Inside AI: Practical Tips for In-House Counsel

Presented By:

Jeffrey Klamut
Cozen O'Connor
jklamut@cozen.com
August 2025

COZEN O'CONNOR

Agenda

- AI Orientation
- AI Regulations
- AI In-House
- AI Compliance Tips

AI Orientation

WHAT are we talking about?

- **Artificial Intelligence (AI):**

1. 1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. 2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
3. 3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. 4. A set of techniques, including machine learning, that is designed to approximate a cognitive task.
5. 5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

- ***Section 238(g) of the Nat'l Defense Authorization Act for FY 2019***

A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to –

(A) perceive real and virtual environments;
(B) abstract such perceptions into models through analysis in an automated manner; and
(C) use model inference to formulate options for information or action.

- **15 U.S.C. § 9401(3).**

An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

- ***Organisation for Economic Co-operation and Development Definition*** **(Mar. 2024)**

WHAT are we talking about?

- **Generative AI:**
  - "The class of AI models that emulate the structure and characteristics of input data to generate derived synthetic content. This can include images, videos, audio, text, and other digital content."

    Exec. Order 14110 § 3(p).

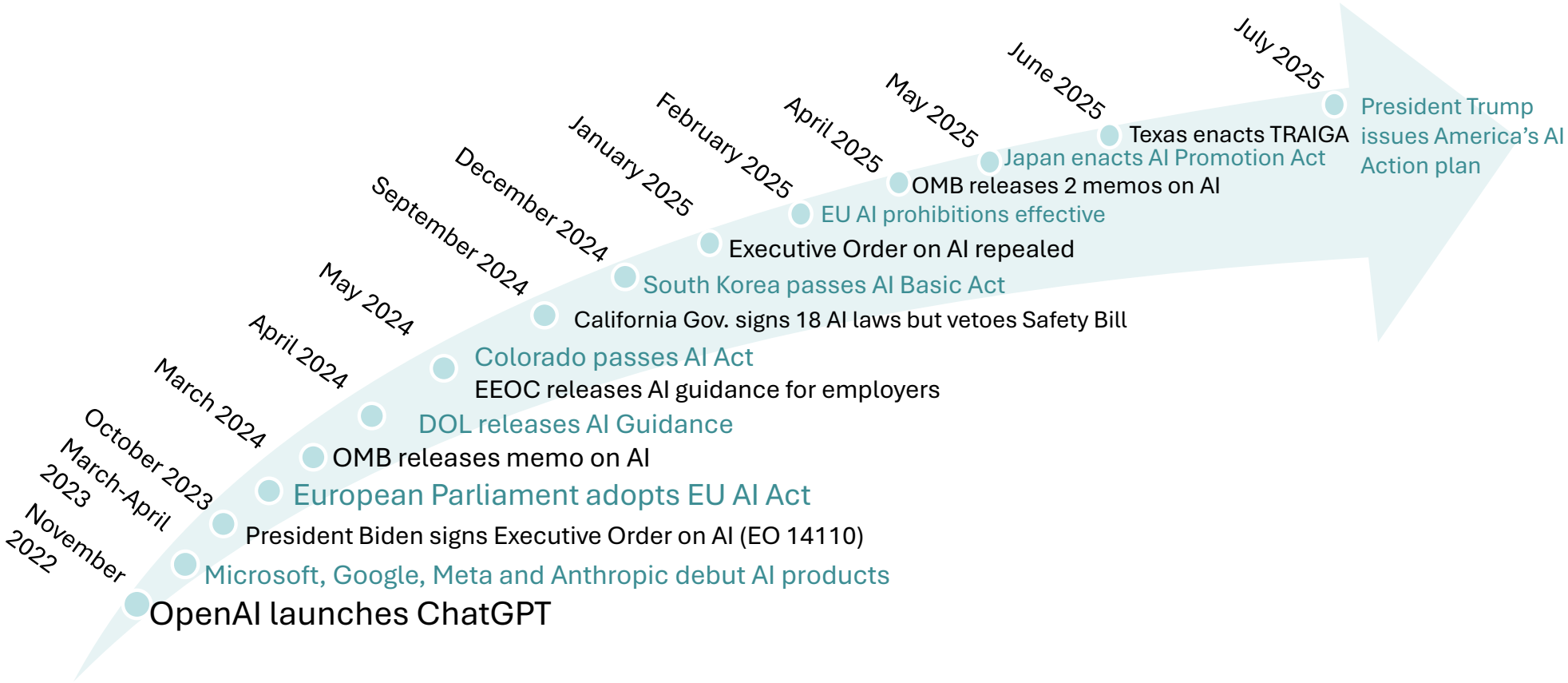
  - "[A] category of AI that can create new content such as text, images, videos, and music."

