ForHumanity is a US 501(c)(3) tax-exempt public charity and our mission is to *examine and analyze downside risk associated with the ubiquitous advance of AI, algorithmic and autonomous systems and where possible to engage in risk mitigation to maximize the benefits of these systems… ForHumanity*

Risk management purpose

Given, ForHumanity's purpose is to mitigate downside risks posed by AI, algorithmic and autonomous systems to humans. Organizations will find themselves minimizing risk exposure (of socio-technical systems), when they maximize risk mitigation for humans, society and environment.

One of the clear ways to mitigate risks is to implement and operationalize a robust & agile Risk Management framework. Our risk management framework is foundational to Independent Audit of AI Systems.

Risk management includes identification, evaluation and prioritization of risks followed by a coordinated approach to minimize the adverse impacts contributed by such risks to individuals, society and environment.

In FH context, Risk management will enable compliance with audit criteria and provide a sustainable method to prevent, detect and respond to emergent risks.

Risk management adequacy in context of Independent Audit of AI Systems (IAAIS)

Risk management good practice, as defined in the FH Audit, is based first on ISO31000 principles, as illustrated below in this document. Domain-specific risk management approaches; perhaps a security-centric assessment, a privacy-centric risk assessment, a code quality focused approach, or examination of alignment with a code of ethics, all have a part to play, but what part of the whole risk management picture do they address?

FH Audit criteria, respecting requirements in the new EU AI Regulation, cover all key risk and control domains either with specific criteria or in supporting guidance for auditors, and can be supplemented, as appropriate, to account for local context and an organization's location in the AI supply chain. Recognising that an increasingly large proportion of AI implementation will involve incorporating one or more trained models into pre-existing or newly developed products and processes.

Understanding risk levels of AI, algorithmic or autonomous systems

The risks we are measuring are the impacts to people from all AI, algorithmic or autonomous systems (AAA Systems). In terms of hierarchy, we want internal and external risk assessors to rank or consider the severity and likelihood of each of these risks. Risk levels of AI, algorithmic or autonomous systems are guided by the EU AI act and FH intends to expand on them as global guidelines or regulations evolve. The risk levels of AAA Systems are classified into four. They are (1) Prohibited AAA Systems, (2) High risk AAA Systems, (3) Moderate risk AAA Systems and (4) Low risk AAA Systems.

The approach towards determining the AAA systems that require a risk management mechanism is detailed below:

Step 1: Is it Prohibited by law

The primary step towards examining AAA systems is to understand if the systems or their nature or components have a high negative impact on health, wellbeing, safety and/ or fundamental rights and freedom of natural persons and is prohibited by regulation. For instance, the EU AI Act prohibits certain AAA systems.

Essentially, Step 1 refers to the Relevant Legal Framework applicable to each system. Many system owners will have to consider multiple jurisdictions and relative prohibitions for each jurisdiction as applicable to their AAA System.

Step 2: Is it Low risk and excluded from independent audit

Determine if the AAA System may be excluded from required compliance with ForHumanity's Independent Audit of AI Systems. Below you will find a filter for AAA Systems. This filter, if passed through successfully will serve as an adequate mechanism for documenting and assuring the system is Low Risk - through self-assessment. If an entity was interested in verification - Low Risk determinations could also be assured by an Independent Auditor. ForHumanity's mission is to identify Low Risk AAA Systems alleviating compliance burden and efficiently allocate risk mitigation and assurance resources. However the assurance of a AAA System being Low Risk may be a sales and marketing tool worthy of an investment in an independent audit using the criteria below.

In most cases, a determination of Low Risk for a AAA System will not relieve entities of the potential risk of non-compliance with the law. Therefore entities will be encouraged to seek legal counsel accordingly. ForHumanity will endeavor to have these exclusions become law, but those decisions are beyond our remit. The best we can do is advise.

Refer approach to assessing low risk AAA - Identifying Low Risk AI, Algorithmic and Autonomous Systems

Step 3: Risk management consideration for all the remaining AAA systems

Risk management considerations for the remaining AAA systems are the focus of the FH Risk management guidelines.

