI system.
- **Harmful bias and other data quality** issues can affect AI system trustworthiness, which could lead to negative impacts.
- Datasets used to train AI systems may become **detached** from their original and intended context or **may become stale or outdated**.
- Use of pre-trained models can increase levels of **statistical uncertainty** and cause issues with bias management, scientific validity and reproducibility.
- It is more difficult to **predict and protect against failure modes**, including security vulnerabilities, in large-scale pre-trained models.
- There is a **privacy risk** due to enhanced data aggregation capability for AI systems.
- Due to their scale and complexity, AI systems may require **more frequent maintenance** and triggers for conducting corrective maintenance due to data, model or concept drift.

Generative AI and cybersecurity risks

Generative AI has given rise to a new generation of cyber threats, giving hackers more opportunities to exploit vulnerabilities and execute malicious campaigns.

- Generative AI can be exploited to expose sensitive data and allow unauthorized access to systems.
- Existing monitoring, detection, alerting and response capabilities may not be adequate to protect against the risk of users making queries that are considered unsafe, unethical or dangerous (e.g., “deepfakes”).
- Existing controls may not prevent data leakage.
- Security practitioners may not understand prompt engineering and prompt injection attacks.
- Existing third-party risk management frameworks may not adequately assess generative AI partners and suppliers.
- Current infrastructure teams may not understand how to secure the technical implementation and integration of AI systems.

Generative AI and cybersecurity risks *(cont'd)*

Cybersecurity leaders should act with urgency, responding to generative AI's cybersecurity risks and securing AI platforms now.

- Understand your AI exposure.
- Secure the entire AI pipeline, including by securing and encrypting the data used to train and tune AI models.
- Continuously scan for vulnerabilities, malware and corruption during model development, and monitor for AI-specific attacks (e.g., data poisoning and model theft) after the model has been deployed.
- Invest in new security controls and defenses specifically designed to secure AI systems. While existing security controls and expertise can be extended to secure the infrastructure and data that support AI systems, detecting and stopping new forms of adversarial attacks on AI models may require new methods.

Current US Legal Landscape

There is no comprehensive federal AI law in the US yet

President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

- **Message to the US government and to the nation**: AI is here to stay and we must be ready to both **use it responsibly and regulate it.** The EO sets in motion a host of actions on AI by every federal executive agency.
- **Theme**: AI holds extraordinary potential for good, but also for harms, including damage to national security, critical infrastructure and privacy; fraud, discrimination and bias; and disinformation and workforce displacement.
- **Key actors**: The EO looks to NIST to develop standards, recommendations, and best practices for AI development and use that federal agencies are directed to build into current and new regulations, leading to new kinds of enforcement.
- **Message to private sector**: Develop AI governance and engage with the NIST Risk Management Framework.

Activity in every branch of the US federal government

White House

- Office of Management and Budget (OMB) draft policy on agency use of AI
- US Dept. of Commerce created US AI Safety Institute Consortium (AISIC) tasked with developing and deploying safe and trustworthy AI

Congress

- Senator Schumer, SAFE Innovation Framework for AI Policy
- Artificial Intelligence Advancement Act of 2023 (S. 3050)
- Artificial Intelligence Research, Innovation, and Accountability Act of 2023 (AIRIA)

Federal Agencies

- Joint pledge to "protect individuals'" rights regardless of whether legal violations occur through traditional means or advanced technologies
- Existing laws such as the FTC Act, FCRA, FHA and ADA can be violated through the use of AI technology
- FTC Civil Investigative Demand of OpenAI
- FCC Declaratory Ruling prohibiting use of AI-generated voices in robocalls

US intellectual property law

Output may infringe

- Most LLMs were trained without license for protected content – but this is changing
- Copyright is the most significant risk
- Litigation currently pending v. all LLMs (fiction, non-fiction, news, images)
- Direct copyright infringement claims are surviving motions to dismiss

Output not protectable

- US Copyright Office: AI is not an author, so AI-generated works are not copyright protectable (UK says the opposite)
- USPTO: patent protection is essentially the same as for copyright
- Images generated by AI are not unique; not a good choice for trademark
- Text generated by AI is not unique; low value in competitive field

