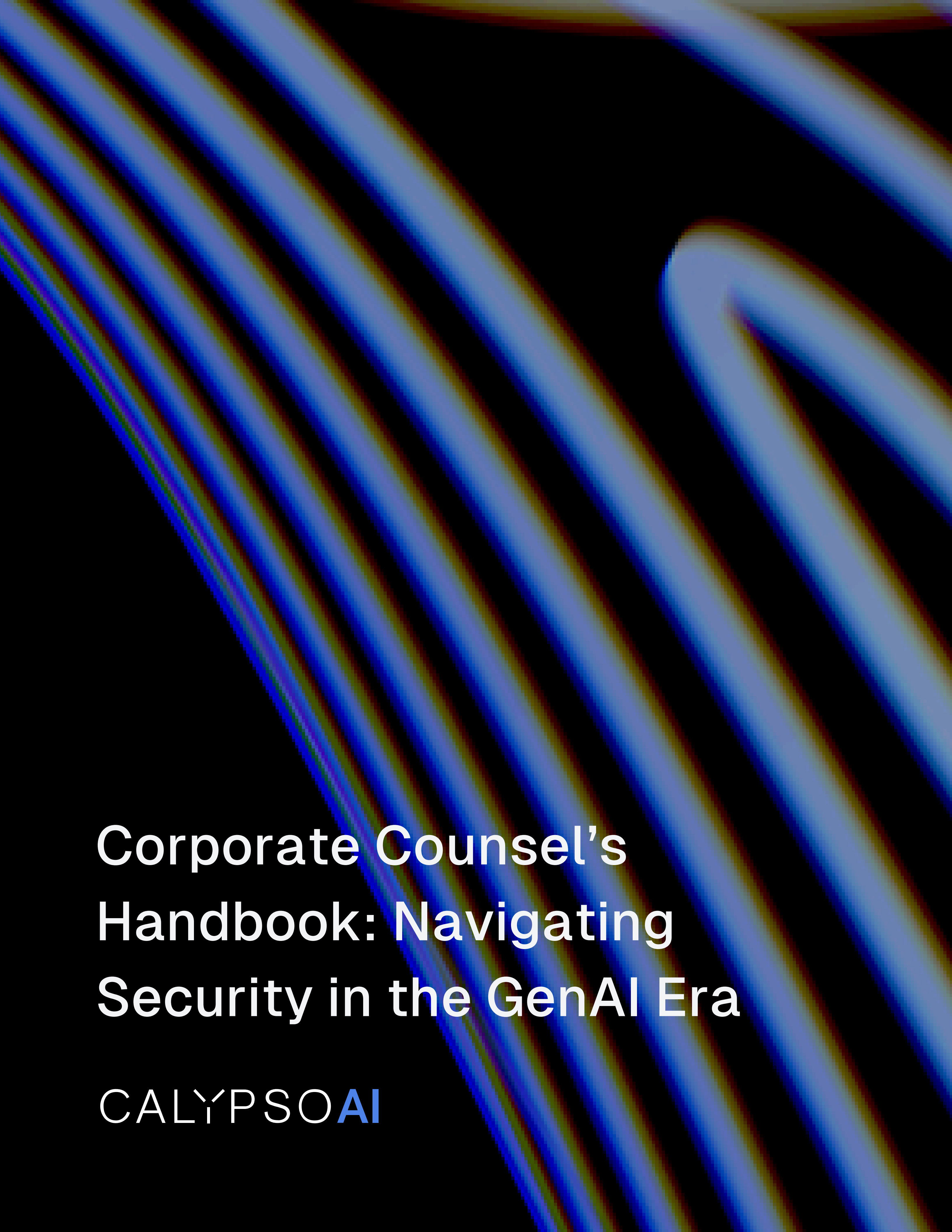


Corporate Counsel's Handbook: Navigating Security in the GenAI Era

CALYPSOAI

Executive Summary

The integration of Generative AI (GenAI) into enterprises presents both opportunities and complexities, requiring a comprehensive governance framework to ensure secure, ethical, legal, and strategic alignment. GenAI's ability to automate content creation and enhance decision-making brings significant benefits, but also introduces risks related to data privacy, intellectual property (IP), bias, and regulatory compliance. For legal leaders, such as general counsels and compliance officers, understanding the capabilities and challenges of GenAI is essential to aligning its use with external regulations and internal governance standards.

According to the 2024 Chief Legal Officers Survey conducted by the Association of Corporate Counsel, the majority of these leaders "oversee at least three additional business functions beyond legal" with 58% overseeing three or more and 27 % overseeing five or more. The most common areas they now bear responsibility for include privacy (44%), ethics (43%), and risk (38%). Additionally, the two categories that are top of mind are regulation/enforcement (53%) and privacy/data security (41%).

We approach crafting AI governance ... as the foundational step to embedding AI-native thinking into broader organizational governance.

Given this added responsibility, a robust GenAI governance framework demands clear leadership and accountability, and must be built atop a cross-functional team. This team, with strong guidance by legal experts working closely with C-suite executives, will ensure AI projects are aligned with the organization's strategic goals while managing legal, ethical, and compliance risks to address:

- Data governance, which is critical to maintaining data integrity and privacy, particularly when dealing with third-party data and AI vendors
- Policies for acceptable use, risk management, and ethical guidelines, and responsible AI principles crafted to mitigate risks, such as bias and discrimination
- Compliance with external regulations that continue to evolve coupled with industry-specific rules
- Internal audits and incident response plans to identify and mitigate risks
- Creating a culture of compliance with employee training, open communication, and continuous improvement practices

> We expect AI policy to become part of the typical general workplace and business policies.

This white paper provides a roadmap for legal counsel seeking to leverage GenAI's transformative potential and turn AI safety and compliance into a market advantage while safeguarding their organization against regulatory, ethical, and operational risks. Over time, we expect AI policy to become part of the typical general workplace and business policies, as AI will no longer be seen as a siloed issue, but as an integral part of every facet of the business landscape.

We approach crafting AI governance, as outlined in this paper, not as a response to current regulator challenges so much as the foundational step to embedding AI-native thinking into broader organizational governance, policy-making, and decision-making processes. By taking proactive measures today, legal leaders will set the stage for a future in which AI is seamlessly woven into the fabric of all policy, process, and strategy, ensuring long-term resilience and competitive advantage.