Step 4: If required, Report to regulators as per relevant legal frameworks after risk mitigation

Reporting to the regulators based on the requirements as per **Relevant Legal Frameworks.** This requirement may exist even if the organizations are mitigating the risks and are progressing towards gaining FH certification. FH Certification does not absolve of any regulatory responsibilities organizations may have based on the **Relevant Legal Frameworks.**

The level of risks from a personal perspective is generally considered using severity and likelihood related to the risk impact. Organizations shall consider Diverse Inputs and Multi Stakeholder Feedback in the process of determining the scale for risk severity and likelihood and risk levels at their intersections. Thereby, the organizations are able to compile risk inputs cumulatively for the AAA systems to determine the risk level of such systems.

It is pertinent to note that the risk severity may change based on cumulative impact for people, society and the environment. A single instance of an outcome is a lower total risk than hundreds of instances of the same outcome. The organization shall take an informed decision on whether a named AI, algorithmic or autonomous system is a high risk, moderate risk or low risk as the case may be.

- Prohibited AAA Systems are those AAA Systems whose use is considered unacceptable as explicitly referred to in regulations. For instance, Prohibited AAA systems in the context of EU AI act are those that are contravening Union values, for instance by violating fundamental rights (listed under Title II of EU AI Act or similar jurisdictional legal decisions)
- High risk AAA Systems are those which have a higher potential of impacting on health, wellbeing, safety and/ or fundamental rights and freedom of natural persons. These could get classified based on regulatory requirements as per **Relevant Legal Frameworks** and based on risks posed by such AAA systems. For instance the EU AI Act provides the following types of AAA systems as high risk including Innovative Technology, Denial of Service, Large-scale profiling, Presence of Biometric Data, Genetic Data, Data Matching, Invisible Processing, Tracking, Targeting of Children or otherwise vulnerable populations and Risk of physical harm.

- Moderate risk AAA Systems are those which have a moderate potential of impacting health, safety or fundamental rights of natural persons.
- Low risk AAA Systems are those which have negligible or very low impact on health, wellbeing, safety and/ or fundamental rights and freedom of natural persons and likely should be excluded from ForHumanity governance, oversight or accountability frameworks

FH Risk Management guidance is best suited for high risk and moderate risks AAA Systems. This approach stems from 2 critical premises. They are:

1. Focus on high and moderate risk AAA Systems.
2. Eliminating low risk AAA systems from the certification process. FH certifications do not mandate risk management process adoption for low risk AAA Systems.

Value of Eliminating Low Risk systems

Robust risk management is one of the cornerstones of building successful systems that benefit most people. This work is imperative in order to classify systems into the risk categories listed above. The first, **Low-Risk** processing, is a vital endeavor. We operate in a world of limited resources. Therefore, we must concentrate our risk mitigation resources on the riskiest of systems. Furthermore, it means we must calibrate and scale down our resources to AAA Systems which have limited or insignificant risk to humans. Resource allocation is critical to maximizing benefits to humanity and excluding Low-Risk systems achieves optimal resource allocation.

Additionally, many of these Low Risk endeavors will be in the hands of small and medium-sized enterprises (SMEs) who may also be resource-challenged to meet the demands of compliance. Audit compliance, while meaningful, is also difficult. It is incumbent on this process to skillfully identify where compliance is valuable to the system and multistakeholders, which means two things: 1) excluding systems where audit compliance would not reduce risk and only introduce compliance burden 2) classify remaining systems into categories of risk which help identify the amount of compliance and mitigations that may be necessary for beneficial operations. Scaling the burden of compliance based upon the overall risk is the best way to aid resource-challenged entities. However, a **High Risk** system is higher risk when operated by an SME that does not possess the same risk management resources as a large organization. Therefore, overall system risk must be the deciding factor and that further highlights the value of ForHumanity's Risk Management framework and specifically the Algorithm Risk Assessment (described below).

Beyond Low Risk Systems

AAA Systems that have meaningful impacts to humans will always be a risky endeavor. It should be treated with the highest regards and entities engaging in this type of processing should desire audit compliance and the maximum mitigation of risk. Once **Low-Risk** processing is calibrated and the efforts are scaled down, the remaining systems (High and Moderate Risk) all require risk mitigation in order to proceed to an operational phase. There are both legal and ethical reasons to engage in comprehensive risk mitigation and third-party independent audit. Third-party Independent Audit is the highest form of compliance and systematic accountability regarding risk mitigation.