Mitigating IP Risks:

- Take advantage of contractual protection offered by LLM provider, with underlying licenses
- Deploy generative tools only on enterprise data
- Use the Data & Trust Alliance's Data Provenance Standards to manage LLM content
- Adherer to regulations and industry standards to manage LLM content
- Use license pools to compensate creators of LLM training data

Evolving state regulatory response

- **NYC Dept. of Consumer and Worker Protection Local Law 144 of 2021** (2023)
- **California Privacy Protection Agency Draft Automated Decisionmaking Technology Regulations**
  - "Automated decisionmaking technology" means any system, software or process – including one derived from machine-learning, statistics, or other data-processing or artificial intelligence – that processes personal information and uses computation as whole or part of a system to make or execute a decision or facilitate human decisionmaking. Automated decisionmaking technology includes profiling.
  - A business that uses automated decisionmaking technology shall inform consumers about the business's use of automated decisionmaking technology and consumers' rights to opt out of, and to access information about, the business's use of automated decisionmaking technology.
  - Consumers have a right to opt out of businesses' use of automated decisionmaking technology.
- **Executive orders on AI in several states, including CA, MD, PA, OK, OR and VA**
- **Numerous bills introduced in many states**

Evolving State Regulatory Response – NAIC/Insurance Regulators

State insurance laws and regulations:

- NAIC Principles on Artificial Intelligence (2020)
- Colorado SB 21-169 (2021)
- NCOIL Resolution (2021)
- CA DOI Bulletin (2022)
- CT DOI Notice (2022)
- NAIC Model Bulletin on Use of Artificial Intelligence by Insurers (Adopted in Alaska, Connecticut, DC (draft), Illinois, New Hampshire, Nevada, Rhode Island and Vermont)
- Colorado Governance Regulation 10-1-1 (2023) effective 11-2023
- Colorado Draft Proposed Testing Regulation *(in progress)*


AI governance and board oversight

The four pillars

1. **AI governance**
2. **Assessment and monitoring of AI systems**
3. **Privacy and data security**
4. **Allocating risk and responsibility in contracts**

National Institute of Standards and Technology (NIST)

AI Risk Management Framework (AI RMF 1.0)

Valid and reliable
Safe
Secure and resilient
Accountable and transparent
Explainable and interpretable
Privacy-enhanced
Fair – with harmful bias managed

Self-governance (Pillar 1)

- Given the complexity of AI systems and their associated risks, governance should start at the highest level, such as the board of directors.
- The board (or responsible committee) should designate the senior leader with accountability for the AI program, and the senior leader should then assign responsibilities to the appropriate functional leaders.
- The internal AI oversight committee should be inclusive: legal, compliance, cybersecurity, marketing, product development, HR and IT.
- Consider policies and procedures for designing and developing AI systems, conducting AI risk assessments, cataloguing AI systems, approving public- and customer-facing statements about AI, evaluating datasets used for AI, and contracting for third-party AI systems.

AI governance should be documented in writing and should clearly set forth decision-making authority for AI systems, including which decisions are reserved for more senior management and the board.

Assessment and monitoring (Pillar 2)
AI assessment principles could include

- **Reliability and accuracy**: AI systems should perform consistently and provide accurate results across varying conditions.
- **Safety**: AI systems should prioritize human safety and avoid causing harm.
  - Any risk associated with the use of AI systems should be mitigated to the greatest extent possible.
- **Transparency and explainability**: AI systems should be transparent in their operations, and their decisions should be explainable and interpretable to users.
- **Fairness**: AI systems should operate in a fair manner, avoiding biases that could lead to discriminatory outcomes. This includes ensuring that AI-assisted decision-making is equitable and does not disadvantage any individual or group.

