Generative AI Questionnaire **Overview**

The **Gen AI Governance** Program is designed to address the complexities and rapid evolution of AI technology in supplier environments. Understanding the challenges associated with AI, including its novelty and the rapid pace of its development, we have crafted a streamlined questionnaire. This tool aims to help companies feel confident about the AI systems their third-party vendors implement, ensuring these systems are secure, compliant with applicable laws and industry standards, and ethically managed.

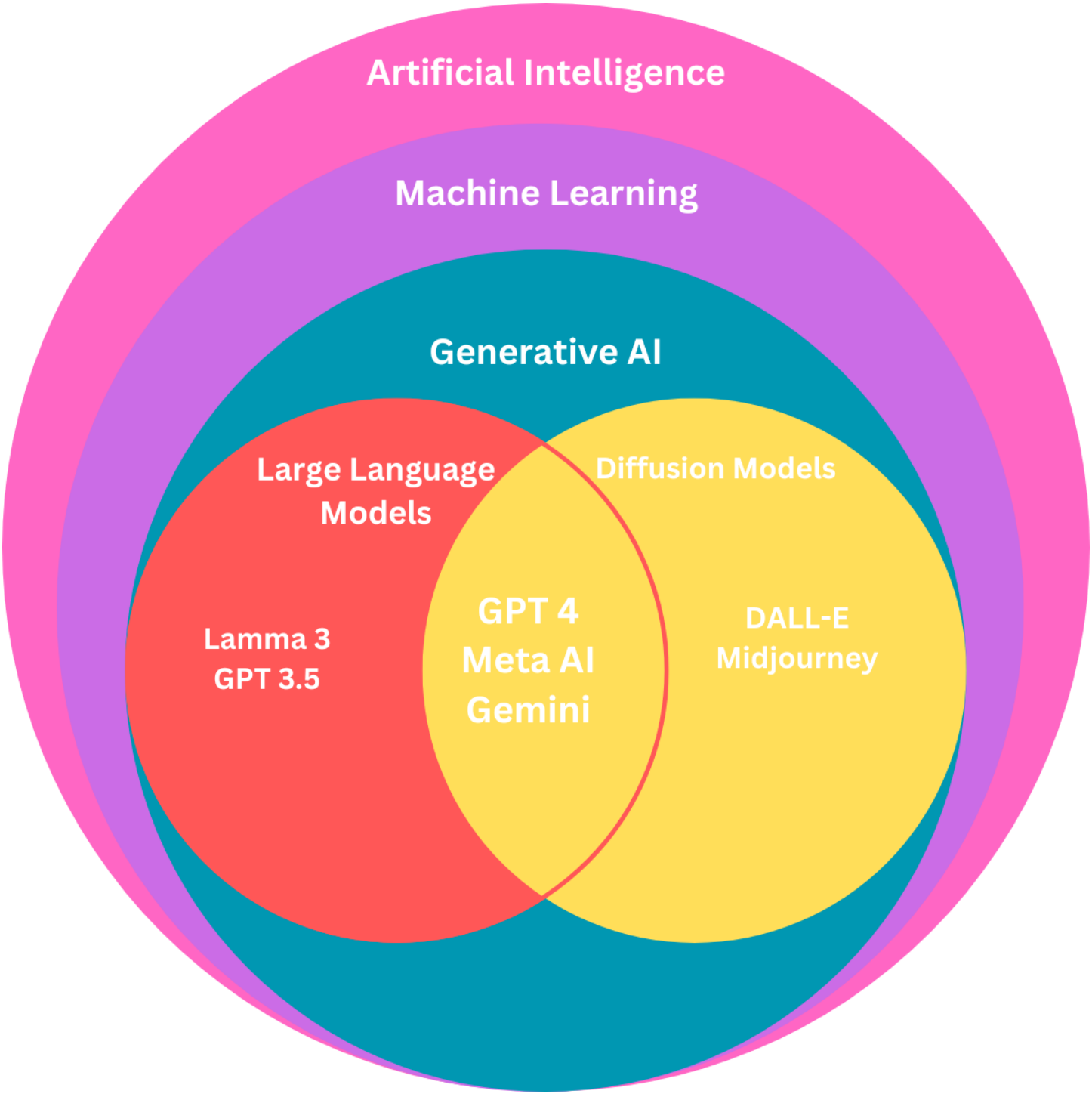
Core Objectives of the Gen AI Governance Program:

