ACC Association of Corporate Counsel

Artificial Intelligence Toolkit for In-house Lawyers

Strategies to drive business success and advance your career

WHAT IN-HOUSE LAWYERS SAY ABOUT THIS TOOLKIT:

"This toolkit is a one-stop-shop for an in-house lawyer's AI questions and needs. New to using AI? Check out the checklist on ways to get started. Experienced AI user? Check out the checklist on ways to refine and improve your existing governance and mitigation processes. This is a great resource that every in-house attorney should use!"

Meganne Thaxton, *Senior Corporate Counsel,* Red Ventures

Thank you to ACC members

The ACC team warmly thanks the global group of ACC members and in-house legal professionals who shared their insight regarding this toolkit *(their input was personal and not on behalf of their organizations)*:

Meganne Thaxton
Senior Corporate Counsel, Red Ventures

Douwe Groenevelt
Former Deputy General Counsel and Former Head of Legal, ASML

Aparna D. Williams
Chief Legal and Compliance Officer, Coalfire

Malaika Roemer CIPP/US
Principal Paralegal and Compliance Program Manager, Coalfire

Schellie-Jayne (SJ) Price
Chief Legal Officer, Nooriam
Founder of ACC Australia's Legal Technology & Innovation Special Interest Group

ACC thanks Kilpatrick Townsend & Stockton LLP for their generous sponsorship of this toolkit and for the content they provided for this resource.

Kilpatrick

ACC also thanks **Christopher Oberst**, *Legal Resources Specialist* at the Association of Corporate Counsel, who served as lead editor in the development of this toolkit.

WELCOME

The AI revolution has landed in legal. In-house lawyers are no longer observers; they are now expected to master artificial intelligence and steer their organizations through this transformative shift.

According to a 2024 survey report published by ACC and Everlaw, ***GenAI and Future Corporate Legal Work: How Ready Are In-house Teams?***, less than half (42%) of in-house lawyers feel prepared for the impact of Generative AI on their careers. The rapid adoption of new AI technologies can feel overwhelming, as businesses face new opportunities balanced against the legal and regulatory complexities inherent in the AI landscape.

Today, we are witnessing AI bring fresh perspectives for innovation, creation, and efficiency, benefiting both businesses and legal departments. Global companies are incorporating AI into their corporate strategies—whether by using Generative AI or other AI tools in their processes, developing their own AI models or systems, or embedding AI functionality into their products and services.

However, AI also presents significant challenges that in-house lawyers and their organizations must address—ranging from ethical considerations and regulatory compliance to issues of intellectual property, privacy, data security, confidentiality, and more.

To support our members as they navigate the evolving world of artificial intelligence, ACC has developed a new AI Toolkit. This resource reflects our ongoing commitment to equipping in-house counsel with the tools they need to thrive. The ACC AI Toolkit is designed to help legal teams support their organizations, build effective AI governance frameworks, harness the benefits of AI, manage potential risks, and grow professionally in an AI-driven landscape.

We would like to extend a special thank you to the ACC members who contributed their insights to this resource. Our thanks also go to Kilpatrick Townsend & Stockton LLP for their generous sponsorship and thought leadership on this critical topic.

As always, ACC is committed to providing members with practical, up-to-date resources that empower in-house counsel to tackle complex issues with confidence. We welcome your feedback and suggestions as we continue to refine and expand this toolkit to meet your evolving needs. Please share your thoughts with us at ***legalresources@acc.com***.

Best regards,

Veta T. Richardson

PRESIDENT AND CEO
ASSOCIATION OF CORPORATE COUNSEL

All companies are now AI companies.

Kilpatrick Connect is a legally focused consulting and advisory offering from Kilpatrick designed to help your business address and leverage all aspects of AI. Our offerings are customized to guide you through the complex legal, regulatory, and policy environment related to AI. We support the creation of practical and actionable strategies and solutions, ensuring your business stays compliant, mitigates risks, and is positioned for growth.

Kilpatrick

ktslaw.com | Attorney Advertising

CONTENTS

Who is this toolkit for?

From junior lawyers to Chief Legal Officers, this toolkit is relevant for all in-house counsel who want to understand Artificial Intelligence (AI) and be AI-savvy leaders for their business.

- **AI presents major opportunities** – to automate tasks, make processes more efficient, analyze vast amounts of data, improve customer service, generate content, and more.
- **It also poses legal, ethical, and business challenges**, and requires fast adaptation and upskilling by business and legal teams.
- **A patchwork of laws and regulations** is unfolding around the world, as authorities seek to establish AI governance principles, foster innovation, and mitigate risks.
- **General counsel and their teams have a leading role** to play in helping the business take advantage of the AI wave in a way that optimizes benefits and mitigates risks.
- **This toolkit offers** practical checklists and insights to help you be an effective leader in your organization's AI preparedness.

Where is this insight from?

The insight in this toolkit is mainly based on:

- Resources from the ***ACC Resource Library*** that the ACC team has found relevant;
- Thought leadership from law firm ***Kilpatrick Townsend & Stockton LLP***, and
- The perspectives of ACC members, experienced in-house counsel who kindly shared input.

The Association of Corporate Counsel

- The Association of Corporate Counsel (ACC) is a global bar association.
- ACC promotes the common professional and business interests of in-house counsel through information, education, networking opportunities, and advocacy initiatives.
- The ACC community includes more than 48,000 members from around the world.
- ACC is invested in your success as an in-house lawyer, a General Counsel, or a Chief Legal Officer. ACC advocates for you to have a "Seat at the Table" and provides value with resources for your team to succeed.
- Are you an in-house counsel? ***Join us!*** Learn, connect with peers, and boost your career.

Disclaimer: *The information in this toolkit should not be construed as legal advice or legal opinion on specific facts. It should not be considered representative of the views of the Association of Corporate Counsel (ACC) or any of its lawyers, unless so stated. This toolkit is not intended as a definitive statement on the subject, but rather to serve as a resource providing practical information to the reader. AI is rapidly evolving. ACC makes no representations or warranties regarding the accuracy or completeness of this toolkit. This toolkit was developed mostly between December 2024 and March 2025.*

AI and In-house Survey Data at a Glance

Most in-house professionals are using or planning to use GenAI at work

38% Already using in legal practice

52% Planning to use

10% Neither using nor planning to use

Reasons for not using GenAI

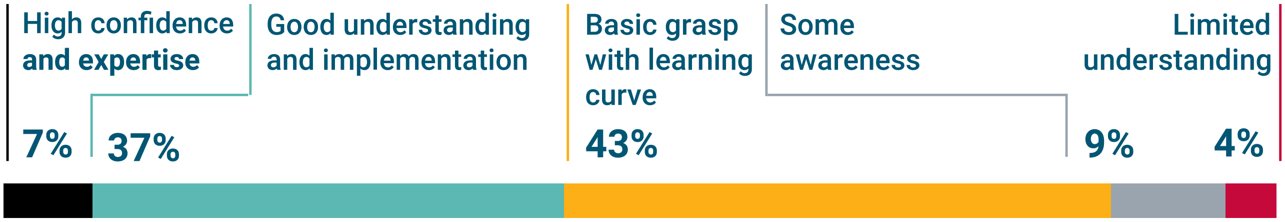
49%	Not a priority
45%	Concern about how data will be used
45%	Don't trust the quality of outputs

More than two-thirds use GenAI at least once a week

69% Use GenAI at least once a week

Chief Legal Officers	79%
Legal Operations Professionals	77%
Other Attorneys	65%

87% have at least a basic grasp on GenAI tools



Top benefits of using GenAI at work

86%	Increased efficiency
38%	Improved communication
25%	Cost savings
22%	Enhanced accuracy and consistency
16%	Improved decision making

Source: ***GenAI and Future Corporate Legal Work: How Ready Are In-house Teams?***, Association of Corporate Counsel and Everlaw, October 7, 2024

AI and Attorney-client Privilege: Survey Insights

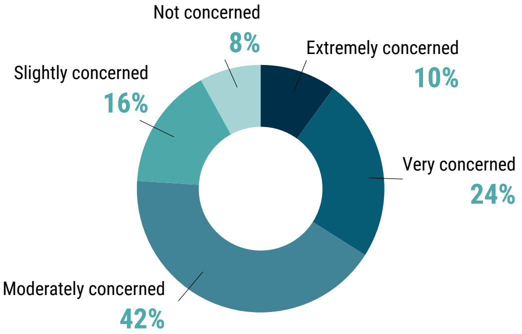
Risk perception, concern about AI's impact on privilege, and proposed actions to mitigate risks

56% believe the use of AI tools has the potential to compromise attorney-client privilege

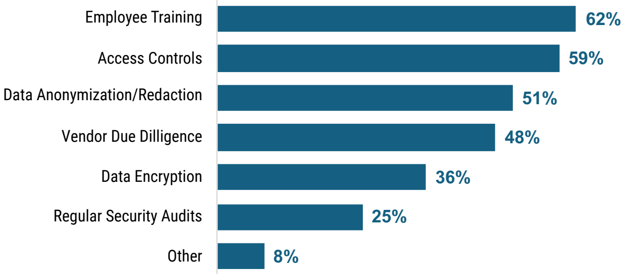
27% said that the risk of compromising privilege is dependent on the AI tool, its usage, or on the specific circumstance.

7% of respondents globally say they have encountered specific instances where the use of AI has raised questions about the applicability of attorney-client privilege.

How concerned are you about the possibility of inadvertently disclosing privileged information when using AI-powered tools?



Measures currently taken to protect privileged information when using AI tools



Proposed Actions to Mitigate Risks to Attorney-client Privilege

80%	Create specific guidelines for AI use in legal practice
56%	Enhance data privacy and security standards
50%	Increase public awareness about the risk of AI and attorney-client privilege
49%	Develop laws and/or regulations for AI tool providers
49%	Use contract clauses or other means to establish liability for AI-related breaches

Source: ***The Impact of AI on Attorney-Client Privilege***, Association of Corporate Counsel, September 11, 2024

Top Five Key Points for In-house Counsel

1. **Identify** how AI tools can improve productivity and business outcomes.
2. **Implement AI governance and usage policies** to encourage effective use of AI tools while mitigating legal and business risks.
3. **Consider how AI solutions** can foster efficiency and automate processes for the legal department. Stay compliant with your ethical obligations.
4. **Protect your organization's intellectual property** when adopting AI systems, and avoid the risk of infringing the IP rights of others.
5. **Address AI-related risks in your contracts with vendors.** Mitigate data privacy, cybersecurity, and other risks. Reduce your organization's risk of liability for misuse of AI by vendors or their subcontractors.

Key Data Insights for In-house Lawyers

Learn how in-house lawyers view AI, through data from recent ACC surveys:

23% of in-house legal professionals are already using GenAI in their work.

From those, 86% report GenAI increased their task completion efficiency.

Only 42% of respondents feel prepared for the impact of GenAI on their career.

Only 26% feel their legal department is prepared for the impact of GenAI.

One in five CLOs lists AI in the top three concerns for regulatory enforcement.

35% of CLOs list operational efficiency as their department's top strategic initiative for the year.

44% of CLOs say they plan to adopt new legal technology in their department to improve efficiency in the next year.

Top technology types that CLOs plan to implement: contract management **(62%)**, document management **(32%)**, and workflow tools **(26%)**.

Learn more

- → Gain more insights from the report on ***GenAI and Future Corporate Legal Work: How Ready Are In-house Teams?*** (October 2024, by ACC and Everlaw).
- → Learn more above privilege-related concerns, in the ACC survey report: ***The Impact of AI on Attorney-Client Privilege*** (September 2024).
- → Read the findings from the ***2025 ACC Chief Legal Officers Survey Report*** (January 2025).
- → Read the findings from the ACC Foundation's ***2025 State of Cybersecurity Report: An In-house Perspective***.

Ten AI Trends in 2025

The rapid rise of Generative AI disrupts industries and forces businesses to adapt. Governments seek to strike a balance between innovation and regulation. Learn ten key trends in the evolving AI landscape in 2025.

1. Overall: Continual Advancement and Novelty.

- The fast-paced development and adoption of increasingly novel AI technology will continue, with impacts on business, law, and society.
- Companies, consumers, and governments work to keep pace and adapt.

2. Regulatory Uncertainty.

Governments have adopted a ***patchwork of AI laws and regulations***. Businesses need to adapt to this shifting regulatory landscape that remains uncertain. For example:

- The European Union adopted an AI Act that places risk-based safeguards and restrictions on AI systems.
- In the United States, some states have modeled laws on the comprehensive EU AI Act, some have narrowly amended existing laws, and others wait. Federal agencies have implemented scope-specific regulations. The new US administration will also probably introduce changes, likely taking a lighter regulatory approach.

3. Litigation and Potential Verdicts.

The rise of Generative AI spawned several lawsuits. These disputes highlight open questions and the challenges for businesses to manage AI-related risks.