Privacy and data security (Pillar 3)

- IAPP: "The use of large volumes of personal data is the very foundation of many of the opportunities that come with the development of AI and machine learning algorithms. Correspondingly, **privacy risks with societal impacts on individuals are at the core of responsible AI**."
- **Existing privacy compliance programs** can be leveraged to establish a solid framework for responsible AI development and deployment.
- Provide clear, **comprehensive and transparent disclosures** about the potential uses of personal/confidential data and, where appropriate, obtain informed, opt-in consent.
- Know how the large language model was **trained** and will be trained.
- Impose **internal restrictions** on the use of certain types of data as inputs/prompts – such as sensitive personal data – in connection with an AI system.
  - e.g., no personal or other company confidential information as prompts in public GenAI model
  - ABA Model Rule of Professional Conduct 1.6 on confidentiality of client data

Privacy and data security (Pillar 3) *(cont'd)*

- All data used by an AI system to fulfill its purposes or to improve or advance the AI system's capabilities – including data uploaded and input in the prompts – must be ***lawfully acquired***.
  - Provide clear, comprehensive and transparent disclosures about the potential uses of data
  - Obtain informed, opt-in consent from the data subjects
  - Impose internal restrictions on the use of certain types of data – such as sensitive personal data (e.g., biometrics) – in connection with an AI system
- What's the security for the data in the model?
  - Cybersecurity by design
- What are the different privacy rules by jurisdiction?
  - Support a "privacy by design" approach to technologies or services incorporating A

Action items for the board

Boards of directors must demonstrate that they are taking on the responsibility of managing AI risk within the company. They must oversee the effective implementation of policies, procedures and processes to manage AI risk.

- Invest in generative AI training for directors and upper-level management so they can make informed decisions going forward.
- Receive regular updates from management about AI incidents and investigations.
- Update compliance protocols to include generative AI usage.

Considerations for the board

When developing AI policies, the board should consider:

- How generative AI might disrupt the industry and company
- How clients and business partners are using generative AI
- How generative AI affects regulatory compliance and governance oversight at the company
- How the AI policy is going to be communicated to employees and how they are going to be held accountable
- How AI is integrated into the decision-making process
- How generative AI can affect the directors' fiduciary duties
  - If the company is going to use generative AI, the board needs to be able to articulate its oversight of AI risks
- New and proposed AI legislation and federal agency guidance
- Why AI could be the right tool to achieve the company's goals

Activity #1: Build a high-level governance model (20 min.)

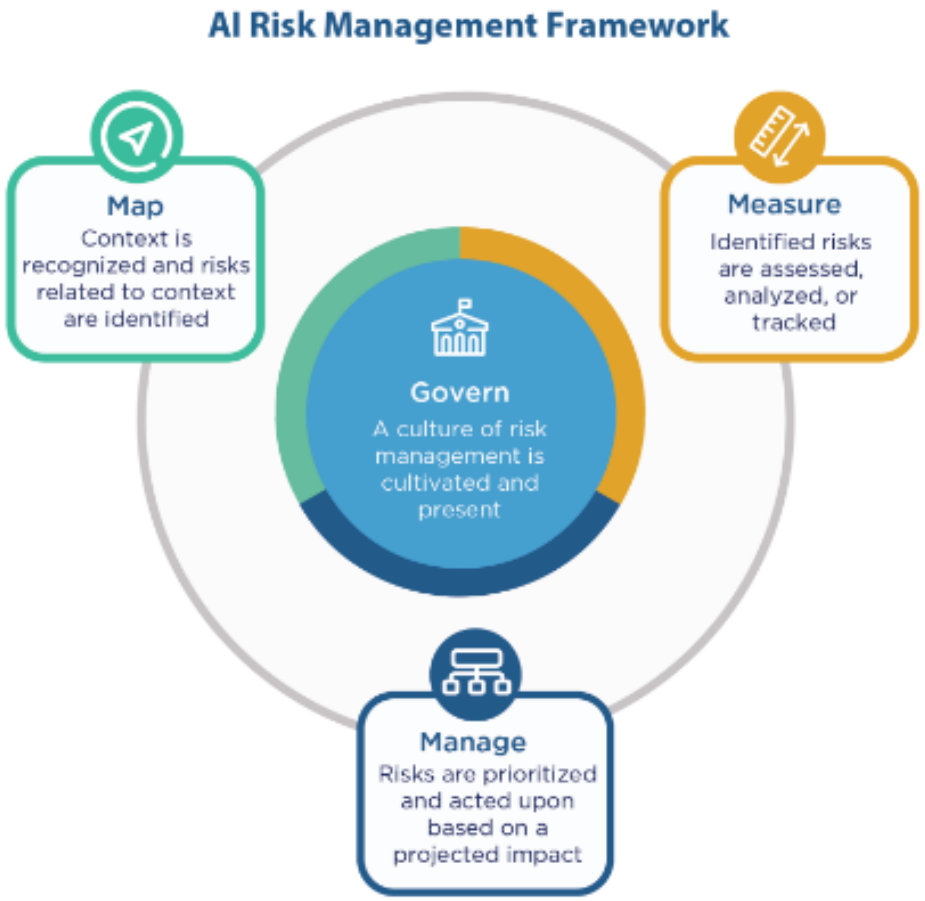
Retail Solutions: A global retail conglomerate, Retail Solutions is committed to enhancing customer experiences through an extensive array of premium products. With its headquarters situated in Grand Rapids, Michigan, Retail Solutions operates across 50 countries. The company boasts a vast customer base, serving over 50 million patrons annually, and maintains a dedicated workforce of more than 100,000 employees.

