Module 10: AI Governance: Creating Trust, Compliance, and Data Privacy

Lesson 1: AI Regulations and Policy

Part I: Regulation in AI

November 30, 2022, was when the world saw ChatGPT 3.5 hit the scene, and since then, generative AI has been in use EVERYWHERE.

This has businesses, individuals, and governments nervous about how such a powerful tool could result in unintended and unknown negative consequences.

Predictably, the powers that be have gained a lot of interest in the governance and regulation of AI, and we expect this interest to be the catalyst for the creation of **regulations** to manage and advise **responsible and ethical AI adoption**.

Because of this interest in governance and regulation, it is important for CAIOs to have a solid understanding of the regulatory landscape to **ensure their AI implementations are fully compliant**.

Note: *Since this is an evolving topic, we will be doing regular interviews with AI Compliance experts that will be made available in the course, as well as updating the Slack workspace with the latest news on the subject.*

Data Privacy and Ethics

Data privacy refers to the **protection and responsible use of personal data** and sensitive information.

In the most compliant environments, it involves giving individuals control over how their personal data is collected, processed, shared, and utilized.

To achieve the powerful results that a user gets from AI, the systems have to utilize vast amounts of data for training and powering algorithms, and as a result, this creates **significant privacy implications** that a CAIO should be aware of and address.

Some **key principles of data privacy** that you should consider as a CAIO include:

- **Consent**. Personal data should only be used with the knowledge and explicit consent of the individuals concerned.
- **Transparency**. Organizations should be transparent about how they collect and use personal data.
- **Data minimization**. Only collect and retain the minimum amount of personal data needed for specified purposes.
- **Purpose limitation**. Personal data should only be used for the purposes stated at the time of collection.
- **Access and correction**. Individuals should be able to access their data and make corrections if inaccurate.
- **Security**. Protect personal data with reasonable security safeguards against risks like loss, unauthorized access, destruction, etc.
- **Accountability**. Organizations that control or process personal data should be accountable for complying with the above principles.

When it comes to **generative AI**, you should be working with your clients on upholding data privacy to ensure personal data is protected and leveraged **ethically and legally** by generative models.

Now let’s address the ethical considerations that will undoubtedly come up in discussion with a savvy client or stakeholder in your company.

Ethics in using AI refers to the **responsible and morally sound application** of artificial intelligence technologies in a business setting.

To effectively address the concerns around ethical AI usage, you have to consider the **potential impacts of AI** to ensure that AI initiatives align with ethical principles, legal regulations, and social norms.

In the context of our CAIO certification course, **ethics plays a crucial role** because it guides CAIOs in making decisions that not only drive business success but also prioritize the well-being of the company, its employees, its customers, and the broader community.

To help you better understand what falls under the scope of “**Ethical AI**,” let’s look at some key considerations.

Transparency

Transparency in AI means being clear and open about how AI systems operate, the data they use, and the algorithms they employ. It involves providing understandable explanations to users and stakeholders about how AI makes decisions and predictions.

Transparent AI fosters trust among users and enables them to have confidence in the technology's outcomes. This is especially crucial when AI is used in critical areas like **healthcare, finance, or criminal justice**, where the decisions made by AI can have significant impacts on individuals' lives.

Fairness and Bias

AI systems are only as unbiased as the data they are trained on. Ensuring fairness in AI means actively seeking to **identify and mitigate biases** in data and algorithms to avoid discrimination against individuals or groups. It's essential to ensure that AI applications do not perpetuate or amplify existing stereotypes, profiles, or misleading information.

CAIOs must **prioritize fairness** in AI development and continuously monitor and evaluate AI systems for potential biases.

Privacy and Data Protection

AI often relies on large volumes of data to train and function effectively. Protecting individuals' privacy and their data rights is critical when collecting, storing, and processing data for AI purposes.

CAIOs must help their clients or company **comply with relevant data protection laws and regulations** and ensure that data handling practices are ethical and secure. Implementing strong data protection measures and **obtaining informed consent from users** is fundamental to maintaining individuals' trust and confidence in AI systems.

Accountability

Accountability in AI refers to taking responsibility for the actions and consequences of AI systems.

CAIOs must **consider the potential risks and impacts of AI applications** and be prepared to address any unintended negative consequences. This includes establishing mechanisms for auditing and monitoring AI systems and having clear protocols for responding to AI-related incidents or errors.