- Cases range from privacy challenges to copyright and trademark disputes, and tort claims for defamation.
- Key disputes concern privacy and intellectual property rights inherent in training large language models and assembling data sets. Such cases could upend the legal landscape.
- One question is whether the use of copyrighted text and images to train AI models will be deemed "fair use" under copyright law, or an infringement of intellectual property rights. The former outcome would leave content owners unhappy about the uncompensated use of their creations; the latter would increase the already high cost of developing AI models, and the cost to consumers, if rights holders obtain compensation.
- Other cases and administrative rulings assess whether AI-generated outputs can infringe copyright, and whether AI-generated material can be protected under copyright law.
- Another wave of litigation challenges new AI regulations.

WITH THANKS TO:

***Kurtis G. Anderson*, *Associate* at *Kilpatrick*,**

for providing this list of AI trends.

4. **Consumer Protection.** Risks of fraud or misuse rise as AI becomes even more prevalent. As consumers' use of AI grows, companies can expect greater regulatory and enforcement pressures.

   - Legislators, regulators, and the public are focused on consumer protection.
   - For example, the European Union and Colorado regulate high-risk AI uses. New York and Colorado prohibit algorithmic discrimination in employment decisions. US federal agencies have put corporate AI use under scrutiny.

5. **Risk of Liability.** As regulation gives way to enforcement, a key question is liability.

   - It remains open whether users, the AI tool provider, or both will be liable for actions performed by or with an AI model.
   - It's unclear who will be held responsible for a "hallucination," misdiagnosis, bad advice, or misreporting.
   - The same is true for users who generate content that infringes a copyrighted work that the AI model used from its training.
   - In the US, some states and federal agencies have made corporate adopters liable.

6. **AI in Action.** Whether or not forecasts will be accurate, the effects of adoption will likely be marked across the board.

   - Speculation has sounded on the impact of Generative AI on everything from personal search habits to entire industries.
   - This speculation will give way to real market impacts.
   - Companies will be pressed to deliver results.
   - The effects of company and industry-wide adoption will be realized, and the promises—and threats—of AI will be tested.

7. **More Power and ESG Challenges.** Energy needs for AI development may become a bottleneck and pose ESG challenges.

   - The demand for training data grows exponentially, as technology companies develop increasingly advanced AI models. Consumer adoption of AI also increases.
   - A single AI data center can consume as much energy in 24 hours as a large metropolitan city.

- The cost of energy will therefore likely increase, along with investments and innovations in energy production.
- These demands and costs may challenge existing corporate and regulatory green-energy and climate-change goals.

8. **Security & Fraud Challenges.** The rise of increasingly convincing scams poses risks to consumers and companies alike, putting intellectual property, money, and reputation at risk.

    - AI has come with abuses and risks, such as “deepfakes.”
    - These dupes of real content and people (in text, audio, or video form) have empowered scammers to create increasingly elaborate schemes and target individuals and corporations.

9. **Novelty.** Increasingly powerful AI models will be used to replace tasks and functions previously thought beyond AI’s limited reach.

    - So far, AI has been integrated into existing business routines and bolted onto established products. The focus has been on efficiency gains and consumer adoption.
    - Going forward, the focus will begin to shift to more novel use cases. The scope of these novel uses is beyond prediction, but they are continually being developed and tested.

10. **The Rise of Agentic AI.** Tasks that once required human agency will be replaced by automated assistants.

    - Generative AI captured public attention for its ability to mimic human speech and generate content in human-like language.
    - However, its limits are apparent. It acts effectively in response to direct human prompts, but struggles to act independently or follow increasingly complex chains of tasks or instructions.
    - The rise of digital agents and automated workflows powered by AI is coming. For example, AI may assist corporate counsel in managing sophisticated nationwide litigation dockets, or in conducting preliminary contract negotiations between and with sub-contractors and suppliers.
    - This evolution will likely come with increased risks to privacy, security (e.g., access control issues), and quality assurance.
    - Companies will need to balance these risks with the potential—or necessity—of adopting novel AI tools.

CHECKLIST 1

Seven AI Basics for In-house Lawyers

Learn what artificial intelligence is (and is not), and get a grounding in the essential terminology.

This checklist is based mainly on the following ACC resources, and on insight from the sponsor Kilpatrick and from ACC members.

→ ***Tech Toolbox: Implications of Generative AI for Law Departments, Part 1,*** by Greg Stern, *ACC Docket*, March 16, 2023

→ ***Tech Toolbox: Implications of Generative AI for Law Departments, Part 2,*** by Greg Stern, *ACC Docket*, June 8, 2023

→ ***Legal Tech: As AI Technology Advances so Must Our Legal System,*** by Olga V. Mack, *ACC Docket*, February 7, 2023

→ ***Visit the ACC AI Resource Collection***

1. **Artificial intelligence and AI tools are not new.** You've likely been using them for years in your work, even if you did not know it.
   - Lawyers have been using AI tools to **assist with many tasks**, such as:
     - **Organizing and searching** through large volumes of documents;
     - **Identifying patterns** in legal documents and cases;
     - **Drafting** contracts and other documents; and
     - **Automating manual tasks** like approval workflows, data collection and entry, and scheduling.
   - For example, well-known **legal research platforms** (such as Westlaw® and LexisNexis® have incorporated AI technology for several years to aid users in **searching and analyzing** large legal data sets like case law, statutes, and regulations.

2. **Hybrid AI models** combine multiple technologies, such as machine learning and **natural language processing (NLP)**, to create powerful tools like chatbots that can interact with users.

3. **Generative AI** is the newest category of AI, and is often what people now mean when they use the term "AI."
   - **GenAI** does not simply organize or analyze data. It is software that can **generate language, pictures, or even other computer programs**, typically from plain language text prompts.
   - This technology relies on **large language models (LLM)**, which analyze massive sets of human-created content to generate and classify text, answer questions in a conversational manner, and translate text from one language to another.
     - Essentially, LLMs use data analysis and NLP to **predict**, word by word, **what type of response a human would give** to a question or instruction. Because each new word is based on what the AI tool already generated, a single misstep by the AI can lead the entire output off track and cause the AI to produce an incorrect response.

4. GenAI does not "think" in the way that a human does.

However, newer AI models are being designed to engage in multi-step solutions to complex tasks and questions and even to analyze their own output for likely mistakes at each stage.

5. GenAI models are only as good as the data they are trained on.

For a GenAI tool to provide quality output of text, images, or sounds, it must have a large volume of high-quality data to analyze.

- **"Unclean"** data, containing errors, contradictions, or irrelevant content, may cause a GenAI model to generate a response to the user's prompt that looks correct but is inaccurate, sometimes wildly so. These **inaccurate** responses can often appear very convincing, so users must check the model's output carefully.
- **"Hallucinations"** in AI outputs are usually caused by training data sets that are too small to 'produce' accurate information. A dataset can be fed with correct training data but may still make mistakes, especially if the set isn't large enough or if its training hasn't incorporated enough computing power.
- **Large public GenAI models** like ChatGPT use training data sets which may contain content scraped from the Internet, including copyrighted text, images, and audio. Even when they use large amounts of training data, GenAI models can yield inaccurate (or made-up) answers.

6. GenAI tools aimed at the legal industry

often aim to be more precise and effective by using processes like "retrieval-augmented generation" (RAG, defined below) to enrich their AI models with additional legal information, such as case law and dockets, statutes and regulations, and regulatory filings.

7. Good practices for these legal-oriented AI tools:

- **Having the tools "*sandboxed,*"** i.e., tested in a secure environment isolated from the rest of your systems and data.
- **Having the tools "gated" or "walled off,"** i.e., operated as an instance that is either hosted solely within your organization's systems or, if hosted in the vendor's environment, an instance that is dedicated to you and not shared or comingled with other users' data and instances (unlike large public models), to **ensure that your users' private data is not publicly released** to the wider Internet (or shared with other users or with the vendor itself) when they interact with the tool.

Also check out:

→ ***Basics for Corporate Counsel to Consider About Generative AI*,**
by Meghan K. Farmer,
Jon Neiditz, and
John M. Brigagliano,
Kilpatrick,
August 24, 2023

→ ***ChatGPT and AI Applications for In-house Lawyers*,**
by Spiwe L. Jefferson,
ACC Docket,
March 8, 2023

» **WITH THANKS TO:**

***Kurtis G. Anderson*, *Associate* at *Kilpatrick*,**

for his insights
in this glossary.

Learn 15 Key AI Terms

1. **Artificial Intelligence ("AI").** A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

2. **Machine Learning.** A set of techniques that can be used to train AI algorithms to improve performance at a task based on data.

3. **Large Language Model ("LLM").** A language model using deep-learning algorithms and trained on a large data set to capture patterns and regularities present in natural language and make assumptions on previously unseen language fragments to perform a task or generate an output.

4. **Algorithmic AI.** Also known as traditional AI. Artificial intelligence that classifies data based on various attributes and then predicts outcomes bound by predetermined rules. It excels at pattern recognition. Examples include search engine results, auto-text generators, and digital content recommendations.

5. **Generative AI ("GenAI").** A class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content. Examples of GenAI include OpenAI's ChatGPT, Microsoft's CoPilot, and Google's Gemini.

6. **Agentic AI.** An AI system that relies on a combination of machine learning, natural language processing, and automation technologies to interact with the world and act autonomously to achieve user goals without the need for constant human guidance. In contrast to GenAI, they are task followers, not predictive content generators.

7. **Input.** Data provided to or directly acquired by an AI system on the basis of which the system produces an output. Inputs are how most users will initially interact with GenAI to generate content.

8. **Output.** The data transmitted by the AI system in text, image, audio, or video format in response to an input. This is the product most end users are currently looking for from an AI program.

9. **Retrieval-Augmented Generation ("RAG").** A method to enhance the accuracy of GenAI models. The RAG system first searches and retrieves relevant external information, such as from a legal-information database (or from the company's internal database), and then adds this information to the user's prompt. This provides more context that allows the GenAI tool to generate a more accurate and relevant response.

10. **Prompt.** The input provided by a user to interact with a GenAI model and generate a response, or output, from the model. Prompts normally include specific instructions for the model to follow or questions for it to answer. Skillful prompt engineering is key to successfully utilizing GenAI. **See** ***Top Six Tips for Prompting Generative AI Tools***.

11. **Token.** These are the smallest units of data processed by an AI model, often words, characters, or sub-parts of words and punctuation.

12. **Token Limit.** The number of tokens the AI model is able to process between both the input prompt and the total generated output.

13. **Hallucination.** Incorrect, misleading, or entirely fabricated information generated by a GenAI model that appears to be true. This is a common caution for GenAI use: The risk of hallucinations must be managed.

14. **Deepfake.** AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to be authentic or truthful. While not all deepfakes are generated to mislead, they often enable fraud or misinformation.

15. **Bias.** An effect of training or preset instructions that results in an unrepresentative or distorted result, favoring certain outcomes and results. Unknowns around the training data and bias can lead to unintended or adverse outcomes.

CHECKLIST 2

» This checklist is mainly based on the following resources and on insight from ACC members:

→ *Legal Tech: The Crucial Role of Legal Stewardship During the AI Revolution,* by Olga V. Mack, Kevin Keller, Kristina Podnar, *ACC Docket*, July 29, 2024

→ *Prompt Engineering: Your Hidden Superpower for AI Mastery,* by Spiwe L. Jefferson, *ACC Docket*, July 23, 2024.

→ *Legal Tech: AI, Legislation, and Your Career Story,* by Olga V. Mack, *ACC Docket*, February 7, 2024

→ Visit the *ACC AI Resource Collection*

20 Tips to Be More AI Savvy and Boost Your Career

The rise of AI presents opportunities for in-house lawyers to demonstrate leadership and advance their career. Sufficient familiarity with AI is also an increasing necessity for lawyers to serve their clients with competence.

1. In-house lawyers should become familiar with key AI concepts and their practical implications.

- This will allow you to better understand how new developments in the field of AI will impact your organization and its environment.
- Your business colleagues likely use or want to use AI tools. You need a minimum level of knowledge in order to be effective in helping them navigate these uses.
- Also satisfy your ethical obligations to develop and maintain sufficient knowledge about new technology, for example under your duty of competence. Learn more at *Checklist 6*.

2. Find opportunities to increase your knowledge.

- **Tip 1: Start somewhere.** Don't let the volume of AI-related news paralyze you. Explore key AI concepts such as those laid out in *Checklist 1* of this toolkit.
- **Tip 2: Gain industry-specific knowledge.** Read AI-focused publications and newsletters (if any) that are focused on **your industry sector**.
- **Tip 3: Sign up for AI-related newsletters** relevant to **your practice**. For example, tailor your *ACC Newsstand* feed to include AI-focused legal updates.
- **Tip 4: Ask your outside counsel** if they can send you informative alerts at no cost regarding AI developments. They will probably be happy to showcase their knowledge.
- **Tip 5: Watch or attend educational programs** created for in-house lawyers on AI, such as on the *ACC Online Education* platform, or at *in-person conferences*.
- **Tip 6: Join AI-focused discussion groups with peers, such as** via the *ACC IT Privacy and eCommerce Network*.
- **Tip 7: Consider free courses.** Some technology companies and universities offer educational programs. See for example those featured in *professional social media* posts.

