

# Leading Through the AI Revolution

A Strategic Blueprint for Managing  
Generative AI Risks and Opportunities



designDATA

# Executive Summary

Generative AI offers extraordinary potential, but without proactive management, it poses serious risks to data security and the integrity of business decisions. Data input by users containing trade secrets, personal information, or intellectual property may be exposed during AI model training, daily employee interactions with AI, or through security breaches. Inaccurate AI-generated outputs can jeopardize strategic initiatives, cause financial harm, and tarnish reputations. This paper lays out a roadmap to mitigate these risks and maximize the benefits of Generative AI, highlighting the cost benefits of action versus inaction and the return on investment (ROI) advantages of equipping employees with AI-powered assistants.



# Table Of Contents

- Executive Summary ..... 2
- Table Of Contents ..... 2
- Introduction ..... 3
- Core Challenges Overview ..... 3
- Mitigation Strategies for Generative AI Input Risk ..... 4
  - Checklist of Initial AI Steps for All Organizations ..... 4
- Mitigation Strategies for Generative AI Output Risk ..... 5
  - Strategies to Safeguard Public AI Outputs..... 6
  - Strategies to Enhance Accuracy and Security with Private AI Capabilities..... 6
- Choosing the Right AI Solution for Your Organization..... 8
  - Regular Security Audits and Compliance Checks ..... 9
  - Ethical and Legal Compliance ..... 9
- Building a Secure and Adaptive AI Ecosystem ..... 9
  - The Building Blocks for Success ..... 9
- Conclusion ..... 10



## Introduction

Generative AI is transforming how organizations operate, offering tools for unprecedented efficiency and innovation. However, that power demands careful assessment and management of risk. Unsecured data input into Generative AI tools can expose trade secrets, violate privacy, or trigger regulatory scrutiny. Also, inaccurate AI outputs can undermine strategic decisions and create operational setbacks.

These concerns reveal the need for proactive governance and policy frameworks. Without them, the risks of data breaches, compromised decision-making, and even regulatory non-compliance increase significantly. This white paper provides a roadmap for organizations to not only harness the power of Generative AI but to do so within strong governance frameworks ensuring both security and long-term success.

We examine core Generative AI vulnerabilities, how to safeguard input data, and ensure the reliability of outputs across government, tribal, associations/nonprofits, and corporate sectors. We explore a spectrum of mitigation strategies tailored for both public and private realms.

By bridging the gap between the expansive possibilities of Generative AI and the imperative of robust risk management, we guide leaders through a balanced path. This journey is not just about mitigating risks but about seizing opportunities to innovate and excel in a rapidly evolving digital landscape, with an eye on optimizing costs and enhancing ROI.

## Core Challenges Overview

In the rapidly evolving technological landscape, Generative AI emerges as a double-edged sword. It offers opportunities for innovation, but it also brings significant challenges that require vigilant management. The integrity of input data and the accuracy of outputs stand at the forefront of these challenges, underpinning trust and effectiveness of AI applications across sectors.

### Input Risks

Consider the case where an employee, with the best intentions, uses a public AI image generator to create visuals, inadvertently submitting confidential land usage plans. These proprietary plans, which could be considered trade secrets, are leaked, risking serious disruptions to crucial negotiations. This scenario underscores why organizations need to adopt robust data security practices by shielding sensitive input data from unauthorized access and potential misuse.

### Output Risks

Similarly, the accuracy of AI-generated outputs is critical. Imagine a government agency that receives skewed AI-generated population statistics, leading to misallocated funding and impacting service delivery to vulnerable and underserved communities. This example highlights the cascading consequences of output inaccuracies, including the spread of misinformation, erosion of public trust, and significant operational setbacks. To mitigate these risks, an organization might

employ strategies like human-in-the-loop oversight while continuously evaluating results to ensure outputs remain accurate and reliable.

Both scenarios underscore the vulnerabilities that arise when clear policies and governance are absent. Without guidelines for data handling, secure data sharing, and output verification, the risks of Generative AI outweigh its potential. Organizations need strong policies to prevent these examples and capitalize on AI's transformative power.

### Contextualizing the Challenges

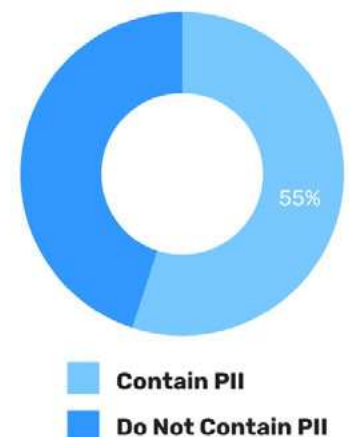
In environments where regulatory compliance is non-negotiable, the stakes are even higher. A breach involving critical data can trigger severe compliance violations under laws like Health Insurance Portability and Accountability Act (HIPAA) in the healthcare sector, or the EU's General Data Protection Regulation (GDPR) for organizations handling European citizens' data. Thus, understanding the intricate link between the core challenges posed by Generative AI and potential legal repercussions is vital. This insight informs the prioritization of mitigation strategies and emphasizes the need for a proactive approach to managing these risks.

## Mitigation Strategies for Generative AI Input Risk

A recent study by Menlo Security showed **55% of corporate Generative AI inputs contained personally identifiable information (PII) or other sensitive information**<sup>1</sup>. While the potential for damage from these exposures is well understood, their sheer prevalence remains underestimated. Last quarter, a leading health data firm suffered a catastrophic loss due to poorly managed input risks. Whether it is the erosion of a competitive edge, financial penalties, or harm to an organization's reputation, the consequences of inaction are severe.

This situation is not inevitable. It simply demands the prioritization of risk management to protect sensitive data and secure innovation. Below, we present a roadmap of safeguards tailored for organizations of all sizes to ensure both Generative AI success and security in handling data.

**CORPORATE GENERATIVE AI INPUTS**




### Checklist of Initial AI Steps for All Organizations

#### Data Anonymization

Implement data anonymization techniques, such as differential privacy, which introduces controlled randomness into datasets to mask individual data points without skewing the overall

<sup>1</sup> <https://www.menlosecurity.com/press-releases/menlo-security-reports-that-55-of-generative-ai-inputs-contained-sensitive-and-personally-identifiable-information>



data utility. This method ensures that the AI models cannot infer specifics about individuals, significantly mitigating the risk of personal data exposure while maintaining the dataset's analytical value.

#### **Understanding and Leveraging Platform Policies**

Encourage a deep dive into the privacy policies and data handling practices of public AI platforms such as OpenAI's ChatGPT, Microsoft's Copilot, Anthropic's Claude, and Google's Gemini. Understanding these data controls - or lack thereof - can reveal ways to maximize data security and integrity within the constraints of public systems. Awareness campaigns can ensure that users are not only familiar with these policies but also understand their implications for data security.

#### **Internal Policies**

Establish stringent internal guidelines that dictate how data is to be managed and protected within your organization. These policies should encompass data encryption, access controls, and regular audits to ensure compliance and detect any potential vulnerabilities. These policies will vary depending on what AI platforms you utilize and how you intend to utilize them. This is more than rule setting, this is about fostering a culture where data security is everyone's responsibility.

#### **User Education**

It is critical to educate users on the safe handling of sensitive data. Develop comprehensive training programs that detail the risks associated with public AI platforms and provide clear guidelines on what constitutes safe data sharing. Your team is the first line of defense against data misuse.

## **Mitigation Strategies for Generative AI Output Risk**

Here is another example to examine: A lawyer tasked ChatGPT with drafting a legal brief, and the results were disastrous. Invented cases surfaced as legal precedents, ultimately costing the lawyer's firm thousands of dollars in fines and underlining the severity of AI output errors or "hallucinations"<sup>2</sup>. Whether this failure arose from misuse or limitations of today's AI, it starkly demonstrates the risks facing organizations, from incorrect reports that distort strategic decisions to misinformation damaging your credibility.

Proactive mitigation of these risks is paramount. Outlined below are strategies tailored to enhance output accuracy, ensuring a balance between Generative AI capabilities and sound decision-making processes.

---

<sup>2</sup> <https://apnews.com/article/artificial-intelligence-chatgpt-fake-case-lawyers-d6ae9fa79d0542db9e1455397aef381c>

## Strategies to Safeguard Public AI Outputs

Ensuring the reliability and integrity of public AI outputs is paramount. The following strategies are designed to fortify the credibility of these outputs, addressing the dual challenges of maintaining accuracy and building trust in AI-generated content.

- **Rigorous Cross-Verification:** Mandate cross-checking AI outputs against trusted factual sources before publication or high-stakes actions. This establishes a baseline check on AI trustworthiness, mitigating the spread of unverified claims.
- **Human-in-the-Loop:** Institute review processes where people assess some or all AI outputs. This adds a layer of critical thinking and domain expertise that machines lack, minimizing the likelihood of erroneous content.
- **Supplemental Use:** Prioritize AI outputs as supporting decision-making rather than the sole basis. Acknowledge the limitations of current AI, using outputs to generate ideas, research leads, or draft content – with human oversight as the final quality check.

## Strategies to Enhance Accuracy and Security with Private AI Capabilities

Harnessing private AI capabilities elevates the accuracy and contextual relevance of AI-generated content, particularly through the customization of AI models and the incorporation of Retrieval Augmented Generation (RAG) systems.

- **Retrieval Augmented Generation (RAG):** Dynamically pulling in relevant information from existing organization data, empowers the model to reference a vast array of accurate, real-time data, thereby enhancing the quality and reliability of the responses. Integrating RAG alongside other tools allows the model to draw on verified, factual knowledge, increasing its ability to self-correct and produce accurate responses.
- **Customized Models:** Invest in models trained on your own data, tailored to your terminology and domain knowledge. This significantly improves output relevance and reduces factual errors that AI 'learns' from more generic datasets.
- **Augment the AI's Learning:** Couple Reinforcement Learning from AI Feedback (RLAIF) - where the AI cross-checks its own results - with Reinforcement Learning from Human Feedback (RLHF) - when a human provides feedback on the AI's output. This two-tiered approach provides ongoing quality assurance.

With a strategic plan focused on these mitigations, organizations reduce the risk of costly mistakes and protect their hard-earned reputations – making confident, data-informed decisions by harnessing the transformative power of Generative AI. The strategic investment in output risk mitigation not only enhances the reliability and effectiveness of AI applications but also drives significant ROI by improving operational efficiency, decision-making quality, and competitive advantage.



## Establishing Governance and Policy Frameworks

Establishing clear policies and robust governance structures is crucial for organizations seeking to leverage the power of generative AI while minimizing its inherent risks. These frameworks provide the necessary guardrails to ensure the responsible development, deployment, and use of AI systems, protecting the organization from potential pitfalls such as data breaches, biased outputs, or regulatory non-compliance.

Effective AI governance involves a multifaceted approach that encompasses data management, model training, output verification, and ongoing monitoring. It requires the active participation and collaboration of stakeholders across the organization, from IT and data science teams to legal, compliance, and business units. By institutionalizing AI governance best practices, organizations can foster a culture of responsible innovation and build trust in their AI initiatives among employees, customers, and the broader public.

Moreover, given the rapidly evolving nature of AI technologies and the regulatory landscape surrounding them, it is essential that organizations view AI governance as an ongoing process rather than a one-time exercise. This necessitates regular review and updating of policies and procedures to keep pace with new developments, ensuring that the organization remains compliant and aligned with industry best practices over time.

Investing in robust AI governance may require upfront effort and resources, but it pays significant dividends in the long run by mitigating risks, enhancing the quality and reliability of AI outputs, and enabling the organization to harness the full potential of generative AI in a sustainable and ethical manner. As such, it should be a top priority for any organization embarking on their AI journey.

To establish effective governance and policy frameworks for Generative AI, organizations should focus on three key areas: developing comprehensive policies, ensuring regulatory compliance, and addressing ethical AI considerations.

- 1. Comprehensive Policies:** These provide scaffolding for secure and responsible AI use. Policies addressing data classification, handling, and protocols for classifying data based on sensitivity should be in place before you start your AI journey. Additionally, appropriate security access, strict encryption and access control standards are requirements for a safe AI environment.
- 2. Regulatory Compliance:** Policies should meticulously address relevant regulations, tailoring data governance protocols to meet stringent compliance requirements in sectors like healthcare and finance. Incorporate protections aligned with regional or international data privacy laws, especially when handling data of global citizens. Remain mindful that the regulatory landscape surrounding AI is in flux and build adaptive governance frameworks that can swiftly respond to new laws or interpretations.

- Ethical AI Considerations:** Your organization’s values should be reflected in your AI governance. Develop policies that proactively identify and mitigate potential biases in datasets and AI outputs, preventing discriminatory or unfair decision-making. Where possible, prioritize models that allow for explainable outputs, fostering trust in AI-supported decisions by providing insights into the AI's reasoning. Finally, ensure clear lines of accountability for AI outcomes, even in the face of complex human-AI interactions. This guarantees responsibility and provides avenues for continuous improvement of your AI systems.

## Choosing the Right AI Solution for Your Organization

Choosing the optimal environment for your AI deployment is a pivotal decision that hinges on balancing control, compliance, and cost considerations. Whether you lean towards the security and customization of Private Hubs — an internal, secure platform dedicated specifically to an organization's AI operations, embrace the agility and resourcefulness of Public Platforms, or opt for Hybrid Approaches to combine the strengths of both, your choice should strategically align with your organization's long-term AI goals.

AI Solution	Who Has Access	Data Security	Price	Customizations
Private AI	Internal Staff	High	Thousands to millions of dollars to build	Virtually limitless
Public AI	Everyone	Low	Free to low-cost monthly subscription/user	Limited

### Private AI Solutions

For extremely sensitive data or operations where control over the AI model's training and outputs is critical, consider the strategic use of private AI hubs. These can offer dedicated security infrastructure and tailored security measures without entirely forgoing the benefits and accessibility of public platforms.

### Public Platforms

Public AI offers affordability and a vast pool of ready-to-use models. Rigorous data anonymization, careful output verification, and a focus on non-critical tasks maximize benefits while minimizing data exposure risk.

### Hybrid Approaches

Explore hybrid models that leverage the strengths of both public and private platforms. For instance, sensitive data can be processed and analyzed within a secure, private environment, while less sensitive tasks can be outsourced to public platforms, maximizing both security and cost-effectiveness.



## Regular Security Audits and Compliance Checks

Whether utilizing public platforms, private hubs, or a combination of both, regular audits of security practices and compliance with relevant data protection regulations are essential. This ensures that security measures are up to date and effective against evolving threats.

## Ethical and Legal Compliance

Ensure ongoing compliance with evolving data protection laws and ethical standards. This commitment must be consistent regardless of whether data is processed on public or private platforms, underscoring the organization's dedication to data privacy and security.

By focusing on robust strategies for public AI platforms while thoughtfully incorporating private AI solutions where and if necessary, organizations can navigate the complexities of Generative AI input risk management effectively. This balanced approach allows for the exploitation of public AI benefits with a keen eye on security, offering a flexible framework that can adapt to varying needs and resources.

## Building a Secure and Adaptive AI Ecosystem

Embarking on the development of a secure and adaptive AI ecosystem is not merely about integrating innovative technologies; it is a comprehensive approach that marries visionary strategy, clear policies, and ground-level pragmatism. This journey hinges on making judicious investments in AI while investing in risk management strategies that boost operational efficiency, elevating productivity, and securing a competitive edge.

## The Building Blocks for Success



- **Strategic Alignment:** Start by identifying where AI aligns with your organization's mission and goals, while ensuring this alignment is grounded in sound governance and data security policies. This is not about adopting AI for its own sake but about leveraging it where it can make a real difference. A strategic assessment that identifies high-impact areas ensures that your AI initiatives drive operational efficiency, enhance decision-making, and spur innovation.
- **Future-Ready Infrastructure:** Build an infrastructure that is both secure and scalable, ready to evolve as AI technologies advance. Start with a security first approach to protect data integrity and privacy, ensuring your AI ecosystem complies with stringent data protection laws. This dual focus on flexibility and security prepares you to adapt to new advancements while maintaining trust.
- **Data Management:** Treat your data as a competitive edge that needs safeguarding. The importance of rigorous encryption, strict access controls, and regular audits, are even more critical with the introduction of AI. Data that may have been buried deep in old files becomes instantly accessible with the introduction of AI. AI does not change the policies you already have in place, but it does make following those policies crucial.
- **Empowered Teams:** AI should augment human domain specific expertise, not replace it. Develop training programs that equip your team with the skills to collaborate effectively with AI technologies. By promoting a culture of innovation and continuous learning, you empower your workforce to unlock new opportunities and drive growth.
- **Small Steps:** Initiate your AI journey with pilot projects and proof of concepts focused on areas with clear ROI potential. These early wins not only demonstrate value but also build organizational confidence in AI technologies. Scaling up from these successes allows for a thoughtful integration of AI into broader workflows, informed by real-world feedback and performance data. The strategy of starting small and validating value ensures a measured approach to AI adoption, maximizing ROI by focusing on high-impact areas and building a solid foundation for future expansion.
- **A Culture of Innovation:** The goal is to create an AI ecosystem that grows with your organization, leveraging AI not just as a tool but as an integral part of your strategic vision. This requires a commitment to adaptability, a willingness to continuously reassess and realign AI initiatives with organizational objectives, and a proactive approach to embracing technological change.

## Conclusion

The AI revolution is not on the horizon; it's already here, reshaping industries and redefining what's possible. As a leader, you have a choice: proactively seize the opportunities while managing the risks, or reactively scramble to catch up as competitors surge ahead.

**Act Now.** Begin with an immediate audit of your data handling practices and pilot projects with enhanced security for sensitive initiatives. In parallel, develop a comprehensive AI strategy aligned with your goals for future expansion.

- **Assess and Scale.** Evaluate your organization's readiness for AI. Consider partnering with experts in the AI field to expedite your AI learnings, balancing speed while maintaining quality and alignment with your strategic objectives.
- **Understand the Stakes.** Inaction poses very real risks - lost efficiencies, misinformed AI-enhanced decisions, and vulnerabilities that compromise your reputation and competitive standing. This is not hypothetical; it is happening to your peers now.
- **Immediate and Informed Action Matters.** Investing in Generative AI secures your organization's future. Make choices that mitigate risks while empowering teams to thrive in an AI-enhanced environment. Every step towards understanding and integrating AI brings you closer to its full potential – transforming operations, driving growth, and outpacing your competitors.

**This is Not Technology for the Sake of Technology.** This is about embracing a future that will be shaped by AI. We are barreling towards a time where we will be using Generative AI daily. Effectively implementing it today ensures you will not be left behind tomorrow. With a clear roadmap and proactive stance, the rewards—operational excellence and efficiency, innovation, and a fortified competitive position—are profound.

Let this paper serve as both a blueprint and a catalyst for your journey with Generative AI. The question is not whether to embrace AI, but how to do so wisely and decisively. The roadmap is clear; the journey begins with a single step.

## About the Author

Greg Starling serves as the Head of Emerging Technology for Doyon Technology Group. He has been a thought leader for the past twenty years, focusing on technology trends, and has contributed to published articles in Forbes, Wired, Inc., Mashable, and Entrepreneur magazines. He holds multiple patents and has been twice named as Innovator of the Year by the Journal Record. Greg also runs one of the largest AI information communities worldwide.



Doyon Technology Group (DTG), a subsidiary of Doyon, Limited, was established in 2023 in Anchorage, Alaska to manage the Doyon portfolio of technology companies: Arctic Information Technology (Arctic IT®), Arctic IT Government Solutions, and designDATA. DTG companies offer a variety of technology services including managed services, cybersecurity, and professional software implementations and support for cloud business applications.



[arcticit.com](http://arcticit.com)



[arcticitgov.com](http://arcticitgov.com)



[designdata.com](http://designdata.com)