

Appendices - Complying with the AI Act

👤 Owner	👤 Jacintha
🏷️ Tags	
🕒 Created time	@June 8, 2023 5:12 PM

Appendix A - Code LLM's

Based on the library: <https://pypi.org/project/llama-index/>, the following code is adapted.

```
#llama index
import os
os.environ['OPENAI_API_KEY'] = ""

from llama_index import GPTVectorStoreIndex, SimpleDirectoryReader

documents = SimpleDirectoryReader('cluster3').load_data()
index = GPTVectorStoreIndex.from_documents(documents)
queries = ["Should technical documentation also be written for non-technical people?"]

query_engine = index.as_query_engine()
for question in queries:
    query = question
    response = query_engine.query(query)
    print(query)
    print(response)
```

Based on the library: <https://github.com/ushakrishnan/SearchWithOpenAI>, the following code is adapted.

```
#SearchWithOpenAI
import streamlit as st
from pathlib import Path
from common.funs import start_capture
from datetime import datetime

def read_markdown_file(markdown_file):
    return Path(markdown_file).read_text()

intro_markdown = read_markdown_file("README.md")
st.markdown(intro_markdown, unsafe_allow_html=True)

#st.write(datetime.now().hour,datetime.now().minute)
st.markdown("## Preparing ... ")

start_capture()

#st.write(datetime.now().hour,datetime.now().minute)
st.markdown("# Ready")
```

```
# makefile to configure the clusters
cluster1:
    rm -f aia/*.pdf
    cp aia/Core/*.pdf aia
    streamlit run Home.py
cluster2:
    rm -f aia/*.pdf
    cp aia/Core/*.pdf aia
    cp aia/Other/*.pdf aia
    streamlit run Home.py
cluster2:
    rm -f aia/*.pdf
    cp aia/Core/*.pdf aia
    cp aia/Other/*.pdf aia
    cp aia/External/*.pdf aia
    streamlit run Home.py
```

Find the full code on this GitHub: <https://gitfront.io/r/user-7646844/ZTQB4rfx5SYN/CustomLLM/>

A.1 Cluster 1: Core AIA Documents

- [AIA – COM – Proposal \(21 April 2021\)](#)
- [AIA – COM – Annexes \(21 April 2021\)](#)

A.2 Cluster 2: Other EU AIA Sources + External Sources

- [AIA – COM – Draft Standardisation Request \(5 December 2022\)](#)
- [AIA – COM – Impact Assessment 1 \(21 April 2021\)](#)
- [AIA – COM – Impact Assessment 2 \(21 April 2021\)](#)
- [AIA – COM – Impact Assessment 3 \(21 April 2021\)](#)
- [AIA – CZ – General Approach \(25 November 2022\)](#)
- [AIA – ECB – Opinion I \(29 Dec 2021\)](#)
- [AIA – ECB – Opinion II \(29 Dec 2021\)](#)
- [AIA – CoR – Opinion \(2 Dec 2021\)](#)
- [AIA – EESC – Opinion \(22 Sept 2021\)](#)
- [AIA – EDPB+EDPS – Opinion \(18 June 2021\)](#)
- [AI Act: a step closer to the first rules on Artificial Intelligence](#)
- [LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE \(ARTIFICIAL INTELLIGENCE ACT\) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS](#)
- [LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE \(ARTIFICIAL INTELLIGENCE ACT\) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS](#)
- [harmonised rules on artificial intelligence Artificial Intelligence Act](#)
- [EU Artificial Intelligence Act: The European Approach to AI](#)
- [Amendments to the Artificial Intelligence Act](#)
- [The European Commission' s Artificial Intelligence Act](#)
- [Artificial intelligence act](#)
- [The Artificial Intelligence Act: A Jurisprudential Perspective](#)
- [Decoding the proposed EU AI Act](#)
- [Strategies, Policies, and Standards in the EU Towards a Roadmap for Robust and Trustworthy AI Certification](#)
- [REVIEWING THE ALGORITHMIC ACCOUNTABILITY ACT IN LIGHT OF THE EUROPEAN ARTIFICIAL INTELLIGENCE ACT](#)
- [Managing complexity: the EU's contribution to artificial intelligence governance](#)
- [ETSI Activities in the field of Artificial Intelligence Preparing the implementation of the European AI Act](#)

Appendix B - Answers from each LLM

▼ Cluster 1 - Core

	Cluster 1 - Core	I	C1	C2
C1	Should technical documentation also be written for non-technical people?			
HGI	Not necessarily, the AIA gives a list of information that should be included in the technical documentation, this documentation should be written to that it can be handed to authorities at any time. Some documentation must be shared with users and must therefore be written for non-technical people, but this does not include all technical documentation.			
SWOAI	Yes, technical documentation should also be written for non-technical people. Source: AIA-COM-Annexes-21-April-21.pdf - Page: 11-12	1	2	1

	Cluster 1 - Core	I	C1	C2
Llama	Yes, technical documentation should also be written for non-technical people. The technical documentation should include concise and clear information that is understandable to all users, including those who are not technically proficient. This information should include the general characteristics, capabilities and limitations of the AI system, algorithms, data, training, testing and validation processes used, as well as documentation on the relevant risk management system.	1	3	2
CGPT	Yes, technical documentation should also be written for non-technical people to ensure understanding and transparency in AI systems. This allows for effective communication and accountability.	1	1	1
C2	Does the AIA stipulate that we need someone monitoring the AI-models full-time			
HGI	No not necessarily, the AIA stipulates that compliance must be monitored even post-monitoring. This means all interactions with the AI should be logged and analyzed to ensure compliance. The AIA does not stipulate that this must happen real-time, but rather states that a plan must be made to describe how compliance after market-release will be ensured. Which plans specifically work towards compliance is not known at the moment.			
SWOAI	No, the AIA does not stipulate that someone needs to monitor AI-models full-time. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 32, 27, 51, 15	3	3	1
Llama	Yes, the AIA stipulates that we need someone monitoring the AI-models full-time. In Section 5.1, it states that "Providing for a robust monitoring and evaluation mechanism is crucial to ensure that the proposal will be effective in achieving its specific objectives. The Commission will be in charge of monitoring the effects of the proposal. It will establish a system for registering stand-alone high-risk AI applications in a public EU-wide database." It also states that "Depending on the pre-existing structure in each Member State, this could amount to 1 to 25 Full Time Equivalents per Member State." The information that is quoted from 5.1 refers to monitoring the effect of the AIA and is thus misinterpreted.	1	3	1
CGPT	The EU Artificial Intelligence Act (AIA) does not explicitly stipulate that someone needs to monitor AI models full-time. However, it does require that organizations implement appropriate risk management and monitoring measures to ensure compliance with the regulation and address potential risks associated with AI systems. The level of monitoring required will depend on the specific characteristics and risks associated with the AI models in use.	3	3	3
C3	Does the AIA require me to work with encrypted data only?			
HGI	No, the AIA does not mention encrypted data.			
SWOAI	No, the AIA does not require you to work with encrypted data only. It does require you to use appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued. Source: AIA-COM-Proposal-21-April-21.pdf - Page: 37, 29, 69, 48	3	3	3

	Cluster 1 - Core	I	C1	C2
Llama	No, the AIA does not require you to work with encrypted data only. It does, however, require that information and data obtained in carrying out tasks and activities related to the AIA be kept confidential, and that appropriate measures be taken to protect intellectual property rights, confidential business information, and trade secrets. <i>Though the conclusion is correct, the data confidentiality is related to people working for the government and auditing organizations and thus misinterpreted here.</i>	2	1	3
CGPT	No, the AIA does not require you to work with encrypted data only. However, it emphasizes the importance of data protection and security measures for AI systems.	3	3	3
C4	How should we deal with missing data according to the AIA?			
HGI	The AIA stipulates that training, validation and testing data should be subject to data governance practices. This includes identifying data gaps and shortcoming and how to address these. Therefore step 1 is to identify missing data and document this. Since the AIA is all for risk-driven approaches, the next step would be to identify the risks related to this missing data. Then finally, it should be documented which risks are accepted and which risks aren't, for these risks new data should be gathered or the risk should be otherwise mitigated.			
SWOAI	Missing data should be handled by using a functionally separate, isolated and protected data processing environment under the control of the participants and only authorised persons having access to the data, and by deleting the data once the participation in the sandbox has terminated or the personal data has reached the end of its retention period. Source: AIA-COM-Proposal-21-April-21.pdf - Page: 78, 29, 12 <i>Though correct, this answer says nothing about how to deal with missing data.</i>	1	3	2
Llama	The AIA does not provide specific guidance on how to deal with missing data. However, it does emphasize the importance of a risk-based approach and the need for a technology-neutral and proportionate regulatory framework. Stakeholders are encouraged to use a sector-by-sector and case-by-case approach when assessing risks and threats, and to take into account the impact on rights and safety. Additionally, the AIA encourages the use of regulatory sandboxes to promote AI.	2	3	1
CGPT	The AIA does not specifically address how to deal with missing data, so it is not explicitly regulated.	1	2	1
C5	What other data risks besides data privacy should my organization be concerned with?			
HGI	The AIA actually doesn't mention data privacy as a risk for compliance. The AIA especially focuses on data bias. Data should be relevant, representative and free of errors. It should also have appropriate statistical properties, with regards to the demographic for which the AI is intended to be used. All this to ensure that data bias is minimal and that accuracy is the same over different demographics. The AIA also stipulates that accepted risks of the system and risks on rights and discrimination are communicated to the user, this means that these risks should also be examined in the data.			
SWOAI	I don't know. Source: AIA-COM-Proposal-21-April-21.pdf - Page: 70, 29, 48, 37	1	1	1

	Cluster 1 - Core	I	C1	C2
Llama	Organizations should be concerned with data quality, data governance, data bias, data gaps or shortcomings, data availability, data quantity, data suitability, data representation, data errors, data completeness, data statistical properties, data preparation processing operations, data assumptions, data annotation, data labelling, data cleaning, data enrichment, data aggregation, data poisoning, and adversarial attacks.	3	3	2
CGPT	Besides data privacy, your organization should be concerned with data security, algorithmic bias, and unintended consequences of AI systems. Data security refers to protecting data from unauthorized access, breaches, or cyberattacks. Algorithmic bias refers to the unfair or discriminatory outcomes that can result from biased data or algorithms. Unintended consequences refer to the potential negative effects or unforeseen outcomes that AI systems may have on individuals or society as a whole.	3	3	1
C6	What does the AIA mean by high-risk AI?			
HGI	The AI Act mentions 8 types of high-risk AI's. 1. Biometric identification and categorisation of natural persons 2. Management and operation of critical infrastructure 3. Education and vocational training 4. Employment, workers management and access to self-employment 5. Access to and enjoyment of essential private services and public services and benefits 6. Law enforcement 7. Migration, asylum and border control management 8. Administration of justice and democratic			
SWOAI	High-risk AI systems are those that create a high risk to the health and safety or fundamental rights of natural persons. They are classified as high-risk based on their intended purpose, taking into account the severity of the possible harm and its probability of occurrence. Source: AIA-COM-Proposal-21-April-21.pdf - Page: 47, 13, 55, 26	3	3	1
Llama	The AIA defines high-risk AI as AI systems that pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence. High-risk AI systems include stand-alone AI systems, remote biometric identification systems, AI systems used in the management and operation of critical infrastructure, AI systems used in education or vocational training, and AI systems used in employment, workers management and access to self-employment.	3	3	2
CGPT	High-risk AI refers to AI systems that have the potential to cause significant harm or impact fundamental rights and include certain sectors such as healthcare, transportation, critical infrastructure, and law enforcement. The AIA aims to regulate these AI systems more strictly to ensure transparency, accountability, and safety.	3	3	1
C7	Does the AIA require an external audit?			
HGI	No the AIA does not require an external audit persé, it is possible to perform a conformity assessment procedure based on internal controls. However, examining the technical documentation is still done by a notified body in some cases. When specifically is not clear at this point.			
SWOAI	No, the AIA does not require an external audit. Source: AIA-COM-Proposal-21-April-21.pdf - Page: 14, 58, 56, 64	2	2	1
Llama	No, the AIA does not require an external audit. The AIA requires a conformity assessment procedure based on internal control, which is outlined in Annex VI of The-AI-Act.pdf on page 10.	2	2	2

	Cluster 1 - Core	I	C1	C2
CGPT	The AIA does not explicitly require an external audit for all AI systems, but it does require some high-risk AI systems to undergo a conformity assessment carried out by a notified body, which can be considered as a form of external scrutiny.	3	3	2
C8	Which documents should be included in the compliance documentation?			
HGI	The following information should be included: - technical documentation - post-market monitoring plan - risk management system - quality management system - user information			
SWOAI	The documents that should be included in the compliance documentation are the EU declaration of conformity referred to in Article 48, the decisions and other documents issued by the notified bodies where applicable, and any documents and certificates linked to designations under any other Union harmonisation legislation. Source: AIA-COM-Proposal-21-April-21.pdf - Page: 81, 54, 68, 59	3	3	1
Llama	The documents that should be included in the compliance documentation are: • The name and address of the provider and, if the application is lodged by the authorised representative, their name and address as well; • The list of AI systems covered under the same quality management system; • The technical documentation for each AI system covered under the same quality management system; • The documentation concerning the quality management system which shall cover all the aspects listed under Article 17; • A description of the procedures in place to ensure that the quality management system remains adequate and effective; • A written declaration that the same application has not been lodged with any other notified body.	2	3	1
CGPT	1. AI System Description: Detailed documentation describing the purpose, functionality, and intended use of the AI system. 2. Data Collection and Processing Policies: Clear guidelines on data collection, processing, and storage practices, including information on data protection, consent, and security measures. 3. Risk Assessment: Comprehensive analysis of potential risks associated with the AI system, including privacy breaches, biases, discrimination, and other adverse impacts. 4. Ethical Guidelines: Document outlining the ethical principles and values guiding the development and deployment of the AI system. @ 5. Human Oversight and Control: Description of mechanisms for human intervention, monitoring, and control over the AI system's operations. 6. Training Data Description: Documentation on the training data used, including its quality, diversity, and potential biases. 7. Accuracy and Robustness Measures: Information on the system's accuracy, performance, and robustness, along with measures taken to mitigate errors and ensure reliability. 8. Transparency and Explainability: Documentation on how the system's decisions are made, including algorithms used, interpretability techniques, and model explanations. 9. Testing and Validation Processes: Description of testing methodologies, validation procedures, and performance metrics used to assess the AI system's functionality and safety. 10. Documentation Maintenance: Plan for documenting updates, modifications, and maintenance processes to ensure ongoing compliance and accountability.	2	3	1
C9	Does the AIA mention metrics that should be used to determine a models risks for rights and discrimination?			

	Cluster 1 - Core	I	C1	C2
HGI	No, the AIA does not mention specific metrics that should be used to determine a models risks for rights and discrimination, it only states that these risks should be identified and addressed.			
SWOAI	Yes, the AIA mentions metrics that should be used to determine a models risks for rights and discrimination, such as accuracy, reliability, transparency, and human oversight measures. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 11, 45, 27, 7 <i>Though these metrics are mentioned, these are not mentioned in the context of measuring risks for rights and discrimination.</i>	1	3	2
Llama	Yes, the AIA mentions metrics that should be used to determine a model's risks for rights and discrimination. Specifically, it states that testing procedures should be suitable to achieve the intended purpose of the AI system and should be made against preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.	1	3	3
CGPT	Yes, the AIA mentions that high-risk AI systems should undergo an impact assessment, including evaluation of metrics related to potential risks for rights and discrimination.	1	3	3
C10	What does the AIA mean by 'human oversight'?			
HGI	Human oversight means that high-risk AI's must be overseen by a natural person, it should be built into the AI-system by the provider before placement on the market.			
SWOAI	Human oversight is the process of ensuring that high-risk AI systems are designed and developed in such a way that they can be effectively overseen by natural persons during the period in which the AI system is in use. This includes measures such as building appropriate human-machine interface tools into the system, enabling individuals to understand the capacities and limitations of the system, and preventing or minimizing risks to health, safety, or fundamental rights. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 51, 30, 51, 8	3	3	3
Llama	Human oversight, as defined by the AIA, is the process of ensuring that high-risk AI systems are designed and developed in such a way that they can be effectively overseen by natural persons during the period in which the AI system is in use. This includes measures such as building appropriate human-machine interface tools into the system, providing users with the ability to understand the capacities and limitations of the system, and providing users with the ability to intervene on the operation of the system or interrupt the system. Additionally, for high-risk AI systems referred to in point 1(a) of Annex III, the measures must ensure that no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons. <i>The reference to Annex III is wrong (as in, that information is not stated there, though it is true) and relates to systems that use biometric identification, which is not relevant for the question.</i>	3	2	3

	Cluster 1 - Core	I	C1	C2
CGPT	'Human oversight' in the EU Artificial Intelligence Act (AIA) refers to the requirement of having human intervention or control to ensure the decisions made by AI systems are accountable, explainable, and aligned with ethical considerations. It emphasizes the need for humans to be able to understand and override AI system decisions when necessary. <i>Though very close, this answer does not highlight the need for human oversight post-release. This sounds more like human oversight during development, but the AIA focuses more on human oversight through monitoring after releasing the model.</i>	2	3	2

▼ Cluster 1 - Process

	Cluster 2 - Compliance	I	C1	C2
P1	To which extent does my ISO certification help towards AIA compliance?			
HGI	There are many types of ISO certification. ISO/IEC 23053 gives a framework specifically for AI, the specific information is not available for free and therefore not known. However, preparing for ISO certification audits will give organizations an idea of what these audits are like and how to have a system in place so that all the required information can be assessed if needed. This will help with AIA compliance, however the AIA does state requirements that are not specifically mentioned in ISO certification. Especially since most organization achieve quality management or data privacy certificates, which although related do not encompass the entire AIA.			
SWOAI	ISO certification does not directly help with AIA compliance, but it is necessary for the provider of the AI system to maintain and apply a quality management system that is approved by the notified body. Source: aia/AIA-COM-Annexes-21-April-21.pdf - Page: 11, 79, 13, 67	3	2	2
Llama	Your ISO certification may help to demonstrate compliance with the requirements set out in Chapter 2 of the AI Act, depending on the extent to which the requirements are covered by the certification. However, if the AI system is a high-risk AI system listed in Annex III, then the provider must follow the conformity assessment procedure based on internal control as referred to in Annex VI, which does not provide for the involvement of a notified body. <i>The information given on when a notified body should be involved is incorrect.</i>	3	2	2
CGPT	ISO certification can help demonstrate your commitment to certain standards and processes, but it does not directly address the specific requirements of the EU Artificial Intelligence Act (AIA).	3	3	2
P2	Does GDPR training also include data bias and model bias training?			
HGI	The GDPR has a fairness principle which states that organizations should check the following: 'We have considered how the processing may affect the individuals concerned and can justify any adverse impact.'. Data bias can be seen as a violation of the fairness principle, since it is unjustifiable if a system performs much worse for one demographic than for another. However, this is only a small part of the GDPR and there are many other, more prevalent, ways the fairness principle would not be obeyed. Therefore, it is not likely that data bias is dealt with in a GDPR training in such a way that it prepares employees for AIA compliance relating to data bias.			

	Cluster 2 - Compliance	I	C1	C2
SWOAI	No, GDPR training does not include data bias and model bias training. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 29, 41, 5	3	3	1
Llama	Yes, GDPR training includes data bias and model bias training. This is indicated in paragraph 44 of the The-AI-Act.pdf document, which states that "In order to protect the right of others from the discrimination that might result from the bias in AI systems, the providers should be able to process also special categories of personal data, as a matter of substantial public interest, in order to ensure the bias monitoring, detection and correction in relation to high-risk AI systems."	1	3	1
CGPT	GDPR training primarily focuses on data privacy and protection, but it may not explicitly cover data bias and model bias training.	3	3	1
P3	What are the biggest risks on AIA compliance when data is gathered in-house?			
HGI	The AIA mentions that high quality data is essential for AI systems. Whether gathering data in-house or using external data, the risks remain the same. Data should be relevant, representative and free of errors. It should also have appropriate statistical properties, with regards to the demographic for which the AI is intended to be used. Data risks should be identified especially concerning data bias and any risks towards rights or discrimination should be communicated with the user. This must be ensured whether using external data or gathering the data yourself. An advantage might be that there is more control over the data in-house, however it might also require more work and expertise to gather a high-quality dataset from scratch.			
SWOAI	The biggest risks on AIA compliance when data is gathered in-house include ensuring the confidentiality of information and data obtained, ensuring the AI system is safe when placed on the market or put into service, and ensuring the AI system is compliant with other Union and Member States legislation supervised within the sandbox. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 37, 69, 29 <i>This answer seems to focus more on the AI model than the data specifically.</i>	2	3	1
Llama	The biggest risks on AIA compliance when data is gathered in-house include: inadequate data governance and management practices, data that is not relevant, representative, free of errors and complete, data that does not take into account the characteristics or elements that are particular to the specific geographical, behavioural or functional setting, data that is not free of bias, data gaps or shortcomings, and inadequate technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures.	3	3	2
CGPT	The biggest risks on AIA compliance when data is gathered in-house include data quality and bias, data privacy and security, compliance with regulations and standards, lack of expertise and resources, and scalability challenges.	3	3	1
P4	Our organizations uses data from customers, what are some of the biggest risks when aiming for AIA compliance?			

	Cluster 2 - Compliance	I	C1	C2
HGI	The AIA mentions that high quality data is essential for AI systems. Whether gathering data in-house or using external data, the risks remain the same. Data should be relevant, representative and free of errors. It should also have appropriate statistical properties, with regards to the demographic for which the AI is intended to be used. Data risks should be identified especially concerning data bias and any risks towards rights or discrimination should be communicated with the user. This must be ensured whether using external data or gathering the data yourself. An advantage of external data might be that there is already a good starting point on which to perform the data analysis, however it might also be harder to fill in data gaps since this requires more data.			
SWOAI	The biggest risks when aiming for AIA compliance include the need for regulatory intervention, the need for a full, effective and properly documented ex ante compliance with all requirements of the regulation, and the need for a quality management system that ensures compliance with the regulation. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 37, 29, 79	3	3	1
Llama	Some of the biggest risks when aiming for AIA compliance include: <ul style="list-style-type: none"> • Ensuring that the data used is relevant, representative, free of errors and complete. • Examining the data for possible biases. • Identifying any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed. • Ensuring that the data sets take into account the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used. • Ensuring that appropriate data governance and management practices are in place, such as data collection, relevant data preparation processing operations, formulation of relevant assumptions, and prior assessment of the availability, quantity and suitability of the data sets that are needed. • Ensuring that any special categories of personal data are processed with appropriate safeguards for the fundamental rights and freedoms of natural persons. 	3	3	2
CGPT	When aiming for AIA compliance while using customer data, some of the biggest risks include ensuring data privacy and consent, mitigating bias and discrimination in AI models, complying with GDPR requirements, and maintaining customer trust and satisfaction. <i>This answer mentions GDPR compliance, but that is not a necessity for AIA compliance.</i>	3	2	1
P5	We only use ChatGPT and other out of the box AI models, should we still be concerned with the AIA?			
HGI	The AIA mentions 8 types of high-risk AI's. These types mainly focus on areas where the AI is applied rather than the specific AI (except for AI's using biometric). So, if your organization only uses ChatGPT or other external AI's, this still means that the organization must ensure that these tools are AIA compliant if they are applied to one of the high-risk areas.			
SWOAI	Yes, we should still be concerned with the AI Alliance as it is a multi-stakeholder forum that provides guidance and support for the development of AI technologies. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 3, 8, 49, 27	1	2	1

	Cluster 2 - Compliance	I	C1	C2
Llama	Yes, you should still be concerned with the AIA. The AIA contains provisions that prohibit certain artificial intelligence practices, lay down requirements for high-risk AI systems, and lay down transparency obligations for certain AI systems. Even if you are only using out of the box AI models, you should still be aware of the AIA and ensure that your practices comply with its provisions.	3	3	2
CGPT	Even if you use out-of-the-box AI models like ChatGPT, you should still be concerned with the AIA as it imposes obligations on both providers and users of AI systems, including ensuring transparency, accountability, and adherence to certain requirements for high-risk AI systems.	3	3	2
P6	What can we do to improve AIA compliance concerning our technical documentation?			
HGI	The AIA lists all the information that must be present in the technical documentation. In short: general description of the system, description of all the elements, an assessment of the human oversight measure, information that is communicated to the user and information around monitoring.			
SWOAI	To improve AIA compliance concerning technical documentation, providers of high-risk AI systems should ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. They should also draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49. Additionally, they should maintain the technical documentation as part of the documentation concerning internal governance, arrangements, processes and mechanisms pursuant to Article 74 of Directive 2013/36/EU. Source: aia/AIA-COM-Annexes-21-April-21.pdf - Page: 11, 68, 30, 54	3	3	3
Llama	To improve AIA compliance concerning technical documentation, we should ensure that the documentation contains all the necessary information as outlined in Annex IV, including a general description of the AI system, a detailed description of the elements of the AI system and of the process for its development, and information about the data requirements and human oversight measures needed. We should also indicate our name, registered trade name or registered trade mark, and the address at which we can be contacted on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation. Finally, we should ensure that storage or transport conditions do not jeopardise the AI system's compliance with the requirements set out in Chapter 2 of the Title.	3	3	2
CGPT	To improve AIA compliance concerning technical documentation, ensure that it includes comprehensive information about the AI system's functionality, limitations, potential risks, and mitigation strategies, following the AIA guidelines and industry best practices.	2	3	1
P7	We currently don't communicate anything about our models with our users, how can we better communicate information with the users for AIA compliance?			
HGI	The AIA mentions a list of information that must be communicated with the users. Some information is easy to start with, like capabilities of the model and its intended purpose. However, some information is harder like performance for different groups of users and any risks to the users health and safety or fundamental rights.			

	Cluster 2 - Compliance	I	C1	C2
SWOAI	To ensure AIA compliance, AI systems must undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. The provider must also draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49. The EU declaration of conformity must state that the high-risk AI system meets the requirements set out in Chapter 2 of this Title. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 7, 34, 49, 50	3	3	2
Llama	In order to comply with the AI Act, providers should ensure that they communicate relevant information to their users about their AI models. This should include information about the capabilities and limitations of the model, the expected level of accuracy, the sources of risks to health and safety, fundamental rights, and discrimination, and the human oversight measures needed. Providers should also provide information about the validation and testing procedures used, the risk management system in place, the changes made to the system through its lifecycle, the harmonised standards applied, and the post-market monitoring plan. Providers should also consider creating codes of conduct intended to foster the voluntary application of the mandatory requirements applicable to high-risk AI systems.	3	3	2
CGPT	To better communicate information with users for AIA compliance, consider implementing clear and transparent communication channels, providing meaningful explanations about the AI system's purpose, its decision-making process, potential biases, and any actions users can take to influence the system's behavior.	2	3	1
P8	Our organization is very small and no one is specialised in compliance, where do we even begin to achieve AIA compliance?			
HGI	A lot of things are still unclear about the AIA, however a lot of things are also stated very clearly. For instance, what should be documented and communicated with users. Start with the things that are clear and within your capabilities, as time passes more information will become available.			
SWOAI	To achieve AIA compliance, providers of high-risk AI systems must ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. This includes drawing up an EU declaration of conformity in accordance with Article 48 and affixing the CE marking of conformity in accordance with Article 49. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 14, 43, 54	3	3	2
Llama	Your organization should begin by familiarizing itself with the requirements set out in Title III, Chapter 2 of the AIA. This includes understanding the requirements related to environmental sustainability, accessibility for persons with a disability, stakeholders participation in the design and development of the AI systems, and diversity of development teams. Additionally, your organization should look into the possibility of drawing up codes of conduct intended to foster the voluntary application of the requirements set out in Title III, Chapter 2. This could be done by individual providers of AI systems or by organisations representing them, including with the involvement of users and any interested stakeholders and their representative organisations.	3	3	3

	Cluster 2 - Compliance	I	C1	C2
CGPT	To begin achieving AIA compliance in a small organization without specialized compliance expertise, start by conducting a thorough assessment of your AI systems, identifying potential risks, and seeking guidance from relevant industry experts or consultants. Prioritize understanding and implementing the AIA's requirements step by step.	3	3	1
P9	We currently have no idea if we communicate with our stakeholders according to the AIA, how should we assess this to make improvements?			
HGI	The AIA does not have any specific requirements for in-house communication with stakeholders. The AIA does give requirements for communication with users, governmental organizations and auditors. It's important to prepare a 'compliance package' with all the required information so this can be handed over when necessary. As for communication in-house, AIA compliance requirements should be communicated with the entire chain of development to ensure that the compliance is achieved at every development step.			
SWOAI	You could assess this by conducting surveys or interviews with stakeholders to get their feedback on how well you are communicating with them according to the AIA. You could also look at the results of the consultations that have been conducted to see if there are any areas where communication could be improved. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 9, 93, 10	2	3	2
Llama	To assess how well the stakeholders are being communicated with according to the AIA, it is important to review the feedback from the stakeholders. This includes reviewing the comments and position papers submitted through the EU Survey website, the results of the workshops and events, and the comments from the Regulatory Scrutiny Board. Additionally, it is important to review the key requirements set out in the HLEG ethics guidelines for Trustworthy AI and the Assessment List for Trustworthy Artificial Intelligence (ALTAI). By reviewing this feedback, it is possible to identify areas where communication could be improved and make changes accordingly.	2	3	3
CGPT	To assess and improve stakeholder communication according to the AIA, review your existing communication processes and materials, align them with the AIA's transparency and accountability requirements, gather feedback from stakeholders, and iterate on your communication strategies based on their input and compliance guidelines.	3	3	1
P10	The AIA stipulates that accuracy should be according to state of the art, this seems very vague, how should I go about achieving state of the art accuracy?			
HGI	The AIA does not provide specific guidance on how to achieve state-of-the-art accuracy for AI systems. However, it does require that high-risk AI systems meet an appropriate level of accuracy, robustness, and cybersecurity in accordance with the generally acknowledged state of the art. This means that providers of high-risk AI systems should use the best available methods and techniques to ensure that their systems are accurate, robust, and secure. To achieve state of the art accuracy it is important to use available sources to gain insight into what accuracies are achievable for a similar project. Then using new techniques and quality data, try to achieve a similar accuracy and document why this accuracy is considered state-of-the-art. Make sure that techniques are updated regularly.			

	Cluster 2 - Compliance	I	C1	C2
SWOAI	You should use the detailed description of the system architecture, data requirements, and assessment of human oversight measures to assess the accuracy of the AI system and ensure it meets the requirements of the AIA. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 93, 7, 11, 6	3	3	3
Llama	The AIA does not provide specific guidance on how to achieve state of the art accuracy. However, providers of high-risk AI systems should ensure that their systems are compliant with the requirements set out in Chapter 2 of the AIA, including the requirements for accuracy and accuracy metrics. Additionally, providers should have a quality management system in place, draw up the technical documentation of the high-risk AI system, and ensure that the system undergoes the relevant conformity assessment procedure prior to its placing on the market or putting into service. These steps can help to ensure that the AI system is as accurate as possible according to the state of the art.	3	3	3
CGPT	Achieving state-of-the-art accuracy in AI systems requires a continuous process of research, development, and benchmarking against the latest advancements in the field. Stay updated with the latest research papers, collaborate with experts, participate in relevant conferences and competitions, and invest in ongoing training and development of your AI models to strive for state-of-the-art accuracy while considering the specific context and requirements of your application.	3	3	2

▼ Cluster 2 - Core

	Cluster 2 - Core	I	C1	C2
C1	Should technical documentation also be written for non-technical people?			
HGI	Not necessarily, the AIA gives a list of information that should be included in the technical documentation, this documentation should be written to that it can be handed to authorities at any time. Some documentation must be shared with users and must therefore be written for non-technical people, but this does not include all technical documentation.			
SWOAI	I don't know Source: aia/AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 143 Source: aia/20230516RES90302.pdf - Page: 20 Source: aia/AIA-COM-Annexes-21-April-21.pdf - Page: 11 Source: aia/cellar e0649735-a372-11eb-9585-01aa75ed71a1.0001.02_DOC_2.pdf - Page: 11 <i>Though not a useful answer, the sources do link to relevant paragraphs.</i>	1	3	1
Llama	Yes, technical documentation should be written for non-technical people. The instructions of use should contain concise and clear information that is easy to understand, and should include illustrative examples to facilitate understanding.	1	2	1
CGPT	Yes, technical documentation should also be written for non-technical people to ensure understanding and transparency in AI systems. This allows for effective communication and accountability.	1	1	1
C2	Does the AIA stipulate that we need someone monitoring the AI-models full-time			

	Cluster 2 - Core	I	C1	C2
HGI	No not necessarily, the AIA stipulates that compliance must be monitored even post-monitoring. This means all interactions with the AI should be logged and analyzed to ensure compliance. The AIA does not stipulate that this must happen real-time, but rather states that a plan must be made to describe how compliance after market-release will be ensured. Which plans specifically work towards compliance is not known at the moment.			
SWOAI	No, the AIA does not stipulate that someone needs to monitor AI-models full-time. Source: aia/HAI_Issue-Brief_The-European-Commissions-Artificial-Intelligence-Act.pdf - Page: 4 Source: aia/20230516RES90302.pdf - Page: 97 Source: aia/AIA-COM-Impact-Assessment-2-21-April.pdf - Page: 30 Source: aia/ETSI-WP52-ETSI-activities-in-the-field-of-AI.pdf - Page: 17	3	3	3
Llama	No, the AIA does not stipulate that someone needs to monitor AI-models full-time. The AIA process includes steps such as pre-acquisition review, initial agency disclosure requirements, comment period, due process challenge period, and renewing AIAs. None of these steps require someone to monitor AI-models full-time. <i>This information is not relevant for monitoring the AI model, but for monitoring the process of AIA compliance.</i>	3	2	1
CGPT	The EU Artificial Intelligence Act (AIA) does not explicitly stipulate that someone needs to monitor AI models full-time. However, it does require that organizations implement appropriate risk management and monitoring measures to ensure compliance with the regulation and address potential risks associated with AI systems. The level of monitoring required will depend on the specific characteristics and risks associated with the AI models in use.	3	3	3
C3	Does the AIA require me to work with encrypted data only?			
HGI	No, the AIA does not mention encrypted data.			
SWOAI	No, the AIA does not require you to work with encrypted data only. Source: aia/AIA-COM-Impact-Assessment-1-21-April.pdf - Page: 7 Source: aia/AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 165 Source: aia/HAI_Issue-Brief_The-European-Commissions-Artificial-Intelligence-Act.pdf - Page: 1 Source: aia/AIA---CZ---General-Approach-25-Nov-22.pdf - Page: 48	3	3	3
Llama	No, the AIA does not require you to work with encrypted data only. The AIA stipulates that actors should be correctly informed about the GDPR and suggests future innovations in the domain of AI and cryptography, such as federated machine learning, differential privacy solutions, homomorphic encryption, secure multi-party computation, and secure hardware implementations. However, it does not require that these solutions be used exclusively. <i>GDPR is actually not mentioned in the AIA.</i>	3	2	1
CGPT	No, the AIA does not require you to work with encrypted data only. However, it emphasizes the importance of data protection and security measures for AI systems.	3	3	3
C4	How should we deal with missing data according to the AIA?			

	Cluster 2 - Core	I	C1	C2
HGI	The AIA stipulates that training, validation and testing data should be subject to data governance practices. This includes identifying data gaps and shortcoming and how to address these. Therefore step 1 is to identify missing data and document this. Since the AIA is all for risk-driven approaches, the next step would be to identify the risks related to this missing data. Then finally, it should be documented which risks are accepted and which risks aren't, for these risks new data should be gathered or the risk should be otherwise mitigated.			
SWOAI	Missing data can be dealt with by data aggregation, data retention, and other operations related to the data before and for the purposes of placing high-risk AI systems on the market or putting them into service. Additionally, risk management systems, post-market monitoring systems, and procedures related to the reporting of serious incidents should be set up, implemented, and maintained. Source: aia/AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 118 Source: aia/AIA-EEESC-Opinion-22-Sept-21.pdf - Page: 9 Source: aia/AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 92, 91	3	3	3
Llama	The AIA does not provide specific guidance on how to deal with missing data. However, it does state that data sets should be relevant, representative, free of errors, and complete. Therefore, it is important to ensure that data sets are as complete as possible and that any missing data is addressed.	3	3	3
CGPT	The AIA does not specifically address how to deal with missing data, so it is not explicitly regulated.	1	2	1
C5	What other data risks besides data privacy should my organization be concerned with?			
HGI	The AIA actually doesn't mention data privacy as a risk for compliance. The AIA especially focuses on data bias. Data should relevant, representative and free of errors. It should also have appropriate statistical properties, with regards to the demographic for which the AI is intended to be used. All this to ensure that data bias is minimal and that accuracy is the same over different demographics. The AIA also stipulates that accepted risks of the system and risks on rights and discrimination are communicated to the user, this means that these risks should also be examined in the data.			
SWOAI	Organizations should be concerned with data security, data accuracy, data integrity, data availability, and data compliance. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 70 Source: aia/cellar e0649735-a372-11eb-9585-01aa75ed71a1.0001.02_DOC_1.pdf - Page: 70 Source: aia/20230516RES90302.pdf - Page: 63 Source: aia/ST-14954-2022-INIT_en.pdf - Page: 142	3	3	2
Llama	Other data risks that organizations should be concerned with include data accuracy, data security, data integrity, data availability, data misuse, data loss, data manipulation, data theft, data exploitation, and data breach. Additionally, organizations should be aware of the potential for unfair business practices, such as those outlined in Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005. <i>Though correct this answer focuses too much on data security and privacy and not enough on data bias.</i>	3	3	1

	Cluster 2 - Core	I	C1	C2
CGPT	Besides data privacy, your organization should be concerned with data security, algorithmic bias, and unintended consequences of AI systems. Data security refers to protecting data from unauthorized access, breaches, or cyberattacks. Algorithmic bias refers to the unfair or discriminatory outcomes that can result from biased data or algorithms. Unintended consequences refer to the potential negative effects or unforeseen outcomes that AI systems may have on individuals or society as a whole.	3	3	1
C6	What does the AIA mean by high-risk AI?			
HGI	The AI Act mentions 8 types of high-risk AI's. 1. Biometric identification and categorisation of natural persons 2. Management and operation of critical infrastructure 3. Education and vocational training 4. Employment, workers management and access to self-employment 5. Access to and enjoyment of essential private services and public services and benefits 6. Law enforcement 7. Migration, asylum and border control management 8. Administration of justice and democratic			
SWOAI	High-risk AI systems are AI systems that could pose a risk to health and safety or fundamental rights if used in accordance with their intended purpose. Source: aia/20230516RES90302.pdf - Page: 29 Source: aia/AIA---CZ---General-Approach-25-Nov-22.pdf - Page: 94 Source: aia/ST-14954-2022-INIT_en.pdf - Page: 94 Source: aia/cellare0649735-a372-11eb-9585-01aa75ed71a1.0001.02_DOC_1.pdf - Page: 47	2	3	1
Llama	The AIA defines high-risk AI systems as those that pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence. High-risk AI systems are subject to specific requirements on logging capabilities and human oversight, and must include a general description of its intended purpose and a detailed description of the key design choices and assumptions made in the development process. Examples of high-risk AI systems include those used for remote biometric identification of natural persons in public spaces for law enforcement.	3	3	1
CGPT	High-risk AI refers to AI systems that have the potential to cause significant harm or impact fundamental rights and include certain sectors such as healthcare, transportation, critical infrastructure, and law enforcement. The AIA aims to regulate these AI systems more strictly to ensure transparency, accountability, and safety.	3	3	1
C7	Does the AIA require an external audit?			
HGI	No the AIA does not require an external audit persé, it is possible to perform a conformity assessment procedure based on internal controls. However, examining the technical documentation is still done by a notified body in some cases.			
SWOAI	The AIA does not require an external audit, but it does require a self-assessment to identify risks related to fairness, justice, bias and inaccuracy. Source: aia/AIA-COM-Impact-Assessment-1-21-April.pdf - Page: 60 Source: aia/AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 8, 70, 100	2	3	2

	Cluster 2 - Core	I	C1	C2
Llama	No, the AIA does not require an external audit. Providers of stand-alone, high-risk AI systems have two options for how to conduct ex-ante conformity assessments: (a) conducting ex-ante conformity assessments based on internal control, or (b) involving a third-party auditor (i.e. a notified body). If the stand-alone, high-risk AI system is fully compliant with the requirements set out in Chapter 2 of Title III of the AIA, then procedure (a) is an option. Otherwise, procedure (b) must be followed.	3	3	3
CGPT	The AIA does not explicitly require an external audit for all AI systems, but it does require some high-risk AI systems to undergo a conformity assessment carried out by a notified body, which can be considered as a form of external scrutiny.	3	3	2
C8	Which documents should be included in the compliance documentation?			
HGI	The following information should be included: - technical documentation - post-market monitoring plan - risk management system - quality management system - user information			
SWOAI	The documents that should be included in the compliance documentation are the technical documentation referred to in Annex IV, any relevant harmonised standards used or any other common specification in relation to which conformity is declared, the name and identification number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued, and an accountability framework setting out the responsibilities of the management and other staff with regard to all aspects listed in Article 18. Source: aia/20230516RES90302.pdf - Page: 20, 18 Source: aia/AIA-CoR-Opinion-2-Dec-21.pdf - Page: 22 Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 54	3	3	3
Llama	The documents that should be included in the compliance documentation are the decisions and other documents issued by the notified bodies where applicable, the EU declaration of conformity referred to in Article 48, and the technical documentation kept under the relevant Union financial services legislation.	2	2	1

	Cluster 2 - Core	I	C1	C2
CGPT	<p>1. AI System Description: Detailed documentation describing the purpose, functionality, and intended use of the AI system.</p> <p>2. Data Collection and Processing Policies: Clear guidelines on data collection, processing, and storage practices, including information on data protection, consent, and security measures.</p> <p>3. Risk Assessment: Comprehensive analysis of potential risks associated with the AI system, including privacy breaches, biases, discrimination, and other adverse impacts.</p> <p>4. Ethical Guidelines: Document outlining the ethical principles and values guiding the development and deployment of the AI system.</p> <p>5. Human Oversight and Control: Description of mechanisms for human intervention, monitoring, and control over the AI system's operations.</p> <p>6. Training Data Description: Documentation on the training data used, including its quality, diversity, and potential biases.</p> <p>7. Accuracy and Robustness Measures: Information on the system's accuracy, performance, and robustness, along with measures taken to mitigate errors and ensure reliability.</p> <p>8. Transparency and Explainability: Documentation on how the system's decisions are made, including algorithms used, interpretability techniques, and model explanations.</p> <p>9. Testing and Validation Processes: Description of testing methodologies, validation procedures, and performance metrics used to assess the AI system's functionality and safety.</p> <p>10. Documentation Maintenance: Plan for documenting updates, modifications, and maintenance processes to ensure ongoing compliance and accountability.</p>	2	3	1
C9	Does the AIA mention metrics that should be used to determine a models risks for rights and discrimination?			
HGI	No, the AIA does not mention specific metrics that should be used to determine a models risks for rights and discrimination, it only states that these risks should be identified and addressed.			
SWOAI	The AIA provides for certain decisions to remain the prerogative of humans, particularly in domains where these decisions have a moral component and legal implications, such as diversity, non-discrimination and fairness. Source: aia/AIA-COM-Impact-Assessment-2-21-April.pdf - Page: 41 Source: aia/AIA-EESC-Opinion-22-Sept-21.pdf - Page: 6, 7, 3	1	3	1
Llama	No, the AIA does not mention any specific metrics that should be used to determine a model's risks for rights and discrimination. However, it does mention the risks of discrimination/manipulation, profiling practices, and automated decision making, as well as the risks of differentiated pricing, financial detriments, filter bubbles, and interference in political processes. Actually, the AIA does not mention those things.	3	1	3
CGPT	Yes, the AIA mentions that high-risk AI systems should undergo an impact assessment, including evaluation of metrics related to potential risks for rights and discrimination.	1	3	3
C10	What does the AIA mean by 'human oversight'?			
HGI	Human oversight means that high-risk AI's must be overseen by a natural person, it should be built into the AI-system by the provider before placement on the market.			

	Cluster 2 - Core	I	C1	C2
SWOAI	Human oversight is the process of ensuring that high-risk AI systems are designed and developed in such a way that they can be effectively overseen by natural persons during the period in which the AI system is in use. It aims to prevent or minimize the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. Human oversight can be ensured through measures such as building it into the AI system by the provider before it is placed on the market or put into service, or by being identified by the provider before placing the high-risk AI system on the market. Source: aia/AIA-COM-Proposal-21-April-21.pdf - Page: 51 Source: aia/cellar e0649735-a372-11eb-9585-01aa75ed71a1.0001.02_DOC_1.pdf - Page: 51 Source: aia/AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 87 Source: aia/AIA-EESC-Opinion-22-Sept-21.pdf - Page: 8	3	3	3
Llama	The AIA defines human oversight as measures that enable individuals to understand the capacities and limitations of a high-risk AI system, remain aware of the potential for automation bias, correctly interpret the system's output, decide not to use the system or disregard its output, and intervene on the system or interrupt it. For high-risk AI systems referred to in point 1(a) of Annex III, the measures must also ensure that no action or decision is taken on the basis of the system's identification unless it has been verified and confirmed by at least two natural persons.	2	2	3
CGPT	'Human oversight' in the EU Artificial Intelligence Act (AIA) refers to the requirement of having human intervention or control to ensure the decisions made by AI systems are accountable, explainable, and aligned with ethical considerations. It emphasizes the need for humans to be able to understand and override AI system decisions when necessary. <i>Though very close, this answer does not highlight the need for human oversight post-release. This sounds more like human oversight during development, but the AIA focuses more on human oversight through monitoring after releasing the model.</i>	2	3	2

▼ Cluster 2 - Process

	Cluster 2 - Process	I	C1	C2
P1	To which extent does my ISO certification help towards AIA compliance?			
HGI	There are many types of ISO certification. ISO/IEC 23053 gives a framework specifically for AI, the specific information is not available for free and therefore not known. However, preparing for ISO certification audits will give organizations an idea of what these audits are like and how to have a system in place so that all the required information can be assessed if needed. This will help with AIA compliance, however the AIA does state requirements that are not specifically mentioned in ISO certification. Especially since most organization achieve quality management or data privacy certificates, which although related do not encompass the entire AIA.			
SWOAI	ISO certification can provide additional support for product conformity assessments by notified bodies, but it is not required to fulfil the requirements of the AIA regulation. Source: AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 164 Source: AIA-COM-Impact-Assessment-1-21-April.pdf - Page: 59, 39, 41	3	3	2

	Cluster 2 - Process	I	C1	C2
Llama	Your ISO certification may help towards AIA compliance to some extent, depending on the requirements set out in Chapter 2 of the AIA. The AIA requires data quality, traceability, technical robustness, and accuracy, which may be addressed by ISO standards. Additionally, the AIA encourages the adoption of voluntary codes of conduct and supports the emergence of complementary, soft governance mechanisms. If your ISO certification meets these requirements, then it may help towards AIA compliance.	3	3	3
CGPT	ISO certification can help demonstrate your commitment to certain standards and processes, but it does not directly address the specific requirements of the EU Artificial Intelligence Act (AIA).	3	3	2
P2	Does GDPR training also include data bias and model bias training?			
HGI	The GDPR has a fairness principle which states that organizations should check the following: 'We have considered how the processing may affect the individuals concerned and can justify any adverse impact.'. Data bias can be seen as a violation of the fairness principle, since it is unjustifiable if a system performs much worse for one demographic than for another. However, this is only a small part of the GDPR and there are many other, more prevalent, ways the fairness principle would not be obeyed. Therefore, it is not likely that data bias is dealt with in a GDPR training in such a way that it prepares employees for AIA compliance relating to data bias.			
SWOAI	Yes, GDPR training includes data bias and model bias training. Source: AIA-COM-Impact-Assessment-2-21-April.pdf - Page: 37 Source: AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 88, 28 Source: 20230516RES90302.pdf - Page: 56	1	1	1
Llama	Yes, GDPR training includes data bias and model bias training. The GDPR transparency rights make it necessary for organizations to be aware of potential biases in their data and algorithms, and to take steps to ensure that these biases are not incorporated into their decision-making processes. The GDPR also requires organizations to be aware of potential proxies and redundant encodings that may lead to discriminatory outcomes.	1	3	2
CGPT	GDPR training primarily focuses on data privacy and protection, but it may not explicitly cover data bias and model bias training.	3	3	1
P3	What are the biggest risks on AIA compliance when data is gathered in-house?			
HGI	The AIA mentions that high quality data is essential for AI systems. Whether gathering data in-house or using external data, the risks remain the same. Data should be relevant, representative and free of errors. It should also have appropriate statistical properties, with regards to the demographic for which the AI is intended to be used. Data risks should be identified especially concerning data bias and any risks towards rights or discrimination should be communicated with the user. This must be ensured whether using external data or gathering the data yourself. An advantage might be that there is more control over the data in-house, however it might also require more work and expertise to gather a high-quality dataset from scratch.			

	Cluster 2 - Process	I	C1	C2
SWOAI	The biggest risks on AIA compliance when data is gathered in-house include legal fees, the need for specialised AI/privacy legal expertise, the need to bring additional data used to achieve compliance with the data quality standards of the AI regulation in line with GDPR standards, and the need to ensure compliance with other regulations such as the GDPR and other privacy laws. Source: AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 165, 91 Source: HAI_Issue-Brief_The-European-Commissions-Artificial-Intelligence-Act.pdf - Page: 4 Source: aia/AIA-COM-Impact-Assessment-1-21-April.pdf - Page: 24	3	3	3
Llama	The biggest risks on AIA compliance when data is gathered in-house include: ensuring accuracy and robustness of the data, ensuring transparency and provision of information, ensuring traceability and documentation of the data, ensuring human oversight of the data, and ensuring data is not used to discriminate against any individuals or groups.	3	3	2
CGPT	The biggest risks on AIA compliance when data is gathered in-house include data quality and bias, data privacy and security, compliance with regulations and standards, lack of expertise and resources, and scalability challenges.	3	3	1
P4	Our organizations uses data from customers, what are some of the biggest risks when aiming for AIA compliance?			
HGI	The AIA mentions that high quality data is essential for AI systems. Whether gathering data in-house or using external data, the risks remain the same. Data should be relevant, representative and free of errors. It should also have appropriate statistical properties, with regards to the demographic for which the AI is intended to be used. Data risks should be identified especially concerning data bias and any risks towards rights or discrimination should be communicated with the user. This must be ensured whether using external data or gathering the data yourself. An advantage of external data might be that there is already a good starting point on which to perform the data analysis, however it might also be harder to fill in data gaps since this requires more data.			
SWOAI	The biggest risks of AIA compliance are that companies may not be able to meet the requirements for high-risk AI systems, such as establishing and maintaining a risk management system, ensuring training, validation, and testing data sets are subject to appropriate data governance and management practices, publishing and updating technical documentation, incorporating logging capabilities, guaranteeing a certain level of transparency, and providing users with relevant information. Additionally, companies may not be able to meet the requirements for ex-ante conformity assessments and ex-post supervision and market surveillance. Source: HAI_Issue-Brief_The-European-Commissions-Artificial-Intelligence-Act.pdf - Page: 4 Source: AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 165, 91 Source: aia/AIA-COM-Impact-Assessment-1-21-April.pdf - Page: 24	3	3	3
Llama	Some of the biggest risks when aiming for AIA compliance include: long-term risks to eroding privacy and human agency in the digital media environment; little to medium degree of intervention for regular digital media use, dependent on service; and the complexity of the system leaving users with little control over their data. Additionally, there is a risk of fundamental rights violations due to AI systems operating outside of the EU legislative scope.	3	3	2

	Cluster 2 - Process	I	C1	C2
CGPT	When aiming for AIA compliance while using customer data, some of the biggest risks include ensuring data privacy and consent, mitigating bias and discrimination in AI models, complying with GDPR requirements, and maintaining customer trust and satisfaction. <i>This answer mentions GDPR compliance, but that is not a necessity for AIA compliance.</i>	3	2	1
P5	We only use ChatGPT and other out of the box AI models, should we still be concerned with the AIA?			
HGI	The AIA mentions 8 types of high-risk AI's. These types mainly focus on areas where the AI is applied rather than the specific AI (except for AI's using biometric). So, if your organization only uses ChatGPT or other external AI's, this still means that the organization must ensure that these tools are AIA compliant if they are applied to one of the high-risk areas.			
SWOAI	The AIA requires that AI systems used for human interaction, such as ChatGPT and other out of the box AI models, must follow transparency rules ensuring that consumers know they are interacting with manipulated content. Source: Notitie BOF 'Amendments to the Artificial Intelligence Act'.pdf - Page: 14 Source: HAI_Issue-Brief_The-European-Commissions-Artificial-Intelligence-Act.pdf - Page: 3, 1 Source: Notitie BOF 'Amendments to the Artificial Intelligence Act'.pdf - Page: 11	3	3	2
Llama	Yes, even if you are only using ChatGPT and other out of the box AI models, you should still be concerned with the potential for AI to lead to discriminatory outcomes. AI models can be used to manipulate public opinion, spread misinformation, and create synthetic media that can deceive the general public. As evidenced by the survey results, a large majority of stakeholders find this to be an important or very important concern. Therefore, it is important to take steps to ensure that AI is used responsibly and ethically.	3	3	3
CGPT	Even if you use out-of-the-box AI models like ChatGPT, you should still be concerned with the AIA as it imposes obligations on both providers and users of AI systems, including ensuring transparency, accountability, and adherence to certain requirements for high-risk AI systems.	3	3	2
P6	What can we do to improve AIA compliance concerning our technical documentation?			
HGI	The AIA lists all the information that must be present in the technical documentation. In short: general description of the system, description of all the elements, an assessment of the human oversight measure, information that is communicated to the user and information around monitoring.			

	Cluster 2 - Process	I	C1	C2
SWOAI	To improve AIA compliance concerning our technical documentation, we should establish and maintain a risk management system, ensure training, validation, and testing data sets are subject to appropriate data governance and management practices, publish and update technical documentation of a high-risk AI system before it is placed on the market or put into service, incorporate logging capabilities to ensure a level of traceability of the AI system's functioning throughout its lifecycle, guarantee a certain level of transparency and provide users with relevant information, and put in place aspects of AI systems and AI components, and notably of foundation models relevant to the compliance and enforcement of this Regulation based on the generally acknowledged state of the art, including as reflected in relevant harmonized standards. Source: AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 143, 145 Source: AIA---CZ---General-Approach-25-Nov-22.pdf - Page: 210 Source: ST-14954-2022-INIT_en.pdf - Page: 210	3	3	3
Llama	To improve AIA compliance concerning technical documentation, applicants should ensure that the documentation is comprehensive and accurate, and that it meets all the requirements of the proposed regulation. Additionally, applicants should consider collaborating with upstream producers to obtain certification of the upstream AI product, which may help to improve the credibility of the documentation. Finally, applicants should consider adopting voluntary codes of conduct that go beyond the requirements set out in the AIA, as this can help to promote post-compliance ethical behaviour.	3	3	2
CGPT	To improve AIA compliance concerning technical documentation, ensure that it includes comprehensive information about the AI system's functionality, limitations, potential risks, and mitigation strategies, following the AIA guidelines and industry best practices.	2	3	1
P7	We currently don't communicate anything about our models with our users, how can we better communicate information with the users for AIA compliance?			
HGI	The AIA mentions a list of information that must be communicated with the users. Some information is easy to start with, like capabilities of the model and its intended purpose. However, some information is harder like performance for different groups of users and any risks to the users' health and safety or fundamental rights.			
SWOAI	The AIA should introduce obligations on users of high-risk AI systems to ensure greater transparency as to how high-risk AI is used, and ensure accountability and redress for uses of AI that pose a potential risk to fundamental rights. This could include informing citizens when they are interacting with an AI system and not a human being, designing AI systems in a transparent and explainable way, providing users with relevant information about the characteristics, capabilities, and limitations of performance of the high-risk AI system, and providing immutable auditable logs of how the AI system has performed in the particular case of the complainant, and available remedies under applicable law. Source: HAI_Issue-Brief_The-European-Commissions-Artificial-Intelligence-Act.pdf - Page: 4 Source: AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 125 Source: Notitie BOF 'Amendments to the Artificial Intelligence Act'.pdf - Page: 11	3	2	3

	Cluster 2 - Process	I	C1	C2
Llama	To comply with AIA requirements, organizations should provide extensive information to the public about the purpose, uses, and implementation of their AI models. This information should include a self-assessment of any potential risks related to fairness, justice, bias, and inaccuracy, as well as a plan for how external researchers can review the system following deployment. Organizations should also provide a comment period for the public to provide feedback on the initial agency disclosure. Finally, organizations should provide a due process challenge period for the public to challenge the agency's decision to deploy an AI model before an agency oversight body or court.	3	3	3
CGPT	To better communicate information with users for AIA compliance, consider implementing clear and transparent communication channels, providing meaningful explanations about the AI system's purpose, its decision-making process, potential biases, and any actions users can take to influence the system's behavior.	2	3	1
P8	Our organization is very small and no one is specialised in compliance, where do we even begin to achieve AIA compliance?			
HGI	A lot of things are still unclear about the AIA, however a lot of things are also stated very clearly. For instance, what should be documented and communicated with users. Start with the things that are clear and within your capabilities, as time passes more information will become available.			
SWOAI	For a small organization, the best way to achieve AIA compliance is to conduct a self-assessment and an ex ante check by national competent authorities responsible for monitoring compliance with the EU voluntary label. Source: AIA-COM-Impact-Assessment-1-21-April.pdf - Page: 25, 87 Source: 5030_robust_and_trustworthy_ai_certification.pdf - Page: 9, 3	3	3	1
Llama	To begin achieving AIA compliance, it is important to understand the five sets of requirements that must be met. These requirements include data, documentation and traceability, provision of information and transparency, human oversight and robustness and accuracy. It is also important to understand the maximum costs of the measures necessary to fulfill each of these requirements. Additionally, it is important to identify which share of these costs would be additional expenditure due to regulatory requirements. Once the requirements and costs are understood, it is important to identify the resources available to the organization to meet the requirements. This may include seeking out legal or technical advice from third parties, relying on harmonized standards, and taking the size of the company into account when setting fees for conformity assessment. Finally, it is important to develop a plan to ensure that the organization is able to meet the AIA compliance requirements. This plan should include steps to ensure that the organization is able to meet the requirements, as well as a timeline for implementation.	3	3	3
CGPT	To begin achieving AIA compliance in a small organization without specialized compliance expertise, start by conducting a thorough assessment of your AI systems, identifying potential risks, and seeking guidance from relevant industry experts or consultants. Prioritize understanding and implementing the AIA's requirements step by step.	3	3	1
P9	We currently have no idea if we communicate with our stakeholders according to the AIA, how should we assess this to make improvements?			

	Cluster 2 - Process	I	C1	C2
HGI	The AIA does not have any specific requirements for in-house communication with stakeholders. The AIA does give requirements for communication with users, governmental organizations and auditors. It's important to prepare a 'compliance package' with all the required information so this can be handed over when necessary. As for communication in-house, AIA compliance requirements should be communicated with the entire chain of development to ensure that the compliance is achieved at every development step.			
SWOAI	Organizations should provide general information on whether AI is used in their products and services, and provide information on what AI is, how AI is used in decision-making in relation to consumers, what are its benefits, why the organization has decided to use AI, and how the organization has taken steps to mitigate risks. Source: AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 89 Source: AIA-EESC-Opinion-22-Sept-21.pdf - Page: 9 Source: AIA-COM-Impact-Assessment-2-21-April.pdf - Page: 21 Source: AIA—CZ—General-Approach-25-Nov-22.pdf - Page: 4	3	2	1
Llama	To assess how well the stakeholders are being communicated with according to the AIA, it is important to review the feedback from the stakeholders. This includes reviewing the comments and position papers submitted through the EU Survey website, the results of the workshops and events, and the comments from the Regulatory Scrutiny Board. Additionally, it is important to review the key requirements set out in the HLEG ethics guidelines for Trustworthy AI and the Assessment List for Trustworthy Artificial Intelligence (ALTAI). By reviewing this feedback, it is possible to identify areas where communication could be improved and make changes accordingly.	2	3	3
CGPT	To assess and improve stakeholder communication according to the AIA, review your existing communication processes and materials, align them with the AIA's transparency and accountability requirements, gather feedback from stakeholders, and iterate on your communication strategies based on their input and compliance guidelines.	3	3	1
P10	The AIA stipulates that accuracy should be according to state of the art, this seems very vague, how should I go about achieving state of the art accuracy?			
HGI	The AIA does not provide specific guidance on how to achieve state-of-the-art accuracy for AI systems. However, it does require that high-risk AI systems meet an appropriate level of accuracy, robustness, and cybersecurity in accordance with the generally acknowledged state of the art. This means that providers of high-risk AI systems should use the best available methods and techniques to ensure that their systems are accurate, robust, and secure. To achieve state of the art accuracy it is important to use available sources to gain insight into what accuracies are achievable for a similar project. Then using new techniques and quality data, try to achieve a similar accuracy and document why this accuracy is considered state-of-the-art. Make sure that techniques are updated regularly.			

	Cluster 2 - Process	I	C1	C2
SWOAI	To achieve state of the art accuracy, activities such as familiarizing oneself with accuracy requirements, calculating an established accuracy metric for the task, writing an explanation of the accuracy metric, procuring external test datasets and calculating additional required metrics should be undertaken. Source: AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 131 Source: AIA---COM---Draft-Standardisation-Request-5-December-2022.pdf - Page: 12 Source: AIA-COM-Impact-Assessment-3-21-April.pdf - Page: 132 Source: AIA-COM-Impact-Assessment-2-21-April.pdf - Page: 31	3	3	3
Llama	To achieve state of the art accuracy, it is important to understand the specific requirements of the AIA and the context in which the AI system is being used. This includes understanding the data quality requirements, the technical robustness requirements, and the accuracy requirements. Additionally, it is important to understand the specific goals of the AI system and the environment in which it will be used. This will help to ensure that the AI system is designed and implemented in a way that meets the accuracy requirements of the AIA. Additionally, it is important to use the most up-to-date technologies and techniques to ensure that the AI system is as accurate as possible. Finally, it is important to use appropriate testing and validation methods to ensure that the AI system is performing as expected.	3	3	3
CGPT	Achieving state-of-the-art accuracy in AI systems requires a continuous process of research, development, and benchmarking against the latest advancements in the field. Stay updated with the latest research papers, collaborate with experts, participate in relevant conferences and competitions, and invest in ongoing training and development of your AI models to strive for state-of-the-art accuracy while considering the specific context and requirements of your application.	3	3	2

▼ Summary of all Scores

Cluster 1 - core

Model	Metric	S1	S2	S3	S4	S5	S6
SWOAI	I	1	3	3	1	1	3
SWOAI	C1	2	3	3	3	1	3
SWOAI	C2	1	1	3	2	1	1
Llama	I	1	1	2	2	3	3
Llama	C1	3	3	1	3	3	3
Llama	C2	2	1	3	1	2	2
CGPT	I	1	3	3	1	3	3
CGPT	C1	1	3	3	2	3	3
CGPT	C2	1	3	3	1	1	1

Cluster 1 - process

Model	Metric	S1	S2	S3	S4	S5	S6
SWOAI	I	3	3	2	3	1	3
SWOAI	C1	2	3	3	3	2	3
SWOAI	C2	2	1	1	1	1	2
Llama	I	3	1	3	3	3	3
Llama	C1	2	3	3	3	3	3
Llama	C2	2	1	2	2	2	3

CGPT	I	3	3	3	3	3	2
CGPT	C1	3	3	3	2	3	3
CGPT	C2	2	1	1	1	2	1

Cluster 2 - core


Model	Metric	S1	S2	S3	S4	S5	S6
SWOAI	I	1	3	3	3	3	2
SWOAI	C1	3	3	3	3	3	3
SWOAI	C2	1	3	3	3	2	1
Llama	I	1	3	3	3	3	3
Llama	C1	2	2	2	3	3	3
Llama	C2	1	1	1	3	1	1
CGPT	I	1	3	3	1	3	3
CGPT	C1	1	3	3	2	3	3
CGPT	C2	1	3	3	1	1	1

Cluster 2 - process

Model	Metric	S1	S2	S3	S4	S5	S6
SWOAI	I	3	1	3	3	3	3
SWOAI	C1	3	1	3	3	3	3
SWOAI	C2	2	1	3	3	2	3
Llama	I	3	1	3	3	3	3
Llama	C1	3	3	3	3	3	3
Llama	C2	3	2	2	2	3	2
CGPT	I	3	3	3	3	3	2
CGPT	C1	3	3	3	2	3	3
CGPT	C2	2	1	1	1	2	1

Appendix C - Justification LLM Answers


The following contains the justification for the answers given on the testset.

 Information from the AIA will be represented in a callout.

1. Should technical documentation also be written for non-technical people?

Not necessarily, the AIA gives a list of information that should be included in the technical documentation, this documentation should be written to that it can be handed to authorities at any time. Some documentation must be shared with users and must therefore be written for non-technical people, but this does not include all technical documentation.

→ Reading this my organization would decide not to write all technical documentation for non-technical people.

 To address the opacity that may make certain AI systems incomprehensible to or too complex for natural persons, a certain degree of transparency should be required for high-risk AI systems. Users should be able to interpret the system output and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate.



Having information on how high-risk AI systems have been developed and how they perform throughout their lifecycle is essential to verify compliance with the requirements under this Regulation. This requires keeping records and the availability of a technical documentation, containing information which is necessary to assess the compliance of the AI system with the relevant requirements. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk management system. The technical documentation should be kept up to date.



1. The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date.

The technical documentation shall be drawn up in such a way to demonstrate that the high-risk AI system complies with the requirements set out in this Chapter and provide national competent authorities and notified bodies with all the necessary information to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV.

2. Where a high-risk AI system related to a product, to which the legal acts listed in Annex II, section A apply, is placed on the market or put into service one single technical documentation shall be drawn up containing all the information set out in Annex IV as well as the information required under those legal acts.

3. The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend Annex IV where necessary to ensure that, in the light of technical progress, the technical documentation provides all the necessary information to assess the compliance of the system with the requirements set out in this Chapter.

2. Does the AIA stipulate that we need someone monitoring the AI-models full-time?

No not necessarily, the AIA stipulates that compliance must be monitored even post-monitoring. This means all interactions with the AI should be logged and analyzed to ensure compliance. The AIA does not stipulate that this must happen real-time, but rather states that a plan must be made to describe how compliance after market-release will be ensured. Which plans specifically work towards compliance is not known at the moment.

– Reading this my organization would not dedicate someone full-time to monitor the systems.



Providers shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system.

1. The post-market monitoring system shall actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.

2. The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV.



In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the design and development process or can take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. This system is also key to ensure that the possible risks emerging from AI systems which continue to 'learn' after being placed on the market or put into service can be more efficiently and timely addressed.



Given the nature of AI systems and the risks to safety and fundamental rights possibly associated with their use, including as regard the need to ensure proper monitoring of the performance of an AI system in a real-life setting, it is appropriate to set specific responsibilities for users. Users should in particular use high-risk AI systems in accordance with the instructions of use and certain other obligations should be provided for with regard to monitoring of the functioning of the AI systems and with regard to record-keeping, as appropriate.

3. Does the AIA require me to work with encrypted data only?

No, the AIA does not mention encrypted data.

→ Reading this my organization would not be worried about using encrypted data to achieve AIA compliance.

4. How should we deal with missing data according to the AIA?

The AIA stipulates that training, validation and testing data should be subject to data governance practices. This includes identifying data gaps and shortcoming and how to address these. Therefore step 1 is to identify missing data and document this. Since the AIA is all for risk-driven approaches, the next step would be to identify the risks related to this missing data. Then finally, it should be documented which risks are accepted and which risks aren't, for these risks new data should be gathered or the risk should be otherwise mitigated.

→ Reading this my organization would identify missing data and identify related risks, then determine how to mitigate the risks and document this information.



1. Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular,

1. (a) the relevant design choices;
2. (b) data collection;
3. (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;
4. (d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;
5. (e) a prior assessment of the availability, quantity and suitability of the data sets that are needed;
6. (f) examination in view of possible biases;
7. (g) **the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.**

5. What other data risks besides data privacy should my organization be concerned with?

The AIA actually doesn't mention data privacy as a risk for compliance. The AIA especially focuses on data bias. Data should be relevant, representative and free of errors. It should also have appropriate statistical properties, with regards to the demographic for which the AI is intended to be used. All this to ensure that data bias is minimal and that accuracy is the same over different demographics. The AIA also stipulates that accepted risks of the system and risks on rights and discrimination are communicated to the user, this means that these risks should also be examined in the data.

→ Reading this my organization would also be concerned with data relevance, representativeness, errors and statistical properties with regards to the demographics.



High data quality is essential for the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become the source of discrimination prohibited by Union law. High quality training, validation and testing data sets require the implementation of appropriate data governance and management practices. Training, validation and testing data sets should be sufficiently relevant, representative and free of errors and complete in view of the intended purpose of the system. They should also have the appropriate statistical properties, including as regards the persons or groups of persons on which the high-risk AI system is intended to be used. In particular, training, validation and testing data sets should take into account, to the extent required in the light of their intended purpose, the features, characteristics or elements that are particular to the specific geographical, behavioural or functional setting or context within which the AI system is intended to be used. In order to protect the right of others from the discrimination that might result from the bias in AI systems, the providers should be able to process also special categories of personal data, as a matter of substantial public interest, in order to ensure the bias monitoring, detection and correction in relation to high-risk AI systems

6. What does the AIA mean by high-risk AI?

The AI Act mentions 8 types of high-risk AI's.

1. Biometric identification and categorisation of natural persons
2. Management and operation of critical infrastructure
3. Education and vocational training

4. Employment, workers management and access to self-employment
 5. Access to and enjoyment of essential private services and public services and benefits
 6. Law enforcement
 7. Migration, asylum and border control management
 8. Administration of justice and democratic
- Reading this my organization would conclude that there are 8 conditions that make an AI a high-risk AI.



Biometric identification and categorisation of natural persons:

(a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;

2. Management and operation of critical infrastructure:

(a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.

1. Education and vocational training:

a. (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;

b. (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.

2. Employment, workers management and access to self-employment:

a. (a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;

b. (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.

3. Access to and enjoyment of essential private services and public services and benefits:

a. (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;

b. (b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use;

c. (c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.

4. Law enforcement:

a. (a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;

b. (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

(c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);

1. (d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;

2. (e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;

3. (f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;

4. (g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.

5. Migration, asylum and border control management:

a. (a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

- b. (b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;
 - c. (c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;
 - d. (d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.
6. Administration of justice and democratic processes:
- (a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

7. Does the AIA require an external audit?

No the AIA does require an external audit persé, it is possible to perform a conformity assessment procedure based on internal controls. However, examining the technical documentation is still done by a notified body in some cases. When specifically is not clear at this point.

→ Reading this my organization would examine if an external audit is necessary in our situation.



CONFORMITY ASSESSMENT PROCEDURE BASED ON INTERNAL CONTROL

1. The conformity assessment procedure based on internal control is the conformity assessment procedure based on points 2 to 4.
2. The provider verifies that the established quality management system is in compliance with the requirements of Article 17.
3. The provider examines the information contained in the technical documentation in order to assess the compliance of the AI system with the relevant essential requirements set out in Title III, Chapter 2.
4. The provider also verifies that the design and development process of the AI system and its post-market monitoring as referred to in Article 61 is consistent with the technical documentation.

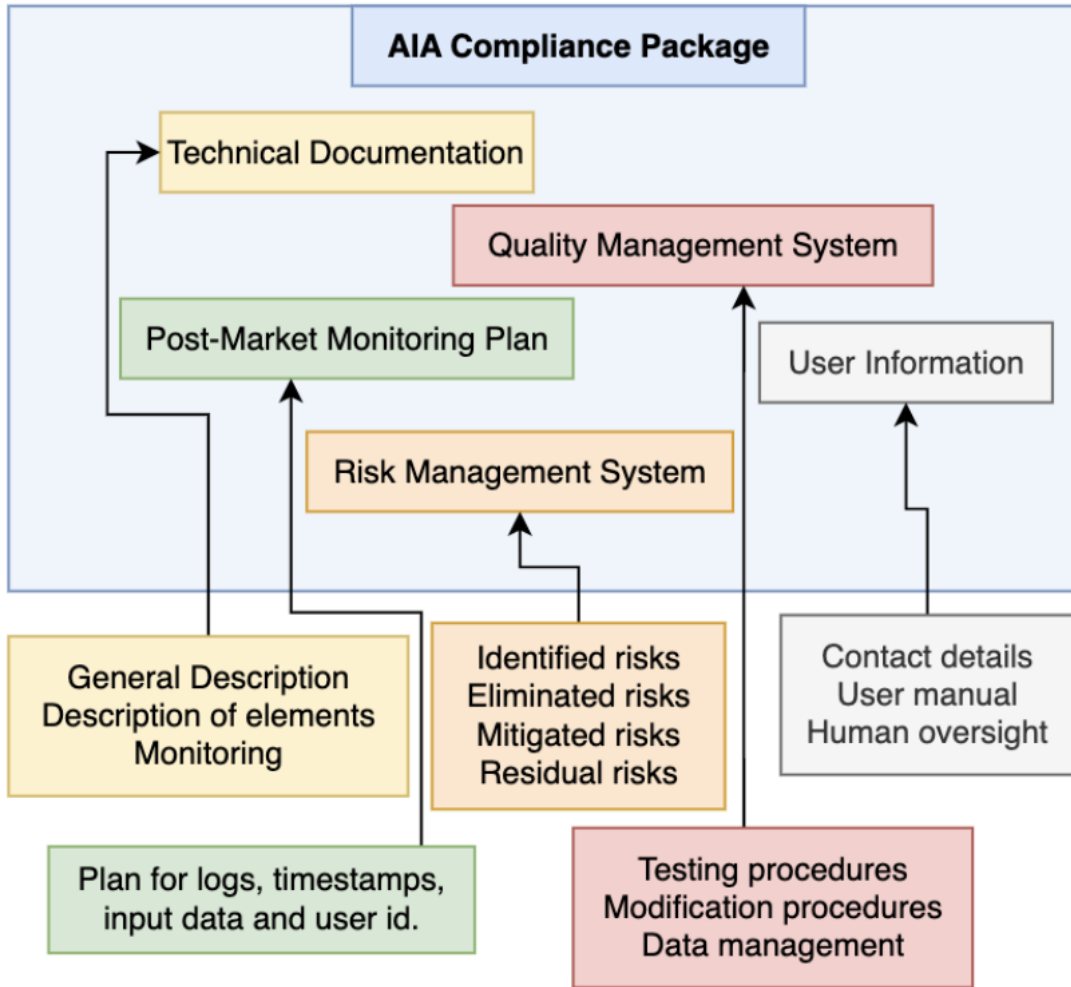


In examining the technical documentation, the notified body may require that the provider supplies further evidence or carries out further tests so as to enable a proper assessment of conformity of the AI system with the requirements set out in Title III, Chapter 2. Whenever the notified body is not satisfied with the tests carried out by the provider, the notified body shall directly carry out adequate tests, as appropriate.

Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the notified body shall also be granted access to the source code of the AI system.

The decision shall be notified to the provider or its authorised representative. The notification shall contain the conclusions of the assessment of the technical documentation and the reasoned assessment decision.

8. Which documents should be included in the compliance documentation?



→ Reading this my organization would prepare the 5 documents as shown.

9. Does the AIA mention metrics that should be used to determine a models risks for rights and discrimination?

No, the AIA does not mention specific metrics that should be used to determine a models risks for rights and discrimination, it only states that these risks should be identified and addressed.

→ Reading this my organization would investigate what metrics can be used.

💡 To address the opacity that may make certain AI systems incomprehensible to or too complex for natural persons, a certain degree of transparency should be required for high-risk AI systems. Users should be able to interpret the system output and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate.

10. What does the AIA mean by 'human oversight'?

Human oversight means that high-risk AI's must be overseen by a natural person, it should be built into the AI-system by the provider before placement on the market.

→ Reading this my organization would understand that the AI must be overseen by a natural person.



1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.
2. Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular when such risks persist notwithstanding the application of other requirements set out in this Chapter.
3. Human oversight shall be ensured through either one or all of the following measures:
 1. (a) identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service;
 2. (b) identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user.

Practical:

To answer these questions, more external sources are used.



Information from or links to sources are placed in the callout.

1. To which extent does my ISO certification help towards AIA compliance?

There are many types of ISO certification. ISO/IEC 23053 gives a framework specifically for AI, the specific information is not available for free and therefore not known. However, preparing for ISO certification audits will give organizations an idea of what these audits are like and how to have a system in place so that all the required information can be assessed if needed. This will help with AIA compliance, however the AIA does state requirements that are not specifically mentioned in ISO certification. Especially since most organization achieve quality management or data privacy certificates, which although related do not encompass the entire AIA.

→ Reading this my organization would examine which ISO certificates are currently obtained and if there is overlap between these and the AIA.



<https://www.iso.org/standard/74438.html>

2. Does GDPR training also include data bias and model bias training?

The GDPR has a fairness principle which states that organizations should check the following: 'We have considered how the processing may affect the individuals concerned and can justify any adverse impact.'. Data bias can be seen as a violation of the fairness principle, since it is unjustifiable if a system performs much worse for one demographic than for another. However, this is only a small part of the GDPR and there are many other, more prevalent, ways the fairness principle would not be obeyed. Therefore, it is not likely that data bias is dealt with in a GDPR training in such a way that it prepares employees for AIA compliance relating to data bias.

→ Reading this my organization would understand that more training is needed on data bias other than GDPR training.



<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/lawfulness-fairness-and-transparency/>

3. What are the biggest risks on AIA compliance when data is gathered in-house?

The AIA mentions that high quality data is essential for AI systems. Whether gathering data in-house or using external data, the risks remain the same. Data should be relevant, representative and free of errors. It should also have appropriate statistical properties, with regards to the demographic for which the AI is intended to be used. Data risks should be identified especially concerning data bias and any risks towards rights or discrimination should be communicated with the user. This must be ensured whether using external data or gathering the data yourself. An advantage might be that there is more control over the data in-house, however it might also require more work and expertise to gather a high-quality dataset from scratch.

→ Reading this my organization would understand that the AIA does not mention specific risks when gathering data in-house.



See question 5 from the substantive questions.

4. Our organizations uses data from customers, what are some of the biggest risks when aiming for AIA compliance?

The AIA mentions that high quality data is essential for AI systems. Whether gathering data in-house or using external data, the risks remain the same. Data should be relevant, representative and free of errors. It should also have appropriate statistical properties, with regards to the demographic for which the AI is intended to be used. Data risks should be identified especially concerning data bias and any risks towards rights or discrimination should be communicated with the user. This must be ensured whether using external data or gathering the data yourself. An advantage of external data might be that there is already a good starting point on which to perform the data analysis, however it might also be harder to fill in data gaps since this requires more data.

→ Reading this my organization would understand that the AIA does not mention specific risks when gathering external data.



See question 5 from the substantive questions.

5. We only use ChatGPT and other out of the box AI models, should we still be concerned with the AIA?

The AIA mentions 8 types of high-risk AI's. These types mainly focus on areas where the AI is applied rather than the specific AI (except for AI's using biometric). So, if your organization only uses ChatGPT or other external AI's, this still means that the organization must ensure that these tools are AIA compliant if they are applied to one of the high-risk areas.

→ Reading this my organization would understand that we must examine the 8 areas to see if we must comply with the AIA.



See question 6 from the substantive questions.

6. What can we do to improve AIA compliance concerning our technical documentation?

The AIA lists all the information that must be present in the technical documentation. In short: general description of the system, description of all the elements, an assessment of the human oversight measure, information that is communicated to the user and information around monitoring.

→ Reading this my organization would use the given checklist to check if we can improve technical documentation.



Summarised:

- **Technical documentation:** document how the system is developed, including general characteristics, capabilities and limitations, algorithms, data, training and testing processes and relevant risk management system. Must be done before placement on the market. Must contain the following:
 - **General description of AI systems**
 - Intended person, persons developing, date and version
 - How the AI system interacts with hardware or software not part of the system itself
 - Versions of software and requirements related to version update
 - Description of forms where the AI is placed on the market.
 - Description of hardware.
 - If the AI is a component of products, internal layout of those products.
 - User-informed, instructions of use for the user and installation.
 - **Description of the elements of the AI system:**
 - methods and steps performed for the development of the system including pre-trained systems and tools by third parties.
 - Design specifications of the system, general logic. Key design choices including rationale and assumptions made, also with regard to persons of intended use. Classification choices, and the relevance of different parameters. Decisions about trade-offs made.
 - Description of the system architecture, how are software components build, computational resources used to develop the AI system.
 - Data requirements describing training methodologies and techniques, training data sets used. How data was obtained and cleaned.
 - **Assessment of human oversight measures and technical measures to facilitate the interpretation of the output.**
 - Description of pre-determined changes to the system and solutions adopted to ensure continuous compliance.
 - Validation and testing procedures used, metrics to measure accuracy, robustness, cybersecurity and compliance.
 - Description of risk management system.
 - Description of change made to the system throughout the lifecycle.
 - List of standards applied.
 - Copy of the EU declaration of conformity.
 - Description of the system to evaluate the performance in the post-market phase, post-market monitoring plan.
 - Information about monitoring, functioning and control of the system, capabilities and limitations in performance. Foreseeable unintended outcomes and sources of risks to health and safety, fundamental rights and discrimination.

7. We currently don't communicate anything about our models with our users, how can we better communicate information with the users for AIA compliance?

The AIA mentions a list of information that must be communicated with the users. Some information is easy to start with, like capabilities of the model and its intended purpose. However, some information is harder like performance for different groups of users and any risks to the users' health and safety or fundamental rights.

→ Reading this my organization would use the given list to communicate to users.



Summarised:

- Identity and contact details of the provider.
- Characteristics, capabilities and limitations or performance.
 - Intended purpose
 - Level of accuracy robustness and cybersecurity
 - Anything that may lead to risks to health and safety or fundamental rights
 - Performance for group of users
 - Specifications for input data
- Changes and performance since initial release
- Human oversight measures including technical measures which facilitate the interpretation of the outputs by users.
- The expected lifetime of the system and maintenance and care measures.

8. Our organization is very small and no one is specialised in compliance, where do we even begin to achieve AIA compliance?

A lot of things are still unclear about the AIA, however a lot of things are also stated very clearly. For instance, what should be documented and communicated with users. Start with the things that are clear and within your capabilities, as time passes more information will become available.

→ Using this my organization would start to identify requirements that are within our capabilities.

9. We currently have no idea if we communicate with our stakeholders according to the AIA, how should we assess this to make improvements?

The AIA does not have any specific requirements for in-house communication with stakeholders. The AIA does give requirements for communication with users, governmental organizations and auditors. It's important to prepare a 'compliance package' with all the required information so this can be handed over when necessary. As for communication in-house, AIA compliance requirements should be communicated with the entire chain of development to ensure that the compliance is achieved at every development step.

→ Reading this my organization would ensure that we prepare a compliance package and that compliance requirements are communicated throughout the development chain.

10. The AIA stipulates that accuracy should be according to state of the art, this seems very vague, how should I go about achieving state of the art accuracy?

The AIA does not provide specific guidance on how to achieve state-of-the-art accuracy for AI systems. However, it does require that high-risk AI systems meet an appropriate level of accuracy, robustness, and cybersecurity in accordance with the generally acknowledged state of the art. This means that providers of high-risk AI systems should use the best available methods and techniques to ensure that their systems are accurate, robust, and secure. To achieve state of the art accuracy it is important to use available sources to gain insight into what accuracies are achievable for a similar project. Then using new techniques and quality data, try to achieve a similar accuracy and document why this accuracy is considered state-of-the-art. Make sure that techniques are updated regularly.

→ Reading this my organization would start to examine what accuracies have been achieved for similar projects.



Summarised:

- **Accuracy:** systems should perform consistently and meet an appropriate level of accuracy in accordance with state of the art. The accuracy must be communicated with the user.