The ARA report is the first and most critical step towards managing risk. Identifying risk must occur before it can be examined, analyzed and ideally mitigated. However, one of the greatest ethical failures in system development is to rely upon a small group of similar individuals. Therefore, the ARA report requires to include Diverse Inputs and Multi Stakeholder Feedback in order to fairly and comprehensively identify the severity and likelihood of risks to individuals, nature or society-at-large .

High Risk Systems and disclosure to regulatory authorities

The high-risk processing that remains high-risk after mitigation efforts must consider the Relevant Legal Framework and determine if consultation with Authorities is required.. The initial phase of the ARA report is the first step in that process. Failure to engage in a meaningful and considered risk input process will subject the entity to risk blindspots, these blindspots become mission-critical when the entity fails to determine that the system contains High Risks.

FH Approach to Risk Management

ForHumanity's approach to risk management is centered on Ethics, Bias Privacy, Trust and Cybersecurity. We have wrapped those pillars with a risk management framework that is: ethical, human-centric, accountable, governable, overseeable, transparent, documentable, proveable, evidence-based, and independently auditable. Here we summarize priorities we considered while developing a comprehensive risk management framework.

Human-centric, Ethical and FAIR	**Actionable, Operational and ACCOUNTABLE**	**Auditable, Certain and TRANSPARENT**
Privacy-by-design	Cybersecure-by-design	Auditable-by-design
Accessible-by-design	Objectivity/Governance/ Oversight	Pre-production evidence (Validity, Accuracy and ground truth)
Data Quality/	Data Control	Disclosure

Representativeness		
Active Bias mitigation	Controllability of autonomous systems	Third-party independent audit on entire process
Cybersecurity-by-design	Post-market monitoring	
Ethics-by-design		
Ethical oversight		
Explainability		

When organizations ensure that above concepts are **always** considered and implemented to the highest standard at every step of the design, development and deployment process, then they are managing downside risks "by-design".

Baseline principles for the FH Risk Management framework

The primary principle of the FH Risk Management framework is Human Centric Risk Management for AI, algorithmic or autonomous systems. This principle enables organizations to expand their considerations (Flexible, Risk based, Outcome based and Cost effective) beyond function, operation and protection for entities and consider impacts and risks directly to human beings (human centric). A human-centric Risk Management encompasses an ethical, fair, actionable, operational, accountable, auditable, certain and transparent approach which not only allows for robust mitigation but also helps achieve the maximum benefit from these systems. There are 4 key sub-principles for Human Centric Risk Management. They are:

1. **Risks as seen from Human impact perspective:** The Socio-Technical nature of the Artificial Intelligence systems requires consideration of risk from the perspective of impact to humans, society and the environment. This should cover risks associated with Bias, Cybersecurity, Ethics, Privacy and Trust. (Refer section on Understanding Risks from the context of AI, algorithmic and autonomous systems)

2. **Risks gathered from sufficiently diverse and multidisciplinary feedback**: The nature of a socio-technical system is to have embedded human ethics. Most design and development teams are siloed, unaware, untrained and ill equipped to handle instances of Ethical Choice leading to significant unmitigated risks. Risks to humans need to be gathered through Diverse Inputs and MultiStakeholder Feedback (internal and external - including civil society) mechanisms all through the lifecycle (design, development, deployment and decommissioning of AI systems). Such inputs include insights provided by civil society representatives, clinical specialists or experts in specific fields (eg. child psychologist in case of apps relating to children), people impacted by the algorithm, people with diverse thought

processes and lived experience and people who are providing independent review from the perspective of potential harms contributed by such systems, besides the organization's internal stakeholders and specialists.

3. **Governance, Accountability and Oversight for Risk Management**: The process of allowing risk inputs and risk consideration across functional areas and disciplines of an organization. Siloes create boundaries and boundaries hinder communication between groups or functions. With siloes in place, risk identification, risk input and risk mitigation becomes more difficult as issues go unidentified and solutions are introduced piecemeal. An unsiloed approach to risk input and consideration will enhance communication, allow for community-wide learning and allow for comprehensive mitigations.