    OECD definition

  - AI that is "designed to mimic the structure and characteristics of input data to generate outputs such as text, sound, images, videos, and other creative content."

    South Korea AI Basic Act

WHERE are we?



COZEN O'CONNOR

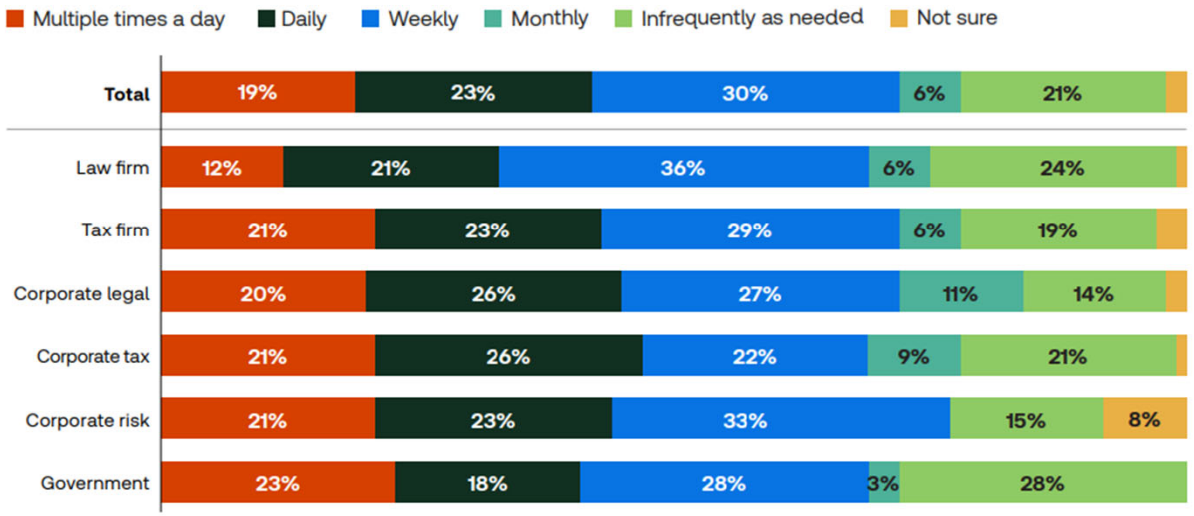
WHO is using AI?

- **Professional Services**: Professionals who said their organizations were actively using GenAI *nearly doubled* over the past year, to 22% in 2025, compared to 12% in 2024.

  2024 Generative AI in Professional Services, Thomson Reuters Institute, available at: https://www.thomsonreuters.com/content/dam/ewp-m/documents/thomsonreuters/en/pdf/reports/2025-generative-ai-in-professional-services-report-tr5433489-rgb.pdf

FIGURE 16:

Frequency of GenAI use among current users



Source: Thomson Reuters 2025

COZEN O'CONNOR

Risks of Using AI

- **Confidential and Proprietary Information Leaks**
  - Amazon (January 2023), Samsung (May 2023).
- **Security Vulnerabilities**
  - AI systems can be vulnerable to adversarial attacks. Generative AI models can create convincing social engineering attacks, including phishing and deepfake media.
- **Accuracy**
  - Generative AI systems deliver polished outputs that can promote a false sense of accuracy. Cases of professionals mistakenly relying upon inaccurate or fabricated information from AI continue to abound.
  - The accuracy of a generative output can be limited by that of the input and/or prompt.
- **Ethical Concerns**
  - AI, particularly GenAI, raises concerns about data collection, use, and retention by AI systems and users; how models are trained on data (and resulting biases are created); how outputs are used and who owns them; human oversight; and transparency.