- **Tip 8: Ask business colleagues** what tools they find the most useful, and what strategies they find the most effective when using these tools. Learn about those tools.
- **Tip 9: Experiment with AI tools.** To truly become familiar with AI technology, you can't stick to mere theoretical knowledge. Experiment with AI tools, in a manner that is safe for your organization and that conforms with your ethical duties and professional obligations - e.g., don't compromise confidential or privileged client information when using AI tools.
- ***Learn how to create effective prompts*** **when you use generative AI tools** (GenAI):
    - **Tip 10: Give the tool context** for your query. For example, in your prompt, let the tool know what role/persona you want it to play, and which audience the output is intended for. Consider including background information (such as your organization's published mission statement).
    - **Tip 11: Also consider mentioning the tone and language complexity** that you want the tool to use in its output, depending on your audience. Are you planning to use the output for a presentation to fellow lawyers who are familiar with legal concepts, or to a business audience that expects simplified, plain-English language?
    - **Tip 12: Use follow-up prompts** to obtain more relevant results or output formats.
    - **Tip 13: Keep in mind that** you can't rely on the output from GenAI. You are responsible for verifying the accuracy of such output. Interactions with (and output from) GenAI tools feel human-like, but are typically based on a predictive algorithm.

3. Demonstrate leadership through AI-related projects.

- **Tip 14: If your company has a dedicated cross-departmental group** focused on AI, ask if you can get involved or invited to its meetings, and demonstrate a business mindset through your contributions to the discussion. If there is no such group, consider starting one.
- **Tip 15: Your legal department is probably already supporting or leading** your organization's AI governance or AI projects. If you're not already involved, identify relevant ways you can get involved.
- **Tip 16: Consider** how AI intersects with practice areas in your existing portfolio, and what you can do to further advance the company's goals or your department's goals by using AI, or by identifying how you can facilitate the use of AI and mitigate risks through your practice.
- **Tip 17: Help the business identify ways to measure outcomes** resulting from the use of AI tools.

» *Also check out:*

→ ***Two-Year Verdict: ChatGPT's Impact on the Legal Practice***, by Spiwe L. Jefferson, *ACC Docket*, November 25, 2024

→ ***Career Advancement Toolkit for In-house Lawyers***, an ACC Toolkit

→ Also watch: ***Lex Machina– The Rise of Artificial Intelligence***, an ACC webcast program with Melanie Laffin, Chief Innovation Architect, Artificial Intelligence, Booz Allen Hamilton, June 18, 2024

> A majority of in-house professionals (59 percent) are enthusiastic about the potential impact of Generative AI ("GenAI") tools on their careers, but only 42 percent feel prepared for that impact.
>
> ***GenAI and Future Corporate Legal Work: How Ready Are In-house Teams?***
>
> by ACC and Everlaw

- **Tip 18: Adopt a business mindset when approaching AI-related issues.** AI presents risks and challenges. When offering guidance to the business, show you balance risks and positive outcomes. Make sure your guidance is informed by the company's strategic goals.
- **Tip 19: Identify effective ways to bring your perspective** to the executive team (if you're the Chief Legal Officer) or to the head of the legal department (if you're not the CLO or General Counsel), regarding how new developments in the AI landscape present new legal and business challenges and opportunities.
- **Tip 20: Show results.** Keep track of how your use (or your team's use) of AI tools yields measurable positive outcomes or improvements. Showcase results internally.

TAKE ACTION:
Write one or two steps that you plan to implement.

Describe	By what date?
1.	
2.	

Notes:

Six Steps to Develop Governance and Compliance Strategies

Learn six tips to develop a robust AI governance for your company. Your business colleagues are probably using AI. They will experiment with use cases and will want to use new tools.

1. Audit your organization's current uses of AI.

An audit evaluates AI systems, algorithms, and data practices to identify risks, such as biases, privacy concerns, and ethical issues.

- It's likely that people within your business are already using generative AI tools for research or document drafting. If not, they may be experimenting with AI tools to evaluate their usefulness.
- **Assemble a cross-departmental team** to assess the current and potential uses of AI. Include these key stakeholders and any others you deem relevant:
  - Information Security
  - Information Technology (IT)
  - Developers and product teams
  - Human Resources (HR)
  - Finance
  - Investor relations
  - Business generators
  - Risk management
- **Engage people at all levels** to find out what is actually happening with AI and what work they intend to perform with it. Conducting a **business-wide survey** may be the most practical way to get this information.
  - This survey may help you find patterns of usage and help determine which AI tools would be best to use across multiple departments.
- **Consider an immediate pause on the riskiest AI uses** while conducting this audit. Understand and communicate that "no AI usage ever" is not the end goal of this process.

CHECKLIST 3

This checklist is based mainly on the following ACC resources and on insights from the sponsor Kilpatrick and ACC members.

- ***Artificial Intelligence Laws (EU and US),*** by Meghan K. Farmer and Gregory P. Silberman, Kilpatrick, March 5, 2025
- ***It's Go-Time — Creating an AI Governance Program,*** by Adam Shedd and Mark Diamond, *ACC Docket*, April 1, 2024
- ***No, Every Company Doesn't Need an AI Policy,*** by Christopher Wlach, *ACC Docket*, April 1, 2024
- ***Employees Are Using Chatbots — Make Sure Your AI Use Policy Works,*** by Robert Falk, Margo Lynn Hablutzel, Heather Peck, and Jonathan Yellin, *ACC Docket*, October 9, 2023
- Visit the ***ACC AI Resource Collection***.

Also check out:

- ***5 Key Takeaways PTLF – Building an AI Governance Program***, by Amanda Witt, Ami Rodrigues, and Christina McCoy, Kilpatrick, March 7, 2025
- ***AI: Virtual Patchwork***, by Stephen M. Anstey and Michael J. Breslin, Kilpatrick, November 8, 2024
- ***Sample Use of Generative AI Policy Template***
- ***The EU Artificial Intelligence Act: What In-house Counsel Need to Know***, ACC, March 19, 2024
- ***Legal Tech: The FTC's Enhanced Scrutiny on AI***, by Olga V. Mack, *ACC Docket*, January 9, 2024

2. Map out your regulatory obligations relating to AI.

- Jurisdictions worldwide are increasing their regulatory oversight of AI development and usage. Staying up to date is vital. Here are some useful resources that can help with this:
    - ***ACC AI Resource Collection*.**
    - ACC newsletters such as *ACC Newsstand* and *In Brief*.
    - Legal research and news platforms.
    - Law firm blogs and alerts, like Kilpatrick's ***Artificial Intelligence and Crypto blog***.
    - Relevant government alerts/guidelines, such as:
        - ***National Institute of Standards and Technology*** – NIST (US)
        - ***Cybersecurity and Infrastructure Security Agency*** – CISA (US)
        - ***Regulators' Strategic Approaches to AI*** (UK)
        - ***European Parliament's page on AI*** (EU)
        - ***Canadian Artificial Intelligence and Data Act [Proposed] – Companion Document***
        - ***Office of the Australian Information Commissioner***
        - ***Singapore's InfoComm Media Development Authority***
    - ***LinkedIn's Legal Generative AI Global Community***
    - ***The Future of Privacy Forum***
    - The ***AI Governance Center*** of the International Association of Privacy Professionals (IAPP)
- Learn about key AI regulatory regimes, such as the EU Artificial Intelligence Act, and AI-related laws in California, Colorado and other US states. ***Check out an overview of some of the key regulatory regimes: View the list in the ACC Resource Library.***
- **Develop a chart breaking down the jurisdictions** where your organization conducts business or has employees, then list regulatory obligations for AI users in each jurisdiction.
- It's possible that there will be **varying or even conflicting compliance obligations** across jurisdictions. An approach may be to choose the most stringent obligations as a company-wide compliance policy.

3. Develop business-friendly AI risk maps and governance structures.

- Map out AI **benefits, risks, and mitigation strategies**. Assemble a team to examine the organization's risk and needs. This could be the same group that conducts the AI audit discussed above. Including a broader group should make governance efforts more likely to succeed.
- Educate **top management and the board of directors** on the importance of AI governance and the specific risks if AI governance policies are not implemented.
- Put in place a formal **AI governance system**. An ***AI governance policy*** sets out the transparent and ethical use of AI and details how AI should be used by the organization. Having a sound AI governance policy helps to demonstrate to regulators and others that AI is being used responsibly.
- **AI Risk Management Tips:**
    - AI risks should not be considered in isolation.
    - AI-related risks should be integrated into the organization's larger risk management strategy.
    - How does your organization quantify and prioritize risks?
    - Consider the tradeoffs between AI use for business operations versus concerns such as privacy and cybersecurity risks.
    - Consider risks to the company's intellectual property and confidential information, and risks of bias and discrimination.

4. Establish clear roles and responsibilities for the AI management team.

- Designate an **AI governance lead** or team. Consider appointing an ***AI Steward*** from the legal department to be the custodian of AI's ethical and strategic deployment.
- **Define roles** in AI governance for data scientists, engineers, legal, HR, and compliance.
- Clarify **accountability** for AI-related decisions. This isn't necessarily a single person, but more likely a designated leader from each team that incorporates AI into its workflows.

> "It's important to deputize a team of AI ambassadors or have your Vice President level be the responsible layer for AI governance in the organization."
>
> **Aparna D. Williams**
> *Chief Legal and Compliance Officer*
> Coalfire

5. Update non-AI policies to take AI into account.

- Many issues raised by GenAI **aren't new**. Businesses already deal with problems involving data security, confidentiality, bias, and intellectual property protection.
- If your organization already has written policies on these topics, **consider amending them to cover AI-specific issues** before you create a standalone AI policy to address them.

6. Create user-friendly AI policies for the entire organization.

- Your organization's AI policy should be **clear and easy** for employees to understand and follow.
- The policy should be **transparent** and explain the risks of AI misuse. An important caveat is that an organization that uses AI may not fully understand the risks (e.g. what's in the algorithms and training data).
- Your policy should also be **realistic** and reflect your company's culture and practice. The goal is to encourage responsible AI use, not to erect excessive barriers.
- Be clear that AI use requires employee **monitoring, training and awareness**.
- Make clear that **non-compliance** may result in **disciplinary action**, which may include termination.
- Define whom the policy applies to. This will typically be **all employees, contractors, and other third parties** that use AI and/or its data on behalf of the organization.
- Set out the **terms of acceptable AI use** within the organization**.**
    - Explain which applications can be used, including their **permissible and prohibited use cases**.
    - Be clear that **security and confidentiality** are key considerations for employees, including **password-protected** AI accounts or VPN systems.

> Using public AI tools to stay up to date can be a real life hack. For example, you can use the "Tasks" module of ChatGPT to define a daily task where you ask ChatGPT to search the web, including sites such as LinkedIn, for any news about AI regulations and create a curated overview for you each morning. […] There are more tools that can do this, and it is not difficult to build your own.
>
> **Douwe Groenevelt**
> *Former Deputy General Counsel and Former Head of Legal,* ASML

Generative AI Usage Policy Example

The following is an example of a simple, high-level Generative AI Usage Policy governing employees' use of commonly available GenAI tools. Customize to your own requirements. Please note this is only a sample policy, not a model policy, and it is provided below for informative purposes only (and not as legal advice).

- **Responsible Use:** Our organization encourages responsible use of AI in your work.
- **Verify Everything:** Don't trust the accuracy of the AI output. Check everything with reliable sources. You are responsible for the accuracy and completeness of your work. Beware of overreliance.
- **Don't include personal, sensitive, proprietary or confidential (or privileged) information** in your prompts to the AI (unless your organization has white-listed AI and clearly indicated that you can use it for such information.)
- **Good Judgment:** Generative AI use is not appropriate for all circumstances. Use good judgment and common sense about when to use it.
- **Acknowledgement:** Where AI-generated content is used in your work, **acknowledge** the use of AI as appropriate or as required by your organization.
- **Regular Review:** This policy will be reviewed regularly and will be updated to reflect our organization's experiences using AI, developing practice, and new technology.