- **Increase Speed and Coverage:** We aim to quickly deliver insightful evaluations to our business stakeholders considering new AI suppliers, while also maintaining the capacity to re-evaluate existing suppliers effectively. This approach ensures a dynamic and responsive vendor management process.
- **Focus on Consequential Questions:** Our questionnaire is designed to only include questions that may directly impact our risk profile. This focus helps to accurately identify risks associated with data privacy, AI ethics, and security vulnerabilities that are critical to the integrity and reliability of AI applications.
- **Support and Educate Our Suppliers:** Understanding that many suppliers may not have advanced in-house AI security capabilities, our program is also geared towards helping them enhance their security postures. By doing so, we aim to prevent breaches and protect both their interests and ours from potential cyber threats.
- **Demonstrate Compliance and Identify Gaps:** This questionnaire allows an organization to better understand where there may be gaps in their compliance management program, and help them develop a plan to mitigate these issues.

Anticipated Challenges:

- **Knowledge Gaps:** Many organizations may initially struggle to answer some of the questions due to unfamiliarity with AI-specific security and ethical considerations. We plan to address this by providing training sessions and detailed guidance to help them understand the relevance and necessity of each question.
- **Rapid Evolution of AI:** The fast-paced development of AI technologies means that our questionnaire may need frequent updates to stay effective. We will establish a routine review process that involves AI security experts to ensure our questionnaire captures the latest in AI security trends and threats.
- **Continuous Improvement:** We expect to refine our process continuously based on constructive feedback and the realities of the continually-evolving AI security landscapes. This iterative improvement will help maintain the relevance and efficacy of our evaluations.

By tackling these challenges head-on and maintaining a flexible, educational approach, the Gen AI Security Program aims to build a culture of trust and cooperation between companies and their AI suppliers, ensuring that third-party AI implementations are secure and aligned with compliance frameworks.


Artificial Intelligence
Machine Learning
Generative AI
Large Language Models
Lamma 3
GPT 3.5
GPT 4
Meta AI
Gemini
Diffusion Models
DALL-E
Midjourney

Ecosystem Security Program Questionnaire

The questions below focus on those areas of a supplier's security program which we believe have the greatest impact to their ability to protect personal data, respond to incidents, and maintain service to our organization. These questions are reviewed and refined for appropriateness on an annual basis.

#	Category	Question	Question Type	Rationale and Guidance
1.	**Ethics** Data Collection	How was the data collected that was used to train the model? Is any one source of data over-represented?	**Question Type:** Free form	Understanding the data collection methodology is essential to assess the diversity and representativeness of the dataset. Over-representation of any data source could introduce biases, affecting the model's fairness and accuracy.
2.	**Ethics** Data Collection	Is there any bias arising from the data collection methodology used?	**Question Type:** Free Form	Identifying potential biases from the outset helps mitigate risks related to model performance across different demographic groups, especially in scenarios excluding non-digital communities or other specific groups.
3.	**Ethics** Data Collection	How do you determine if there is bias in the data?	**Question Type:** Free Form	Evaluating personal data against immutable characteristics as defined in human rights or anti-discriminatory laws or legal codes will ensure that the identification and eradication of bias is formalized in the AI building process.
4.	**Ethics** Decision Making	Is there any potential for automated decision making (ADM) as defined under GDPR that could impact a human?	**Question Type:** Yes/No	This question aims to identify the use of ADM systems that significantly affect individuals, requiring additional regulatory compliance measures.
4.1	**Ethics** Decision Making	If you answered "Yes" to ADM as defined above, confirm the legal grounds that permit you to do so.	**Question Type:** Free Form	Aligns ADM processing against applicable legislation. This is only permitted in strictly defined circumstances.
4.2	**Ethics** Decision Making	If you answered "Yes" to ADM as defined above, confirm if there is any human intervention in the process.	**Question Type:** Free Form	ADM may be permitted in limited circumstances if the process has a non-automated decision-making component to it. If the results of any ADM is then reviewed and evaluated by a person, then that would remove the data processing activity out of the strict definition of ADM.
5.	**Ethics** Decision Making	How do you ensure transparency and	**Question Type:** Free Form	Transparency in AI processes is crucial for trust and accountability, particularly in high-stakes decisions. It involves clarifying