Risks of AI In-House (continued)

- **Employee Data Privacy and Confidentiality**
  - If employee data is inputted to an AI system without adequate security protocols (or used to train an AI without adequate anonymization), it could lead to unauthorized data exposure, data exfiltration, or even identity theft.
- **Disparate Impact and Unintentional Bias**
  - An AI system trained on intentionally or unintentionally biased data could favor certain demographics over others. *See Mobley v. Workday*, 3:23-cv-00770-RFL (N.D. Cal) (now a collective action alleging disparate impact in AI hiring).
  - AI has potential to produce skewed results from additional phenomena, such as overfitting, inappropriate focus, and interpretive bias.
- **Job Displacement and Workforce Impact**
  - AI may reduce the need for certain entry-level roles, leading to layoffs and potential reputational risks for a deploying company.

AI Regulations

Key International AI Laws

The EU AI Act (most provisions effective August 2, 2026)

- Applies to all entities that use, make, or supply AI systems in the EU or, if outside the EU, use AI in a way that affects people in the EU.
- Takes a risk-based approach to regulating AI.
  - "Unacceptable" risk AI systems are prohibited, effective February 2025. These include:
    - **AI systems that conduct emotion recognition in the workplace or educational institutions, and**
    - **AI systems that use biometric information to infer sensitive data such as religion, orientation or union status.**
  - "High" risk AI systems, which include systems used for employment (job ads, resume screening, etc.) come with regulations for developers, suppliers, and users, including:
    - **Human oversight to competent people, ensuring inputs are relevant and tailored to the system's purpose;**
    - **Notice to users that they are subject to high-risk AI system, its purposes and types of decisions it makes, and right to an explanation; and**
    - **Recordkeeping, use monitoring and reporting obligations for certain incidents.**
  - "Limited" risk AI systems, like chatbots, have transparency requirements.
  - "Minimal" risk AI systems, like spam filters, can be used freely.
  - Penalties include fines up to €35 million or 7% of global annual turnover.

Key International Laws (continued)

South Korea AI Basic Act (effective January 2026)

- Applies to AI Business Operators in Korea or affecting the Korean market/users.
- Takes a risk-based approach to regulating AI .
  - High impact AI ("HI AI") systems: **pose significant risks or impacts on human life, physical safety, or fundamental rights. Covers areas such as access to essential services, health care, and employment and hiring.**
  - Generative AI ("GenAI"): **designed to mimic the structure and characteristics of input data to generate outputs such as text, sound, images, videos, and other creative content.**
- Obligations
  - Preliminary Review: Businesses must determine if they are using HI AI. Can seek decision from government.
  - Transparency: Business using HI AI or GenAI in products or service must provide notice to users.
  - Risk: Large systems must conduct risk monitoring and management and submit results to officials.
  - HI AI Requirement: Businesses providing or incorporating HI AI systems into their products or services, must:
    - **develop and implement a risk management plan;**
    - **establish and execute measures to explain the AI system (including an overview of the training data);**
    - **develop and implement a user protection plan;**
    - **ensure human supervision and oversight of the high-impact AI system;**
    - **maintain documentation on safety and reliability measures;**
  - Foreign businesses: Required to assign a local compliance representative if they meet certain thresholds.

Key International Laws (continued)

Japan's AI Promotion Act (May 28, 2025)

- Adopts a top-down approach to promoting AI-related technologies (AIRT).
- Basic principles:
  - Promote R&D, development, and use of AIRT to improve security and prosperity; and
  - Transparency, coordination, and international cooperation to prevent against risks of AIRT
- Directives
  - National Government: Implement AIRT policies, use AIRT to improve efficiency, strengthen stakeholder collaboration, and take all necessary legislative and financial measures to promote AIRT.
  - Local Governments: Implement independent AIRT policies tailored to local contexts in cooperation with the national government.
  - Research and Development (R&D) Institutes: Conduct AIRT research, disseminate findings, foster talent, and cooperate with government policies.
  - Business Operators: Encouraged to actively utilize AIRT to improve efficiency and innovate, and to cooperate with government policies.
  - Citizens: Expected to deepen their understanding of AIRT and cooperate with government policies.