Mission Statement: Retail Solutions' mission is multifaceted:

1. Exceptional Products and Services: We strive to deliver cutting-edge products that meet the evolving needs of our customers. Our commitment to quality ensures that every purchase enhances the lives of our patrons.
2. Culture of Innovation: As we embark on the journey of integrating AI into our operations, we foster a culture of innovation. Our collaboration with legal experts aims to create an AI governance framework that balances technological advancement with ethical responsibility.
3. Community Impact: Retail Solutions recognizes its role as a positive force in the communities it serves. Through responsible AI deployment, we aim to contribute to societal well-being while maintaining transparency and accountability.


Third-party risk management and contracting

AI System Impact Assessments



AI Impact Assessments (AIIAs) are one tool to anticipate and manage an AI system's benefits, risks and limitations throughout its entire life cycle.

An AIIA is an investigative framework to gather information, identify and quantify benefits and risks, and deliver recommendations to minimize risks while maintaining benefits.

Key objectives of an AIIA include:

1. Identify an AI system's risks and assess strategies to mitigate and manage these risks effectively.
2. Verify that the implementation of an AI system complies with applicable laws, regulations and industry standards.
3. Establish effective governance and increase accountability for an AI system through a multi-stakeholder analysis.
4. Facilitate effective decision-making (e.g., go/no-go).
5. Document and demonstrate that a thorough due diligence process has been conducted on the AI system.

Third-party risk management (Pillar 4)

It is important for both developers and licensors of AI systems, as well as companies acquiring third-party AI systems, to assign responsibilities and allocate liability in a written contract.

At a minimum, the contract should address the following:

- Standards or requirements for external datasets and other inputs used with the AI system, including those that may include data or materials subject to privacy or intellectual property law considerations
- Requirements around transparency and explainability of the AI system
- Security and resiliency standards both for the AI system and for any integrated or interconnected systems and technology
- Responsibility for compliance with applicable privacy and data protection laws
- Ownership rights in the inputs and outputs of the AI system and any restrictions on use of the same (e.g., can customer inputs be used to train the system?)

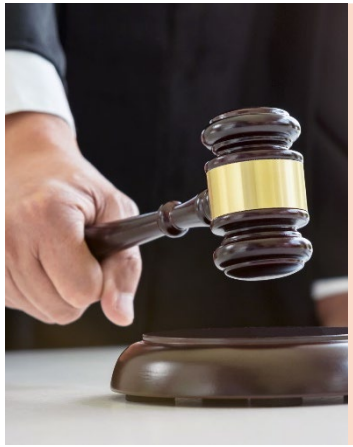
Third-party risk management (Pillar 4) *(cont'd)*

At a minimum, the contract should address the following *(continued)*:

- Ownership of intellectual property rights in the AI system (including the training datasets) and liability for any infringement of third-party intellectual property rights as a result of the use or operation of the AI system
- Rights and obligations of the parties with respect to changes in law
- Responsibility for ongoing testing and monitoring of the AI system, including testing and monitoring for fairness and accuracy, transparency and explainability, security and safety, and potential bias or discrimination
- Alignment with recognized frameworks for AI risk assessment, such as the NIST AI Risk Management Framework, and with any new international AI standards (ISO/IEC 42001)
- Insurance coverage to protect against potential losses arising from use of the AI system

Microsoft’s Customer Copyright Commitment (CCC)

Extends Microsoft’s existing intellectual property defense protections to any Azure OpenAI Service or Microsoft Copilot that is available for a fee through Microsoft volume licensing (“Covered Products”).



If a third party sues a commercial customer for IP infringement due to its use of a Covered Product or the output generated by such a service, Microsoft will defend the customer and pay the amount of any adverse judgments or settlements that result from the lawsuit, as long as the customer used the guardrails and content filters that Microsoft built into its product.

Note that the CCC does <u>not</u> apply to use of trademarks in trade or commerce

Shared responsibility – Conditions applicable to the CCC

To benefit from the CCC, the following conditions must be met:

- Customer must not have disabled, evaded, disrupted, or interfered with the content filters, restrictions in Metaprompts, or other safety systems that are part of the applicable Covered Product;
- Customer must not modify, use, or distribute the Output Content from such Covered Product in a manner that the customer knows, or should know, is likely to infringe or misappropriate any proprietary right of a third party;
- Customer must have sufficient rights to use the Input that the customer provides in connection with such Covered Product, including, without limitation, any Customer Data that the customer used to Customize the model that produced the Output Content that is the subject of the claim;
- The claim does not allege that the Output Content, as used in commerce or the course of trade, violates a third party's trademark or related rights; and
- For Azure OpenAI Service and any Microsoft Generative AI Service with configurable Metaprompts or other safety systems, Customer must have also implemented all mitigations required by the Azure OpenAI Service documentation in the offering that delivered the Output Content that is the subject of the claim.

Activity #2: AI System Impact Assessment (20 min.)

Retail Solutions AI-Powered Personalized Shopping Assistance (PSA)

Retail Solutions is embarking on an exciting venture to integrate cutting-edge third-party AI technology into its website and mobile app to create a **Personalized Shopping Assistance (PSA)** that revolutionizes the retail experience. Here's an overview of this innovative system:

- **Individualized Recommendations**: The AI-driven PSA will analyze user behavior, preferences, and historical data to provide hyper-personalized product recommendations. Customers will receive tailored suggestions that align with their unique tastes.
- **Virtual Stylist Interaction**: Customers can engage with a virtual stylist powered by AI. This stylist will generate outfit ideas, recommend complementary items from Retail's extensive online store.
- **Personalized Discounts and Offers**: The AI system will dynamically generate discounts and special offers based on individual profiles.
- **Inventory Optimization and Product Placement**: Leveraging data-driven insights and predictive analytics, the AI system will optimize inventory management. It ensures that popular items are well-stocked, minimizes overstock situations, and strategically places products both online and in physical stores.
- **Seamless Integration Across Channels**: Retail Solutions recognizes the importance of a consistent customer experience. The AI technology seamlessly bridges the gap between online and offline channels, allowing customers to transition effortlessly from browsing the website to visiting a brick-and-mortar store.
- **Privacy and Security Commitment**: While enhancing the shopping journey, Retail Solutions maintains a strong commitment to privacy and security. Customer data is handled with utmost care, adhering to industry standards and regulations. Transparency and user consent are at the core of this AI implementation.