Introduction to GenAI in the Enterprise

Generative AI (GenAI) represents a significant evolution in the use of AI technologies across industries. It involves machine learning models capable of creating new content —such as text, images, or code—based on the data they've been trained on. As companies integrate GenAI tools into their operations, the potential benefits are substantial: Automating content creation, enhancing decision-making, and driving innovation in ways that were previously unimaginable.

For general counsels (GCs), chief legal officers (CLOs), chief compliance officers (CCOs), and other leaders in the legal field, the adoption of GenAI also brings new complexities and risks. These leaders must become conversant on issues surrounding the technical aspects of data usage, as well as governance, and understand how this technology works and what it can and cannot do. In short, these leaders must understand the capabilities of GenAI before they can ensure its use within the enterprise aligns with existing legal, ethical, and regulatory standards. Decisions made at this juncture will have lasting implications for corporate risk exposure, compliance practices, and legal liability.

These leaders must become conversant on issues surrounding the technical aspects of data usage.

Additionally, legal counsel must navigate complex issues such as:

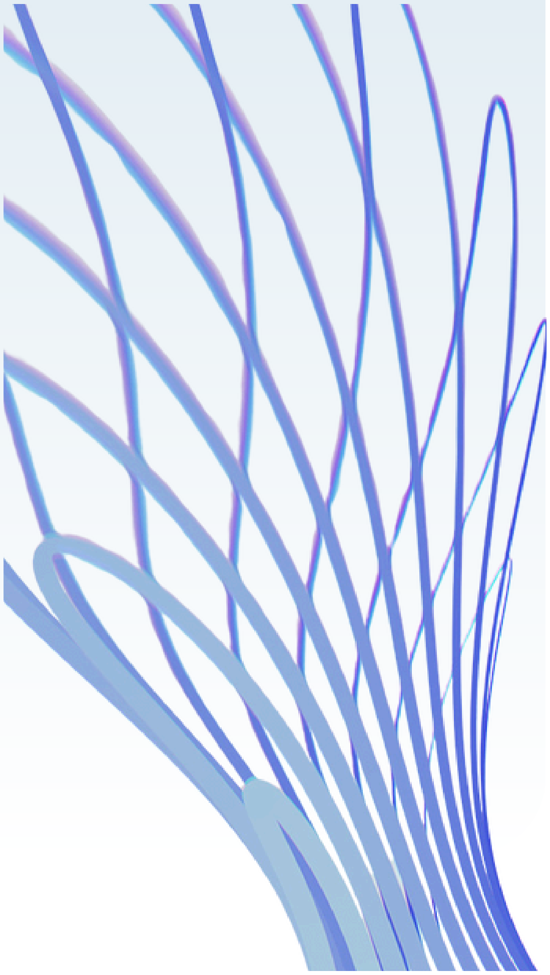
- Understanding the novel legal challenges AI presents to IP rights, data privacy, and ownership of AI-generated outputs
- Knowing the risks related to using third-party data in AI models
- Assessing potential biases in AI decision-making, which could lead to discrimination claims
- Ensuring contracts with AI vendors and service providers include adequate indemnities and warranties to protect the organization from undue risk

Strategically, legal teams must align GenAI adoption with the company's overall governance framework, balancing innovation with legal and ethical compliance. This involves working closely with other C-suite executives to establish protocols for the ethical use of AI, managing personal data in accordance with data protection laws, creating a culture of compliance within the company, and ensuring the organization's use of GenAI aligns with external regulatory requirements and internal policies.

Compliance: External Regulations

The regulatory environment is evolving, which means that while it is increasingly complex, it is also inconsistent, edging toward chaotic at times. The one established fact everyone understands is that governments are imposing critical requirements on the development, deployment, and use of AI technologies. Many companies, especially those in market sectors not familiar with heavy regulation, like tech, might not understand the impetus to prioritize compliance as much as growth and product development.

That's a miscalculation in-house legal experts must correct because "[w]hile such an approach may have been feasible with other regulations in the past, AI regulations demand early and proper adherence." Compliance is both a legal obligation and a strategic necessity. Lately, it can also be considered a key differentiator. Legal and compliance leaders are central to ensuring the enterprise remains aligned with current laws while anticipating future regulatory shifts.



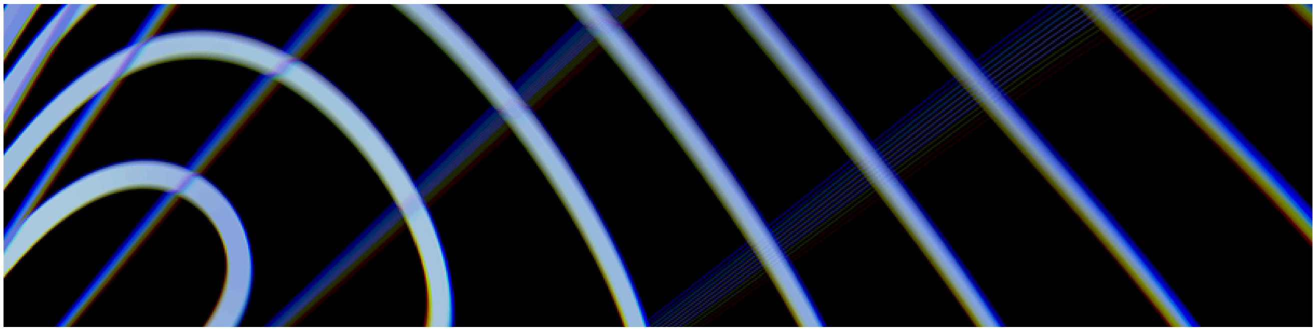
Existing and emerging regulations govern data privacy, AI ethics, consumer protection, and industry-specific issues. While these vary across jurisdictions, the regulations share a common objective: To mitigate the risks associated with AI technologies and ensure these tools are used in a responsible, transparent manner. Understanding the scope and application of these regulations is essential for legal leaders as they work to ensure organizational compliance.

Key Regulatory Issues Affecting GenAI

As of the time of publication, the laws and initiatives below are in effect or will be imminently. This guide will be routinely updated to reflect changes in the regulatory landscape.