Key U.S. Federal Regulations

- **The U.S. Does Not Have Comprehensive Federal AI Legislation.**
  - **Executive Order 14110** (October 30, 2023 repealed January 20, 2025)
    - Ordered federal agencies to issue regulations for the use of AI in their respective areas of enforcement and called for studies and reports.
    - Reporting requirements for certain large AI models, large-scale computing clusters, and infrastructure as a service (IaaS) providers.
  - **America's AI Action Plan** (July 23, 2025): Latest policy focused on three "pillars":
    - Accelerating AI innovation
      - Remove regulatory barriers, review prior agency action, promote free speech.
        - » Contemplates restricting federal funds to states that unduly regulate AI.
      - Invest in developments, AI ecosystem, and workers.
      - Combat synthetic medial in the legal system.
    - Building American AI infrastructure
      - Focus on data centers, energy, grid, semi-conductors, and workforce.
    - Leading in international AI diplomacy and security

Key U.S. Federal Regulations

- **OMB memos** (April 3, 2025)
  - M-25-21: *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*
  - M-25-22: *Driving Efficient Acquisition of Artificial Intelligence in Government*
    - Set structure and expectations for procurement of AI by the U.S. Government.
    - Require governance boards, compliance plans, policies, use case inventories, risk assessments.
  - Keys for businesses
    - Preference for U.S.-made AI programs
    - Preference for interoperable programs
    - Preference for certain contractual terms:
      - » Government retains rights to its data and any improvements to that data, including the continued design, development, testing, and operation of AI.
      - » Data is protected from unauthorized disclosure or use, and from being used to train or improve the functionality of the vendor's model without express permission.
      - » Vendor lock-in should be prevented.
    - Providing access to the underlying AI source code, models, or data, will facilitate an agency's compliance with pre-deployment testing obligations.

Key State and Local Regulations

- **Colorado**
  - Artificial Intelligence Act (effective 2/2026). Colo. Rev. Stat. § 6-1-1701.
  - Requires certain companies using AI to:
    - Develop an AI risk management policy and program;
    - Conduct yearly AI impact assessments and keep them for three years;
    - Annually review deployment "to ensure that the high-risk artificial intelligence system is not causing algorithmic discrimination";
    - Provide pre-notification to applicants and employees concerning AI;
    - Provide information on right to opt-out of the processing of personal data for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects; and
    - Provide "adverse decision" notices with reason for decision, extent to which AI was involved, types of data processed and their sources, and opportunity to correct source data and appeal.
  - Requires statement on website summarizing types of high-risk AI systems deployed, how risks of algorithmic discrimination are managed, and "[i]n detail, the nature, source, and extent of the information collected and used by the deployer."
  - Must disclose to consumers if they are interacting with an AI system.

Key State and Local Regulations

- **California**
  - AI Transparency Act (SB 942, eff. 1/1/2026) requires large GenAI producers to provide AI detection tools and disclosures, and to follow certain contract procedures for GenAI.
  - GenAI Training Data Transparency Act (SB 2013, eff. 1/1/2026) requires GenAI providers to publicly disclose on website detailed information about the datasets used in development.
  - Enacted AB 1836 & AB 2602 re: unauthorized digital replicas of voice or visual likenesses.
- **Illinois**
  - Digital Voice & Likeness Protection Act (HB 4762) and Right of Publicity Act (HB 4875).
  - Human Rights Act Amendments (HB 3773) (eff. 1/2026) will require employers to notify employees when they use AI for employment decisions; prohibit AI discrimination.
  - The AI Video Interview Act restricts the use of AI-enabled video interviews. 820 ILCS 42.
- **New York**
  - NYC Local Law 144 requires employers to conduct bias audits on automated employment decision tools and provide related notices.
  - Mini-WARN act will require businesses with 50+ employees to report AI-driven layoffs.

Key State and Local Regulations

- **Texas**
  - Texas Responsible Artificial Intelligence Governance Act ("TRAIGA") (H.B. 149)
    - Applies to a person who (1) promotes, advertises, or conducts business in Texas; (2) produces a product or service used by residents of Texas; or (3) develops or deploys an AI system in Texas.
    - Disclosure requirements for Gov't and healthcare institutions using AI to interact with people.
    - Prohibits:
      - Developing or deploying an AIS to influence another to (1) commit physical self-harm (2) harm another person; or (3) engage in criminal activity; developing or distributing an AIS to simulate criminal activity/child abuse; developing or using an AIS to violate others' Constitutional Rights;
      - Government social scoring, biometric data scraping; and
      - Discrimination: developing or deploying an AIS *with the intent* to unlawfully discriminate against a protected class in violation of state or federal law (disparate impact is not dispositive of intent).
    - AG enforcement, audit powers, NIST defense.
- **Utah Artificial Intelligence Policy Act** (2024R Utah S.B. 149)
  - Commercial deployers of an AI system must "clearly and conspicuously disclose" to consumers that they are interacting with generative AI. "Regulated" deployers must do so at the outset, others must do so if prompted.

New York Proposed AI Legislation

- **Responsible AI Safety and Education ("RAISE") (S6953B)**
  - Comprehensive AI Regulation of "Frontier Models"
    - Systems trained using more than 10^{26} integer operations, exceeding $100 mil in compute cost
    - Models produced by knowledge distillation of frontier models, exceeding $5 mil in compute cost
      - Knowledge distillation means "any supervised learning technique that uses a larger [AI] model or the output of a larger [AI] model to train a smaller [AI] model with similar or equivalent capabilities. . . "
  - Developer requirements
    - Before deploying a frontier model in NY:
      - Implement a written safety and security protocol, publish it (with redactions),
      - Transmit redacted copy (and make less-redacted copy available) to AG and DHSES,
      - Retain protocol and info on assessment test results (sufficient for replication) for 5 years, and
      - Implement safeguards to prevent unreasonable risk of harm, or do not deploy.
    - Ongoing requirements:
      - Annual review of protocol to account for changes/best practices, modify as needed
      - Disclose each safety incident affecting the FM to the AG and DHSES within 72 hrs.
  - Violations: injunctive, declaratory relief, civil penalties
    - Up to $10 mil for first violation, $30 mil for subsequent violations.

Pennsylvania Proposed AI Legislation

House Bill 1598/Senate Bill 1044 (2024): would have amended the Unfair Trade Practices and Consumer Protection Law to require businesses to provide clear and conspicuous disclosures on content generated by artificial intelligence. This includes written text, images, audio, and video content, ensuring consumers are informed when they are interacting with AI-generated material.

House Bill 1729 (2023) would have amended the Pennsylvania Human Relations Act to regulate employer usage of "automated employment decision tools" (AEDT). AEDTs are tools that automatically filter individuals for employment-related purposes. (Died in committee).

Bias Audits: to use an AEDT, an independent bias audit must have been conducted within the previous year with results published on employer's website

Notice and Consent: individuals must be given at least 10 days' notice of intended AEDT use, including how the AEDT evaluates individuals for an employment decision, and must consent to such use.

AI In-House
What you can expect to see

AI In-House: Where you will see it

- **Everyday Use and General Amazingness:**
  - Employees may already be using generative AI through Google searches.
  - Various large language models may be used to research, write, and even code.
  - Enterprise solutions like Microsoft CoPilot offer functionalities across the entire Microsoft 365 platform, allowing employees to use AI to check schedules, answer emails, generate images, create power points, and call excel functions.
  - AI chatbots and interactive avatars can power customer interactions and employee training, and increasing accessibility.
- **Confidentiality/Data Protection:**
  - If not properly managed, AI provides a major window through which confidential information can be viewed or leaked. Who is using AI in your company? How?
  - Public AI models are not inherently secure and may not follow data protection laws. Are you restricting access to public AI models? If not, do you have rules on using confidential information or personal data as inputs in such models?

AI In-House: Where you will see it (cont'd)

- **Cyber-Security:**
  - AI increases already-known risks and reinforces the need for basic security measures such as pw hygiene, 2FA, software patches, and phased protection along the cyber kill chain (training, inside-security, penetration testing, threat intelligence, honey pots, etc.).
  - AI introduces some new risks too, such as data poisoning/back doors during fine tuning, jailbreaking AI models, and tricking others into inputting sensitive data to open models.
  - The good news is that AI also allows companies to scale-up defenses to cyber threats.
- **Contracts/Supply Chain:**
  - Expect to see AI compliance questions in supply chain questionnaires, particularly if you are a vendor to an EU company or US government agency.
  - The right contractual language regarding AI can protect your company's interests and make you a more attractive vendor, even in the U.S.
  - IP issues about who owns inputs, outputs, or ideas that expand a platform's offerings.
- **Document Management, Collection, and Review/Litigation:**
  - AI can improve efficiency in organizing, collecting. and reviewing documents.