WITH THANKS TO:

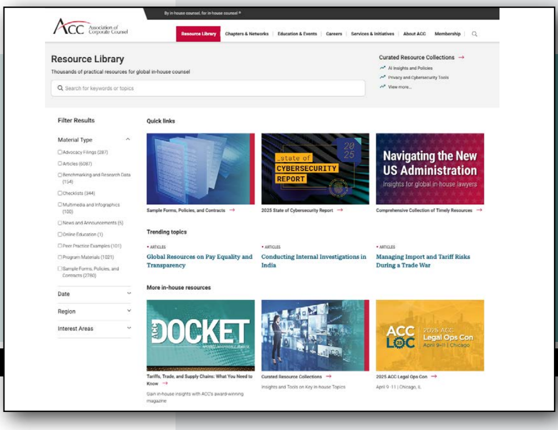
***Schellie-Jayne (SJ) Price*, *Chief Legal Officer*, Nooriam, *and Founder* of ACC Australia's Legal Technology & Innovation Special Interest Group**

for providing this sample policy.

Visit the

ACC Resource Library

to find more sample AI policies.


By in-house counsel, for in-house counsel ®
ACC Association of Corporate Counsel
Resource Library
Chapters & Networks
Education & Events
Careers
Services & Initiatives
About ACC
Membership
_state of CYBERSECURITY REPORT 20 25
Navigating the New US Administration
Insights for global in-house lawyers
ACC DOCKET
ACC LOC 25 2025 ACC Legal Ops Con April 9-11 | Chicago

Resource Library

Thousands of practical resources for global in-house counsel

Search for keywords or topics

Curated Resource Collections →

AI Insights and Policies

Privacy and Cybersecurity Tools

View more...

Filter Results

Material Type

☐ Advocacy Filings (287)
☐ Articles (6087)
☐ Benchmarking and Research Data (154)
☐ Checklists (344)
☐ Multimedia and Infographics (100)
☐ News and Announcements (5)
☐ Online Education (1)
☐ Peer Practice Examples (101)
☐ Program Materials (1021)
☐ Sample Forms, Policies, and Contracts (2780)

Date

Region

Interest Areas

Quick links

Sample Forms, Policies, and Contracts →

2025 State of Cybersecurity Report →

Comprehensive Collection of Timely Resources →

Trending topics

• ARTICLES
Global Resources on Pay Equality and Transparency

• ARTICLES
Conducting Internal Investigations in India

• ARTICLES
Managing Import and Tariff Risks During a Trade War

More in-house resources

Tariffs, Trade, and Supply Chains: What You Need to Know →

Gain in-house insights with ACC's award-winning magazine

Curated Resource Collections →

Insights and Tools on Key In-house Topics

2025 ACC Legal Ops Con →

April 9-11 | Chicago, IL

WITH THANKS TO:

Meghan K. Farmer, ***Partner***, and *Gregory P. Silberman*, ***Counsel***, at *Kilpatrick*,

for contributing this list.

13 Principles of AI Regulatory Frameworks

While AI regulations differ, below are key principles commonly found in AI regulatory regimes - and tips regarding their implications for businesses:

1. Transparency and Disclosure.

IMPLICATIONS:

- Disclose the use of AI systems to users and stakeholders.
- Provide clear information about how the AI system operates, including its purpose, capabilities, and limitations.

2. Privacy and Data Protection.

IMPLICATIONS:

- Limit data collection to what is necessary, and implement robust data anonymization and encryption practices.
- Obtain proper consent for data collection and processing.

3. Fairness and Non-Discrimination.

IMPLICATIONS:

- Avoid bias and discrimination in AI outputs.
- Regularly audit AI algorithms to ensure fairness and equity.
- Implement measures to prevent discriminatory impacts on protected classes of persons.

4. Accountability and Governance.

IMPLICATIONS:

- Clearly assign accountability for AI-related decisions and outcomes.
- Maintain detailed documentation of AI system development, use, and decision-making processes.
- Establish oversight mechanisms, such as AI ethics committees or internal governance frameworks.

5. Accuracy and Reliability.

IMPLICATIONS:

- Ensure AI systems deliver accurate and reliable outputs.
- Test and validate AI models regularly to minimize errors and inaccuracies.
- Communicate any limitations of the AI system to users.

6. Safety and Security.

IMPLICATIONS:

- Implement safeguards to prevent misuse, hacking, or other security vulnerabilities.
- Regularly monitor and update AI systems to address evolving threats.
- Ensure AI systems operate within predefined safety parameters.

7. Human Oversight and Control.

IMPLICATIONS:

- Design AI systems to allow for human intervention and oversight where necessary.
- Avoid full automation of high-risk or critical decisions without human review.

8. Intellectual Property (IP) Compliance.

IMPLICATIONS:

- Ensure AI systems do not infringe on third-party IP rights (e.g., patents, copyrights, or trademarks).
- Address ownership of AI-generated content and clarify IP rights in contracts.

9. Regulatory Compliance.

IMPLICATIONS:

- Adhere to sector-specific and jurisdiction-specific AI regulations.
- Monitor emerging AI regulations and adapt systems as laws evolve.

> “It’s important to deputize a team of AI ambassadors or have your Vice President level be the responsible layer for AI governance in the organization.”
>
> **Aparna D. Williams**
> *Chief Legal and Compliance Officer*
> Coalfire

10. Ethical Considerations.

IMPLICATIONS:

- Align AI development and use with ethical principles, such as promoting societal benefit and avoiding harm.
- Consider the broader impact of AI on stakeholders, including employees, customers, and society.

11. Explainability.

IMPLICATIONS:

- Ensure AI systems provide outputs that are interpretable and explainable to users.
- Avoid “black box” AI models that lack transparency in their decision-making processes.

12. Liability and Risk Management.

IMPLICATIONS:

- Define liability for AI-related damages in contracts with vendors and partners.
- Carry appropriate insurance to cover potential risks associated with AI deployment.

13. Consent for AI Use.

IMPLICATIONS:

- Obtain informed consent when deploying AI tools that directly affect users, such as chatbots or recommendation systems.
- Clearly inform users of their rights, including opting out of AI interactions.

Seven Steps to Integrate AI Governance Across the Business

✦This checklist was developed with the assistance of Google's Gemini AI tool.

Once your organization has developed an AI governance strategy and the necessary AI policies, it's time to implement them across the business.

1. Incorporate your AI strategy, governance,and compliance into your organization's business processes, services, and products.

- **Map AI use cases to specific business functions.** Work with leaders across the business to make sure they apply the overall governance strategy as they implement AI into their workflows and business processes.
- **Embed governance checks into existing workflows** (e.g., product development, marketing, HR, procurement).
- **Monitor and reevaluate AI tools embedded in your organization's products and services**. Changes in both AI technology and law make product compliance an ongoing issue and not just a one-time process during development.
- **Ensure AI development aligns with the overall business strategy.** Many employees and leaders may be excited to try an AI tool as the "big new thing," but technology tools should be analyzed based on how they serve business needs.

2. Prioritize explainability and transparency.

- **Strive for understandable AI decision-making processes.** Document who is responsible for making AI-related decisions and how those decisions are made. Employees at all levels should be clear on whom to contact if they have questions or concerns about AI usage.
- **Document** how AI systems work and their limitations.
- **Communicate transparently about AI use to stakeholders.** This can include both warnings about misuse and encouragement to make full use of AI tools within the bounds of AI policies.

CHECKLIST 4

This checklist is based mainly on the following ACC resources and on insights from the sponsor Kilpatrick and ACC members.

← ***It's Go-Time — Creating an AI Governance Program,*** by Adam Shedd and Mark Diamond, *ACC Docket*, April 1, 2024

← ***Legal Tech: Integrate AI Compliance by Asking These Questions***, by Olga V. Mack, *ACC Docket*, April 10, 2023

← ***Legal Tech: 5 First Steps Toward Responsible AI Oversight***, by Olga V. Mack, *ACC Docket*, September 12, 2023

← ***Using AI in HR Decisions: Tips for In-house Counsel***, ACC Checklist, March 22, 2023

← Visit the ***ACC AI Resource Collection***

» *Also check out:*

→ ***5 Key Takeaways – Managing the Risks in Using Generative AI or How I Learned to Stop Worrying and Love AI***, by Steve R. Borgman and Jordan P. Glassman, Kilpatrick, February 20, 2025

→ ***Legal Tech: Liability and Responsibility in the Age of AI***, by Olga V. Mack, Minh Hoang Merchant, and Brian E. Mack, *ACC Docket*, April 9, 2024

→ ***Legal Tech: The Crucial Role of Legal Stewardship During the AI Revolution***, by Olga V. Mack, Kevin Keller, and Kristina Podnar, *ACC Docket*, July 29, 2024

3. Train employees to use AI responsibly.

- **Consider whether it would be helpful to partner with outside vendors for training.** This may be especially useful for issues involving cybersecurity and data privacy, which could be folded into existing cybersecurity training.
- **Educate everyone in the business** on AI risks, ethics, and compliance requirements. Employees may be aware of AI's potential but less aware of the business risks – or vice versa.
- **Provide practical training for all employees** on AI tools and responsible use. This will foster effective use of AI to improve productivity and ensure that AI is used safely.
- **Tailor this training to specific roles and departments.** AI use cases may vary across the business, so employees should receive training relevant to their work.

4. Implement robust data governance.

- "***Garbage in, garbage out!***" To use AI effectively, **you need quality data**.
- **Establish data quality standards and validation processes.** AI tools will not produce useful outcomes without clean, consistent business data to analyze. Relevant data sets should be validated and cleaned up before AI systems are installed or trained.
- **Implement data security measures and access controls.**
- **Ensure data privacy compliance,** e.g., as applicable, under the EU's General Data Protection Regulation (GDPR), or the California Consumer Protection Act (CCPA). Your organization should already have privacy compliance protocols in place for its business data. AI usage considerations can likely be added into these protocols.

5. Conduct regular technology audits.

- **Evaluate AI systems for bias, fairness, and accuracy.**
- **Consider engaging an independent auditor** to conduct your AI audits, as they will have the latest expertise on AI technology and may be able to suggest improvements to your AI governance practices.
- **Assess compliance with AI policies and regulations.** Government oversight of AI development and usage is expanding globally, making it necessary to review your systems' compliance regularly.
- **Document audit findings** and implement **corrective actions**.

6. Establish a feedback and monitoring system across the business.

- **Create channels** for employees to report AI-related concerns.
- **Monitor AI system performance** and identify potential issues.
- **Regularly review and update** the AI governance program.

7. Ensure that generative AI use in HR is monitored and augmented by human intelligence.

- **Anti-discrimination and other employment laws** apply to AI-enabled decisions as they do to human-made decisions.
- **AI is just a tool to enhance HR processes,** not a substitution for human judgment.
- **Consider implementing a full validation procedure** to ensure the tool meets business needs without introducing bias.
- **Keep human judgment in the loop** and ensure there is a mechanism to audit and override AI decisions as needed.
- **Ensure employees and job applicants are informed when AI tools are in use.** Consider asking them to confirm in writing they understand. Seek a signed consent/release from employees.
- **Consider privacy aspects** and how to set up the tool to mitigate privacy risks. For example, using AI tools could potentially expose employees' personal data to others, and AI systems should be designed to prevent this.

> "A big issue that we and many of our international peers talk about is the fact that AI tools can create risks when applied in combination with internal databases. When these databases suffer from suboptimal rights management, this can be hugely exacerbated by AI tools and can lead to people finding restricted information through internal tools."
>
> **Douwe Groenevelt**
> *Former Deputy General Counsel and Former Head of Legal,* ASML

WITH THANKS TO:

Joel D. Bush, ***Partner***, and *Gregory P. Silberman*, ***Counsel***, **at** *Kilpatrick*,

for their input in this roadmap

AI Maturity Roadmap

AI Roadmap	Ad-hoc (initial)	Defined	Integrated	Optimized	Transformative
Governance Framework	Lacks formal governance; governance efforts are reactive and sporadic.	Basic governance framework established, focused on compliance.	Governance is integrated into organizational processes.	Proactive governance framework aligns with strategic objectives.	AI governance is predictive and shapes industry best practices.
Policies and Procedures	No documented policies for AI usage or ethical considerations.	Initial documentation of AI policies, including data use and privacy.	Policies are standardized, covering ethics, bias mitigation, and transparency.	Policies are dynamic, regularly reviewed, and updated for emerging trends.	Policies drive innovation while maintaining high ethical standards.
Risk Management	Minimal or no risk assessments; unaware of regulatory requirements.	Early-stage risk assessment processes developed, but not robust.	Formalized risk assessments and impact evaluations are regularly conducted.	Advanced tools for monitoring and mitigating AI risks are in place.	AI systems are self-monitoring with automated compliance checks.
Stakeholder Involvement	Limited to no stakeholder involvement in AI decisions.	Key stakeholders identified but inconsistently engaged.	Cross-functional teams are actively involved in AI governance.	Stakeholders are fully engaged, with regular consultations and feedback loops.	Continuous and inclusive stakeholder collaboration fosters trust and transparency.
Accountability	Responsibility for AI governance is unclear or absent.	Roles and responsibilities are defined but not uniformly enforced.	Accountability structures include clear escalation and reporting mechanisms.	Accountability mechanisms include internal audits and external oversight.	Transparent accountability mechanisms influence public trust and regulatory leadership.