   The process of allowing risk inputs and risk consideration across functional areas and disciplines of an organization. Siloes create boundaries and boundaries hinder communication between groups or functions. With siloes in place, risk identification, risk input and risk mitigation becomes more difficult as issues go unidentified and solutions are introduced piecemeal. An unsiloed approach to risk input and consideration will enhance communication, allow for community-wide learning and allow for comprehensive mitigations.

4. **Feedback loops:** Risk inputs should also be gathered from incidents, adverse events tracking and/ or post market & continuous monitoring of AI systems and feed-back to provide specific risk mitigations. Such an approach not only considers assessed levels of risk, but also provides an opportunity to incorporate risks emerging beyond the limitation in the perspective of risk assessment exercises.

5. **Four Layers of Defense model:** The risk management framework deploys 4 layers of defense described below:
   a. The first layer is the operational layer that manages the risks arising from the AI, algorithmic or autonomous systems.
   b. The second layer is the oversight layer, including the Ethics Committee, Algorithmic Risk Committee, Testing and Evaluation committee etc. These committees oversee the mitigation actions by the operational layer. In addition, these committees will collaborate with operational risk management to ensure that appropriate AI risks are considered as part of the Enterprise Risk Management process.

c. The third layer of defense is the internal audit function which provides an objective and independent assurance on the overall effectiveness and efficiency of the controls.
d. The fourth layer is external independent auditors providing assurance on risk mitigation of risks arising from AAA Systems

In addition, the organization may involve advisors and pre-audit service providers who conduct a review of the organizational risk management or controls therein on behalf of the management. These may not always be fitting into a defense as they are structured around a specific scope, limitations and terms of engagement. However, FH Risk management recognises the value of such services in the process of augmenting the third line of defense, though they may not independently be a third line of defense.

Independent Audit of AI Systems provides a fourth line of defense from the assurances provided by independent, third party auditors acting as verification proxies for the public. This fourth line of defense has become increasingly necessary as the impact from AI systems has grown. These systems have substantial impacts outwardly on humans, communities, society and the environment that need to be assessed and mitigated throughout the life cycle to minimize downside risk to humans.

Understanding Risks from the context of AAA Systems

ForHumanity advocates for a risk management framework that is omni-directional and multivariate. Multivariate in that the risk framework considers corporate risk (which damages employees and shareholders), risk to humans (which damages users/clients/prospects and unwitting participants), societal risk (which damages our systems, groups, communities, markets and collectives) and environmental risks (which damages nature and sustainability considerations). All of these vectors result in a residual risk after optimizing risk mitigations. These residual risks, well disclosed and considered, will empower an increased ability to deal with emerging risks, support concentrated research on novel mitigations and encourage informed acceptance of consequences when residual risk manifests itself.

FH considers risk from the above context including considerations to the long term societal implications and proportional scale of cumulative insignificant impact to humans (petty disturbance for a hundred thousand people is still significant). Further, risks cannot be limited to those which could be anticipated. Risks should be viewed from 3 tiers (1) Foreseeable risk (2) Emergent risk and (3) Systemic societal impact. Anticipated risk is a limited view and may cover only the first point of foreseeable risk. Risk Management systems become very fragile if they do not have a process in place to manage emergent or systemic societal impacts.

i. Foreseeable risk refers to risks that are anticipated and includes the risk inputs from multi-stakeholder feedback and adverse event tracking/ post market monitoring mechanisms.
ii. Emergent risk refers to risks that are future and disruptive threats that require an agile mechanism and wide lens of risk observation, leading to triage, understanding and subsequent plans for mitigation.
iii. Systemic societal impact as a critical observation on long-term adverse impacts contributed to people, people groups and the environment.

In summary, the FH risk management process is aimed at ensuring all the foreseeable, emergent and systemic risks are appropriately considered from the perspective of humans.