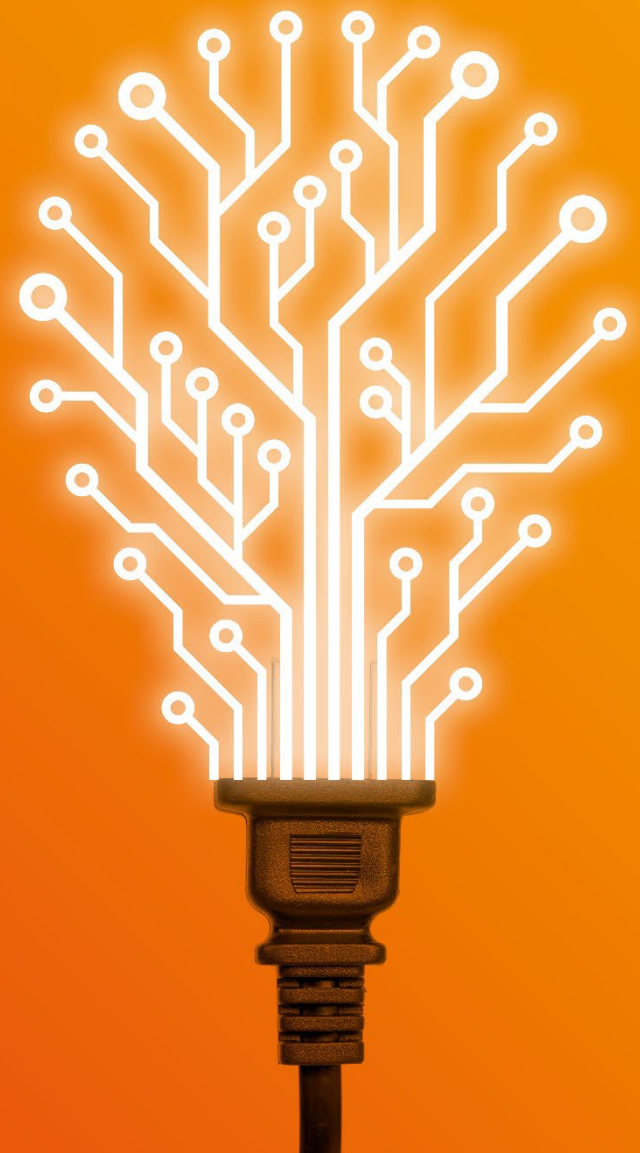
How in-house lawyers are using GenAI

EVERSHEDS SUTHERLAND

Thank you!

AI Unplugged

Are you prepared for the wave that is coming?



EVERSHEDS SUTHERLAND

Activity #1: Build a High-level Governance Model

Company: _____

Guiding questions

1. Does the company have an existing governance structure that can be leveraged to oversee the organization's use of artificial intelligence (AI)? If your organization does not have an existing structure to leverage, has your organization put in place a governance structure to oversee the organization's use of AI?

   Things to consider:

   - Is it useful to adapt existing governance, risk and compliance (GRC) structures to incorporate AI governance processes?
   - Is it necessary to establish a committee comprising representatives from relevant departments (e.g., legal/compliance, technical and sales and communication) to oversee AI governance in the organization?
   - Should we implement a process where each department head develops and is accountable for the controls and policies that pertain to the respective areas, overseen by relevant subject matter experts such as the chief security officer and data protection officer?
     - Is it necessary to establish checks and balances (e.g., an internal team to oversee methodology, algorithms and deployment of AI, and a separate team to conduct validation and testing)?
   - Will the AI governance processes ensure that the deployment of AI solutions complies with existing laws and regulations?
   - Should we adopt a centralized or decentralized decision-making approach based on certain guidelines? For example:
     - Take a centralized decision-making approach. For the deployment of an AI solution that is not determined to be low risk or would potentially be contentious, respective departments would bring the issue to the senior management or the AI ethics committee.
     - Take a decentralized decision-making approach. Respective departments can make the decision of whether to deploy the AI solution based on a predetermined whitelist and/or blacklist. Considerations that could be included in a blacklist are AI applications that would likely cause overall harm and direct injury. Having clear policies that describe off-limits practices (i.e., blacklisting) would be useful for organizations that adopt decentralized models where tracking AI is more challenging.

2. How does the company's board and/or senior management sponsor, support and participate in your organization's AI governance?

   Things to consider:

- Is it useful to form a committee/board that is chaired by a member of senior management and includes senior leaders from the various teams (e.g., chief data officer, chief privacy officer and chief information security officer)? Including key decision-makers is critical for efficiency and the credibility of the committee/board.