Incorporate AI into the Legal Team's Work

AI tools can help legal teams increase their efficiency and quality of service.

1. Treat the adoption of AI tools by Legal as a project that needs to be managed.

- **Ensure there are clear project goals,** scope, and timelines, and adequate allocation of responsibilities and resources.
- **Consider assigning responsibility** for AI expertise and for AI project management within Legal to a dedicated team member.
- **Ensure this strategy includes** project evaluation, planning, implementation, metrics, monitoring, and ongoing improvement.
- **These projects may involve substantial time and effort.** Make sure adequate resources are allocated, and that stakeholders' contributions are recognized.
- **Highlight team members' contributions.** Weave such projects into their professional development path, as an opportunity for them to increase their skills, demonstrate leadership, and advance.
- **Project implementation may be frustrating** and may include failures. Use lessons learned to improve your team's approach.
- **Celebrate and reward achievements,** as possible. If you are a supervisor, recognize these contributions in your team members' performance reviews.
- **Showcase the legal department's innovations** with the business teams and senior leadership. If possible, use metrics to show improvements made.

2. Don't approach AI as a magic solution that replaces the lawyer's judgment.

- **Keep in mind AI is just a tool.** It typically relies on algorithms and data sets – both of which are imperfect and not necessarily suited for your purposes. Also, you can't trust that the output will be true, complete, accurate, and relevant.
- **GenAI and analytical AI tools may be** ***compared to a fast new intern or law clerk*** who can process large amounts of information quickly, but who has no real-life experience in the field, little or no understanding of your specific context, and who might "hallucinate" by producing inaccurate or made-up information.
- **Keep in mind AI may feel human, but it is not human.** It has no experience exercising good judgment, and it doesn't feel emotions, despite the impression you may have when reading output from AI tools.

CHECKLIST 5

» **WITH THANKS TO:**

***Michael J. Breslin*, *Partner*, at *Kilpatrick*,**

for his contribution to this checklist.

« *This checklist is based mainly on the following ACC resources and on insights from the sponsor Kilpatrick and ACC members.*

← ***ChatGPT and AI Applications for In-house Lawyers***, by Spiwe L. Jefferson, *ACC Docket*, March 8, 2023

← ***Prompt Engineering: Your Hidden Superpower for AI Mastery***, by Spiwe L. Jefferson, *ACC Docket*, July 23, 2024

← Visit the ***ACC AI Resource Collection***

» *Also check out:*

→ ***Don't Throw the Bot Out with the Bathwater: Embracing Generative AI in eDiscovery Work***, by Jimmy Chestnut, Tarek Ghalayini, and Danielle T. Davidson, *ACC Docket*, April 22, 2024

3. **Identify AI use cases for your department.** Ask yourself and your team how AI tools could be used to perform or automate specific tasks, processes or workflows. For example, consider the following applications:

- **Document drafting, review, and management.**
  - ***Contract analysis and management.*** AI's text analysis can help spot and classify key contract terms. **There are tools that facilitate contract reviews** by analyzing a draft agreement in seconds and flagging problematic clauses for your attention – this may be based on parameters that you set in the tool.

    Look for tools that also allow you to perform a risk analysis by providing your organization's risk guidelines and tolerance level. The tool may then be able to analyze contract language to provide a risk rating.

    - Off-the-shelf large language models (LLMs) like ChatGPT can **quickly review dense documents and summarize provisions** such as notice and renewal terms, limitations of liability, and dispute resolution procedures.
    - By performing such an analysis across multiple agreements, you can **create a customized and searchable database of key provisions**, allowing you to manage your third-party agreements more efficiently or reduce the costs of M&A due diligence.
    - However, **unique or highly complex agreements may require additional model training or specialized AI models** to achieve desired performance levels.
  - ***Contract creation.*** There are tools that can be used by legal departments to **set up a self-service workflow for business teams to create draft agreements**. This is probably more limited to frequent, standard agreements for which the legal department can set up a few limited variables for the business to pick from, with escalation to Legal in case any variation from the accepted standards is needed.
  - ***Policy and procedure development***. Some GenAI tools can produce a **first draft of a sample policy**. You will need to review and tailor the draft to your needs, though.
  - ***Communications.*** In addition to producing draft contracts or policies or lists of red flags in contract reviews, GenAI tools may be able to **create related sample communications that you can then tailor**. For example, a draft email to your business team regarding clauses to further negotiate with the other party, or an internal email regarding a draft policy you created using AI. Again, be mindful of using tools in a way that preserves attorney-client privilege and the confidentiality of client information.

  - ***Presentations.*** AI tools can help you **produce slide decks and other materials for your internal presentations,** and create bullet points for your topics, layout ideas, or even graphics.
  - ***Meet with AI vendors to get demos*** of how their products can help legal departments - for example at the *ACC Annual Meeting*.

- **General knowledge research.**
  - When there is something you are unfamiliar with, such as a business term or process, a scientific or medical concept, or a government agency you haven't encountered before, **consider asking a GenAI tool for an explanation rather than using a search engine**. Keep in mind that the output you obtain may be inaccurate or incomplete – you should verify the information.
  - A useful approach is to tell the AI tool to provide an explanation written for a teenager. This will typically remove jargon, with the AI likely using a metaphor to help you better understand the term or concept.

- **Initial legal research and case law analysis.**
  - **GenAI tools may be used for preliminary research.** However, don't rely on the output as accurate. Again, beware of hallucinations, check the sources, and verify the accuracy, completeness and relevance of the information. The tool may give you a general idea of key issues and rules, but you need to **verify and do your own research**.
  - **Don't rely solely on GenAI tools to learn a new area of law.** GenAI can give you a first idea of the landscape and key issues, but you'll need to check and research. Ideally, you should have prior knowledge of the topic researched, in order for you to evaluate the accuracy or completeness of the output.
  - **Explaining the context of your query** to an AI tool can greatly help the tool to provide a more tailored and relevant answer. ***Also see the checklist of prompt engineering tips***.
  - However, before entering information in a tool, **carefully consider which information you should enter (or not enter)** into the tool, even for purposes of explaining the context of your query. Don't compromise attorney-client privilege or the confidentiality of client information.

- **Multi-jurisdictional surveys.** There are GenAI tools that can retrieve current information from government websites across multiple jurisdictions and create a comparison chart or summary of the legal or regulatory information you are researching.

- **Regulatory compliance monitoring.** Douwe Groenewelt, Former Deputy General Counsel and Former Head of Legal at ASML, shared a shortlist of some of the compliance-related AI tools that European in-house legal professionals use, including:
  - *EU Data Protection Impact Assessment (DPIA) Assessment Assistant*
  - *Marketing Claim Analyzer, a type of tool that helps to check whether marketing claims are compliant with applicable regulations*
  - *EU Corporate Sustainability Due Diligence Directive (CSDDD) Compliance Assistant*
  - *Export Control Classification Assistant*
  - *Sales Tender Review Assistant*
- **eDiscovery** assistance. AI tools can help manage discovery requests. LLMs can quickly process and categorize discovery requests based on criteria such as subject matter, time frame, and type of material requested:
  - This allows in-house counsel to **more efficiently route each request** to the appropriate resources and track progress.
  - LLMs can also **generate response templates** and be trained to include objections and responsive statements based on your organization's litigation practices and standards.
- **Meeting summaries and action item tracking.**
- **Internal client-facing tools** to deliver legal services. Some law departments develop internal chatbots that can address basic/commonly asked questions from business teams, such as regarding the content of core corporate policies, signature authorities rules, etc.
- **Intra-department knowledge sharing** within Legal. Some departments may wish to develop a platform for knowledge sharing within the department – especially in large departments, or organizations with a large number of policies.
- **Workflow management.** Some AI-powered tools may be used to automate workflows, such as for procurement purposes, or contract approvals and signatures.
  - AI tools may also be useful for creating checklists to guide non-automated workflows, such as contract reviews and negotiations.
- **Filling out forms and questionnaires.** With AI systems that are secure and that meet your confidentiality requirements, consider providing the tool with a copy of a form/questionnaire you need to fill out along with the relevant information, and ask it to draft responses.

- **Find out what AI tools other in-house lawyers use. Connect through the *ACC Networks* and *ACC online forums*.**

4. Evaluate the benefits and risks of AI usage in Legal.

- **Consider the risks** in terms of attorney ethics, accuracy, copyright, data privacy, regulatory compliance, business impact of potential tool failures, etc.
- **Identify specific benefits** expected from the use, and the associated metrics.
- **Decide which matters and tasks** can safely be handled using AI, with what tools, and under what conditions/settings.
- **Test before use.** Consider using fake test data during the testing phase.
- When launching a use case, consider starting with just a few **pilot users** before expanding the use to a broader team.
- Determine whether using a **free version** of a tool is sufficient and acceptable, or whether you should purchase a **paid individual or enterprise license**. For some tools, the paid version may offer not only more up-to-date output, but also the ability to "gate" an instance of the tool so that your company's information is not accessible by the vendor or by third parties.

5. Consider leveraging AI features within existing tools

(Microsoft Office, browsers, etc.) to boost productivity. For example, users of Microsoft 365 may already have access to various tools (such as Copilot, Power Apps, Power Automate, Power BI). Many of these uses may involve **confidential or privileged information**, so make sure the existing AI tools you use are **approved by your organization** and are **verified to maintain adequate confidentiality.**

- **Accelerate and improve day-to-day drafting.** LLMs and embedded AI assistants (like Microsoft's Copilot) can significantly reduce the time required to summarize complex information, write letters, and prepare drafts of agreements.
  - They can also quickly **refine existing drafts** to meet specified needs and objectives you specify, make improvements to existing language, and propose revisions based on stylistic preferences.
  - With practice, these tools can greatly reduce drafting time and help improve the quality of final drafts.

- In-house lawyers may want to **consider creating internal company chatbots** (such as a corporate policy chatbot) using Microsoft Copilot Studio as an add-on to Office 365 (a tip shared by Douwe Groenevelt, Former Deputy General Counsel and Former Head of Legal at ASML).
- **Consider using AI transcription features** in Zoom or other online meeting platforms to summarize meetings both for those who could not attend and as meeting notes (first assess suitability of using such features for your meetings, such as regarding any confidentiality requirements or concerns).
- **Ask your department's CLM vendor if they have AI functionality** to help locate agreements quickly and if they have an AI review feature to assist with contract review.

6. Evaluate specialized AI tools for specific Legal Department tasks.

There are many specialized AI tools offered by vendors for contract management, legal research, workflow management, etc. Consider key aspects such as:

- Quality of output
- Ease of use and access
- Data handling protocol
- Integration with the organization's existing business systems
- ***Also see** Checklist 8 on vetting an AI tool for adoption*.

7. Keep in mind the limitations of AI tools and the risks of errors.

- Understand that you are responsible for how you use AI tools and their output.
- You can't rely on output to be accurate and/or exhaustive. It's your responsibility to verify the information.
- **Beware of hallucinations.** GenAI tools sometimes make up information. **Lawyers who use information made up by GenAI** put their clients at risk (*as case law shows*). They also put their own reputation and their professional responsibility at risk, and may face penalties and professional sanctions.
- **Verify the information you obtain through AI tools.** Ensure that the information you use is accurate, relevant, and complete, and that you provide the guidance that best serves your client's interests.

> "We work with our CISO and IT team to review every tool so we understand if it has an AI feature and whether or not our organization is actually using those features."
>
> **Aparna D. Williams**
> *Chief Legal and Compliance Officer,*
> Coalfire

8. Beware of disclosure risks, and remain compliant with your professional obligations and ethical duties.

- Ensure that your use of AI tools won't compromise **attorney-client privilege** and/or the **confidentiality** of the company's information.
- **Understand how information will be used** by a tool, and for what purposes.
  - Look out for any **automated decision-making processes** carried out by the tool if it is integrated into workflow systems.
- **Understand if information will be stored**, where, for how long, and for what purposes.
- Understand whether the data entered in the tool by you or your colleagues (or the output data you generate when using the tool) will be:
  - **entirely confined** to an instance of the tool that only your organization has access to,
  - **comingled or aggregated** with other parties' information, or
  - **accessible by others.**
- **Will any information be accessible to other parties** than you? For example:
  - the vendor,
  - the vendor's subcontractors or partners,
  - other users of the tool.
- If so, what information, to whom will each category of information be made accessible, for what purposes, for how long, and under what conditions (data protection, confidentiality obligations, etc.)?
- **Understand who will have access to what information** in connection with your use of the tool, such as:
  - the information you **input** into the tool,
  - the **output** information that you generate through the tool, and
  - **usage** information (information regarding your use of the tool).
- **Training purposes.** Will information be used as "training data," i.e., to train the tool's Large Language Model?
- **Output source.** Will information become part of the corpus of information that serves as a source for output (can other users find your information in the output that they obtain through the tool)?