Definitions relevant to Risk Management Framework

Defined Term	**Definition (examples may be offered from a single jurisdiction of renown**	**Reference**
AAA System User Guide	Accountable by the Algorithmic Risk Committee (iv.g)instructions of use for the user and, where applicable installation instructions	
AAA Systems List	list, either by name or other identifier that tracks all distinct AI, algorithmic or Autonomous Systems	
AI Governance Assessment	An analysis and designation of accountability, oversight and responsibility for committees (Ethics Committee, Algorithm Risk Committee, Children's Data Oversight Committee and Testing and Evaluation Committee), designated individuals (per a Duty Designation Letter), the Chief Executive Officer and the Board of Directors for any/all risk associated with an AI, algorithmic or autonomous system including duties associated with compliance with audit criteria.	

Algorithmic Risk Assessment	An analysis of all risks associated with the comprehensive lifecycle of an AI, algorithmic or autonomous system, not covered by the TEC AT-Risk report, the Ethical Risk Analysis, the **AI Governance Assessment** and the Systemic Societal Impact Analysis	
Algorithmic Risk Committee	group of employees (or outsourced expert group) tasked with assuring that all AI, algorithms and autonomous systems have taken the necessary steps to identify, remediate, explain and document all instances of Algorithmic Risk	
At-Risk Protected Category	Any Protected Category or intersection of Protected Categories that is explicitly identified by law, identified during an Algorithm Risk Analysis or anticipated by an Ethics Committee to exhibit Disparate Impact, bias or restriction on rights and freedoms. Validity, Accuracy and Reliability of the model must prove sufficient for an At-Risk Protected Category. The Algorithm Risk Committee shall accept and document sufficiency prior to implementation.	
cAIRE report	Comprehensive Artificial Intelligence Risk Evaluation report, comprising all risk inputs, risk mitigations and residual risks gathered from any of the following reports: Algorithm Risk Assessment, Systemic Societal Impact analysis, TEC At-Risk Report, Ethical Risk Assessment, and an **AI Governance Assessment** a review of all operational governance, control and risk assessment resulting in the identification of risk mitigations and residual risk. Residual Risk that cannot be mitigated shall be disclosed. The cAIRE report shall establish within itself the frequency for automatic reassessment where not defined by one of the underlying assessments.	
Causality	Relationship between variables and features that combine to produce an effect, result, or consequence.	

Child's Data Oversight Committee (CDOC)	group of employees (or outsourced expert group) tasked with reviewing all aspects of data collection, risk and procedures associated with data related to Children or Minors for the jurisdiction	
Code of Data Ethics	set of guidelines, principles and procedures by which data is acquired, analyzed, processed, adjusted, compiled or otherwise sold, traded or shared with other entities	
Code of Ethics	a Publicly documented set of principles and rules concerning moral obligations and regards for the rights of humans and nature, which may be specified by a given profession or group. The document is drafted and kept up to date by an entity's Ethics Committee and outlines said entity's shared moral framework within the Relevant Legal Frameworks, providing context to instances of Ethical Choice, diversity and anti-discrimination	
Context	The circumstances in which an event occurs; including geographical, behavioral and functional	
AI Risk Categories	areas where the organization has an responsibility and opportunity to treat, mitigate and/or manage risks	
Data Management Report	Accountable by Data Management Committee the data requirements in terms of datasheets describing the training methodologies and techniques and the training data sets used	

Data Quality	The quality of data that makes it representative and aligned to the scope, nature, context and purpose of the intended use as applicable to an algorithm. Quality of data refers to data that is reasonably and sufficiently relevant, complete and free from errors in aggregation, annotation, maintenance, enrichment, ground truth constructive (inference or proxy or causative), correct syntax, sampling and training-test split as appropriate to the specific domain and/or industry context from reasonably calibrated sources	
Decommissioning Procedure Document (DPD)	A document that states the order of operations for the effective decommissioning of an Artificial Intelligence system including notifications to users, log and database retention, personal data deletion, purge or retention per the Relevant Legal Framework. The DPD should consider each interface to a subsequent system and how that system may be impacted by the decommissioning.	
Diverse Inputs and Multi Stakeholder Feedback	As accepted by the Ethics Committee in compliance with the Code of Ethics and/or a diversity policy, it is a collection of individuals noteworthy by their myriad representation of lived experience, background, and culture, diversity of thought process, skills and expertise, and representation of protected categories and intersection thereof. This group is used for risk inputs, risk evaluation, assessment of foreseen misuse and this evaluation occurs throughout the algorithmic lifecycle from design to decommissioning (captured in an Algorithm Risk Assessment)	
Ethical Choice	awareness of a set of options to be made In the context of automated and intelligent systems, using a set of principles and rules concerning moral obligations and regards for the rights of humans and for nature, which may be specified by a given profession or group. The result, outcome or judgment is made using a shared	