#	Category	Question	Question Type	Rationale and Guidance
		explainability in AI decision-making processes?		the mechanisms and logic behind AI decisions.
6.	**Ethics** Decision Making	Is there an accountability framework that the organization follows (someone who has the responsibility for the AI system?)	**Question Type:** Free Form	Establishing accountability within the organization is key to managing and mitigating risks associated with AI systems. The framework should outline roles and responsibilities to specific stakeholders.
7.	**Ethics** Diversity	If there is any potential for impact in the outputs of a model, were diverse communities consulted during development to understand and mitigate potential impacts?	**Question Type:** Yes/No/NA	Consulting diverse communities helps ensure the AI model's outputs are fair and inclusive, improving the model's effectiveness and societal acceptance.
8.	**Ethics** Diversity	Were your models built by a diverse team with diverse perspectives and backgrounds?	**Question Type:** Yes/No	Diversity in team composition can reduce biases in AI models by bringing varied perspectives into the development process.
9.	**Ethics** Biases	Are your data scientists trained on the recognition of and testing against biases and ethical standards?	**Question Type:** Yes/No	Training data scientists on recognizing and mitigating biases is essential for developing ethical AI systems.
10.	**Ethics** Biases	Do you test your models throughout all stages of the software development lifecycle (e.g. design, implementation, testing, etc), or only upon conclusion? Note that some models cannot be modified easily after construction and baked-in biases can be difficult or impossible to remove	**Question Type:** Checkbox/Multi Choice: ● During Each Stage ● Only at Conclusion ● Not Applicable	Forward-thinking and Requires Review. Smaller organizations are likely to do this only with native cloud tools, but with small tenancies, that might be ok. Larger ones may be using third party platforms. Our assessors will need to have cloud security competency and awareness of emerging solutions.

#	Category	Question	Question Type	Rationale and Guidance
11.	**Ethics** Standards	Do you comply with any ethical AI standards or laws that govern the use of AI?	**Question Type:** Free Form	Compliance with recognized ethical AI standards demonstrates a commitment to responsible AI practices.
12.	**Ethics** Standards	What frameworks for ethical AI do you train your employees on?	**Question Type:** Yes/No/NA	Training on ethical AI frameworks equips employees with the necessary knowledge to uphold ethical considerations in AI development.
13.	**Ethics** Standards	Have your models been verified or audited by any third parties for compliance against ethics standards	**Question Type:** Yes/No/NA	Third-party verification or auditing of AI models for ethical compliance provides an independent assessment of the model's adherence to ethical norms.
14.	**Security** System Security	How do you ensure the physical security of the infrastructure where AI models are developed and maintained?	**Question Type:** Free Form	Physical security measures are crucial to protect AI infrastructure from unauthorized access and potential sabotage, helping to maintain the integrity of AI systems.
15.	**Security** System Security	Describe the security measures in place for your development and deployment environments.	**Question Type:** Free Form	Ensuring secure development environments helps prevent unauthorized access and code manipulation, which could compromise the AI system.
16.	**Security** Network Security	Do you implement segmentation in your network architecture to protect critical AI systems?	**Question Type:** Yes/No	Network segmentation helps isolate and protect critical systems from breaches in less secure parts of the network.
17.	**Security** Network Security	What protocols are in place for secure communication between AI components?	**Question Type:** Free Form	Secure communication protocols are essential to prevent data leaks and ensure that data transmitted between AI components is not intercepted or altered.
18.	**Security** Data Security	What encryption methods are used to secure AI training and operational data?	**Question Type:** Free Form	Encryption is crucial for protecting sensitive data used in AI systems, both at rest and in transit, from unauthorized access.
19.	**Security** Data Security	How do you manage and secure access to datasets used for training AI models?	**Question Type:** Free Form	Proper data access management ensures that only authorized personnel have access to sensitive data, reducing the risk of data breaches. Access must only be granted on a pure “need to know” basis.
20.	**Security** Incident Response	Describe your incident response plan specifically designed for AI systems.	**Question Type:** Free Form	An AI-specific incident response plan is critical for quickly addressing security incidents and minimizing their impact on AI operations. This is separate from a privacy