- **Use of "aggregated data."** Beware of claims that information will be used only in aggregate.
    - Is this sufficient?
    - Will the information be anonymized in way that it won't be re-identifiable?
    - Will it be adequately encrypted?
- **Check on the cybersecurity** of the vendor's tool. Is it sufficient for your needs?
- Even if the vendor agrees to contractual terms that give you satisfaction on paper (***See Checklist 9 for more information***), **ask yourself if you trust the vendor's ability** to uphold its promises or representations.
    - Is it a large, well-established provider with a robust reputation, or a start-up company with a higher risk profile and very limited assets?
    - Evaluate the risks in light of the sensitivity of the information, and the potential impact of a tool malfunction or data breach on your organization.
- Carefully **review the terms and conditions** of the AI tools that you use.
- **Engage in discussions** with the vendor as needed to understand these aspects.
- Be mindful of the **potential need to inform the client** about your use of AI tools - and the potential need to obtain the client's consent about AI uses.

TAKE ACTION:
Write one or two steps that you plan to implement.

Describe	By what date?
1.	
2.	

Notes:

Examples of Use Cases: How In-house Lawyers use AI

Meganne Thaxton, Senior Corporate Counsel at Red Ventures, mentioned the following uses of AI tools:

- Review contracts using an add-on tool for the company's CLM software (Contract Lifecycle Management).
- Generate first drafts of:
    - New contract templates.
    - A contract clause more favorable to the company.
    - Email responses.
    - A legal memo.
- Personalize documents for tone and length.
- Write and rewrite annual performance reviews.
- Create a short sample form for legal disclaimers and disclosures.
- Produce summaries of:
    - Legal research.
    - Recent case decisions.
    - Regulation and its impact on the business.
- Generate insights and analysis across multiple sources to get up to speed quickly.
- Translate non-English agreements, emails, and case summaries.
- Brainstorm legal strategies, key considerations, and agendas.

Top Six Tips for Prompting Generative AI Tools

Consider these strategies to increase the chances of obtaining relevant output when you query a Generative AI tool. Keep in mind that each tool has its own features, advantages, and limitations. Below are general prompt ideas. You will need to create your own prompts relevant to the context of what you are trying to accomplish.

1. **Use direct, simple and focused prompts.** Avoid including too many variables. Consider applying the ***CO-STAR framework*** or similar alternatives to design your prompt.

2. If possible, **include context** to help the tool offer a more tailored response. For example, ask the tool to assume a role, and to create output for a specific type of audience.

   - Depending on the tool, it may be helpful to upload relevant documents or website URLs it can reference to add context.

   - **Here is an example:** "*Assume you are the general counsel of a large global industrial group that needs to deliver a one-hour training session to sales staff regarding what constitutes a binding contract. The topic should include key points such as […] Create a slides deck for a one-hour presentation. Don't include more than […] slides. Use simple wording (fifth grade level).*"

3. To help the tool adopt the desired voice and tone, **consider providing examples of publicly available language or messaging that your organization has used**. For example, if you ask a tool to come up with the draft policy, consider pasting in the tool your organization's core values, for a result that aligns better with these values. For example: *"As context, assume that the trainees are familiar with industry x, and that core values of the company are x, y, and z."*

4. **Use iterative prompts.** Once you have a first answer from the tool, add follow-up questions or instructions to further tailor the output to your needs. For example, ask the tool to rephrase the output using a different tone; or ask the tool to present the content in a specific format (e.g., x number of bullet points of no more than x number of words in each bullet point).

5. **Bonus Tip 1: Adapt your prompts to the model you are using.** Different AI models may require different prompting techniques - for example, reasoning models like Open AI's o1/o3 or Anthropic's Claude 3.7 already incorporate iteration, backtracking, and multi-step reasoning and may actually work less well if "overprompted" to add those steps – a tip shared by Douwe Groenevelt, Former Deputy General Counsel and Former Head of Legal at ASML.

6. **Bonus Tip 2: Save successful prompts.** Malaika Roemer, CIPP/US, Principal Paralegal and Compliance Program Manager at Coalfire, shared that it may be helpful to save prompts that produce good responses, especially for AI uses likely to be often repeated. Some AI tools will let you store prompts for reuse.

Learn more

→ **Learn more prompting strategies and tips** in ***Prompt Engineering: Your Hidden Superpower or AI Mastery***, by Spiwe L. Jefferson, *ACC Docket* (July 23, 2024)

TAKE ACTION:
Write one or two steps that you plan to implement.

Describe	By what date?
1.	
2.	

Notes:

CHECKLIST 6

WITH THANKS TO:

***Joel D. Bush*, Partner, at *Kilpatrick*,**

for contributing this checklist.

Meet Ethical Obligations While Using Generative AI

If you are an in-house lawyer in the US, your ethical obligations extend to your use of AI tools. Learn how to satisfy ethics requirements while advising the business.

1. **Further your duty of competence by effectively using AI tools.** In the United States, under the American Bar Association's rules (*ABA Rule of Professional Conduct 1.1*), a lawyer is required to provide competent representation to their clients. *Comment 8* to this rule, adopted by 37 US states, indicates that this includes being up to date with "relevant technology."

   - **Lawyers are thus ethically required to learn about new technology and develop skills for using new technologies,** such as generative AI, in ways that can serve their clients.
   - Despite this ethical balance in favor of using GenAI, **it cannot replace independent analysis and judgment**. Use it wisely and responsibly on the client's behalf.
   - **Uploading client information** into a public GenAI platform without client consent can violate both the duty of competence and the duty of confidentiality.
   - **GenAI can hallucinate by producing fake results,** including making up summaries, quotes and citations for nonexistent court opinions.
     - This is illustrated by the well-known case of *Mata v. Avianca*, where a federal court in New York sanctioned a lawyer for citing to nonexistent cases in his brief based on legal research conducted using GenAI.
     - The more obscure the topic, the more likely it is that the AI tool will hallucinate.
   - **Verify the accuracy of your GenAI work product,** whether it is for a submission to a court, a memo to corporate leadership, or any other purpose.
   - **Consider these parameters for making competent use of GenAI:**
     - Follow your company's GenAI use guidelines.
     - Be mindful before using any self-learning GenAI platform.
     - Depending on the type of information you want to enter in the AI tool, only use a private/enterprise GenAI platform with company information, unless you obtain informed written consent to use an open GenAI platform. Even if you obtain the client's informed consent to use a tool, ensure that your use of the tool will not contravene your duty of confidentiality or other ethics obligations.

  - ○ Where productive, use specific and custom instructions. Provide inputs/instructions to use specific trusted information sources to generate work product.
  - ○ Validate all outputs. Treat all GenAI outputs as a draft that must be reviewed and checked for accuracy.

2. Maintain your duty of confidentiality when using AI tools.

ABA Rule of Professional Conduct 1.6 requires lawyers not to reveal client information without the client's informed consent or under special circumstances.

- **Consider that public generative AI platforms are typically not secure (at least in their default settings).** Uploading confidential company information to these public platforms without consent could violate this duty of confidentiality, and may also potentially:
  - ○ Waive any attorney-client privilege covering the information,
  - ○ Violate privacy and data protection laws,
  - ○ Destroy any trade-secret protection,
  - ○ Violate export control laws,
  - ○ Put patentability of inventions at risk, and
  - ○ Risk liability under employment laws.
- **Use private/enterprise AI platforms whenever confidential company information will potentially be uploaded for legal work.** However, first ensure that these systems are, in fact, secure. This could include due diligence on vendor dependencies and data practices.
  - ○ **Private AI platforms are becoming more common,** including downloading more compact GenAI models to in-house private servers walled off from the public Internet.
  - ○ **"Private platforms" mean platforms that do not share information outside your enterprise.** Such private platforms may provide a greater degree of comfort that the user will not breach confidentiality, if adequate cybersecurity protocols are in place.

3. Extend your duty of supervision to your oversight of Legal's AI usage.

ABA Rule of Professional Conduct 5.1 requires supervisory attorneys to make reasonable efforts to ensure that their subordinates comply with the ABA Rules.

- This duty includes **deciding whether and how the legal department will use generative AI.**
- All supervising attorneys – not just the GC or CLO – need to be educated on how technology works, the risks of uploading company information, the risks of using downloaded content, etc.
- Supervising attorneys need to participate in determining parameters of AI use, expectations for verifying content, establishing adequate security protocols, etc.
- This duty to supervise extends to supervising GenAI vendors if their tools are used for legal work. This supervision includes determining use parameters, expectations for verifying content, and establishing adequate security protocols.

4. Carry out your duty of communication to the business as your client.

- *ABA Rule of Professional Conduct 1.4* requires lawyers to "reasonably consult" with their client and to keep them "reasonably informed" about the status of legal matters.
- **This duty includes communicating the risks, limitations, and potential uses of AI.**
- You should also discuss whether it may cost the business more not to use beneficial AI technology than to take on the costs and risks of implementing it.

Learn more

→ *Practical Lessons from the Attorney AI Missteps in Mata v. Avianca*, by William A. Ryan, Allen Garrett, and Brad Sears, August 8, 2023

→ **Watch:** *Closing Ethics Program - Something's Gotta Give*, an ACC AI-focused program by Stuart Teicher, from the ACC Annual Meeting (October 2024).

→ **Visit** the *ACC AI Resource Collection*

Five Tips to Protect Intellectual Property When Using Generative AI

Using generative AI comes with significant risks to intellectual property – both your organization's IP and that of others. Use these tips to help avoid potential legal pitfalls.

1. Make sure your organization's creative output includes human contributions to trigger copyright or patent protection, if ownership is a priority for the organization.

- **As of the date of production of this toolkit, creative works produced purely by GenAI** are not copyrightable in the view of the US Copyright Office, even if they result from hundreds of human prompts. The federal Court of Appeals for the District of Columbia *recently affirmed* the Copyright Office's view. However, works containing a mixture of human-generated and machine-generated content can be protectable to the extent of human creation.
- **A significant judicial body in China** has held that AI-generated works can, theoretically, be protectable under copyright, in contrast to the approach taken in the United States.
- **Other major jurisdictions, such as the EU and UK, have yet to address this issue definitively.** The best practice for a global business is to ensure that public-facing creative works, such as marketing text and graphics and creative products, are made with significant human contributions.
- **GenAI tools cannot be "inventors"** without human contributions for purposes of patent protection in every jurisdiction, except South Africa, that has addressed the issue. Patent-generating businesses, from software to pharmaceuticals, should take this into account in their product development processes.

2. Be aware of the evolving legal landscape on fair use and generative AI if your organization builds or incorporates GenAI models.

- Many GenAI tools rely heavily upon the **ingestion of copyrighted works** in order to train and learn. This is an essential part of the process in developing a model that will generate meaningful content.
- **Copyright owners** across multiple industries and disciplines have taken **legal action** against the developers of GenAI products, arguing that the ingestion of their content without permission constitutes copyright infringement.
- **Developers** counter that training is **"fair use"** under copyright law.

CHECKLIST 7

WITH THANKS TO:

***Joel D. Bush*, Partner, and *James A. Trigg*, Partner, at *Kilpatrick*,**

for contributing this checklist.

- These legal battles are playing out globally in ongoing cases, for example, in the US, UK, India, and Canada.
- ***A court in China ruled in favor of a copyright owner*** in a dispute over copyrighted training data.
- In the US, a federal district court in February 2025 ***denied*** a fair-use defense to a company that allegedly used its competitor's copyrighted content to train an AI-driven legal research platform. However, this ruling did not involve a GenAI product and did not establish a blanket rejection of the fair-use defense for AI developers in the US. The decision is being appealed.
- As the law on AI fair use evolves globally, companies seeking to develop AI models should **proceed with caution**:
  - A GenAI tool need not be built upon copyrightable material to be usable; factual data, government content, and public-domain material can be used as training data.
  - Developers can obtain permission or seek licenses for the training sets used to develop their AI model.
  - The nature and purpose of a GenAI tool can affect whether its training data will be covered by fair use. GenAI applications that are built for purely *internal* uses – such as for ideation or research and development – appear more likely to survive copyright scrutiny than products that are intended for external use, such as for the creation of public-facing output.

3. End users of GenAI tools may also face liability for using AI-generated output that infringes copyrights.

- For example, ***cases over training data*** brought in the US by Getty Images and The New York Times against AI developers allege that the **developers' products can be used to produce images and text** that are close enough to the originals used as training data as to be **copyright violations**.
- **Businesses should exercise caution when using "off the shelf" AI tools for content generation**, whether for text, graphics, music, or other materials. Without a special enterprise license, many AI programs are offered without representations and warranties and without guarantees that outputs will not infringe third parties' rights.
- **Use enterprise AI offerings when possible.** Such products may come with representations and warranties, along with undertakings to indemnify users, if a piece of content created with such a tool infringes a work on which the tool was trained.