- Should we have top management set clear expectations/directions for AI governance within the organization?

3. Are the responsibilities of the personnel involved in the various AI governance processes clearly defined?

   Things to consider:

   - Is it useful or practical for the board and senior management to champion responsible AI deployment and ensure that all employees are committed to implementing responsible AI governance practices?

   - Who should be responsible for risk and strategy? Who will approve the AI models?

   - Are the roles and responsibilities for managing model risks and ensuring regulatory compliance clearly established and documented?

   - Who will be responsible for data practices, security, stability and error handling?

4. Are the relevant staff dealing with AI systems properly trained to interpret AI model output and decisions as well as to detect and manage bias in data?

5. Are the other staff who interact with the AI systems aware of and sensitive to the relevant risks when using AI? Do they know whom to raise such issues to when they spot them (e.g., subject matter experts within their organizations)?

6. Does your organization have an existing risk management system that can be expanded to include AI-related risks?

AI System (AIS) Impact Assessment Questionnaire

Index	Section / Question	Response
1	AIS Governance and Risk Management Framework	
	Does the company have a written AI Policy that provides a framework for setting AI objectives, and that addresses AI governance, risk management controls, the role of internal audit and third party AI systems that are acquired, used or relied upon by the organization?	
	Was the AI Policy adopted by the Board, senior management and/or a cross-functional committee?	
	Who in senior management is responsible for the operations for the AIS, including troubleshooting, managing, operating, testing, overseeing and controlling the AIS during and after deployment?	
2	AIS Overview	
	For what specific task(s) or purpose(s) will the AI system be used?	
	How does AI technology contribute to performing the task(s) or achieving this purpose(s)?	
	What potentially beneficial results of the AI system have been identified? For instance, does the AIS perform the relevant task(s) or achieve the relevant purposes(s) more effectively compared to the alternatives that do not use AIS (e.g. faster processing, higher accuracy, lower costs)?	
3	User Inputs and Interactions	
	Describe the types of data that users will input to the AI system?	
	Do the inputs include any personal data, or derivative thereof?	

	Do the inputs include anything proprietary to the Company, such as proprietary software code or other copyrighted material?	
4	AIS Outputs	
	What will be the outputs from the AI system?	
	Who will own the outputs from the AI system?	
	Do the outputs include any data or materials intended to be proprietary or confidential to the company?	
5	Risk Management and Internal Controls	
	Describe the AIS lifecycle management process.	
	Describe the process for identifying, assessing and tracking operational, financial, legal and compliance risks associated with the AIS.	
	Describe associated internal controls and other measures put in place to detect and mitigate risks with regard to the AIS.	
6	Documentation	
	Does the company have documented processes for monitoring the performance of the system to demonstrate that the AIS is operating as intended and within normal operating margins?	
	Does the company document standard operating procedures for the AIS, including events that should be monitored, how event logs are prioritized and reviewed, and how to investigate system failures?	
	Does the company have a documented plan for managing AIS failures, including a rollback plan for the AIS, turning off features of the AIS, a plan for notifying senior management, a plan for notifying customers and users of changes to the AIS, and how to mitigate system failures?	
7	Responsible AI Principles	

	Data Accuracy; Accuracy, Reliability and Robustness of the AIS	
	Has the company documented the standards and requirements around data quality for this AIS?	
	Transparency and Explainability	
	How will the company inform users and the public about the existence and functioning of the AIS? Do you adequately inform users that they are interacting with an algorithmic decision-making system?	
	Fairness, Bias and Disparate Impact	
	Does the AIS make or support decisions that could potentially result in a disparate impact to people on the basis of any of the following grounds (non-exhaustively): sex, gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, place of birth, disability, age or sexual orientation?	
8	Training Data	
	What data sets were used to train the AIS? Does the training data include public data or only Company data?	
	How were the training data sets be selected and acquired (licensed, purchased, collected directly, scrapped from the web, etc.) and from whom?	
	Has the company confirmed the data was lawfully acquired and is suitable or appropriate for the purpose?	