	moral framework. or set of moral principles based upon the entity's Code of Ethics	
Ethical Risk Analysis	A study of instances of Ethical Choice, softlaw, application of Code of Ethics and Code of Data Ethics principles and shared moral frameworks across the lifecycle of the AI, algorithm or autonomous systems shared Publicly.	
Ethics Committee	A group of persons trained in Algorithm Ethics and Ethical Choice, guided by the Code of Ethics and Code of Data Ethics, which they create and maintain on behalf of the organization. The Ethics Committee is responsible for all instance of Ethical Choice related to AI, algorithmic and autonomous systems and producing the Ethical Risk Analysis	
Governance	structure of rules, practices, and processes used to direct, manage and oversee an organization	
High Risk AAA Systems	AAA Systems that have a higher potential of impacting health and safety or fundamental rights of natural persons (listed under Title III of EU AI Act). These include AL, algorithmic or autonomous systems that have Innovative Technology, Denial of Service, Large-scale profiling, Presence of Biometric Data, Genetic Data, Data Matching, Invisible Processing, Tracking, Targeting of Children or otherwise vulnerable populations and Risk of physical harm (as referred by EU AI Act).	

HTL and Integration Report	Accountable by the TEC Committee Process, Roles, Responsibilities, Interfaces, Procedural Guideline, and exception management, training, effectiveness (iv.d) the description of all forms in which the AI system is placed on the market or put into service (iv.f) where the AI system is a component of products, photographs or illustrations showing external features, marking and internal layout of those products (iv.2.e) assessment of the human oversight measures needed in accordance with Article 14, including an assessment of the technical measures needed to facilitate the interpretation of the outputs of AI systems by the users, in accordance with Articles 13(3)(d)	
Information Management Report	Accountable by Data Management Committee (iv.2.d) information about the provenance of those data sets, their scope and main characteristics; how the data was obtained and selected; labeling procedures (e.g. for supervised learning), data cleaning methodologies (e.g. outliers detection)	
Information Quality	The quality of the content of AI, algorithm or autonomous systems that is representative of the fitness for use (scope, nature, context and purpose). It refers to accuracy of data in representing ground truth and relevance of the data for the slated scope, nature, context and purpose	
Interpretability Report	Accountable by the TEC Committee	
Low Risk AAA Systems	AAA Systems that have negligible or very low impact on health, wellbeing, safety and/ or fundamental rights and freedom of natural persons.	
Moderate Risk AAA Systems	AAA Systems that have a moderate potential of impacting health, safety or fundamental rights of natural persons.	

Nature	The forces and processes that influence and control the variables and features.	
Personal Data	any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity. Personal Data may be a collective term encompassing specialized terms such as Inferences, Proxy Variables, and Special Category Data	
Pipeline Quality	The quality of the model refers to the collective integrity of its components including the Algorithm (including its versions), pipeline, serving infrastructure and integrations between pipeline components	
Post-deployment Model management Report	Accountable by the Algorithmic Risk Committee (Incident management AETS, continuous monitoring, post-market monitoring (iv.2.f) where applicable, a detailed description of pre-determined changes to the AI system and its performance, together with all the relevant information related to the technical solutions adopted to ensure continuous compliance of the AI system with the relevant requirements set out in Title III, Chapter 2 (iv.2.g - partial) cybersecurity and compliance with other relevant requirements set out in Title III, Chapter 2 as well as potentially discriminatory impacts	