- **Avoid prompts that invite AI tools to infringe.** Steer clear of prompts that ask a tool to replicate some specific piece of content. A prompt such as, "Provide a general recap of the outcome of Super Bowl LIX" is preferable to "Provide a copy of the *New York Times* article from February 10, 2025 regarding Super Bowl LIX."
- **As noted above, internal uses appear safer than external-facing uses.** Using GenAI tools for internal ideation and research seems to carry lower risk than using AI-generated content in public-facing settings.
- **Use programs to track which pieces of company collateral contain AI-generated materials.** This will assist the business in responding to potential copyright infringement claims and in assessing the viability of claims against third parties.

4. Use a closed GenAI tool to better protect your organization's outputs as trade secrets.

- Unlike with patent and copyright law, **AI-generated content can be protected as a trade secret, if confidentiality requirements are satisfied.** There is no requirement that the creator of a trade secret be a "natural person."
- **Ensure that your product development, IT, sales, and content teams use closed enterprise AI systems or subscriptions** rather than publicly available tools when engaging in work for the business. Using publicly available default versions of the tools will produce work that may not be confidential, and thus not a trade secret.

5. Avoid accidental public disclosure of your trade secrets when using GenAI.

- **Prohibit employees from discussing or uploading company trade secrets in conversations with public GenAI platforms.** Where needed, closed systems should be used for this purpose.
- GenAI platforms often warn users not to share sensitive information in conversations with the tool. These conversations are typically retained and used to further train the AI model.
- A ***real-world example happened in 2023*** when engineers at a prominent technology company unintentionally leaked confidential data – including source code and internal meeting notes – while using ChatGPT to fix errors in their source code. This data is now stored on OpenAI's servers and is potentially discoverable by competitors.

Learn more

- → ***Gen AI: The "Artificial" Threat to Trade Secrets***, by Joel D. Bush and Kurtis G. Anderson, Kilpatrick, April 4, 2025
- → ***Robots are Coming – But They Still Can't Register Copyright***, by Gabriel M. Ross, James A. Trigg, Mehrnaz Boroumand Smith, and Joseph Petersen, Kilpatrick, March 24, 2025
- → ***The Impact of AI on Attorney-Client Privilege***, ACC Research Report, 2024
- → ***ACC AI Resource Collection***
- → Explore how other in-house lawyers use AI: **Connect with peers in the *ACC forums***
- → Learn more about ***Trade Secrets: Legal Framework and Best Practices for Enforcement (United States)***, ACC Guide, sponsored by Kilpatrick (2020).

TAKE ACTION:
Write one or two steps that you plan to implement.

Describe	By what date?
1.	
2.	
Notes:	

Top 10 Steps to Evaluate AI Features, Products, and Services

Learn 10 steps to help the business vet the adoption of AI tools. Make informed decisions, mitigate risks, and harness the potential of AI responsibly to achieve strategic goals.

1. Develop use cases for AI in your organization.

- **Make sure you fully understand the problem** you are trying to solve with AI.
- **Consider the necessity and appropriateness of using AI** to address this problem.
- **Is AI the best solution**, or could traditional methods suffice?
- Will the integration of AI create a **high risk/impact system** (one with significant impact or significant potential risk to the organization)?
- If the adoption of AI for a particular use case would result in a high risk/impact system, **how will regulatory requirements be met** and does the organization have enough technical resources to meet those requirements?
- **Is the proposed use of AI prohibited?** Determine whether the proposed use of AI is lawful under existing and pending regulations. This determination will vary by geography and use case.

2. Assess the value proposition.

Ask what tangible benefits the AI tool promises to deliver, and how critical they are to your business strategy.

- Evaluate whether these expected improvements or efficiencies justify the costs and risks of implementation. **See the checklist below to "*Evaluate Four Key Risk Factors in AI Systems*."**

3. Address data considerations.

Be clear on where the data for your AI tool comes from, and whether your organization has the right to use it. Also, consider how the data will be protected and whether these measures comply with relevant laws and regulations.

- **Training Data.** AI models are trained on large datasets, which may be sourced from public, private, or proprietary sources.
  - ○ **Ownership & Licensing** – Does the organization/vendor have legal rights to use this data?
  - ○ **Bias & Representativeness** – Has the data been vetted for fairness, demographic balance, and regulatory risks?

CHECKLIST 8

WITH THANKS TO:

***Meghan K. Farmer*, *Partner*, and *Gregory P. Silberman*, *Counsel*, at *Kilpatrick*,**

for contributing this checklist.

    - **Privacy & Consent** – Does the dataset contain personal data that requires compliance with privacy laws (e.g., EU GDPR, California Privacy Rights Act (CPRA))?
    - **Safety & Security** – Has the data been vetted to ensure that it has not been "poisoned?" **Data poisoning** is a type of cyber attack where malicious or misleading data is intentionally introduced into a model's training set to compromise its integrity, performance, or security. This can result in biased, inaccurate, or exploitable AI outputs ("exploitable" means that the output presents vulnerabilities that can be used by bad actors to perpetrate attacks).
- **Input Data** (prompts, uploads, embeddings, etc.)
    - **Confidentiality & IP Risks** – Could sensitive business data or trade secrets be exposed?
    - **Data Retention & Usage** – Does the vendor store input data, and is it used for model training or retraining?
    - **Privacy Compliance** – Does the input contain regulated data, requiring additional safeguards?
- **Output** (responses)
    - **Accuracy & Reliability** – Are outputs fact-checked, and can they be legally relied upon?
    - **Intellectual Property Risks** – Does the organization own AI-generated content, and is there risk of infringement?
    - **Bias & Fairness** – Could outputs result in discriminatory or non-compliant decision-making?

4. **Consider jurisdictional implications.** Assess whether ***specific local or international regulations*** will impact your organization's intended use of AI.

    - The **EU AI Act** places significant obligations on developers and deployers of high-risk AI systems and prohibits certain uses of AI altogether (e.g., social credit, real-time biometric evaluation, sentiment analysis – "social credit" means a system that assigns a trustworthiness score to people, potentially impacting their ability to take certain actions such as engaging in business transactions).
    - Emerging **US state or local AI regulations** (such as NY Local Law 144, the Colorado AI Act, the Illinois Human Rights Act, etc.) may be a factor.

- **Existing data protection and consumer protection regulations** may also apply to your intended AI use case (such as the EU's General Data Protection Regulation (GDPR), or the California Consumer Protection Act (CCPA)). For example:
    - Decisions made by an AI-powered loan application processing system may trigger fair-lending regulations in the US, such as the ***Equal Credit Opportunity Act*** and the ***Fair Credit Reporting Act***.
    - Such a system also uses applicants' personal financial data, and this could trigger requirements for explicit consent and the right to contest automated decisions (for example, under the EU's GDPR).
- Consider if the AI system needs to be adapted to meet the **legal and cultural expectations of different regions** (and industry verticals), especially if your organization is multinational or offers products or services across borders.

5. Review the technical details and history of the model you are considering. Has the model been reviewed or tested?

- **Inquire about the type of AI models** used by the tool, and the rationale behind their selection.
- **Examine model documentation** (bias audit, conformity assessments, compliance statements, and other regulatory mandated reporting).

6. Check for vendor dependencies.

- **Will your vendor be dependent on any external entities** for the AI's operation and maintenance?
- **Is the vendor providing a wrapper** for a third-party AI model?
    - An **AI wrapper** is a software layer that encapsulates an AI model or system. This provides a structured interface for integration, customization, or enhanced functionality.
    - Wrappers can manage inputs and outputs, enforce security controls, apply business logic, or facilitate the interaction between the AI model and external applications.
- **Does the vendor have adequate support and indemnification** from the service providers on which it depends?
- **Evaluate the availability, safety, and security** of the vendor's dependencies.
- **Consider the vendor's credibility** and the stability of their service.

7. Assess possible legal or business issues with the AI tool's output.

- **Factor in what business decisions this AI tool will influence** and how its outputs will be utilized.
- **Consider any possible intellectual property rights** your organization or others may have in the AI tool's outputs.
- **Investigate how outputs are validated** for accuracy and relevance.
- **Evaluate possible bias and fairness implications.** This is especially important for AI tools to be used in HR functions.

8. Ensure adequate human oversight will be in place. It is vital to decide who will be responsible for monitoring the AI tool's decisions.

- **Confirm** if there is a system in place for human oversight.
- **Discuss with stakeholders** the protocols for handling discrepancies or failures in the AI's performance.
- **Make sure there will be a human in the loop** for any decisions or actions taken by the AI tool. This will be especially important as new agentic AI tools come into use.
- Watch out for **over-reliance** on a tool.
- Ensure that employees responsible for working with the AI system or overseeing it **will be properly trained** on using it safely and effectively.

9. Have a plan if the AI tool fails or has negative impacts.

- **Consider the broader legal and business implications of failure** for your organization, for example if the AI tool behaves unexpectedly or makes biased decisions.
- Consider how these risks will be mitigated, including in your organization's business continuity plans.
- **Plan for mitigation strategies** to address potential harms or biases. Similarly to cybersecurity plans, this may involve creating a crisis team of stakeholders in IT, communications, the C-suite, and potentially others outside the organization.
- **Prepare an AI Impact Assessment ("AIIA")** prior to going live with new AI systems or features. See the checklist below: "***Tips for Conducting an AI Impact Assessment***."

10. Establish how the AI tool will be monitored and evaluated.

- **Decide which business metrics will be used** to assess the AI tool's performance and success.
  - For example, a customer service chatbot's effectiveness may be measured by response accuracy, customer satisfaction scores, and issue resolution time.
- **Establish how the AI will be monitored over time.**
  - For example, a fraud detection AI may require weekly accuracy reports and quarterly audits to assess false positive rates.
- **Ensure there are processes for ongoing review and improvement** of the AI system.
  - For example, an HR resume-screening AI tool that was evaluated for bias before being deployed should also undergo bias audits periodically to ensure fair candidate selection. Other talent acquisition metrics should also be evaluated periodically to determine whether the AI system is providing a valuable return on investment.
- **Ensure that someone is monitoring the tool for model drift** (i.e., a change in the model's accuracy).
  - For example, an AI used for financial forecasting should have automated alerts if its prediction accuracy drops below a set threshold, to trigger human review when accuracy declines.
- **How will model updates be evaluated?**
  - Before deployment, new AI model versions should be tested in a controlled environment to compare performance against the current model.

Learn more

→ *Kilpatrick Connect*

→ *ACC AI Resource Collection*

» **WITH THANKS TO:**

***Gregory P. Silberman*, *Counsel*, at *Kilpatrick*,**

for contributing this checklist.

Checklist: Evaluate Four Key Risk Factors in AI Systems

When vetting an AI system and weighing the benefits vs. the risks, evaluate these four key areas for regulatory or compliance risks:

1. **Privacy.** AI systems that process personal data are likely subject to privacy laws that regulate data collection, usage, storage, and sharing.

    - **Data Collection and Processing**
        - Does the AI system process personal, sensitive, or biometric data?
        - Is data processing covered under your existing privacy policies and user agreements?
    - **Data Minimization and Purpose Limitation**
        - Are data collection and processing limited to what is necessary for the AI system's intended function?
        - Is there a clear legal basis for collecting and processing personal data?
    - **Transparency and Notice**
        - Are AI-generated decisions or profiling disclosed to users?
        - Does the company provide adequate privacy notices about how AI processes personal data?
    - **Cross-Border Data Transfers**
        - If the AI system processes data across jurisdictions, does it comply with cross-border data transfer restrictions (e.g., GDPR)?
    - **Retention and Deletion Policies**
        - Does the AI system have clear data retention and deletion mechanisms that comply with legal requirements?

2. **Security.** AI introduces new attack vectors and security risks, particularly related to data exposure, model manipulation, and adversarial threats.

   - **Data Security and Encryption**
     - How is confidential, trade secret, or personal data used by the AI system?
     - Does the system use encryption, access controls, and audit logs to safeguard data?
   - **Adversarial Attacks and Model Security**
     - Can the AI model be manipulated or exploited (e.g., prompt injection, adversarial Machine Learning attacks)?
     - What safeguards exist against model inversion (where attackers extract sensitive training data)?
   - **API (Application Programming Interface) and Third-party Access Security**
     - Are AI models accessed via third-party APIs? If so, how are API security risks mitigated?
     - Are third-party dependencies properly vetted and secured?
   - **Incident Response and Security Testing**
     - Is there an AI security assessment process? Are regular penetration tests conducted?

3. **Trust & Safety.** AI products and services must ensure user safety, prevent harm, and uphold ethical standards.