#	Category	Question	Question Type	Rationale and Guidance
				breach response protocol, although the processes may be integrated (see separate requirement).
21.	**Security** Incident Response	Do you conduct regular security audits and penetration testing on your AI systems?	**Question Type:** Yes/No	Regular audits and penetration tests help identify and mitigate vulnerabilities in AI systems before they can be exploited.
22.	**Security** Compliance and Governance	Do you conduct annual tests of restoration from backup capabilities for systems supporting services to our organization?	**Question Type:** Free Form	Compliance with security standards and regulations ensures that AI systems meet established security benchmarks and legal requirements.
23.	**Security** Compliance and Governance	Do you use a Privileged Access Management (PAM) vault, with one-time password auto-rotation and check-out procedures for:	**Question Type:** Free Form	Ongoing compliance is necessary to adapt to evolving security threats and regulatory changes, ensuring long-term protection of AI systems.
24.	**Security** Compliance and Governance	Do you use third party AI`s? List the third party AIs that are being used.	**Question Type:** Free Form	Understanding the use of third-party AIs is essential to evaluate security vulnerabilities, compliance with regulations, and manage dependencies, ensuring the robustness and integrity of the overall AI system.
25.	**Privacy** Deletion	Do you have data retention and destruction schedules? Do your vendors also have data retention and schedules and, if so, how long do they retain your data? What are the governing laws or industry regulations that compel them to retain data after their use has expired?	**Question Type:** Free Form	Compliance with data retention and destruction schedules is crucial for managing data responsibly and adhering to legal obligations.
26.	**Privacy** Deletion	What policies govern the retention and deletion of sensitive data used in AI systems?	**Question Type:** Free Form	Proper data retention and deletion policies are crucial to comply with privacy regulations and manage data lifecycle responsibly.
27.	**Privacy** PII	Is the personal data being used for any activities considered to be “high risk” by the EU AI Act?	**Question Type:** Yes/No	This question ensures awareness and compliance with the EU AI Act's regulations regarding high-risk AI applications. This requires the vendor to

#	Category	Question	Question Type	Rationale and Guidance
				specifically align the data processing activity with the risk categorization set out by the EU AI Act.
28.	**Privacy** PII	Is the personal data you are processing given to you in an identifiable format? If the personal data is de-identified, are there contextual clues in the data set that may *re-identify* any identifiable persons?	**Question Type:** Yes / No	Although some vendors say they do not use personal data in their processing or AI model / training, they may still receive personal data that is still in a raw identifiable format. If that is the case, somewhere in the organization the raw data needs to be itemized in the data mapping / inventory. This also carries a privacy risk if there is ever a security breach and that raw personal data is compromised.
29.	**Privacy** PII	Describe the methods by which you de-identify any personal data being disclosed to you, and when those points of de-identification occur.	**Question Type:** Free Form	De-identification techniques are essential to protect personal data and comply with privacy standards.
30.	**Privacy** PII	Are you receiving personal data via indirect means, i.e. are you collecting it from third parties and not from the individuals to whom that data pertains?	**Question Type:** Yes/No	This question helps assess the transparency and consent mechanisms in place for data collection.
31.	**Privacy** PII	What are the legal grounds on which you rely upon to process personal data? If you are relying on a specific enumerated ground or legislative permission, cite the applicable law(s) and provide a copy of the notification or consent form you provide to individuals prior to the processing of their data.	**Question Type:** Free Form	It is critical to verify the legal basis for data processing to ensure compliance with privacy laws.
32.	**Privacy** Vendors	If your third-party vendors are receiving personal data as part of service delivery and fulfillment, please confirm their jurisdiction / location(s) and what contractual or other	**Question Type:** Free Form	Ensuring third-party compliance with applicable data protection laws and agreements safeguards against data breaches and unauthorized access.