Explainability

Explainable AI refers to the ability of AI systems to **provide understandable explanations** for their decisions and predictions. This is particularly important in critical applications where AI's decision-making process needs to be transparent and interpretable.

CAIOs must ensure that AI models are explainable, especially in sectors like healthcare, where medical professionals and patients need to **understand the rationale** behind AI-driven diagnoses and treatment recommendations.

Informed Consent

Informed consent through a company's terms and conditions and similar policies is essential when AI systems collect and use personal data for various purposes.

CAIOs must ensure that **individuals are aware of how their data will be used** and provide them with the opportunity to give informed consent. Transparent communication about data usage and user rights is vital to establishing trust and ensuring that individuals have control over their data.

When you make sure you've got this covered, it shows a level of **responsibility and seriousness** about your contribution as a CAIO. Particularly in entrepreneur-led companies where speed is an everyday expectation or in a dysfunctional SMB where corners are cut, your leadership on this topic will save the day (remember AlphaTech?)

Here's a bonus tip: *if you want to circulate in business with "A-players" (clients, employers, peers, vendors, etc), you'll find that they respect people who pay attention to risk.*

AI Regulations

AI regulation is still emerging and a complex issue that varies by country and sector. The intention of the discussion on this topic isn't to make you a legal expert but to educate you about the need for **providing guardrails and a sense of safety** for users and developers.

In general, AI regulation refers to the set of **rules, guidelines, and legal frameworks** that govern the development, deployment, and use of artificial intelligence technologies.

These regulations are designed to address ethical concerns, protect user privacy, ensure fairness, and mitigate potential risks associated with AI applications.

There are three main approaches to AI regulation:

1. **Promoting** AI development and innovation
2. **Protecting** human rights and values
3. **Preventing** AI harms and risks

Below are some examples of **current AI regulation** (see Additional Resources for more detail).

In the European Union:

The General Data Protection Regulation (GDPR) has clauses that impact AI, such as the right to explanation, data protection, and consent. If you have been involved in digital marketing, you may already be familiar with some of the policies outlined in the GDPR.

The proposed AI Act assigns AI usage to three risk categories: unacceptable, high-risk, and low-risk.

In the United States:

The AI in Government Act of 2020 codifies the GSA AI Center of Excellence and provides guidance for agency use of AI.

The Algorithmic Accountability Act of 2019 requires companies to assess their automated decision systems for bias, discrimination, and privacy.

Upcoming Regulation

Some examples of **AI regulation that are being discussed**, and expected to pass into law in the near future, are:

- The US's National Artificial Intelligence Initiative Act of 2020, which aims to establish a national AI strategy and coordinate federal AI research and development.

- The UK's Online Safety Bill, which seeks to hold online platforms accountable for harmful content generated by AI.

- The OECD's Principles on Artificial Intelligence, which provides a set of ethical and human-centered guidelines for AI policy making.

Again, although you don't need to be a policy wonk to be an effective CAIO, we advise you to **be familiar with the frameworks these policies expect** to be followed by companies seeking to deploy AI into their business operations.

Potential Impact of Policy Regulation

Impact on Business Operations

AI regulation can impact business operations by **introducing compliance requirements** that businesses must adhere to when implementing AI technologies.

Companies may need to invest in internal audits, documentation, and processes to ensure that their AI applications comply with relevant regulations.

More advanced AI systems may also require additional testing and validation to meet regulatory standards, which could affect the pace of implementation and operational efficiency.

Impact on Marketing

AI regulation can influence marketing practices by imposing restrictions on how businesses use AI for advertising, targeting, and customer profiling.

Companies must ensure that their AI-driven marketing strategies comply with data privacy laws and do not infringe on user rights.

This may require transparent communication with customers about data usage and the use of AI in personalized marketing campaigns.

Impact on Sales Processes

In sales, AI regulation may impact the use of AI-powered chatbots, virtual assistants, and automated customer interactions.

Businesses must ensure that AI systems provide accurate and reliable information to customers and do not engage in deceptive practices. Compliance with consumer protection laws and regulations is still expected and continues to allow a company to maintain trust and avoid potential legal issues.

Impact on Data Collection and Storage

AI regulation directly affects **how businesses collect and store data** used to train AI models.

Companies must obtain explicit consent from individuals when using their data to train LLMs or additional tools being used by the company.

Additionally, companies will still be expected to **implement robust data security measures** to protect sensitive information and prevent data breaches. Compliance with data protection regulations should already be in place in a business, as this is not a new requirement.

As a CAIO, it is essential to **stay updated on AI regulations in your region and industry** to ensure that your organization's AI initiatives align with legal requirements and ethical standards. By staying plugged into the ChiefAIOfficer.com community through **our Slack channel**, you'll be made aware of the relevant, most up-to-date information related to the regulation of AI usage in business operations.

Ensuring Compliance of Data Privacy, Ethics, and Regulations in AI

In any company you work with, you'll be expected to **help keep your company or clients out of trouble** when it comes to compliance and the topics we've covered - data privacy, ethics, and regulations related to using AI in your business.

Below are **specific examples of how you can ensure compliance** in each of these areas.

Data Privacy Compliance

Implementing Privacy by Design

Ensure that privacy considerations are integrated into the design and development of AI systems from the outset. This involves incorporating data protection measures into the architecture of AI applications.

Obtaining Explicit Consent

Obtain explicit and informed consent from individuals before collecting and processing their data for AI applications. Keep detailed records of consent to demonstrate compliance.

Anonymization and Pseudonymization

Use anonymization or pseudonymization techniques to protect individual identities and comply with data privacy regulations.

Secure Data Storage

Ensure that the data used for training AI models is securely stored and accessible only to authorized personnel. Implement encryption and access controls to prevent unauthorized data access.

Ethical AI Use

Bias Mitigation

Take proactive steps to identify and address biases in AI algorithms that may result in discriminatory outcomes. Regularly audit AI models to ensure fairness and inclusivity.

Transparency and Explainability

Make AI decisions transparent and explainable to users and stakeholders. Ensure that individuals understand how AI is being used and can challenge decisions if needed.

Human Oversight

Incorporate human oversight and intervention in critical AI decision-making processes, especially in areas with significant social impact or ethical considerations.

Regulatory Compliance

Stay Abreast of Legal Changes

Keep yourself updated on the evolving AI regulations and ensure that your AI initiatives comply with the latest laws and guidelines.

Conduct Compliance Audits

Regularly conduct internal audits to assess the compliance of AI systems with relevant regulations and address any identified gaps or issues promptly.

Document Compliance Measures

Maintain comprehensive documentation of your AI compliance efforts, including data handling practices, privacy impact assessments, and ethical guidelines.

Examples of Compliance Implementation

Here are 3 examples of implementing compliance in various types of fictional businesses.

Scenario: ***A digital marketing agency that manages the online advertising for their clients***

Data Privacy Compliance: Obtain explicit consent from clients and their customers to collect and use their data for advertising purposes. Implement data encryption and secure storage for client and customer information. Comply with relevant data protection regulations such as GDPR or CCPA.

Ethical AI Use: Regularly audit the AI advertising system to ensure fairness and avoid discriminatory or misleading ads based on gender, race, or other sensitive attributes. Ensure transparency and accountability for the AI decisions and outcomes.

Regulatory Compliance: Monitor and comply with relevant advertising standards and laws in the jurisdictions where the agency and its clients operate. Avoid violating intellectual property rights, consumer rights, or competition laws.

Scenario: ***A business consultancy that advises companies on their AI deployment***

Data Privacy Compliance: Obtain explicit consent from clients and their customers to collect and use their data for AI consultancy purposes. Implement data encryption and secure storage for client and customer information. Comply with relevant data protection regulations such as GDPR or CCPA.

Ethical AI Use: Regularly audit the AI consultancy system to ensure fairness and avoid biased or harmful recommendations based on gender, race, or other sensitive attributes. Ensure transparency and accountability for the AI decisions and outcomes. Follow ethical principles and guidelines for AI development and use.

Regulatory Compliance: Monitor and comply with relevant AI regulations and standards in the jurisdictions where the consultancy and its clients operate. Avoid violating intellectual property rights, professional ethics, or contractual obligations.

Scenario: ***A real estate investing business focused on single-family residences***

Data Privacy Compliance: Obtain explicit consent from property owners, tenants, and buyers to collect and use their data for real estate investing purposes. Implement data encryption and secure storage for property and personal information. Comply with relevant data protection regulations such as GDPR or CCPA.