   - **User Safety & Harm Prevention**
     - Are there safeguards against generating harmful, deceptive, or abusive content?
     - Are there controls to prevent misuse, fraud, or misinformation?
   - **AI Explainability & Transparency**
     - Can users understand why an AI system made a particular decision?
     - Are AI limitations, risks, and reliability documented?
   - **Consumer Protection & Accountability**
     - Are AI-driven decisions contestable?
     - Are AI uses in customer interactions, hiring, or decision-making disclosed?

- **Automated Content Moderation & Safety Features**
  - If AI is used for content moderation, does it adequately detect hate speech, harassment, misinformation, and deepfakes?
  - Does the system avoid over-moderation?

4. **Bias & Fairness.** Regulators are increasingly scrutinizing AI for bias, discrimination, and fairness. This is especially true in hiring, lending, health care, and applications directed towards children.

   - **Bias Detection & Fairness Audits**
     - Has the AI model undergone bias and fairness testing?
     - Are demographic disparities evaluated in training data and outputs?
   - **Automated Decision-making & Discrimination Risks**
     - Does the AI system make decisions that could trigger anti-discrimination laws?
     - Are human-oversight mechanisms in place?
   - **Inclusiveness & Representation in Training Data**
     - Does the AI system rely on biased data sets that could lead to unfair outcomes?
     - Are mitigation measures in place?
   - **"Fairness in AI" Audits & Compliance Documentation**
     - Is there internal documentation proving compliance with fairness and anti-discrimination laws?
     - If AI decisions are challenged, is there a process to explain and correct unfair outcomes?

Tips for Conducting an AI Impact Assessment

1. An AI Impact Assessment (“AIIA”) is a structured evaluation of an AI system’s risks, benefits, and compliance obligations. It helps organizations identify and mitigate legal, ethical, security, and operational risks throughout the AI lifecycle.

2. The **level of documentation** should correspond to the system’s potential impact.

   - For example, an AI analyzing surveillance footage to assess real-time threats would require a comprehensive AIIA.

3. **Low-risk AI tools** that do not process personal or sensitive data, make impactful decisions, or raise legal compliance concerns, **may not require a formal AIIA** (e.g., AI-based video compression software).

4. **Key Components of an AI Impact Assessment:**

   - ***Risk Identification:*** Assess potential harms, including bias, discrimination, privacy violations, and security vulnerabilities.
   - ***Regulatory Compliance:*** Evaluate whether the AI system aligns with relevant laws (e.g., GDPR, CCPA, EU AI Act).
   - ***Business and Legal Implications:*** Determine the financial, reputational, and liability risks of AI failures or unexpected outcomes.
   - ***Mitigation Strategies:*** Develop oversight mechanisms, human-in-the-loop processes, and corrective action plans.
   - ***Ongoing Monitoring:*** Establish procedures for tracking AI performance, detecting drift, and addressing emerging risks.

5. An AIIA ensures AI systems are **responsibly designed, legally compliant, and aligned with organizational goals** while minimizing risks to users and stakeholders.

» **WITH THANKS TO:**

***Gregory P. Silberman*, *Counsel*, at *Kilpatrick*,**

for contributing this checklist.

CHECKLIST 9

» **WITH THANKS TO:**

***Joshua S. Ganz*, *Partner*, at *Kilpatrick*,**

for contributing this checklist.

Top Eight Tips to Address AI issues in Contracts with Third Parties

Your organization's vendors are most likely using AI. When entering into contracts with vendors, make sure their use of AI tools safeguards your business data and is legally compliant.

1. Consider including general restrictions or prohibition, disclosure and "prior approval" clauses as a due diligence mechanism to address AI use.

- Have a **designated AI review process** to conduct due diligence on vendors' use or provision of AI functionality.
- Develop a **standard workflow** for seeking, granting, and revoking approvals for AI use cases.
- Create templates for **documenting vendor-provided information** about AI functionality.
- Consider including a **general prohibition** in your contracts that the vendor must obtain **prior written approval** for the use or provision of any AI functionality. This can serve as a backstop to force diligence conversations during the contracting process.

2. Understand your vendors' AI usage.

- **Request a clear description** of how the vendor and its subcontractors/third parties propose using any AI functionality to perform services for your company.
- This should include a description of **specific use cases** and the **data and information** that will be input into or generated from their AI systems.

3. Get documentation from vendors. Require vendors to provide detailed documentation about their AI system, including details regarding:

- **How their AI system collects data and inputs and processes data** to generate outputs/results, including any modifications made to the inputs by the system before it renders results;
- **Assumptions, inputs, and decision paths** used by the AI to generate results;
- **Degree of human oversight** in managing AI-generated outputs; and
- Circumstances under which **outputs or results can be overridden or modified** by the vendor.

4. Obtain assurances regarding the vendor's legal compliance.

- Check that the vendor has implemented **policies, procedures, and testing protocols** to
  - mitigate risks of illegal, unethical, biased, inaccurate or infringing AI outputs and
  - comply with applicable laws and industry standards.
- Require the vendor to maintain and comply with these policies and procedures and **test the AI** on an ongoing basis to ensure compliance.
- Consult **your company's AI usage policies** to ensure that the vendor's policies and procedures are consistent and at least as protective.

5. Take subcontractors or third parties into account.

- If possible, confirm and require that any subcontractors of the vendor provide at least the same level of information as part of the diligence process and are **bound by the same AI-related contractual obligations** as the primary vendor.

6. Develop standard AI-related terms to facilitate negotiations.

- Include a contract provision **in your standard procurement forms, or develop an addendum** for use with vendor forms, to address the vendor's rights and obligations regarding the use or provision of an AI system in connection with their services.
- Keep in mind that the vendor's rights and obligations may differ depending on whether:
  - the vendor is the direct user of an AI system in delivering services or developing work product (for example, to create content that your company then uses in marketing campaigns), or
  - the AI system is provided by the vendor for direct use by your company as part of a SaaS solution or software license.

7. Tips for AI terms and conditions. When drafting an AI provision:

- **Include clear definitions** for critical terms such as AI functionality, Inputs, Outputs, Training Data, Vendor Models, and Customer Developed Models. This ensures consistent understanding across all stakeholders.

> "It may be really tough for smaller organizations to get any traction on contractual changes, so another option is to make sure you obtain and review AI whitepapers and other technical information published by the vendor."
>
> **Aparna D. Williams**
> *Chief Legal and Compliance Officer,*
> Coalfire

- **Include clear limitations on:**
  - The vendor's ability to use the AI system for any purposes other than as approved;
  - The storage of input or outputs, the vendor's ability to share inputs or outputs with third parties, and the use of inputs or outputs by the vendor for its own purposes or for the benefit of anyone other than your company (including the use of inputs or outputs for AI training purposes);
  - The use of AI systems other than non-public, enterprise-level AI instances, to ensure privacy and security of your data and mitigate the risk of data leaks; and
  - Using training data or other content in the AI functionality without having obtained all necessary consents, licenses, and permissions.
- Clearly outline provisions for **data ownership, confidentiality, and intellectual property rights.**
- Ensure that all inputs and outputs (and, if applicable, any derivative models developed by your company or the vendor on your company's behalf) are classified as **confidential and proprietary** to your organization.
- Where the vendor is providing work product that was developed using an AI functionality, **require that the vendor review and validate all AI-generated outputs prior to providing it to your company**.
- **Include strong indemnification clauses** requiring the vendor to defend your business against claims arising from their use of AI functionality, including infringement or misuse of intellectual property.
- **Consider appropriate rights to revoke approval** of the vendor's use of AI systems.
- **Consider requiring the ability to disable** AI functionalities provided by the vendor as part of a SaaS or software tool.

8. Create a user-friendly playbook.

- Your standard AI contract provision or addendum can be used as the basis for developing a user-friendly negotiation playbook.
- **Develop approved fallbacks and approval mechanisms for deviations from the standard terms** depending on the use cases, the types of data and information that will be input into the AI system, and/or the types of output that will be generated using the AI tool or functionality.

AI Thought Leadership and Resources by Kilpatrick

1. ***AI: Virtual Patchwork***,
by Stephen M. Anstey and Michael J. Breslin, Kilpatrick, November 8, 2024
2. ***Gen AI: The "Artificial" Threat to Trade Secrets***,
by Joel D. Bush and Kurtis G. Anderson, Kilpatrick, April 4, 2025
3. ***Robots are Coming – But They Still Can't Register Copyright***,
by Gabriel M. Ross, James A. Trigg, Mehrnaz Boroumand Smith, and Joseph Petersen, Kilpatrick, March 24, 2025
4. ***5 Key Takeaways – Artificial Intelligence: What Tax Professionals Need to Know***,
by Kilpatrick, March 13, 2025
5. ***5 Key Takeaways – Building an AI Governance Program***,
by Amanda Witt, Ami Rodrigues, and Christina McCoy, Kilpatrick, March 7, 2025
6. ***5 Key Takeaways – Managing the Risks in Using Generative AI or How I Learned to Stop Worrying and Love AI***,
by Steve R. Borgman and Jordan P. Glassman, Kilpatrick, February 20, 2025
7. ***Basics for Corporate Counsel to Consider About Generative AI***,
by Meghan K. Farmer, Jon Neiditz, and John M. Brigagliano, Kilpatrick, August 24, 2023
8. ***Kilpatrick's Generative AI Insights Hub***
9. ***Kilpatrick's Artificial Intelligence and Crypto Blog***
10. ***Kilpatrick Connect***

Additional Insights on AI Topics

1. ***ACC AI Insights – an ACC resource collection***.
2. ***GenAI and Future Corporate Legal Work: How Ready Are In-house Teams?***,
ACC Research Report, October 7, 2024
3. ***The Impact of AI on Attorney-Client Privilege***,
ACC Research Report, September 11, 2024
4. ***CLOs Lead the Charge on "Transformative" GenAI Use***,
ACC Docket, November 12, 2024
5. ***The Promise and the Peril: AI and Disruptive Technologies in Operations and Compliance***,
by Daniel Christmas, Kathryn M. Rattigan, and David E. Carney, *ACC Docket*, January 27, 2025
6. ***HR Privacy in the Age of AI***,
by Monica Dongre, Martha Wewer, Denise Bahena-Bustos, William O'Bannon, and MH Tillman, *ACC Docket*, August 19, 2024
7. ***Legal Tech: The Crucial Role of Legal Stewardship During the AI Revolution***,
by Olga V. Mack, Kevin Keller, and Kristina Podnar, *ACC Docket*, July 29, 2024
8. ***It's Go-Time — Creating an AI Governance Program***,
by Adam Shedd and Mark Diamond, *ACC Docket*, April 1, 2024
9. ***Two-Year Verdict: ChatGPT's Impact on the Legal Practice***,
by Spiwe L. Jefferson, *ACC Docket*, November 25, 2024
10. ***State of Play: Adoption of Gen AI in Corporate Legal Departments***,
by Catherine J. Moynihan, Epiq, December 13, 2024

Sample Tools, Forms, and Checklists

1. *Sample Use of Generative AI Policy Template*
2. *Tips for Developing a Corporate AI Policy*
   by Elizabeth Matecki, iCIMS
3. *Using AI in HR Decisions: Tips for In-house Counsel*

More Resources

1. ***Visit the ACC Resource Library. Find thousands of resources:***
   - Sample contracts and policies
   - Checklists and articles
   - ACC in-house survey reports
2. ***Explore ACC Curated Collections:***
   - *Artificial Intelligence*
   - *Privacy and Cybersecurity*
   - *Teaching Law School*
   - *And More*

Connect with Peers and Boost Your AI Skills

Connect with the ACC IT, Privacy & e-Commerce Network

- Monthly **live discussions** with other in-house counsel and outside speakers.
- A dedicated **e-forum** to connect with peers and seek their insights.
- *Join the Network!* For ACC members only.
- Not an ACC member? *Join ACC.*

Explore trends and tips at the ACC Annual Meeting

- **Enjoy** the largest annual gathering of the global in-house community.
- **Engage** in lively sessions and learn the latest in-house strategies, tips, and trends.
- **Bring** your in-house team. Get CLE/CPD credits.
- Enjoy the **unique experience** of our vibrant ACC in-house community.
- *Learn more*

Learn strategies at the ACC Foundation Cybersecurity Summit

- Learn about the latest cyber threats and innovations for in-house.
- Participate in deep-dive sessions with leading cybersecurity and in-house professionals.
- Discuss emerging issues, and tips for preventing and responding to data breaches.
- *Learn More about ACC Foundation events*

Disclaimer: *No information in this toolkit shall be construed as a recommendation or endorsement of any vendor or tool by ACC. Microsoft, Microsoft 365, Power Apps, Power Automate, Power BI, are trademarks of the Microsoft group of companies. Westlaw® is a trademark of Thomson Reuters or its affiliates. LexisNexis® is a trademark of RELX Inc. This toolkit is a publication of the Association of Corporate Counsel and is neither affiliated with, nor authorized, sponsored, or approved by, Microsoft Corporation, Thomson Reuters, or RELX Inc.*