AI In-House: Where you will see it (cont'd)

- **Workforce Management:**
  - AI can be a powerful tool for workforce management/HRIS with proper controls.
  - AI can assist with recruiting efforts, but algorithmic discrimination is a key concern of policy makers, so various interventions may be required depending on the jurisdiction.
  - AI can improve timekeeping, productivity measurements, and payroll functions, but there can be problems associated with assumptions that are tied to legal implications.
- **Customer Interactions:**
  - AI can supercharge customer interactions, but this requires compliance with transparency, disclosure, and privacy laws where the interactions occur or reach.
    - Any use of AI that touches customers in the EU must comply with EU AI act.
    - California Consumer Privacy Act covers personal information in AI inputs or outputs.
  - Chatbots require guardrails to avoid inappropriately manipulating customers *and* to avoid being inappropriately manipulated by "customers."
- **Reporting**:
  - DOJ and SEC are prosecuting cases of "AI washing."

AI Compliance Tips

Tips For Compliance

- **Inventory how your organization is using AI.**
  - Which tools are officially *allowed*?
  - Which tools are employees *actually using*?
- **Gain basic understanding of your AI systems' architecture.**
  - What are the main components and how do they interact with each other?
  - Where is your data and how is it collected and processed?
  - What hardware or software is used and how is it protected?
- **Understand fundamental security concepts.**
  - No Training: Is your organization's data being used to train the AI model?
  - Zero Day Retention: Is your AIS provider retaining inputs/outputs that can be accessed by third parties (including within the AIS provider)?
  - Data Minimization: Only collect and retain the data that is absolutely necessary for the AI system's function, thereby reducing the risk of exposure.

Tips For Compliance (cont'd)

- **Determine which laws are relevant to your business.**
- **Determine if any industry-specific guidelines apply to your business or role**
  - E.g., ABA's Model Rules, NAIC AI Principles, DOD's RAI.
- **Become familiar with the major risk management frameworks.**
  - NIST AI Risk Management Framework (AI RMF 1.0)
  - ISO/IEC 42001:2023, an int'l standard focusing on ethics and risk management
  - NIST Generative AI Profile (NIST AI 600-1)
  - ISO/IEC 23894:2023, guidance for managing lifecycle of AI systems risks
- **Identify prohibited and encouraged use cases and how to monitor them.**
  - "Public AI" vs. "Enterprise AI"
  - No confidential, personally identifying data.
- **Develop compliance plan (including policy) tailored to applicable laws and train.**

AI Policy Tips

- **Establish the scope and relevant definitions**
  - Policies may change depending on where they apply and who they cover so defining scope (particularly user vs. developer) is important.
  - Work through how concepts of AI, GenAI, Permitted AI, and Prohibited AI will interplay in your organization so that you know which terms you want to define and how. This is not "one size-fits all."
- **State General Principles**
  - Stating principles can fill-in any gaps and help align with risk management frameworks or industry-specific objectives.
  - Examples: fair, accountable, transparent, safe/secure, etc.
- **Establish key stakeholders and decisionmakers for AI governance, accountability, and responsibility mapping.**

AI Policy Tips

- Establish procedures for the scope of covered activities.
  - Incorporate relevant existing policies and procedures.
  - Using AI
    - Explain the generally permitted and prohibited use cases.
    - Address any specific use cases that may require special attention (e.g., customer data, employee data, AI decision-making, etc.).
    - Provide examples or an appendix of approved AI systems.
    - Establish employee responsibilities for inputs, outputs, monitoring, and reporting.
  - Developing AI
    - State whether your organization intends to generally follow any relevant frameworks.
    - Cover data/model documentation, risk reviews, testing, training, and monitoring.
- Include a reporting mechanism (e.g., ethics hotline).
- Allow for variability and iterative modification.

QUESTIONS?