#	Category	Question	Question Type	Rationale and Guidance
		safeguards you have with them to protect the data.		
33.	**Privacy** Training	Is user generated data used for training?	**Question Type:** Yes/No	Understanding if user-generated data is used is essential to ensure compliance with data privacy laws and to assess potential privacy risks.
34.	**Privacy** Location	Where does the AI process the data?	**Question Type:** Free Form	This question is designed to identify the geographical locations where data processing occurs. Knowing the processing locations is essential for ensuring compliance with data sovereignty laws and regulations, which vary widely across jurisdictions. It helps assess potential jurisdictional risks, such as varying levels of data protection standards and enforcement practices. Clear understanding of where the data resides and is processed enables companies to evaluate whether appropriate legal and security measures are in place to protect the data according to the local and international regulations that apply, thereby managing risks related to cross-border data transfers effectively. Cross-border transfer of personal data may also require you to provide notice to the data subjects that their personal information is going to another country or jurisdiction, and you may need additional consent prior to doing so.
35.	**Privacy** Legal Requirements	Have you completed a data privacy impact assessment (DPIA) or a privacy impact assessment (PIA) on the AI system? If so, please provide a copy of the document.	**Question Type:** Yes/No	This question is aimed at verifying compliance with GDPR requirements, which mandate a DPIA for any data processing activities that are likely to result in a high risk to the rights and freedoms of individuals. Other jurisdictions mandate a PIA, although it may not necessarily follow the GDPR template. Conducting a DPIA is crucial not only for compliance but also for identifying and mitigating any potential data protection risks associated with the AI system. This assessment helps ensure that privacy considerations are embedded in the design and operation of the system, enhancing transparency and trustworthiness. A positive response

#	Category	Question	Question Type	Rationale and Guidance
				should be supported by documentary evidence, which allows for an evaluation of the thoroughness and effectiveness of the privacy impact assessment.
36.	**Privacy** Product	If you are using personal data to produce Gen AI products, what remediation or quality assurance do you have to ensure that the service(s) or product(s) are compliant with applicable law(s)?	**Question Type:** Free Form	This question probes the mechanisms and processes that ensure compliance of Gen AI products with legal and regulatory frameworks concerning personal data use. It aims to verify that there are effective quality assurance and remediation strategies in place to address potential non-compliance issues swiftly. Clear documentation of these processes helps in understanding how the organization mitigates risks related to data privacy and adheres to standards such as GDPR, HIPAA, or other relevant data protection laws, which are critical for maintaining legal and ethical standards in AI development and deployment.
37.	**Privacy** Legal Requirements	Do you have a dedicated privacy breach response protocol? If not, do you evaluate privacy risks within the standard Incident response protocol?	**Question Type:** Yes / No	An organization often has security IRPs, but often does not have a privacy breach response. Privacy laws like GDPR have strict requirements when it comes to reporting privacy breaches to regulators and notifying affected person(s). Failure to abide by breach notification requirements may lead to legislative fines.
38.	**Privacy** Legal Requirements	Does your privacy policy address how your organization deals with processing personal data vis-a-vis AI models?	**Question Type:** Yes / No	This is the governing document that shows your commitment to data privacy protection. If you answered “No” to this question, provide a policy or similarly binding governance document evidencing your firm’s handling of personal data in AI models.
39.	**Privacy** Legal Requirements	What notification, notice, or consent form do you give to persons from whom you collect personal Data?	**Question Type:** Free Form	A written notice or consent form must outline the express reason(s) for which personal data is being processed. It is the basis for which individuals provide their consent to the collection, use, disclosure, and storage of their personal data. A consent form or notification differs from a privacy policy as it is akin to an agreement between the organization and the person,

#	Category	Question	Question Type	Rationale and Guidance
				whereas a privacy policy is a governance document.

Created by Anthony Green

Contributors -

Ritchie Po

Sergey Bhukarov

Ads Dawson

Mary Carmichael

Resources:

OpenAI - Reimagining secure infrastructure for advanced AI | OpenAI

World Health Organization (WHO) - Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models https://www.who.int/publications/i/item/9789240084759

Canadian Gov Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems - Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems

EU AI Act (full text) (English): https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf