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

Lesson 1: Why Companies Need a GAIUP

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.

So, What Is a GAIUP, Exactly?
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.

Some of the top reasons why companies need such a policy include:

- **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 Alpha Tech'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.

Before we move into the training on how to create a GAIUP for your company or your clients, it might be helpful for you to watch the included video walkthrough of ChiefAIOfficer.com's GAIUP which you can find in the "Watch" section of this lesson in the members area.

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

- 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.

- 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?

- 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.

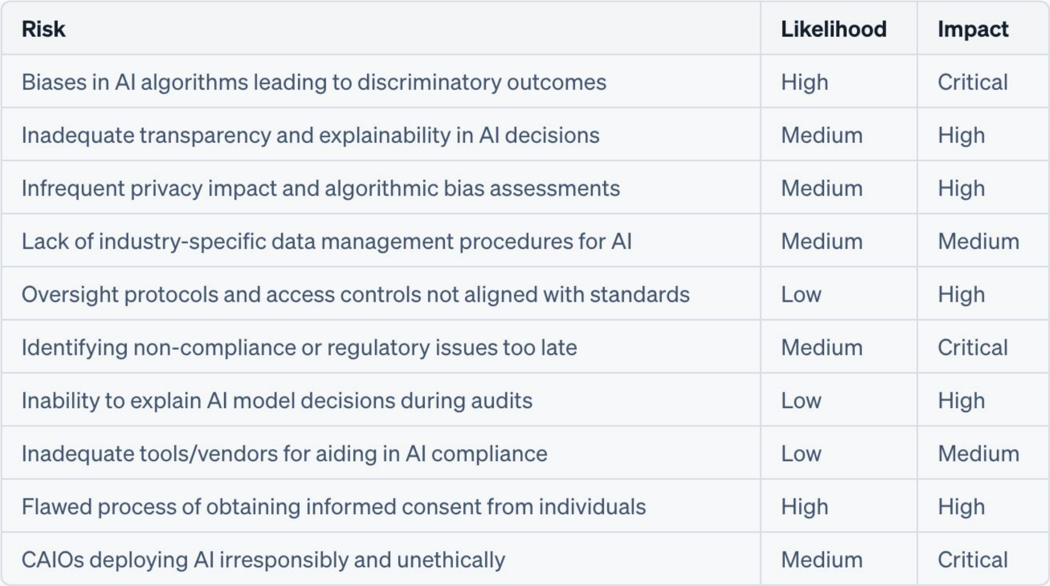
Step 2 - Conduct a Risk Assessment

Next, identify **any risks** associated with different generative AI use cases identified in Step 1 — potential legal, ethical, data privacy, cybersecurity, or harmful content creation risks, etc. 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.

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 the two factors to prioritize what to address in the GAIUP:

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

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

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

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

Step 4 - Consult Stakeholders

- Identify key internal stakeholders — legal, IT, cybersecurity, HR, executives etc.

- 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?

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

Step 5 - Draft Initial Policy

- Outline **core principles and statements** on ethical AI, legal compliance, data privacy, security, etc. 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.

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

- 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

- Present draft GAIUP to executive leadership and legal counsel for review.
- Incorporate leadership feedback into an updated draft.
- Obtain leadership sign-off on updated draft before company-wide release.

Step 7 - Refine and Finalize

- Circulate your refined draft to key stakeholders for a final round of feedback.
- Make any further adjustments and edits based on review.
- Finalize and publish the official GAIUP.

Step 8 - Communicate and Train

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

- 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.

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

Step 9 - Implement Oversight

- 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

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

- 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

- 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.

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

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

Conclusion

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.

I 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.

Summary

In this module, we explored the imperative for companies to establish a formal Generative AI Use Policy to govern the usage of AI systems like ChatGPT.

We discussed key reasons policies are crucial, including compliance, risk mitigation, guidance for employees, and more.

We provided a definition and examples of relevant laws the policy must align with.

Through a cautionary tale about AlphaTech's missteps in AI usage, we illustrated the reputational, legal, and ethical dangers of deploying AI without governance. Policies establish oversight, controls, and accountability to prevent outcomes like what happened to AlphaTech.

We then outlined a 10-step process to create a robust Generative AI Use Policy tailored to an organization's needs. This included:

1. Aligning with business strategy
2. Conducting a risk assessment
3. Reviewing existing policies
4. Consulting stakeholders
5. Drafting the policy based on a template
6. Gaining leadership approval
7. Refining and finalizing the policy
8. Communicating and training employees
9. Implementing oversight procedures
10. Reviewing regularly to update as needed

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