Data Privacy and Protection

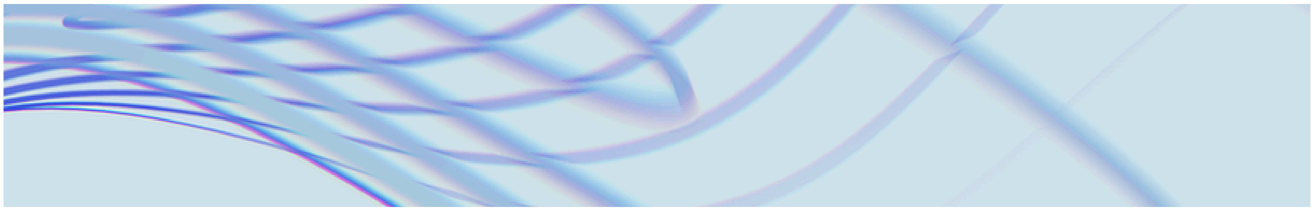
- **General Data Protection Regulation (GDPR):** This European Union rule is one of the most stringent data privacy regulations, directly impacting how organizations collect, process, and store personal data. Under GDPR, GenAI models that use personal data for training must adhere to strict requirements regarding consent, transparency, and data minimization. Legal teams must ensure their organization's AI tools are designed with "privacy by default" to limit exposure to potential fines and reputational damage.
- **California Consumer Privacy Act (CCPA):** This law places similar obligations on companies operating in California or targeting its residents. The law emphasizes consumer rights, such as the right to access, delete, and restrict the sale of personal data. GenAI tools must comply with these rights, ensuring that data-subject requests are documented and honored. Compliance programs must include mechanisms for managing data requests related to AI applications in use across the organization.
- **Emerging Privacy Laws:** As AI use becomes more ubiquitous, privacy regulations are emerging worldwide, most recently in Australia, Brazil, Canada, Chile, Japan, and Singapore, among others. Legal teams must stay informed of global developments and ensure their organization's GenAI solutions remain compliant across all relevant jurisdictions.



AI-Specific Regulations

- EU Artificial Intelligence Act (EU AI Act): This newly enacted law has established a comprehensive regulatory framework for AI technologies, classifying them based on risks posed to people affected by, or who interact with, the software. High-risk AI systems—such as those used in healthcare, finance, or law enforcement—are subject to stringent obligations, including requirements for transparency, human oversight, and accountability. Legal teams must understand how the Act's requirements affect their organization's AI tools, and collaborate with other departments to ensure compliance.
- U.S. Federal Initiatives: There is no unified federal AI regulation in the U.S.; however, in March, the Biden administration issued "binding" guidance requiring federal agencies to undertake specific steps to safeguard their use of AI technologies. Among the requirements is the appointment of a chief AI officer for each agency. Individual agencies are taking additional steps proactively. For example, the Federal Trade Commission (FTC) has issued guidance on fairness and transparency in AI use. Misuse of AI has also taken on a new level of importance. U.S. Deputy Attorney General Lisa Monaco recently stated that, in an effort to detect misconduct and ensure that executives and employees follow the law, the Justice Department will consider how well a company manages AI risks when it evaluates corporate compliance programs.
- U.S. State Initiatives: Half of the states, including the four most populous, have enacted laws addressing data privacy, biometric data, or other AI-related data, as well as activities regarding or driven by AI. For example, Utah passed a bill in March 2024 that defines generative AI and synthetic data, and provides clear direction for companies in both regulated and non-regulated industries regarding when they must inform consumers that they are interacting with a GenAI tool. A bill awaiting the governor's signature in California would require companies that create large AI systems to "test their models and publicly disclose their safety protocols to prevent the models from being manipulated" to execute harmful or illegal acts.

Legal and compliance teams must build continual monitoring into their routine processes to ensure ongoing compliance across national and international jurisdictions, and prepare for additional developments that may be unforeseen.



Industry-Specific Guidelines

- **Healthcare:** GenAI technologies must comply with sector-specific laws. For instance, the Health Insurance Portability and Accountability Act (HIPAA) governs the protection of sensitive patient information and establishes guidelines for data security and privacy. AI systems handling personal health information (PHI) must be designed with built-in safeguards to protect patient data and maintain confidentiality.
- **Financial Services:** In the financial services sector, U.S. regulations like the Sarbanes-Oxley Act (SOX) and the Gramm-Leach-Bliley Act (GLBA) impose stringent requirements on financial reporting and data privacy. GenAI tools used to automate financial decision-making or customer interactions must comply with these rules. Any AI-driven processes in the financial sector must be auditable and have adequate controls in place to ensure compliance with financial regulations.
- **Other Regulated Industries:** In other regulated industries, such as energy and manufacturing, regulatory agencies may impose specific requirements on AI technologies that involve safety or environmental issues, or industry-specific risks. Organizational GenAI implementations must meet these requirements to avoid incurring potential regulatory penalties.

Ensuring Compliance with External Regulations

Organizations must adopt a proactive approach to compliance to avoid unnecessary exposure. Legal and regulatory considerations must be embedded into every stage of AI development and deployment, including:

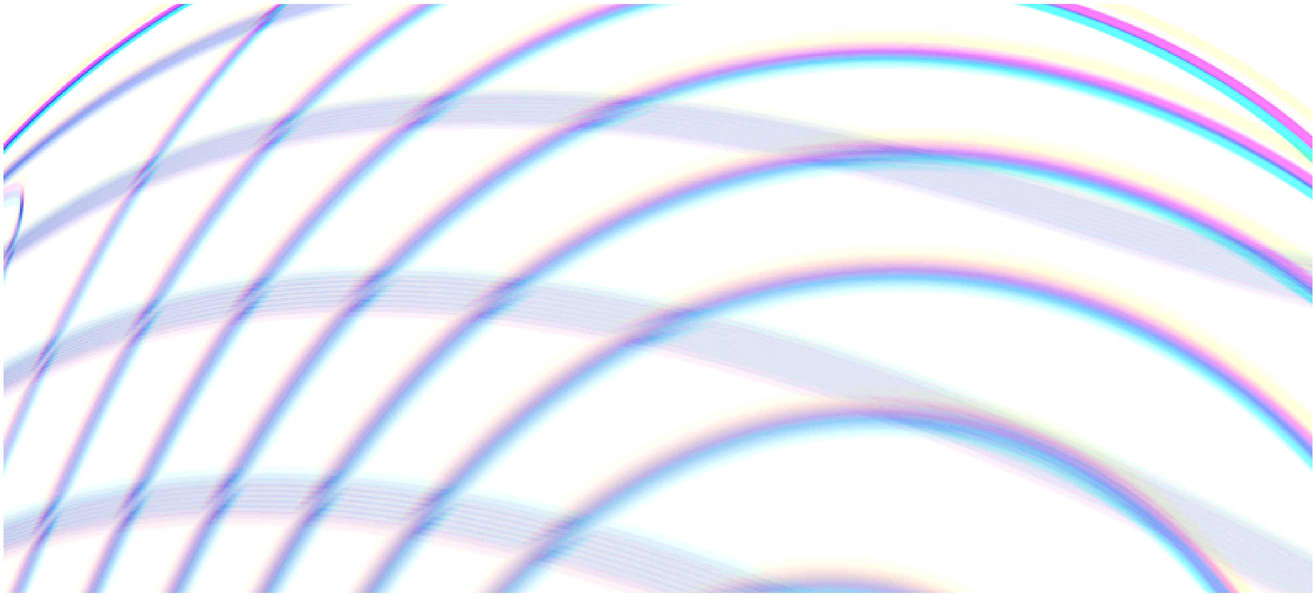
- **Conducting Comprehensive Risk Assessments:** A thorough risk assessment that evaluates organizational use of GenAI across all functions will identify areas of high regulatory exposure. The assessment must identify how AI tools interact with personal data, sensitive information, and decision-making processes to determine where potential compliance gaps exist.
- **Collaborating Across Departments:** Legal teams must collaborate with IT departments and business units to establish cross-functional governance structures that facilitate compliance.

- Monitoring Regulatory Changes: The ability to adapt to new requirements as they emerge and interpret their impact on the organization's AI initiatives is critical.
- Documenting Compliance Efforts: Creating detailed documentation of compliance efforts, such as records of data usage, AI model development, risk assessments, and regulatory audits will ensure the organization can demonstrate regulatory adherence and prove it has met compliance obligations.

Internal Governance Frameworks

The Need for Governance in GenAI Implementation

GenAI introduces new complexities that demand thoughtful oversight and a structured approach to governance. However, governance in the context of GenAI encompasses more than just compliance with external regulations. It requires establishing policies, processes, and controls that define how AI tools are developed, deployed, and monitored within the enterprise. This governance framework must ensure that AI systems are transparent, auditable, and aligned with the company's risk appetite and ethical standards.



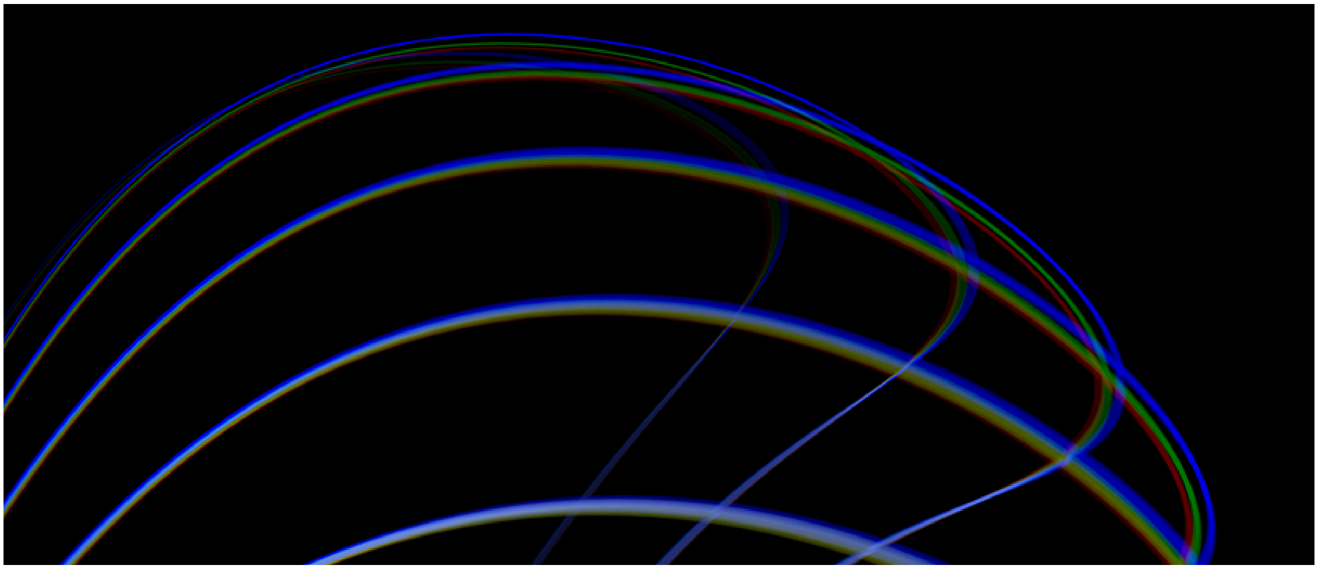
Key Components for an Effective GenAI Governance Framework

Clear Leadership and Accountability Structures

- **Executive Leadership and Oversight**: Establish clear lines of leadership as the foundation of your GenAI governance framework. GCs, CLOs, and CCOs must collaborate with chief information officers (CIOs), chief technology officers (CTOs), and other C-suite executives to design governance structures aligned with organizational objectives. Ensure leadership responsibility for GenAI initiatives is explicitly defined, with clear roles, risk ownership, reporting obligations, and accountability established across all departments.
- **AI Steering Committee**: Form a cross-functional AI steering committee to oversee GenAI projects. This committee must include representatives from Legal, Compliance, IT, and Data Science departments, along with other business units. The committee is responsible for ensuring AI projects undergo regular review, and that all key stakeholders participate in assessing risks, legal exposures, and ethical considerations.

Organizational Parameters

- **Risk Tolerance**: Determine the organization’s risk tolerance for GenAI technologies through frank discussions of “must-avoid” outcomes and the operational areas or processes that might produce them. Align on balancing potential risks with the benefits of GenAI deployment and innovation.
- **Define Use Cases**: Develop a comprehensive “living” list of potential applications and use cases for GenAI across the organization. Categorize them according to risk level and identify appropriate controls based on risk.



Policy Development and Risk Management

- **Acceptable Use Policies**: Develop and enforce a comprehensive AI acceptable use policy to manage risk and guide employees on the ethical and responsible use of GenAI tools. Senior legal management should lead this process, ensuring the policy covers essential areas such as data usage, AI system development, decision-making processes, user behavior, and ethical considerations. Policies must be reviewed regularly to ensure ongoing relevancy.
- **Risk Management Frameworks**: Implement a risk-based governance framework to evaluate potential harms associated with AI adoption. This framework must address legal liabilities, compliance risks, and ethical concerns, as well as internal and external threats to data and organizational security. Conduct routine risk assessments to inform both short-term decisions and long-term strategic planning for AI initiatives.

Data Governance and Management

- **Data Integrity and Privacy Controls**: Establish robust data governance policies that dictate how data is collected, stored, and processed in GenAI systems, and mandate strong access controls for all sensitive or personal data. These policies must ensure compliance with external regulations and internal ethical standards, including consent, anonymization, and data retention.
- **Third-Party Data and Vendor Management**: Clearly define data usage rights, IP ownership, liability, and regulatory compliance in contracts with third-party data sources and vendors. Regularly audit vendor performance to verify they consistently adhere to the organization’s compliance and ethical standards.

Ethical Guidelines and Responsible AI

- **Ethics Committees and Responsible AI Principles**: Form an AI ethics committee or board to oversee the ethical implications of AI deployments. This board must ensure AI use aligns with organizational values and ethical commitments, such as fairness, transparency, and accountability in AI decision-making processes.
- **Addressing Bias and Discrimination**: Establish protocols to prevent and mitigate bias in AI outputs, including employee use of GenAI models, such as large language models (LLMs). Instruct teams about what biased language in prompts or other instructions looks like and deploy tools to scan and block unacceptable content. Ensure your teams use unbiased training datasets, regularly audit AI outputs, and create channels for addressing potential discrimination claims. Bias in GenAI systems must be identified proactively and corrected.

Audits and Assessments

- **System Audits**: Conduct internal audits focused on data handling practices, decision-making processes, model performance, and adherence to internal policies. Use audits as both risk management tools and mechanisms for continuous improvement. Adapt AI governance practices as new risks and challenges emerge.
- **Compliance Monitoring**: Continually monitor organizational compliance with external regulations. Integrate compliance metrics into broad, enterprise-wide monitoring systems to provide visibility into AI system operations, data flows, and decision-making transparency. Monitor user behavior and model performance to ensure alignment with organizational values and adherence to internal policies.

Incident Response and Mitigation

- **Incident Response Plans**: Develop and implement a robust response plan The plan must detail steps for addressing compliance breaches, ethical concerns, and system failures. Include clear protocols for containment, remediation, reporting, and recovery, and communication with regulators, stakeholders, and the public.
- **Continuous Improvement**: Adopt a culture of continuous improvement by regularly revisiting governance policies, risk assessments, and ethical guidelines. Ensure your practices evolve in response to technological developments, regulatory changes, and shifting business objectives.

A Culture of Compliance and Ethical AI

The effectiveness of your GenAI governance framework depends on the policies and the culture supporting it.

- **Encouraging Transparency and Accountability:** Promote transparency and accountability throughout all stages of AI deployment. Establish open communication channels for reporting AI-related concerns, and guarantee that employees can raise issues or seek guidance without fear of retaliation.
- **Training and Education**: Mandate employee training at all levels, focusing on the legal, ethical, and operational aspects of GenAI. Ensure training programs reflect the organization’s governance priorities and prepare employees to navigate GenAI risks responsibly and in accordance with company policies.

Liability and Risk Management

Identifying Potential Liabilities in GenAI Deployment

The potential liabilities associated with GenAI integration can arise from several issues, including IP infringement, data breaches, bias or discrimination in AI-generated outputs, and failures in the decision-making process of AI models. Understanding the scope of these liabilities and implementing proactive risk management strategies is essential for minimizing exposure.

IP Concerns

- Copyright Infringement in AI Outputs: AI models are trained on large datasets, which may include copyrighted material. If an AI tool produces content that replicates or closely resembles protected works, the organization could be held liable for copyright infringement.
- Data Ownership and Licensing: Using third-party data to train GenAI systems raises questions about data ownership and licensing. Proper agreements must be in place with data providers, clearly defining data usage rights, ownership of AI-generated outputs, and liability for potential misuse. Establishing clear contractual terms with vendors and partners will mitigate IP-related liabilities.

Data Security and Privacy Violations

- Personal Data and Privacy Laws: The improper handling of personal data in GenAI systems can lead to violations of privacy regulations. Any GenAI tools in use must comply with applicable privacy laws.
- Data Breach Liability: Plans for managing liability due to breaches must be part of incident response plans if the system has access to PII or other sensitive data.

Algorithmic Bias and Discrimination

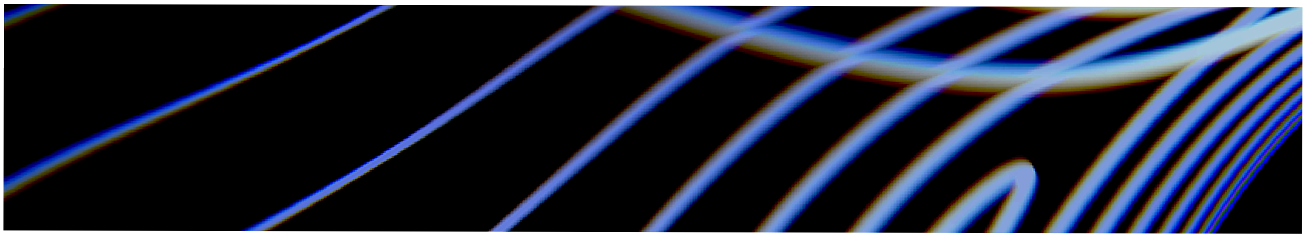
- **Bias in Decision-Making**: Algorithmic bias is one of the most prominent risks in GenAI systems because it can lead to discriminatory outcomes. AI models trained using biased algorithms or unrepresentative datasets may perpetuate inequalities in hiring, lending, customer service, or other areas that can affect a person's life. If an organization's AI system produces biased results that lead to discriminatory practices, lawsuits or regulatory enforcement actions could follow.
- **Liability for Discrimination Claims**: The risk of potential discrimination claims can be mitigated by taking steps to prevent bias in AI outputs, such as regularly auditing AI decision-making processes, using diverse training data, and maintaining transparency around AI-generated decisions.

Allocating and Managing Liability Across the Organization

A key challenge when managing AI-related liability and lowering risk is determining who within the organization is responsible for specific aspects of AI governance, oversight, and compliance. Senior legal management has a pivotal role in clarifying and distributing these responsibilities to minimize organizational risk.

Defining Accountability for AI Oversight

- **Cross-Departmental Responsibility:** Accountability for AI governance should be distributed across all relevant departments and business units. By assigning clear roles and responsibilities, organizations can create a more resilient risk management framework that addresses potential liabilities from multiple angles.
- **Board-Level Oversight**: Senior legal management should advocate for AI-related liability concerns to be addressed at the board level. Board oversight of AI risks can help ensure governance and risk management strategies align with corporate objectives, strategies, and risk tolerance.



Managing Liability Insurance for AI Risks

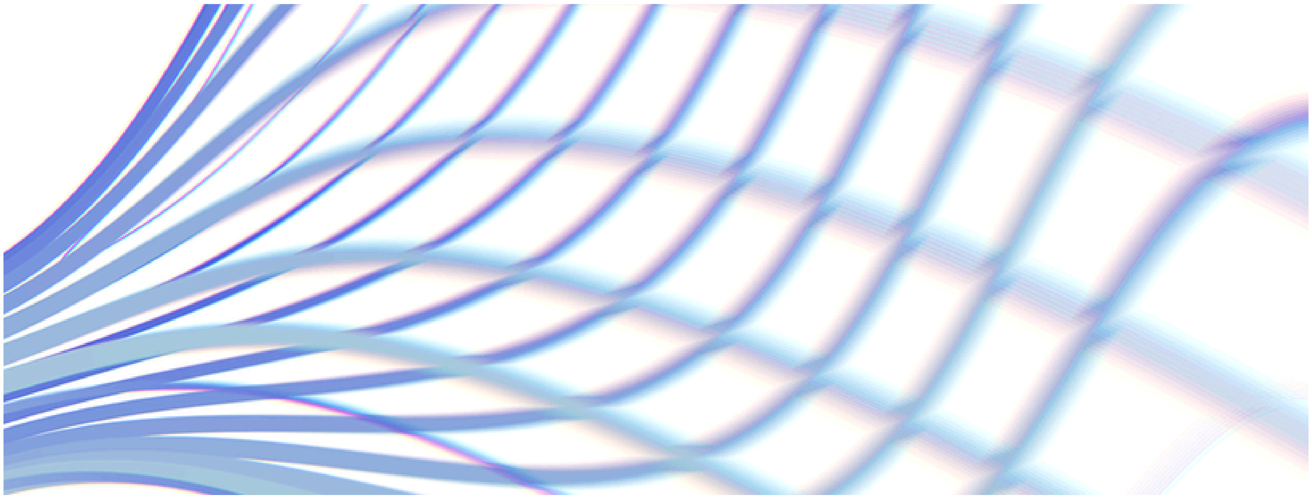
- **AI-Specific Liability Insurance**: Having AI-specific liability insurance can ensure coverage of potential claims arising from the use of AI tools, including data breaches, IP infringement, or discrimination claims related to AI outputs.
- **Reviewing Existing Coverage**: Review existing liability insurance policies to determine whether AI-related risks are adequately addressed and whether the policies align with the organization's risk profile and AI usage.

Balancing Innovation with Risk Management

Creating a culture of responsible innovation is foundational for ensuring AI deployments are both legally compliant and ethically sound.

Embedding Risk Management into Innovation Processes

- **Legal Involvement in AI Development**: Legal considerations should be discussed in the early stages of AI development and deployment. Collaborating with IT, Product, and Security departments can assist Legal teams identify potential risks before they become liabilities.
- **Continuous Risk Monitoring and Adaptation**: Risk management for GenAI is not a one-time exercise. Strategies for mitigating associated risks must be ongoing to ensure emerging threats and legal challenges are addressed appropriately and efficiently.



Ethical Considerations in GenAI Adoption

As organizations increasingly rely on AI-driven systems for decision-making, content generation, and data analysis, ensuring ethical use of these technologies becomes more and more important. Legal leaders must establish an AI adoption framework that addresses:

- Ethical concerns, such as transparency, fairness, accountability
- The impact of AI systems on individuals and society
- Responsible AI use across the enterprise
- Potential ethical dilemmas
- Ways to promote trust and integrity in AI-driven processes

Transparency and Explainability

AI models—particularly complex machine learning algorithms—often function as "black boxes," making it difficult to understand how they reach specific outcomes.

- **Explainability of AI Outputs:** AI-generated outputs, particularly those influencing critical business decisions, must be explainable and justifiable to regulators, employees, customers, and other stakeholders. This means organizations must be able to clearly articulate how the AI system works, including its underlying data, the decision-making processes it follows, and the factors it considers when generating outputs. This is especially important when organizations rely on AI systems to make or contribute to decisions that affect individuals' rights, such as in hiring, credit scoring, or law enforcement activities.
- **Auditing AI for Bias:** Even if AI outputs cannot always be fully explained due to the complexity of the underlying models, conducting regular audits, as discussed earlier, enhance transparency and guard against potential ethical violations.

Fairness and Non-Discrimination

AI systems, including GenAI, are only as unbiased as their training data. If the training data reflects biases, the AI system will default to perpetuating or even amplifying those biases in its outputs, leading to bad decisions and discriminatory outcomes.

- Avoiding Bias in AI Training Data: Datasets used to train GenAI models can be assessed and curated to ensure they don't reflect biased or unrepresentative societal patterns that can lead to biased AI behavior. Legal teams should work with data scientists to ensure that training datasets are diverse and representative of the populations and scenarios they are intended to serve.
- Preventing Discriminatory Outcomes: Even with diverse training data, AI systems can still produce unintended discriminatory outcomes. Continual monitoring and auditing of AI-generated decisions can help detect and correct any instances of unfair treatment, which would otherwise expose the organization to lawsuits and/or regulatory penalties.

Accountability and Responsibility

GenAI tools can generate outcomes that impact individuals and business processes in significant ways, including while operating autonomously and without human intervention. This raises the question of where the responsibility lies when an AI system makes a mistake or produces harmful outputs

- Human Oversight: Striking a balance between AI autonomy and human oversight is a necessary and critical undertaking. While AI systems can improve efficiency and decision-making accuracy, organizations must maintain human oversight to ensure accountability. This includes assigning clear responsibility for AI decisions within the organization and establishing protocols for addressing errors or unintended consequences of AI decisions. Two common types are human oversight are:
  - **Humans in the loop (HITL)**, meaning human intervention is required in the AI workflow, or an action is required and a human can start or stop that action
  - **Humans on the loop (HOTL)**, which means a human has the ability to interact with the system or the obligation to provide feedback to the system to ensure continuous learning

- **Ethical Use of AI Tools**: Clear guidelines must define the ethical use of AI systems within the organization. These guidelines should address:
  - When and how human oversight is required
  - What types of decisions AI systems are authorized to make
  - Steps to take if an AI system produces an ethically questionable or harmful outcome

Social Impact and Responsibility

Organizations must consider the social impact of using AI systems in their business operations. For instance, using GenAI tools to generate news articles or influence public opinion raises questions about the ethical obligations organizations have in shaping social narratives.

- **AI and Misinformation**: GenAI has tremendous and proven potential to produce and disseminate very convincing misinformation, and organizations must be mindful of the risks associated with using AI for creating public-facing content. GenAI tools must be used responsibly and safeguards must be put in place to prevent dissemination of false or misleading information.
- **Corporate Social Responsibility (CSR) and AI**: Senior leadership across the organization must agree on how their organization’s use of GenAI aligns with broader CSR goals. This includes evaluating whether AI systems are being used in a manner that promotes social good, respects human rights, and contributes to sustainable business practices. Aligning AI use with CSR objectives can enhance the organization's reputation and ensure it meets its ethical obligations to society.

Ethical Dilemmas in Autonomous AI Decision-Making

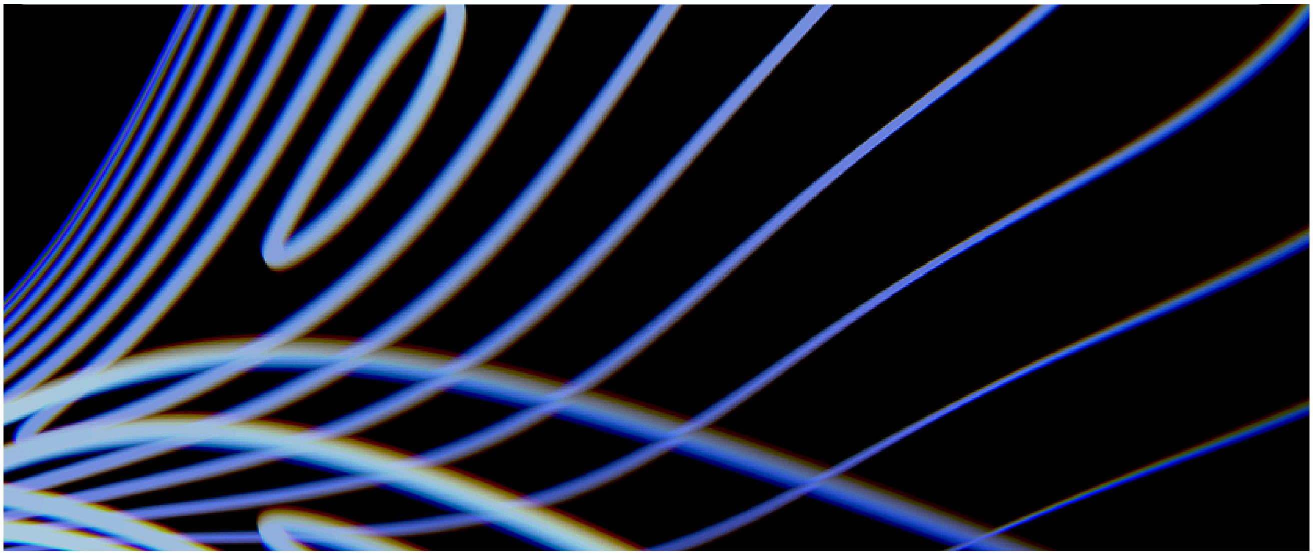
As GenAI systems become more autonomous, they will increasingly encounter ethical dilemmas requiring moral judgment. For example, autonomous vehicles powered by AI must make real-time decisions in complex situations in which human lives may be at stake. Similarly, AI systems in healthcare or finance may face scenarios with unavoidable ethical trade-offs, such as decisions involving admission to clinical trials or access to newly approved medications or procedures.

- Establishing Ethical Guidelines for AI: External ethical AI experts can assist in establishing clear guidelines for addressing how AI systems should prioritize competing ethical values, such as safety, fairness, and efficiency. While it may not be possible to pre-program every ethical decision an AI system will face or create, having a clear framework in place can guide AI developers and operators.
- Ethical AI Audits and Accountability: A cadence of regular ethical AI audits to assess whether AI systems are adhering to established guidelines can help identify potential ethical issues before they escalate and provide a mechanism for holding AI systems—and their developers—accountable for their decisions.

Best Practices

The adoption of GenAI tools is accompanied by a full suite of complexities—technical, operational, security-related, and legal. As gatekeepers of corporate integrity, legal and compliance leaders play a central role in shaping how GenAI is adopted and managed across the enterprise. By addressing these challenges head-on and working collaboratively, they can safeguard their organizations while enabling innovation, ensuring that the adoption of GenAI contributes to both business growth and long-term sustainability.

The following best practices roadmap for GCs, CLOs, and CCOs outlines collaborative management of GenAI tool deployment while mitigating legal and ethical risks.



Implement Rigorous Risk Management Processes

A thorough risk management framework involves identifying, assessing, and mitigating risks related to AI operations, including security vulnerabilities, IP concerns, risk exposure, and regulatory compliance.