Pre-deploy Model Development and Validation Report (application architecture)	Accountable by the TEC Committee (IV.2.a) the methods and steps performed for the development of the AI system, including, where relevant, recourse to pre-trained systems or tools provided by third parties and how these have been used, integrated or modified by the provider, (IV.2.b) the design specifications of the system, namely the general logic of the AI system and of the algorithms; the key design choices including the rationale and assumptions made, also with regard to persons or groups of persons on which the system is intended to be used; the main classification choices; what the system is designed to optimize for and the relevance of the different parameters; the decisions about any possible trade-off made regarding the technical solutions adopted to comply with the requirements set out in (iv.2.g - partial) the validation and testing procedures used, including information about the validation and testing data used and their main characteristics; metrics used to measure accuracy, robustness, test logs and all test reports dated and signed by the responsible persons	
Prohibited AAA Systems	AAA Systems whose use is considered unacceptable as contravening Union values, for instance by violating fundamental rights (listed under Title II of EU AI Act)	
Protected Category Variables	Defined under law or regulation by Jurisdiction, may include race, age, gender, religion, ability/disability, sexual orientation, creed, color, nation of origin, socioeconomic class etc	
Purpose	an aim or goal	

Relevant Legal Frameworks	can contain a broad range of applicable law such as the laws that govern an entity or organisation, that govern the rights and privileges of a Data Subject, that restrict the activities and behaviors of a Data Controller or Data Processor, or put positive obligations upon an entity Note: These include consideration for human rights, equalities and anti-discrimination law, access to goods and services (having due regard to who is included/excluded from such goods and services), Children's law and laws with regard to the platform and/or laws with regard to the sector in and through which the AI (and data processing) is being provided, amongst other risks law, as it applies to Data Subjects, specific to the Jurisdiction of Data Subject being included in the data processing for the audit or certification.	
Residual Risk	Unmitigated risk pertaining to a specific risk input or the aggregation of all risk in an AI, algorithmic or autonomous system. (Refer AVR3)	
Risk Analysis	A process of examining Risk Input impact on people, communities and the environment, and their underlying root causes	
Risk Assessment Policy	A plan established by Algorithmic Risk Committee (ARC) to consider the context (size, profile and population turnover of data points), construction/variation of inputs to the AI/ML process, purpose and impact on users or Data Subjects of outputs/outcomes in order to identify the reasonable frequency and process for systemic reassessment of risk and associated mitigations. Thresholds (KPIs/KRI's) should be established that trigger automated reassessment processes (e.g. Systemic Societal Impact Assessment)	
Risk Evaluation	A process wherein the risks from the Risk Log are ranked in the context of the likelihood and severity of the said risks	

Risk Indicator	information, insight or perspective about negative impacts with unknown causality/ root cause that requires further examination for gaining clarity on the root causes prior to mitigation or management (eg. Key Risk Indicators in IAAIS audit criteria, Adverse Event Tracking System).	
Risk Input	information, insight or perspective about negative impacts along with their causality/ root cause that provides clarity for mitigating or managing them.	
Risk Managemen t Process	The process involving the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk with reference to data processing and AI, algorithmic or autonomous systems.	
Risk Spectrum	negative impacts that can result from non existent, inadequate, ineffective or inefficient mitigations within control domains of AI, algorithms and / or autonomous systems, with potential to impact people, society, and the environment	
Risk Thresholds	The discrete levels quantitatively measured that are tested against either periodic risk assessments or real-time post-market monitoring that automatically trigger a risk mitigation event in regards to the good and reasonable operation of the system	
Risk Treatment	The process of identifying and implementing appropriate measures to modify risk impact	
Scope	The boundaries of a system	

Special Category Data	data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, Biometric Data, data concerning health or data concerning a natural person's sex life or sexual orientation [SOURCE: UK GDPR]	
Statistical Characteristics	Realized statistical properties of a dataset with respect to Protected Category Variables	
Technical Architecture Report (infrastructure)	Accountable by the TEC Committee (iv.a) Version control with data of release, persons involved, (IV.b)AI system interacts or can be used to interact with hardware or software that is not part of the AI system itself (iv.c)versions of relevant software or firmware and any requirement related to version update (iv.e) the description of hardware on which the AI system is intended to run (Iv.2.c) the description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing; the computational resources used to develop, train, test and validate the AI system	
Traceability	the ability to trace a data right back to its origin through documentation, including a chain-of-custody (“paper trail,” physical or otherwise) for data provenance that chronologically records the ownership, viewing, analysis, and transformations of a data record or data sources	

More details about the process, considerations and framework are described in the relevant documents.