Ethical AI Use: Regularly audit the AI investing system to ensure fairness and avoid discriminatory or predatory practices based on gender, race, or other sensitive attributes. Ensure transparency and accountability for the AI decisions and outcomes. Follow ethical principles and guidelines for AI development and use.

Regulatory Compliance: Monitor and comply with relevant real estate laws and regulations in the jurisdictions where the business operates. Avoid violating property rights, tenant rights, or consumer rights.

As you can imagine, **proactively addressing data privacy, ethics, and regulations** related to AI is vital to **maintaining trust** with customers, avoiding legal issues, and fostering ethical AI use in a business.

We work with our clients to create a regular tempo (at least 1x per year, but more frequently is ideal) of **reviewing and updating their compliance measures** to align with evolving regulations and industry best practices.

Best Practices for Ensuring Regulatory Compliance in AI Systems

- Perform privacy impact and algorithmic bias assessments before deployment using tools like EqualAI's free Algorithmic Impact Assessment
- Develop responsible data management procedures in line with regulations that are applicable to the industry or geographic area the business operates.
- Implement oversight protocols and access controls aligned with industry standards.
- Continuously monitor systems for regulatory issues or non-compliance.
- Maintain explainability of model decisions for auditing.
- Update policies and protocols to reflect regulatory changes.
- Proactively engage regulators to demonstrate commitment to compliance.

This is one area where our catalog of preferred vendors comes in handy, as there are firms that specialize in helping companies stay compliant in their AI usage within their businesses.

Key Takeaways

- Obtain informed consent from individuals before collecting data to train AI systems. Be transparent about how data will be used.
- Regularly audit AI systems for bias, fairness, and discrimination. Address any issues promptly and mitigate algorithmic harms.
- Implement robust cybersecurity measures to protect sensitive data used in AI applications. Follow best practices for encryption and access controls.
- Stay current on evolving regulations in your jurisdiction and industry. Conduct regular compliance audits to avoid regulatory infractions.
- Maintain detailed documentation of your data practices, model explanations, and compliance programs. This supports transparency and accountability.
- Engage with stakeholders, including customers and regulators, to build trust in your AI initiatives and demonstrate commitment to ethical practices.

As CAIOs, we have an obligation to **help our companies deploy AI responsibly and ethically** while driving business success.

The framework provided in this training will equip you to fulfill this role.

You’re encouraged to use the resources shared and apply the methodologies covered to ensure your AI projects uphold the required standards of privacy, ethics, and regulatory compliance.

Part II: Generative AI Use Policies

Why Companies Need a Generative AI Use Policy

Although there is a lot of demand and buzz around leveraging AI in business, there isn’t yet a universal framework on HOW companies should be addressing issues like acceptable use, privacy, data protection, and other topics related to **creating guardrails for AI use**.

As more and more companies adopt generative AI technologies like ChatGPT, DALL-E, and others, it has become imperative that they establish policies governing the use of these powerful tools.

But don’t be surprised if you find yourself working with companies that have zero guidance for their employees on using AI in the enterprise. The latest research points to about 60%+ of companies saying someone in their business is using Gen AI in a business function. But only about 20% of all companies claim to have any usage guidelines in place!

At a minimum, your company or clients’ companies should develop a **Generative AI Use Policy (GAIUP)** that can provide those guardrails and mitigate risks.

A Generative AI Usage Policy is a **documented set of guidelines** that outlines how employees and contractors **may or may not use** generative AI systems, tools, and applications on behalf of an organization.

It establishes the company’s rules, protocols, and boundaries for appropriate and ethical generative AI usage aligned with the company's values and legal obligations.

Here are examples of laws/regulations a Generative AI Usage Policy helps companies comply with:

- **Copyright law -** Avoids plagiarism or illegal use of copyrighted content.
- **Data privacy regulations like GDPR -** Ensures proper data handling as per regulations.
- **Equal employment laws -** Prevents biased/discriminatory content harmful to protected groups.

Why Companies Need a GAIUP

Ensures Legal Compliance

Generative AI may create content that violates copyrights, trademarks, data privacy regulations like GDPR, equal employment laws, etc. A policy helps ensure your company is in legal compliance.

Avoids Reputational Damage

Unguided generative AI could produce offensive, biased, or inappropriate content that could damage a brand's reputation if released publicly. A policy helps prevent this.

Promotes Ethical AI Use

A policy establishes boundaries for using generative AI ethically, such as prohibiting the creation of illegal, unethical, dangerous, or harmful content.

Reduces Business Disruption

Clear guidelines minimize generative AI misuse that disrupts workflows and productivity or harms business operations.

Provides Employee Guidance

A policy gives employees unambiguous guidelines for appropriate generative AI use in their roles. It helps prevent AI misuse out of ignorance.

Sets Data Security Protocols

Policies can specify how sensitive data can/cannot be used with generative models to improve data security.

Establishes Oversight and Controls

A policy puts in place oversight procedures, controls, and accountability measures governing generative AI use.

Enables Risk Assessment

Documented policies allow organizations to better assess risks associated with generative AI use cases.

A Generative AI Usage Policy can also help to:

- Protect the company's intellectual property and trade secrets from being lost or disclosed by generative AI.
- Ensure transparency and accountability for the use of generative AI and avoid confusion or deception with human-generated content.
- Establish trust and confidence among customers, partners, regulators, and other stakeholders in the company's use of generative AI.
- Enhance the company's reputation and brand value as a responsible and innovative user of generative AI.

Let’s take a look at an **example scenario** of **what could happen** when a company just jumps in with Generative AI **when no use policy is in place**:

> *It was a Monday morning in the gleaming offices of AlphaTech, one of Silicon Valley's hottest software startups.*
>
> *As employees sipped their cold brew coffees and hammered away at keyboards, they were blissfully unaware of the legal firestorm that was about to engulf their company.*

Mark Davis, AlphaTech's CEO, was definitely feeling a case of FOMO when it came to using AI in the company. Ignoring the concerns of his legal counsel, he had greenlit integrating powerful models like ChatGPT across AlphaTech's operations without any policies to govern their use.

With the enthusiastic encouragement of their fearless leader, his developers deployed the AI widely — generating content, coding software, and chatting with customers.

At first, everyone was praising Mark's dedication to staying ahead of the curve on AI.

Until that is, a cease-and-desist letter from a major publishing house landed on Mark's desk, threatening legal action over copyrighted material in AlphaTech's blog posts. As Mark investigated further, his face paled. Much of their popular content was written by AI, drawing text from across the web with no regard for copyright law.

But it was too late to contain the damage.

Negative publicity swirled as customers shared experiences of racist comments from AlphaTech chatbots.

Recruiters struggled to hire new employees amid rumors of unethical practices.

Software output suffered as engineers scrambled to redo work produced by AI.

As Mark sat in his office, head in hands, his general counsel blasted him with, "I told you so." He had allowed his obsession with generative AI to cloud his judgment. In his recklessness, he had exposed the company to massive legal liability and tarnished its reputation, resulting in a significant negative reaction from Wall Street and his investors.

As lawsuits mounted and an SEC investigation loomed, he regretted not having governance policies to oversee AI use before unleashing it recklessly across AlphaTech's systems. He had compromised the company's future in his haste. Now the roosters had come home to roost …

Yes, the story above is a bit dramatic, but not far from the truth of what is currently happening to some companies who didn't have the foresight to consider creating and adopting a Generative AI Use Policy.

Now that you have some context on how important a GAIUP is for a company let's talk about some of the **steps involved in developing a Generative AI Usage Policy**.

Here is an **expanded 10-step walkthrough for CAIOs to use** when guiding a company through generating their Generative AI Usage Policy (GAIUP):

Step 1. Align the GAIUP with the AI Business Strategy

a. Review the company's **AI Business Strategy** that was developed during the Ignition phase, and determine the scope of the Generative AI Usage policy, including which departments or individuals it applies to, breaking out the key functions — sales, marketing, product development, customer service, etc.

b. Analyze **how generative AI could help advance each strategy and objective**. What use cases make sense? What use cases should be explicitly barred from using Generative AI?

c. Ensure the GAIUP provides **clear guidelines** tailored to the intended strategic and tactical uses of generative AI that resulted from the answers to your analysis above.

Step 2. Conduct a Risk Assessment

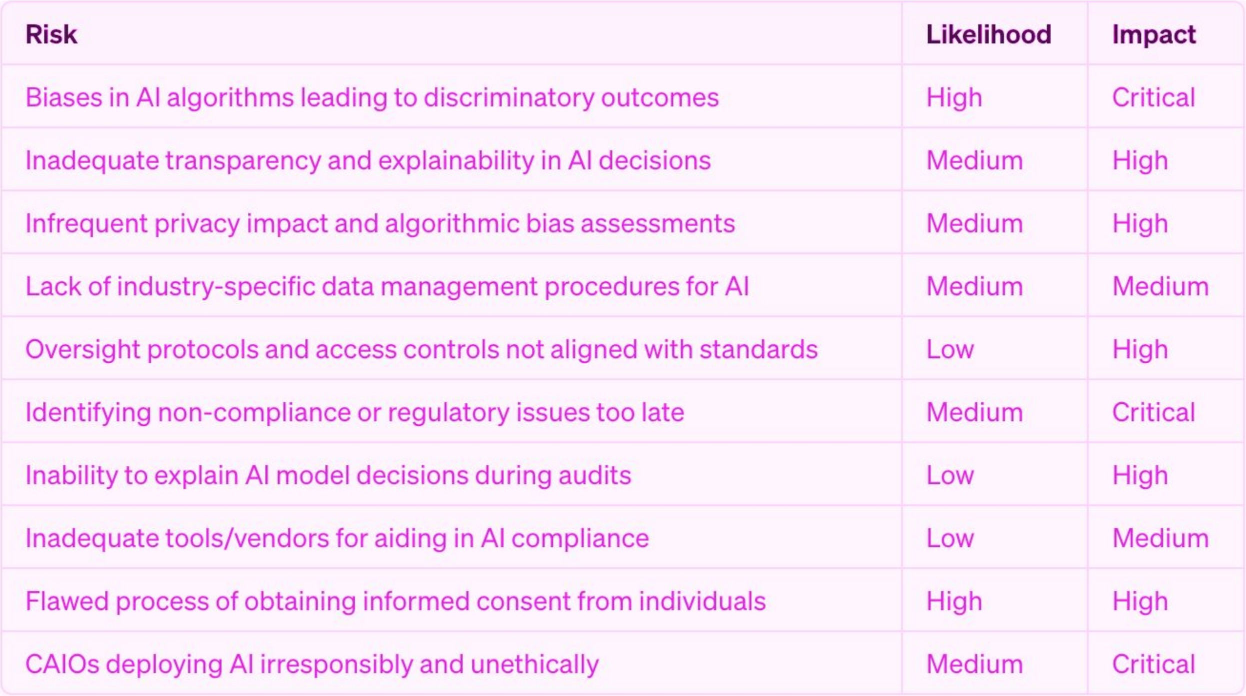
a. Identify **any risks** associated with different generative AI use cases identified in Step 1, such as potential legal, ethical, data privacy, cybersecurity, or harmful content creation risks. Some example risks by department include:

- Marketing: Generative AI could create harmful/biased content that damages the brand's image.
- Sales: AI conversations with prospects could violate regulations or company values.

- Product: AI-generated content/code could lack explainability or introduce dangerous flaws.
- Customer Service: AI chatbot conversations could breach customer privacy.
- HR: AI tools could make biased hiring/promotion decisions violating EEO laws.

b. Evaluate the **likelihood and potential impact** of each identified risk to classify them into high, medium, and low priority. The easiest way is to plot risks on a matrix using these two factors to prioritize what to address in the GAIUP:

- Likelihood: Probability of risk occurring from low, medium, high
- Impact: Level of potential damage if risk occurs from low, medium, critical



Risk	Likelihood	Impact
Biases in AI algorithms leading to discriminatory outcomes	High	Critical
Inadequate transparency and explainability in AI decisions	Medium	High
Infrequent privacy impact and algorithmic bias assessments	Medium	High
Lack of industry-specific data management procedures for AI	Medium	Medium
Oversight protocols and access controls not aligned with standards	Low	High
Identifying non-compliance or regulatory issues too late	Medium	Critical
Inability to explain AI model decisions during audits	Low	High
Inadequate tools/vendors for aiding in AI compliance	Low	Medium
Flawed process of obtaining informed consent from individuals	High	High
CAIOs deploying AI irresponsibly and unethically	Medium	Critical

Once you have documented these key risks, determine mitigation strategies which will inform the policy principles.

Step 3. Review Existing Policies

a. Gather all existing organizational policies related to ethics, acceptable use, data privacy, security etc.

b. Identify relevant elements to incorporate into the GAIUP and any gaps that need to be addressed.

c. Calibrate the GAIUP language and provisions with the existing organizational policies that are already in place.

Step 4. Consult Stakeholders

a. Identify key internal stakeholders, such as legal, IT, cybersecurity, HR, executives etc.

b. Schedule Interviews with those stakeholders so you can better understand their concerns, requirements, and expectations regarding the GAIUP.

Typical stakeholder interview questions include:

- What concerns do you have regarding generative AI use?
- What risks should the policy address in your domain?
- What requirements/expectations do you have for ethical AI use?
- What oversight measures would you want established?
- What loopholes could the policy create?

c. Incorporate the information you gathered in the interviews to cover areas that were discovered in your research.

Step 5. Draft Initial Policy

a. Outline **core principles and statements** on topics such as ethical AI, legal compliance, data privacy, and security based on research and the stakeholder interviews. To assist with this, we have provided a **template GAIUP** in the Additional Resources section of this module that you can use as your foundation

b. Specify **clearly acceptable and prohibited uses** of generative AI based on risk assessment and use cases.

c. Define **processes** for oversight, monitoring, reporting violations, and non-compliance consequences.

Typical oversight and compliance processes would include:

- Random audits of AI-generated content
- An oversight committee made up of stakeholders
- Anonymous employee reporting channel
- Required acknowledgment of policy terms
- Disciplinary measures like warnings, suspensions, or termination

Step 6. Get Leadership Approval

a. Present draft GAIUP to executive leadership and legal counsel for review.

b. Incorporate leadership feedback into an updated draft.

c. Obtain leadership sign-off on updated draft before company-wide release.

Step 7. Refine and Finalize

a. Circulate your refined draft to key stakeholders for a final round of feedback.

b. Make any further adjustments and edits based on review.

c. Finalize and publish the official GAIUP.

Step 8. Communicate and Train

a. Announce the new GAIUP through all-hands meeting, email, intranet posting, or the most suitable distribution channel for the company.

b. Conduct required training on the policy provisions for current employees. Make sure you provide time for a Q&A session or other feedback loop at the end of the training.

c. Include GAIUP training as part of onboarding for new hires so it becomes part of the understood company culture.

Step 9. Implement Oversight

a. Create **oversight procedures** for monitoring and auditing compliance, such as:
   - Usage audits
   - Monitoring of AI outputs
   - Assessing outputs for policy compliance
   - Documentation of oversight findings

b. Establish **internal reporting channels** for suspected violations.

c. Define consequences for policy non-compliance to include:
   - Retraining on the company's GAIUP policy
   - Temporary AI usage suspension
   - Formal warning/performance improvement plan
   - Removal of AI access
   - Termination for repeated/egregious violations

Step 10. Review and Iterate

a. Set a timeline for periodic GAIUP review and updates as needed. We've found that a **quarterly review is ideal**, but at a minimum, a biannual review is required to make sure the GAIUP is keeping up to date with AI's advancements and expanding use cases.

b. Adjust the policy as needed based on lessons learned, new use cases, and technologies.

c. Have your AI Council continue to focus on evolving the policy to support ethical generative AI usage.

At this point, it should be clear that a comprehensive, well-crafted Generative AI Use Policy is a **foundational governance document** for organizations adopting AI.

It aligns usage with ethics, values, and laws to build trust with your team internally, as well as with a company's customers and vendors.

We encourage you to **leverage the template GAIUP provided** and to keep the right voices in the company involved at each step.

And remember, policy creation is an **ongoing process** requiring continuous refinement. We suggest it be reviewed at each Quarterly meeting described in Module 2.

Now, with the guidelines established in this module, you are equipped to create a Generative AI Use Policy that **keeps your clients or company from making missteps** in their implementation, deployment, and usage of generative AI in their business operations.

Key Takeaways

- It is imperative for companies to establish a formal Generative AI Use Policy to govern the usage of AI systems like ChatGPT.
- Policies are crucial for a number of key reasons, including compliance, risk mitigation, and guidance for employees.
- Your GAIUP must be aligned with appropriate governmental policies.
- Deploying AI without governance is a high-risk endeavor. Policies establish oversight, controls, and accountability to prevent negative outcomes.
- Follow the 10-step process to create a robust Generative AI Use Policy tailored to your organization's needs.

Following this process will produce a custom policy upholding ethics, managing risk, and guiding employees in responsible AI utilization.