General Counsel	Focus on the legal implications of risk management, such as liability exposure and contractual risk allocation, while ensuring corporate insurance policies and indemnities adequately cover AI-related risks
Chief Legal Officer	Align the enterprise's risk management strategies with external legal standards and regulations, and work with external counsel as necessary to benchmark organizational risk practices against peers
Chief Compliance Officer	Develop protocols for ongoing AI risk audits to ensure potential vulnerabilities are continually assessed, and ensure ongoing compliance by monitoring adherence to internal policies and regulatory requirements

Prioritize Data Privacy and Security

The vast datasets relied on by GenAI systems pose significant privacy and security risks, if not properly managed. Organizations must prioritize data protection at every stage of the GenAI lifecycle—from data collection and storage to processing and dissemination of generated outputs.

General Counsel	Ensure data usage complies with applicable privacy laws and that contracts with third-party AI providers include adequate data protection clauses
Chief Legal Officer	Ensure organizational data protection policies are continually updated to reflect changes in the legal landscape, and that they focus on maintaining legal defensibility in cases of data breaches or misuse
Chief Compliance Officer	Enforce stringent data handling protocols, including encryption, access controls, and data retention policies; oversee compliance with internal and external privacy regulations; and ensure AI systems adhere to data minimization principles

Develop Clear Ethical Guidelines for AI Use

Ethical guidelines for GenAI use must be simple and straightforward, aligned with the organization's core values, and integrated into its AI governance framework.

General Counsel	Lead in drafting and reviewing the ethical AI use policies, ensuring they mitigate legal risks and promote fairness, transparency, and accountability while providing advice on emerging ethical dilemmas in AI, such as biases and automation impacts
Chief Legal Officer	Ensure the organization's ethical guidelines align with industry best practices and global regulatory frameworks, and update internal policies to remain current
Chief Compliance Officer	Implement ethical guidelines, including internal training programs and audit processes, and establish reporting mechanisms for employees to raise concerns about unethical AI behavior

Promote Continuous Education

Staying informed about developments in AI law, governance, and ethics enables senior legal leadership to proactively adapt to changes and ensure their organizations remain compliant.

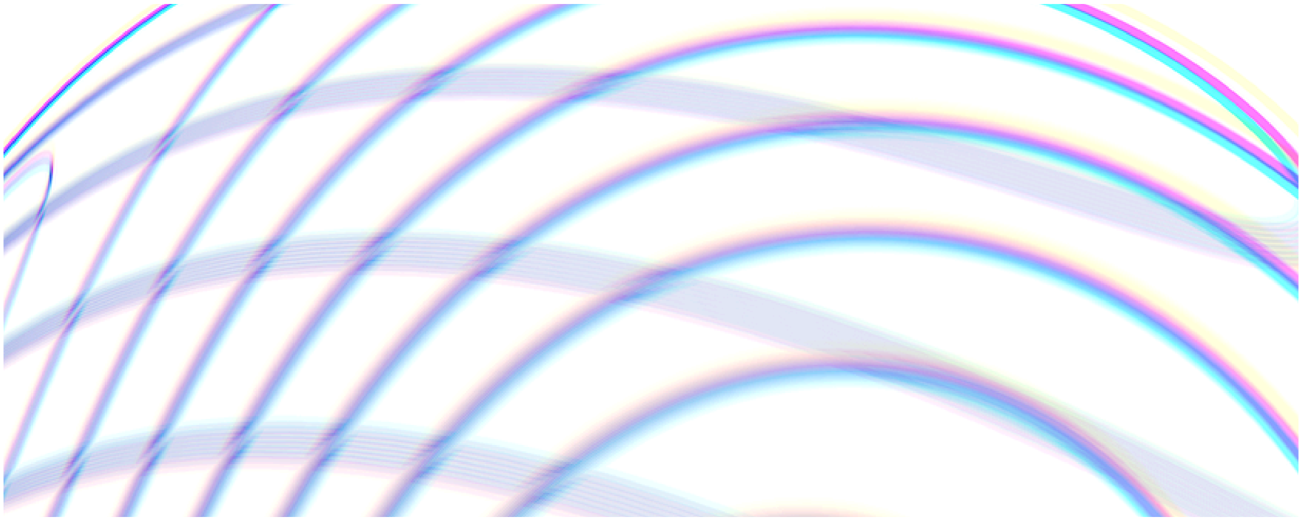
General Counsel	Collaborate with external AI law experts and internal stakeholders to provide regular updates on AI-related legal developments and share insights from AI litigation cases, regulatory enforcement actions, and global AI policy trends
Chief Legal Officer	Develop educational resources about AI governance that provide guidance on integrating AI technologies while maintaining legal compliance, and that offer practical solutions for issues that might arise
Chief Compliance Officer	Create compliance training programs that address GenAI-specific risks to ensure that employees across the enterprise are aware of relevant legal and ethical considerations when using AI tools

Conclusion

Legal leadership teams must carefully navigate evolving regulatory landscapes, address liability concerns, and establish robust ethical guidelines to govern AI use. At the same time, they must ensure AI systems operate in alignment with both internal policies and external standards. These efforts are critical for organizations to realize the full potential of GenAI while safely avoiding legal and ethical pitfalls.

> Over time, AI governance will no longer be a standalone concern—it will be an essential part of every policy and decision-making process.

However, this is just the beginning. Over time, AI governance will no longer be a standalone concern—it will be an essential part of every policy and decision-making process. Legal leaders must not approach AI governance as a one-time task, but as the first step in an ongoing journey toward embedding AI-native thinking into broader organizational governance frameworks. By taking proactive measures now, they will help shape a future in which AI is seamlessly integrated into all aspects of policy, ensuring long-term regulatory compliance, ethical responsibility, and strategic advantage. Those who act today will be best positioned to navigate the increasingly AI-driven world of tomorrow.



CalypsoAI is shaping a future in which AI and security coalesce to transform how businesses operate, while contributing to a better world. Founded in Silicon Valley in 2018 by top minds in the fields of data science, machine learning, and defense, the company has secured investments from Lightspeed Venture Partners, Lockheed Martin Ventures, Paladin Capital Group, Hakluyt Capital and Expeditions Fund, and strategic angels, including Auren Hoffman and Anne and Susan Wojcicki.

To learn more, visit the website or follow CalypsoAI on Twitter and LinkedIn.

CALYPSOAI