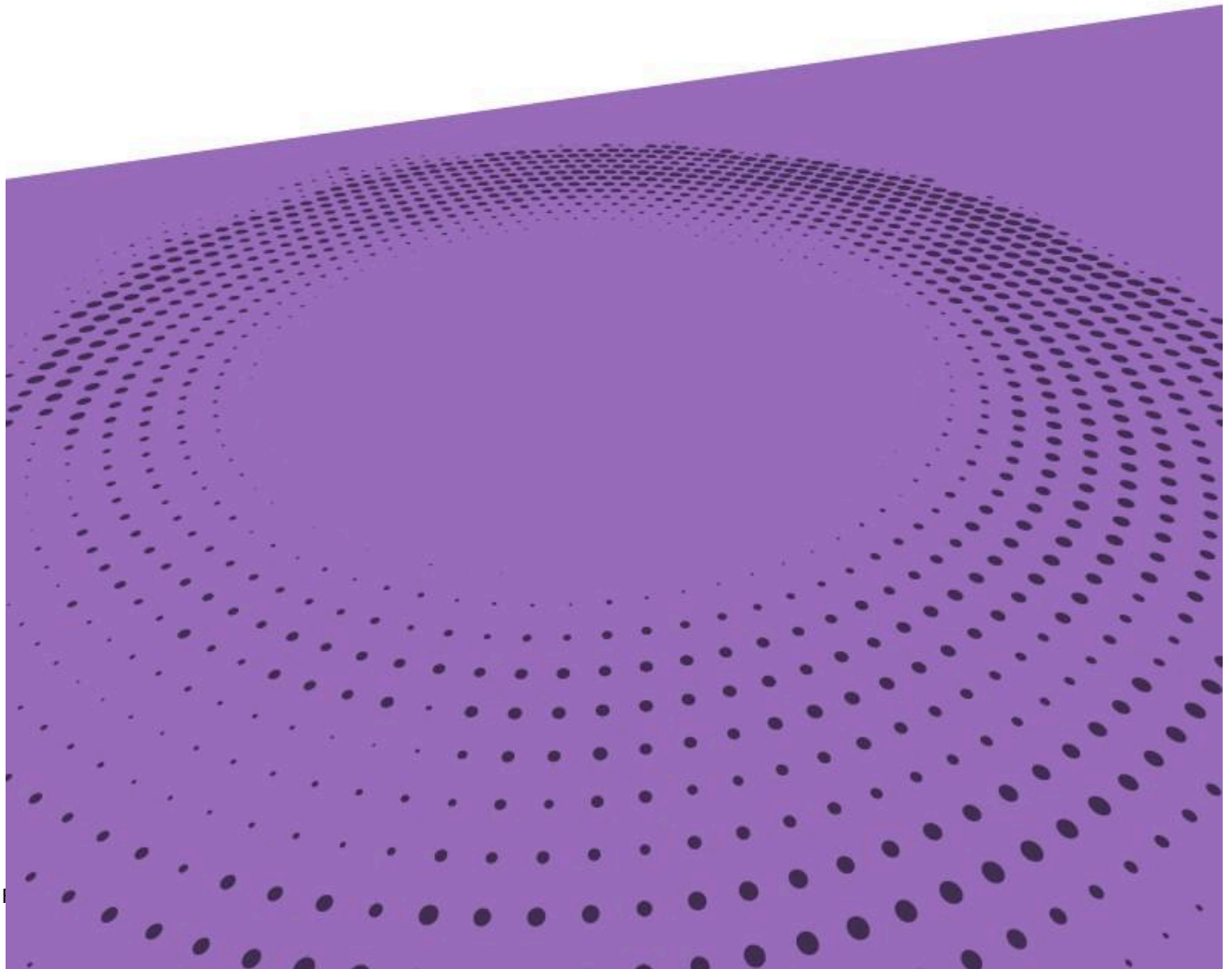

FORHUMANITY
980 Broadway #506 Thomwood, NY 10594
(+1) 9146028663
ryan@forhumanity.center
www.forhumanity.center

FORHUMANITY EUROPE
12 rue Frédéric Petit
80000 Amiens France



EU AI Act – Deployer only

CERTIFICATION SCHEME V1.5
Artificial Intelligence, Algorithmic and Autonomous (AAA) Systems





[Introduction](#)

[Infrastructure of Trust](#)

[For Humanity's Role in an Infrastructure of Trust](#)

[EU Artificial Intelligence Act](#)

[1.0 Scope](#)

[1.0.1 Determination of Deployer Status](#)

[1.1.3 Relevant Legal Frameworks](#)

[1.1.3.1 In scope - GDPR Applicability](#)

[1.1.3.2 In scope - European Accessibility Act of 2019 \(EU\) 2019/882](#)

[1.1.3.3 In scope - Digital Service \(EU\) 2022/2065](#)

[1.1.3.4 In scope - Cybersecurity minimum requirements](#)

[1.2 Audit Period of Validity](#)

[1.3 Out of Scope Systems](#)

[1.3 Target of Evaluation Determination Process](#)

[1.4 Territorial Scope](#)

[2.0 Normative References](#)

[3.0 Terms and Definitions](#)

[3.1 Policies, Plans, and Assessments](#)

[4.0 General Requirements for Accreditation](#)

[4.1 Interoperability with Standards](#)

[4.2 Normative Criteria explanation](#)

[4.3 Documentation of Assessments and Certification](#)

[4.4 Evaluation Methodology](#)

[5.0 Use of the term “Algorithmic Lifecycle”](#)

[5.1 Criteria catalog](#)

[Expert Oversight](#)

[Top Management and Oversight Bodies](#)

[Relevant Legal Framework and Modular Assurance Assessments](#)

[Organisational Controls](#)

[Training and Education \(AI Literacy\)](#)

[Specialty Committees](#)

[Prohibited System - Article 5](#)

[Excluded AI Systems \(Recital 53-60\)](#)

[Business Rationale](#)

[General-Purpose AI Determination](#)

[Ethical Oversight](#)

[Consumer Protection](#)



[Data Privacy and Protection](#)

[AAA System Procurement](#)

[Risk Management - Article 9](#)

[Article 10 - Data Management and Governance](#)

[Bias Mitigation](#)

[Explainability](#)

[Technical Infrastructure](#)

[Design Choices](#)

[Accommodations - Recital 80](#)

[Choice Architecture](#)

[Security and Cybersecurity](#)

[Integration Testing and Evaluation](#)

[Article 72 - Monitoring \(Continuous and Post-Market\)](#)

[Incident Management \(Article 73.6\)](#)

[Article 11 - Technical Documentation](#)

[Article 12 - record-keeping - Logs](#)

[Article 13 - Transparency and Disclosure to AI Subjects](#)

[Controls](#)

[Article 14 - Human Oversight and Interaction](#)

[Exceptions Interpretability](#)

[Vendor Management](#)

[Change Management](#)

[System Development Life Cycle](#)

[Article 17 - Quality Management System](#)

[Regulatory Compliance](#)

[Article 18 - Documentation Keeping](#)

[Decommissioning](#)

[Article 49 - EU Database Registration](#)

[Article 50 - Transparency Obligations](#)

[Article 51 - General-Purpose AI Classification](#)

[Article 52 - Notification of a General Purpose AI as Systemically risky](#)

[Article 53 - Obligations of a Provider of a General-Purpose AI Model](#)

[Article 55 - Obligations of a Provider of a General-Purpose AI Model with Systemic Risk](#)

[Article 60 - Real World and Beta Testing](#)

[Article 61 - Informed Consent for Real World Testing](#)

[Appendix A - Infrastructure of Trust for AI - Guide to Entity Roles and Responsibilities](#)

[Background on Independent Audit](#)



Certification Scheme for:
EU AI Act - Deployer v1.5

[Adapting to AI and Autonomous Systems](#)

[Role on Independent Audit of AI and Autonomous Systems](#)

[Participants in the System](#)

[Licensing](#)



Introduction

ForHumanity (<https://forhumanity.center/>) is a 501(c)(3) non profit organization and ForHumanity Europe is a French 1901 Association, dedicated to addressing risks associated with Ethics, Bias, Privacy, Trust, and Cybersecurity in Artificial Intelligence, Algorithmic, and Autonomous (AAA) Systems. ForHumanity uses an open and transparent process that draws from a pool of over 2600+ international contributors to construct audit criteria, certification schemes, and educational programs for legal and compliance professionals, educators, auditors, designers, developers, and legislators to mitigate bias, enhance ethics, protect privacy, build trust, improve cybersecurity, and drive accountability & transparency in AAA Systems. ForHumanity works to make AAA Systems safe for all people and makes itself available to support government agencies and instrumentalities to manage risk associated with AAA Systems. Our mission is to *examine and analyse downside risk associated with the ubiquitous advance of AI, algorithmic and autonomous systems and where possible to engage in risk mitigation to maximise the benefits of these systems... ForHumanity*

Infrastructure of Trust

ForHumanity supports an infrastructure of trust predicated on the 50+ year track record of financial accounting and reporting. This infrastructure of trust is founded on a principle of jurisdictional sensitivity, which means that each sovereign nation-state or region has the right to establish their own laws, regulations, guidelines, and shared moral framework.

ForHumanity affirms that right by ensuring that our certification program upholds local laws and seeks approval, where applicable, from local authorities. Key elements of Independent Audit of AI Systems are critical to ensure that it functions properly across multiple different jurisdictions, these are non-negotiable elements of the shared moral framework that constitutes Independent Audit of AI Systems and they include concepts such as transparency, disclosure, independence, risk management, and ethical oversight.

ForHumanity believes that a binary (compliant/non-compliant) set of criteria, either adopted by common practice in the marketplace or approved by the sufficient governmental authorities, and subsequently assured for compliance independently by certifying bodies (auditors), can create an infrastructure of trust for the public that assures compliance with laws, regulations, guidelines, standards, and best practices in a proactive manner when combined with the requirement for regular, mandatory, independent audits.



An infrastructure of trust, as it relates to certification, is an unconflicted process deploying a segregation of duties, conducted by certified and trained experts, that establishes a robust ecosystem that engenders trust for all citizens and protects those who have no power or control.

The infrastructure of Trust that For Humanity supports is grounded on four core tenets:

1. ForHumanity produces accessible, binary (compliant / not compliant) certification criteria that transparently and inclusively aligns laws, regulations, standards, guidance and best practice that embeds compliance and performance into practice, and is considerate of corporate wisdom, but impervious to corporate dilution and undue influence, while being mindful of the regulatory burden and dedicated to maximizing risk mitigations to humans.
2. Individuals are trained and accredited on certification criteria as experts by ForHumanity. They perform pre-audit and audit services on behalf of certification bodies and are individually held to a high standard of behavior and professionalism as described in the [ForHumanity Code of Ethics and Professional Conduct](#) - they are ForHumanity Certified Auditors (FHCAs)
3. Certification Bodies employ FHCAs to independently assure compliance with certification criteria on behalf of the public. They are licensed, independent, robust organisations that take on the task and risk, on behalf of the public, to ascertain assurance of compliance. They are held to standards of independence and anti-collusion and are further subject to third-party oversight (“watching the watchers”), by entities such as national accreditation bodies (e.g. COFRAC, UKAS, DaKKE) and ForHumanity.
4. Corporations and public sector Providers and Deployers of AAA Systems can use the criteria to operationalise governance, oversight, and accountability that helps them to achieve required conformity under the law. Compliance with ForHumanity certification schemes will create leverageable governance, oversight, and accountability that will simultaneously lead to more sustainable profitability and reduce the risk of negative outcomes for their stakeholders.

See Appendix A for more details on Roles and Responsibilities in an Infrastructure of Trust¹.

¹ [Infrastructure of Trust for AI – Guide to Entity Roles and Responsibilities](#)



ForHumanity's Role in an Infrastructure of Trust

Founded in 2016, ForHumanity first wrote about Independent Audit of AI Systems in 2017 and it has been our primary focus since that time. We advocate for mandatory independent audits and the establishment of the aforementioned infrastructure of trust similar to those required in financial accounts and reporting.

Transforming an audit ecosystem from financial audits to process audits for AAA Systems requires thoughtful adaptation. Transformation occurs by accomplishing the following tasks:

1. Understanding how financial audit rules & standards mitigate risk, provide clarity, and translate opaque controls and processes into public trust and valuable cross-sectional comparability through third-party independent assurance
2. Understanding the risks of AAA Systems and developing rules & standards to treat and mitigate risks to stakeholders, including individuals
3. Drafting audit criteria that are binary, implementable, solution-oriented to the identified risks
4. Mapping steps #1-3 onto an ecosystem that recreates the assurance and infrastructure of trust nurtured in financial audit for more than 50 years

In support of this transformation, ForHumanity is replicating and augmenting the role of the Financial Accounting Standards Board (FASB) and the International Financial Reporting Standards (IFRS) foundation, who drafted GAAP and IFRS respectively. Unlike those predecessors, ForHumanity is a grassroots, civil-society organization with contributors from more than 98 countries around the world. Our approach ensures globally-harmonized, audit criteria that operationalize the law, standards, and best practices sourced by diverse input and multi stakeholder feedback contributors.

We draft audit criteria for AAA Systems in the context of new legislation all around the world, such as, the EU's General Data Protection Regulation (GDPR), and the EU Artificial Intelligence Act, Consumer Protection and Consumer Privacy Protection Act in the United States, Lei Geral de Proteção de Dados Pessoais (LGPD) in Brazil, and India's Digital Personal Data Protection Act

ForHumanity's authority for producing audit criteria is grounded in the robustness of our crowdsourced, transparent process (no one is excluded from participating), however we always seek the endorsement of Federal, state, and local authorities, as applicable, when they support the approval of audit criteria, such as the manner in which most nation-states and regional blocks have adopted Generally Accepted Accounting Principles (GAAP) or International Financial Reporting Standards (IFRS) to govern financial accounting and reporting. When



governments are unprepared to endorse uniform, objective audit criteria, then ForHumanity seeks adoption directly from the marketplace, which is what occurred in 1973 with GAAP and the predecessor to IFRS, prior to Federal adoption in the years afterwards.

EU Artificial Intelligence Act

The EU Artificial Intelligence Act (EU AI ACT) - (EU) 2024/1689 is part of an intertwined set of laws and regulations that govern the use of artificial intelligence (AI) in the European Union². This law prohibits certain uses of AI and regulates the use of AI that have been deemed to be a “high risk” to the health, safety, and fundamental rights of EU citizens. “High Risk” is defined in multiple places in the law, especially Annex I Section A & B and III and can be described in Recital 5 as being material or immaterial including physical, psychological, societal or economic harm. Further the law aims to govern the use of General-Purpose AI by both Providers and Deployers in the European Union, including a designation for General Purpose AI as systemically risky. The Act establishes a set of compliance requirements and regular oversight to ensure conformity. Conformity may be determined by self-assessment or third party assurance by notified bodies. Transparency and disclosure requirements are also included and must be submitted to national supervisory authorities.

AAA Systems are (often complex) socio-technical tools. As a result, the EU AI Act, and this certification scheme are considerate of other related laws and regulations. For example, any AAA System that is covered by the EU AI Act and uses Personal Data of Data Subjects in the EU, must also be concurrently compliant with the (EU) 2016/679 General Data Protection Regulation. Other laws, regulations, and guidance that impact the AAA Systems governed by the EU AI Act include:

1. General Data Protection Regulation
2. Digital Services Act
3. European Accessibility Act of 2019
4. EU Data Act

This interconnected web of laws and regulations establishes legal obligation groups known as, Providers, Deployers, Controllers, and Processors. This certification scheme is dedicated to the obligations of Deployers. The ForHumanity EU AI Act Provider-only v1.5 certification scheme is

² All references in this document to EU Member States, EU Data Subjects, the Union, Union Law, etc. shall be understood to include, in addition to their meaning in the regulation, European Economic Area (EEA) states, EEA Data Subjects, the EEA, and the EEA Agreement respectively



to be used by Providers of AAA Systems. The distinction between Provider and Deployer is a necessary first step in the deployment of either certification scheme and can be found in Section 1.0 Scope. The terms Provider and Deployer are defined specifically by both the law and in the Terms and Definitions Section 3.0.

1.0 Scope

ForHumanity designed this certification scheme for Deployers (Auditees) of any size. The scheme may be applied to one or more specific AI, Algorithmic, or Autonomous Systems (including General-Purpose AI) that have been placed on the market or put into service, however it may not be used for AAA Systems that are prohibited under Article 5 of the Act. The certification scheme will cover all obligations under the EU AI Act and is valid for 12 months unless significant changes occur (see section 1.0.1 for the Audit Period of Validity).

If the AAA System is a necessary safety component of any harmonised legislation in Annex I Section A or B, and is placed on the market or put into service independently from the Product, as identified in the harmonised legislation (Recital 87), then the safety component is in scope for this certification scheme.

If the AAA System is described in Annex III, then it is in scope for this certification scheme.

If the AAA System incorporates a general-purpose AI model and a general-purpose AI usage, placed on the market or put into service in the Union, irrespective of whether those Deployers are established or located within the Union or in a third country, then it is in scope for this certification scheme and will be subject to additional audit criteria based upon Chapter V of the EU AI Act.

Any AAA System, even one that is not “high-risk”, may voluntarily choose to abide by this certification scheme.

1.0.1 Determination of Deployer Status

Prior to engaging with this certification scheme, it is necessary for the organization that will be the auditee to verify that they are a Provider of the AAA System in order to use this scheme effectively.



An organization is defined as a **Provider** of an AAA System if any of the following are true:
natural or legal person, public authority, agency or other body that:

1. *Develops (designs, trains, tests, builds) an AAA System*
2. *Places its Brand on the AAA System*
3. *Makes an AAA System available to the market (sells, shares, leases, or trades) an AAA System for any of the following:*
 - a. *Usage by a Deployer or AI Subject*
 - b. *Distribution by a distributor*
 - c. *Import by an importer*
4. *Engages in any modification of an AAA System that results in changes to any of the following:*
 - a. *Functions/Capabilities*
 - b. *Scope, Nature, Context, Purpose*
 - c. *Risk*

That deviate from stipulations in an executed contract AND/OR that are not covered by existing third party assurance

An organization is defined as a one of two types of Deployer, described as either a Deployer (standalone) or Deployer (multi-agent) as delineated below:

Deployer of an AAA System is described as the following:

natural or legal person, public authority, agency or other body that:

1. *Acquires, configures, and/or operates a single AAA System OR multiple AAA Systems where integration testing can be assured and documented for conformity such that the usage of each AAA System is in compliance with the Provider's contractual terms and conditions regarding:*
 - a. *Functions/Capabilities,*
 - b. *Scope, Nature, Context, Purpose*
 - c. *Risk*

OR

Provider (Multi) of an AAA System that has more than one AI, Algorithmic and/or Autonomous agent, model, and/or component and is described as the following:

2. *Combines multiple AAA Systems in a manner that establishes interactions between or amongst any of the agents, models, and/or components such that a new system is created with unique:*
 - a. *Functions/Capabilities,*
 - b. *Scope, Nature, Context, Purpose*



- c. Risk and/or*
- d. Sources Pipeline data from any of the other agents, models, and/or components*

An Auditor shall issue conditional certification for a Deployer's AAA System upon demonstrating assurance of compliance with this certification scheme, pending concurrent (within a 12 month) assurance of any of the following Relevant Legal Frameworks, if applicable:

1. EU 2016/679 (GDPR),
2. EU 2019/881, (Cybersecurity)
3. EU 2019/882 (Accessibility Act)
4. EU 2022/2065 (Digital Services Act)

1.1.3 Relevant Legal Frameworks

1.1.3.1 In scope - GDPR Applicability

AAA Systems often include the use of Personal Data, therefore it is necessary to determine if the Target of Evaluation uses Personal Data in order to know whether GDPR is applicable.

1.1.3.2 In scope - European Accessibility Act of 2019 (EU) 2019/882

ForHumanity and the European Union both uphold the rights of Disabled Persons according to the United Nations Convention on the Rights of Persons with Disabilities (UNCRPD). Recital 80 of the EU AI Act states "... It is therefore essential that Deployers ensure full compliance with accessibility requirements, including Directive (EU) 2016/2102 of the European Parliament and of the Council and Directive (EU) 2019/882."

ForHumanity recognises that the very nature of the design and development of AAA systems is often exclusionary in the name of higher accuracy rates. Therefore, tangible remediations in support of Inclusion and Accessibility, especially accommodations, are critical to uphold the law. ForHumanity has established a certification scheme called Global Disability Inclusion & Accessibility which augments this certification scheme to assure high-risk AI systems are compliant with the law.

1.1.3.3 In scope - Digital Service (EU) 2022/2065

The Digital Services Act aims to create a safer online environment for consumers and companies in the European Union (EU), with a set of rules designed to:



1. protect consumers and their fundamental rights more effectively;
2. define clear responsibilities for online platforms and social media;
3. deal with illegal content and products, hate speech and disinformation;
4. achieve greater transparency with better reporting and oversight; and
5. encourage innovation, growth and competitiveness in the EU's internal market.

These goals match to ForHumanity's mission and as a result, ForHumanity has created the ForHumanity Digital Services Act Certification Scheme v1.1 for Covered Entities to assurance compliance with this regulation. Recital 118 states "This Regulation regulates AI systems and AI models by imposing certain requirements and obligations for relevant market actors that are placing them on the market, putting into service or use in the Union, thereby complementing obligations for providers of intermediary services that embed such systems or models into their services regulated by Regulation (EU) 2022/2065. To the extent that such systems or models are embedded into designated very large online platforms or very large online search engines, they are subject to the risk-management framework provided for in Regulation (EU) 2022/2065"

1.1.3.4 In scope - Cybersecurity minimum requirements

High-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and the references of which have been published in the Official Journal of the European Union shall be presumed to comply with the cybersecurity requirements set out in Article 15 of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.

ForHumanity provides integrated and harmonised certification scheme so that the auditee can be able to document satisfaction in regards to Article 15.

1. ForHumanity Cybersecurity Certification scheme
2. Regulation (EU) 2019/881- Article 54 certification - Regulation (EU) 2024/482

1.2 Audit Period of Validity

A certification is good for one year provided additional applicable certifications (e.g., GDPR, Digital Services Act) are currently valid. Compliance should be renewed each year and an auditee is expected to maintain compliance with the current version of the audit. In any areas where the certification criteria have been changed, the auditee will have until the next annual audit to bring their systems into compliance.



Some examples of a significant change or **Substantial Modification** that require recertification to maintain status are:

1. Changes in Scope, Nature, Context, and Purpose
2. Model, Data, or Concept drift
3. Acquisition/Change in Control
4. Complaint(s) or Adverse Incident reports
5. Regulatory intervention
6. ForHumanity's Cause for Concern

1.3 Out of Scope Systems

AAA Systems prohibited by the Act may not be certified using this scheme.

AAA systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities or AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

AAA Systems placed on the market by Providers are out of Scope for this certification scheme, however ForHumanity offers a separate certification scheme for them.

AAA systems operated by public authorities in a third country or international organisations, where those authorities or organisations use AAA Systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the Union or with one or more Member States are out of scope for this certification scheme.

AAA Systems operated for the sole purpose of scientific research and development are out of scope when all of the following conditions apply:

1. There is documentable evidence of the application of the scientific method
2. There are no direct impacts to AI Subjects
3. There is no commercialisation of the AAA System, including through the monetisation of Personal Data
4. Where the live environment is not freely available



1.3 Target of Evaluation Determination Process

The organisation seeking certification determines the AAA System to which the certifying body will apply the scheme and documents this agreement in a contract. The Target of Evaluation (ToE) shall be defined by contract between the certifying body and the organisation. The certification is valid for 12 months from the date certification is issued by the certifying body.

The contract shall document all information required by the certifying body for a sufficient Certification Plan and shall include all of the following:

- 1) Name/identifier of the ToE, specifically noting all inputs and outputs of the **AAA System** as described in the **System Architecture Report** - Document that describes the overall, top-level blueprint of conceptual/logical/physical structure of the system including relevant frameworks and applicable standards (e.g., ISO, CEN/CENELEC, IEEE) and includes descriptions of **Processor**, and sub-**Processor** relationships including databases, processing, flow and movements, pipeline, data collection, UX interfaces, and location/**Jurisdiction** and the **Data Flow Diagram**
- 2) Systems or organisations expected to be “in” or “out” of scope (including a visual representation as appropriate). “In” and “out” of scope applies to third parties (including Processors) under contract.
- 3) The AAA System will be specifically identified including its Scope, Nature, Context, Purpose. For “out” of scope adjacent or interdependent processing or systems shown in the **System Architecture Report**, the organisation shall document and justify “out” of scope boundaries for those adjacent or interdependent processing or systems
- 4) Description of the data deployed in the system, specifically noting the Personal Data and Special Category Data that may be present (including Inferences and/or potential Proxy Variables)
- 5) Specify where the processing of data happens in terms of physical location, including whether or not there are transfers to third countries or international organisations and whether such transfers are a part of the ToE or out of scope to the ToE.
- 6) Identify all applicable jurisdictions in which the AAA System processes data in order to determine additional applicable legal obligations, beyond GDPR, called Relevant Legal Frameworks (as documented in Section 5.0 criteria #6).

The certifying body will only perform an audit of the documented scope. The Deployer bears the responsibility of ensuring that all necessary components of the AAA System are covered in the definition of the ToE.



The ToE shall be defined in such a way that it is not misleading or likely to be misinterpreted by third parties.

The ToE may include elements of the application that are NOT AAA Systems themselves but are necessary to ensure that the AAA System functions according to the defined Scope, Nature, Context, and Purpose. This certification scheme is NOT limited to certifying only the AI, Algorithmic or Autonomous component, but rather the entirety of the AAA System application.

1.4 Territorial Scope

This certification scheme applies to Deployers whose output from the AAA System impacts EU Citizens as AI Subject, regardless of the jurisdiction of the Deployer. It further applies to an AAA System that impacts EU Citizens regardless of their physical location.

2.0 Normative References

[ISO 27001/27002:2022 - Information security management](#)

[ISO 15288:2015 - Systems and software engineering — System life cycle processes](#)

[ISO 31000 - Risk management](#)

[ISO 9001 - Quality Management Systems](#)

[ISO 9001:2015 - Quality Management Systems](#)

[ICO DPIA Guidance Template³](#)

3.0 Terms and Definitions

Defined terms are bolded and capitalised throughout this document.

Defined Term	Definition
AAA Cybersecurity Lead	An expert accountable for security and cybersecurity policies, processes, procedures, risk management, incident response, business continuity and disaster recovery
AAA System	Any end-to-end application containing an AI, Algorithmic, or Autonomous component including both technical elements (e.g., databases, data, networks, hardware) and lifecycle elements (e.g., pre-processing, monitoring, human oversight) that allow the system to achieve a specific Scope, Nature,

³ Information Commissioner's Office, Guide to Data Protection, April 2021, licensed under the [Open Government Licence](#).



Defined Term	Definition
	Context, and Purpose
AAA Systems List	A list, either by name or other identifier that tracks all distinct AI, Algorithmic or Autonomous Systems
AAA System AI Subjects Guide	A digital documentation that intends to enable and empower the AI Subject with information about the AAA Systems from the Provider or Deployer that is necessary to successfully operate the AAA System . It is digital information that is concise, complete, correct, clear, relevant, accessible and comprehensible to the AI Subject
Accessibility	degree to which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use [SOURCE: ISO/IEC 25010:2011]
Accessibility Conformance Report	Evaluation, overseen by the Disability Inclusion and Accessibility Committee , that determines how well AAA System and associated ecosystem meet accessibility standards (e.g., VPAT EN 301 549, Model Accessibility Statement, GPAT, Open ACR) https://www.w3.org/WAI/test-evaluate/conformance/
Accommodation	A timely adjustment made in a system (such as the provision of tools or changes to the environment or the way in which the AAA System is usually provided) to accommodate or make fair the same system for individuals, including Persons with Disabilities based on a need, which will likely vary. Accommodations can be religious, physical, mental or emotional, academic, or employment related and are often mandated by law and are jurisdictionally sensitive
Accuracy	The closeness of agreement between a test result and the accepted reference value SOURCE: ISO 3534-1 [A measure of a system's Functional Correctness]
Adaptability	The degree to which a product or system can effectively and



Defined Term	Definition
	efficiently be adapted for different or evolving hardware, software or other operational or usage environments [SOURCE: ISO/IEC 25010:2011]
Adverse Impact	When the selection rate is below a fairness threshold (e.g., 70%, 80%, 90%) established by the Ethics Committee to identify when the selection rate may indicate a detrimental impact
Adverse Incidents	Negative outcomes or impacts to natural person caused by AAA System
Adverse Incident Reporting System (AIRS)	A system available to the Consumer/Customers/Users/AI Subjects (including internal stakeholders, partners, customers, civil society, industrial associations, and the general public) to report or register confidentially (and maturely anonymously) information regarding their perceived or realised adverse incidents attributable to AAA Systems
Age-Appropriate	A commitment to delivering suitable information, content, services, applications, interfaces and design that considers a Child's specific developmental stage (capacity, skills and behaviours) and understanding, leading to beneficial engagement that supports the well-being of the Child. Age-Appropriate content and disclosure includes the identification of target age ranges per the ICO's breakdown This includes signposting for when a child is instructed to seek parental assistance. Notifications shall be in plain language
AI Compliance Lead	A natural person assigned by the Provider to be responsible for leading regulatory compliance functions associated with the act including acting as a Point of Contact for communications with notified bodies and national competent authorities
AI Subject	A natural person who is impacted by the outcomes of a AAA System



Defined Term	Definition
Algorithm	A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer
Algorithm Ethics	A sub field of Ethics focused on instances of Ethical Choice emerging from AI, algorithmic and autonomous systems. Training and expertise include areas such as Necessity, Proportionality, Benchmark setting, Validity, Reliability , Model, Data and Concept Drift and thresholds for Bias mitigation.
Algorithmic Risk	Any risk input or indicator identified in the Algorithmic Risk Assessment, exclusive of security and cybersecurity risks inputs and indicators
Algorithmic Risk Assessment	An analysis of all risks associated with the comprehensive lifecycle of an AAA System, not covered by the Cybersecurity Risk Assessment, the Ethical Risk Assessment, the Committee 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, mitigate, explain, monitor and document all instances of Algorithmic Risk
Architectural Inputs	Parameters, variables, hyperparameters, weights, and other elements that are used to establish an algorithmic calculation or process
Artificial Intelligence System (EU)	machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments - SOURCE EU AI Act
Assistive	Any item, piece of equipment, service, or system including



Defined Term	Definition
Technologies	software that is used to increase, maintain, substitute or improve functional capabilities of Persons with Disabilities or to alleviate and compensate for impairments, activity limitations or participation restrictions
Augmentation Data Set	Source data from a downstream Provider or any type of Deployer (e.g., organization specific data), consisting only of unique data that is owned and controlled by the auditee intended to customize and/or enhance the Provider's AAA System outcomes
Authenticity	The degree to which the identity of a subject or resource can be proved to be the one claimed [SOURCE: ISO/IEC 25010:2011]
Authorised Representative	A natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation (Source EU AI Act)
Authority	The legal right to hold or provide data
Automation Bias Curriculum	A body of learning designed to raise awareness of the Human-in-Command and other employees associated with the AAA System in regards to a general over-reliance of AAA Systems. The curriculum is designed to establish a healthy scepticism in regards to AAA Systems and to educate users when AAA Systems can be relied upon and when they should be stopping, pausing, disregarding, overriding, and reversing. The curriculum further encourages users to acquire knowledge and understanding of underlying assumptions, data inputs, risk mitigations, and Residual Risk associated with the AAA System.
Autonomous System	Any self-governing system, operating without a human-in-the-loop (excluding pre-start inputs and design



Defined Term	Definition
	plus maintenance, recalibration, retasking and repair) , producing characteristics of human dexterity, such as arm or leg motion and their results (e.g., travelling distances) or any one of the five human senses
Availability	The degree to which a system, product or component (including data) is operational and accessible when required for use [SOURCE: ISO/IEC 25010:2011]
Bias Risk Assessment	Subset of an Algorithmic Risk Assessment , still including Diverse Inputs and Multi Stakeholder Feedback (DI & MSF) , focused on uncovering and mitigating risk associated with Bias (e.g. Cognitive Bias and Technology Barrier) in the data, architectural inputs and outcomes
Biometric Categorisation	The act of assigning natural persons to specific categories on the basis of their biometric data. Such specific categories can relate to aspects such as sex, age, hair colour, eye colour, tattoos, behavioural or personality traits, language, religion, membership of a national minority, sexual or political orientation [SOURCE: EU AI Act)
Biometric Data (EU)	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data
Biometric Identification	as the automated recognition of physical, physiological and behavioural human features such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes characteristics, for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database, irrespective of whether the individual has given its consent or not and without their active involvement



Defined Term	Definition
Bug Bounty Program	A way for a Provider to reward an external security tester for identifying flaws, vulnerabilities, errors and bias in an AAA System and reporting them to the Provider through a predetermined mechanism and process
Business Rationale Report	In the context of the Fundamental Rights Impact Assessment, Proportionality Study and Necessity Assessment, document the system's underlying logic, Causal Hypothesis, Construct Validity, and feature relevance that upholds and supports the EU Charter of fundamental rights
Business Continuity Plan (BCP)	Scheme that describes a system of prevention and recovery from potential threats to a company, ensuring that personnel and assets are protected and are able to function quickly in the event of a discontinuity, threat or disaster. The BCP is integrated with a Contingency plan and restoration prioritisation plan
cAIRE report	Comprehensive Artificial Intelligence Risk Evaluation report, comprising all risk inputs, risk mitigations and Residual Risks gathered from any of the following reports: Algorithmic Risk Assessment, Systemic Societal Impact analysis, Integration Test Completion Report, Ethical Risk Assessment, and Committee Governance Assessment
Capacity	degree to which the maximum limits of a product or system parameter meet requirements [SOURCE: ISO/IEC 25010:2011]
Causal Hypothesis	An assessable proposition, to be proven or disproven, that predicts a relationship between two variables, where the change in the first variable brings about change in the second variable
CE marking of Conformity	a marking by which a provider indicates that an AI system is in conformity with the requirements set out in Chapter III, Section 2 and other applicable Union harmonisation legislation providing for its affixing (Source EU AI Act)



Defined Term	Definition
Change Management Impact Assessment	An assessment of metrics, measurements, and thresholds pre-determined to delineate between minor changes that can be classified as version updates versus major changes that represent meaningful risk to the organisation, Deployers, or AI Subjects
Change Management Plan	An ISO 9001:2015 document that delineates implementation, risk, impact, and adaptation/migration strategies as well as communication procedures, procedures for unplanned outages from change, processes for protection of production data, defined backup and rollback procedures, and supporting documentation for approval
Child (ren)	a person under the age of 18
Child's Data Oversight Committee (CDOC)	A group of 3 or more people which may comprise outside experts, tasked with reviewing all aspects of data collection, risk and procedures associated with data related to Children for the Jurisdiction
Child-Friendly	To present information using diagrams, cartoons, graphics, video and audio content, and gamified or interactive content that will attract and interest Children, rather than relying solely on written communications
Choice Architecture	The inputs to a recommender system that may be controlled or modified by the AI Subject
Code of Data Ethics	Set of guidelines, principles and procedures by which data is acquired, analysed, 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 organisation's Ethics Committee and outlines said organisation's shared moral framework within the Relevant



Defined Term	Definition
	Legal Frameworks, providing context to instances of Ethical Choice, diversity and anti-discrimination
Cognitive Bias	The way a particular person understands events, facts, and other people, which is based on their own particular set of beliefs and experiences and may not be accurate in regards to the Data Subject or sample population resulting in discriminatory outcomes (e.g., confirmation bias, anchoring bias)
Committee Governance Assessment	An analysis and designation of accountability, oversight and responsibility for committees (Ethics Committee, Algorithmic Risk Committee, and specialty committees such as the Children’s Data Oversight Committee, Disability Inclusion and Accessibility 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
Common Specification	a document, other than a standard, containing technical solutions providing a means to, comply with certain requirements and obligations established under this Regulation
Concept Drift	The change in the measured relationships (e.g., correlation, covariance) between input and output data resulting in misalignment
Confidentiality	The degree to which a product or system ensures that data are accessible only to those authorised to have access [SOURCE: ISO/IEC 25010:2011]
Conformity Assessment Report	Record and document publicly that the AAA System meets established conformity assessment criteria in regards to the EU AI Act, including the assurance provided by a duly authorised Notified Body.



Defined Term	Definition
Conformity Assessment Body	a body that performs third-party conformity assessment activities, including testing, certification and inspection
Consent (EU)	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her
Construct validity	How well a set of indicators represent or reflect a concept that is not directly measurable. The extent to which feature (indicator) relevance, Functional Correctness , and causality of a model or algorithm represent the ground truth with the theoretical construct
Context	The circumstances in which an event occurs; including jurisdiction and/or location, behaviour and functional inputs to an AAA System that are appropriate (e.g. domain, operating environment)
Contingency Plan	A plan to make the system inaccessible and unavailable, or to continue processing, in the context of a security related event.
Controllability	degree to which a Provider, Deployer and/or AI Subject can appropriately intervene in an AAA System's functioning in a timely manner Modified from the ISO definition [SOURCE: ISO/IEC 25059:2023]
Corrective Action Plan	Summarizing responses to a Change Management Plan or Incident Response, including containment, eradication, recovery, and implementation of new risk controls, treatments, and/or mitigations
Cybersecurity Risk Log	A separate and secure risk log that contains risk inputs and indicators in regards to security and cybersecurity risks and vulnerabilities



Defined Term	Definition
Data Age	The elapsed time between the original acquisition or compilation of each datum and current state
Data Curation Report	Documenting the evaluation of the system's sample data and describing the data collection process including Availability , quantity, suitability, Provenance , sampling method, Ground Truth Availability /verifiability. Documenting the sample data preparation process, including the treatment of anomalies and exceptions, specifying data cleaning, encoding, transforming, enriching and aggregating tasks.
Data Drift	Occurs when the distribution of incoming data to a model changes over time, or differs from the data used to train and test the model resulting in misalignment
Data Evaluation Report	Documenting a technical understanding of the sample data, including describing, in detail, the statistical characteristics (syntactic metadata) of the sample data (e.g., range, mean, median, mode, missing values, volatility, shape, modality, ratio of features values, data format). Documenting that the sample data is sufficiently diverse, balanced, and representative including all bias remediations
Data Entry Point Attacks	Vulnerabilities and attacks associated with the data used for training and processing data, where the adversary manipulates the data in order to attack, alter or otherwise corrupt the intended purpose, scope and nature of the algorithmic system (e.g., data poisoning, model inversion, model evasion)
Data Flow Diagram	Picture or graphic which visually represents all inputs and outputs of data (e.g., Personal and Non-Personal Data) associated with an AI, Algorithmic or Autonomous (AAA) System across controller and processor relationships including databases, processing, flow and movements, pipeline, data collection, UX interfaces, location/Jurisdiction
Data Integrity	A property possessed by data items that have not been altered in an unauthorised manner since they were created,



Defined Term	Definition
	transmitted, or stored (NIST)
Data Lead	An expert accountable for data governance and management of an AAA System
Data Poisoning	An adversarial attack targeted at training, testing/validation, Data Quality , Information Quality , Pipeline Data in an attempt to render the data useless or alter/damage the model's ability to achieve its scope, nature, context and purpose potentially altering outputs in favour of the adversary. Intentional subversion of Data Quality
Data Protection Impact Assessment	To assess the data protection risks related to the processing of Personal Data
Data Quality	Data that is expected to be fit for purpose, representative, and aligned to the Scope, Nature, Context and Purpose of the intended use as applicable to an AAA System. Data Quality is characterised as complete, accurate, categorically representative, consistent, precise collected from reasonably calibrated sensors, surveys, or other tools to gather data
Data Subject	An identifiable natural person who can be identified, directly or indirectly, in particular by referencing an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. SOURCE - (EU) 2016/679
Data Transparency Document	A clear and plain language, public report created by the Algorithmic Risk Committee designed to collect and document all relevant steps taken by the Ethics Committee and the Algorithmic Risk Committee to mitigate risk of Bias , insufficient Data , Information , and Pipeline Quality
Dataset	A collection of data intended for use in AI, algorithmic or autonomous systems



Defined Term	Definition
	<ol style="list-style-type: none">1) Raw - capture of data, prior to any manipulation (e.g. cleaning, labelling, organising) as acquired from any source in its original form2) Structured - collection of data, post enhancement by cleaning, labelling, organising)
Deceptive Design	Encompasses “dark patterns”, coercion, conditioning and subliminal behaviour modifications
Decommissioning Policy	A document that identifies all of the process, procedures, metrics, measurements and thresholds that might lead to decommissioning of the AAA System
Deletion	(delete) in the context of data, is when data is removed and is no longer available in plain sight or can easily be recovered
Deployer (EU)	A natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity (Source EU AI Act)
Deployer and AI Subject Contract log	A log of contractual relationships between the Provider and a Deployer or AI Subject including required deliverables per the contract (related/integrated to AAA Systems List and Identity and Access Management log)
Deployment Testing Dataset	Data used for providing an independent evaluation of the AAA System deployment output after combining a Provider’s (TTV) and Deployer’s datasets (Augmentation) in order to confirm the expected performance of that system before deployment
Destruction	(destroy) in the context of data, is when data is removed from your device and can never be restored, even be professional data recovery experts
Disabled Person(s)/	Includes those who have long-term physical, mental,



Defined Term	Definition
People with Disabilities (EU)	intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others
Disability Inclusion and Accessibility Committee (DIAC)	A group of 3 or more people which may comprise outside experts, tasked with reviewing all aspects of data collection, risk and procedures associated with data related to Persons with Disabilities for the Jurisdiction
Discrimination	Treatment or consideration based on class or category (interaction focused - injustice, partiality, or deception)
Distributor	any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market without affecting its properties
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 representation of lived experiences, backgrounds, cultures, diversity of thought processes, skills, expertise (including domain experts), and inclusion of Protected Categories and Intersectionalities . 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 Algorithmic Risk Assessment)
Emergent Risk	An unforeseen risk that was not contemplated and is presently manifest as a harm or incident. A risk where the potential for harm or loss is not fully known presently.
Emotion Recognition System	An AI system for the purpose of identifying or inferring emotions or intentions (including apparent expressions (e.g., frown, smile, raised voice, whispering) gestures and movements), of natural persons on the basis of their biometric data, excludes physical states such as pain or fatigue



Defined Term	Definition
Ethical Choice	For a natural person, an ethical choice is the result, outcome or judgement made using a shared moral framework, or set of moral principles based upon the organisation's Code of Ethics. It requires awareness and consideration of a set of options to be made in the context of Artificial intelligence, algorithmic or autonomous 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
Ethical Choice Curriculum	Body of learning designed to raise awareness of instances of Ethical Choice for designers, developers, governance and oversight teams involved in the creation of AI, algorithmic and autonomous systems. The curriculum raises awareness of instances of Ethical Choice as well as the organisation's preferred procedure for handling the instance of Ethical Choice.
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 organisation. The Ethics Committee is responsible for all instance of Ethical Choice related to AI, algorithmic and autonomous systems and producing the Ethical Risk Assessment
Ethical Risk Assessment	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.
Event Log	<p>An event is any activity carried out by the system(e.g., request for data, remote login, automatic shutdown of the system, or deletion of a file) or through an interaction with the system.</p> <p>The Event Log must contain five main components:</p> <ul style="list-style-type: none">● user ID



Defined Term	Definition
	<ul style="list-style-type: none">• System activity can be monitored to identify what took place.• At a certain date and time, an event occurred.• The event took place on the device/system and its location was identified.• Network addresses and protocols – IP information. <p>Paraphrased from [ISO 27001:2002]</p>
Exceptions Interpretability	<p>A timely interface designed for human oversight during the period in which the AAA System is in use for identification of:</p> <ul style="list-style-type: none">A. Anomalies,B. Dysfunctions,C. Exceptions,D. Expected foreseeable misuse,E. False positive and false negativeF. Key Risk Indicators (KRIs) <p>to enable and empower a Human-in-Command to stop, pause, disregard, override, and reverse the AAA System</p>
Explainability Statement (EU AI Act)	<p>A description of the AAA System, its logic and any applicable automated decision-making, including profiling (inferences), when the outcome impacts the health, safety, and fundamental rights of an AI Subject that sufficiently describes the model in plain language in order to provide understanding to the AI Subject on how conclusions were reached both globally and in the context of a specific case (locally)</p>
Explainability+	<p>A human-centric process by which an AI Subject is helped to understand the decision making process and educated on how they could have earned a favourable result from the system, in order to improve their interaction, their outcome or their satisfaction</p>
Failure Mode and Effects Analysis	<p>A methodology for collecting knowledge about possible points of failure in a design, process, product, or service</p>



Defined Term	Definition
Free and Open-Source license	allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available
Functional Correctness	The degree to which a product or system provides the correct results with the needed degree of precision [SOURCE ISO/IEC 25010:2011, 4.2.1.2]
Fundamental Right Impact Assessment	An analysis of the manner in which an AAA Systems interacts with the rights and freedoms guaranteed to EU Citizens under the Charter of the EU
General Data Protection Regulation (GDPR)	General Data Protection Regulation, passed by the EU and put into effect in 2018, governs certain rights and principles around personal data for individuals - (EU) 2016/679
General Purpose AI	An AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market
General Purpose AI Technical Specifications	Requirements as listed in Annex XI, including documentation of energy consumption and compute resources
Geolocation	process of finding, determining and providing the exact location of a computer, phone, tablet, networking device or equipment, and may including inputs such as wifi, IP Address, bluetooth connectivity, GPS, latitude, longitude, altitude, direction of movement and time period recorded



Defined Term	Definition
Ground Truth	Information ascertainable as real or true through observation or experience
Guardian	person of legal age and ability who can act on behalf of an Minor, Child or Disabled person
Harmonised Standard	A European standard as defined in Article 2(1)(c) of Regulation (EU) No 1025/2012
Human Interactions Report	this report tracks all human interactions, their effectiveness and impact on a AAA System produced and kept current by the Human-in-Command
Human Interactions Log	This records all Human-in/on-the-Loop/Command interactions with the high risk AAA System , including measures implemented during interactions
Human-in-Command	A natural person assigned by a system Provider or Deployer to act as no less than a 3rd line of defence governance Human-on-the-Loop, knowing the Capacity and limitations of the system, possessing sufficient training for the regular operation including the identification of anomalies, dysfunctions and unexpected performance.
Human-in-the-loop	Any model that is unable to offer an answer or conclude processing without human intervention
Human-on-the-loop	Human supervision and/or control of AI, algorithmic or autonomous systems, however the system is able to conclude processing without the need for human intervention
Illegal Content	Any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law
Importer	A natural or legal person located or established in the Union that places on the market an AI system that bears the name



Defined Term	Definition
	or trademark of a natural or legal person established in a third country (Source EU AI Act)
Inclusivity Risk Assessment	A process examining Training Data, designed to identify risk inputs associated with bias, inclusivity, accessibility, safety and security of AAA Systems, and further identify treatments and mitigation. The testing examines the potential for adverse incidents associated with AAA Systems when tested with extreme examples (including black swan, fat-tail, boundary values, failure of expected inter-relationships etc) and “Edge-in” thinking designed to balance the innate nature of most algorithms to “normalise” or find the “best fit”
Inequality	Unfair situation in society when one protected category has different opportunities (different starting, ending points or access to necessary tools)
Inference	Assumption or conclusion reached by a data processing algorithm, which may not be treated as fact and shall be labelled as such.
Information Quality	Data Quality that has demonstrated fitness for purpose, representative and aligned to the Scope, Nature, Context and Purpose of the intended use as applicable to an AAA System . Information Quality is characterised by Construct Validity, Provenance, Authority, Authenticity, Relevance, and Data age , legal basis and Consent , if applicable
Instructions for Use	The information provided by the Provider to inform the Deployer of in particular an AAA System’s intended Purpose and proper use, inclusive of the specific geographical, behavioural or functional setting within which the high-risk AAA System is intended to be used
Integration Test Plan	Detailed description of test objectives to be achieved and the means and schedule for achieving them, organised to coordinate testing activities for some test item or set of test



Defined Term	Definition
	items [SOURCE: ISO/IEC/IEEE 29119-2:2021, 3.50]
Integration Testing Dataset	Test Data , exclusive to a Deployer , that combines the Provider's AAA System , Deployer's Pipeline Data , and data generated by the nature and context (e.g., cloud storage performance data) of the deployment, for the Integration Test Plan
Integrity	The degree to which a system, product or component prevents unauthorised access to, or modification of, AAA Systems and/or data Modified from [SOURCE: ISO/IEC 25010:2011]
Internal Independence	A requirement that natural persons assigned to assess or validate any of the following: <ol style="list-style-type: none">1. specifications,2. requirements,3. processes,4. procedures, or5. Implementations were not involved in the design, development, data curation, or implementation of the assessed or validated activities
Internal Sign Off Report	Assess whether the system is fit to be deployed, legally, ethically and consistently with the original Causal Hypothesis , especially in consideration of impacts to health, safety, and fundamental rights.
Interpretability	The output of a system, using technical language or jargon that allows a design, developer or expert Deployer of the system tune the model for further training or learning
Intersectionalities	The places, ways, and sources of Inequality in systems based on combinations of gender, race, ethnicity, sexual



Defined Term	Definition
	orientation, gender identity, disability, class, and other forms of discrimination to create unique dynamics and effects. A subset of categories of Protected Categories .
Intervenability	Degree to which an operator can intervene in an AI system's functioning in a timely manner to prevent harm or hazard [SOURCE: ISO/IEC 25059:2023]
Jurisdiction	A defined geographic area over which a particular legal authority may lawfully exercise control
Just-in-Time	The moment a notification is presented to the AI Subject prior to an interaction with the AAA System that could be any of the following: A. A statement of rights (e.g., Disability Inclusion and Accessibility Statement) B. A legal obligation (e.g., the collection of Personal Data) C. Terms and conditions
Key Detrimental Indicators (Digital Services Act)	Parameterised content, where the content, regardless of medium (e.g., AR/VR, audio, images, video, profile/comments, etc), is determined to be any of the following: A. Illegal Content (e.g., Terrorism, Child Sex Abuse Material, Hate Speech , discriminatory) B. harmful or negatively impacting to the well-being of recipient of the service, including Vulnerable Populations , such as: a. Adult Content b. Bullying c. Defamatory/Slander/Libellous content d. Misrepresentation and identity fraud e. glorification of self-harm, suicide, violence, and disorders



Defined Term	Definition
	<ul style="list-style-type: none">f. intentional censorship designed to circumvent monitoring (e.g., F***, S*!T)g. Representations of any of the aforementioned items (e.g., emojis, GIFs)h. Via goods or services (e.g., Spam, Malware, illegal goods, fraud) <p>C. Disinformation</p> <p>D. restricted by guidelines and codes of practice</p> <p>E. Breach of copyright and other intellectual property rights</p> <p>where the parameters are subsequently deployed for monitoring and measuring in order to censor, filter or restrict the content in the ISS</p>
Key Language Indicators	Parameterised content, in the context of KSA's (e.g., ESCO , ONET), and Protected Categoriness (e.g., Ageism, Racism, Genderised, Ableism terms), that are designed to identify and remediate word choices, from an LLM, LMM, or questionnaire that could otherwise bias the reader and lead to a discriminatory outcome
Key Performance Indicators (KPIs)	Measurements indicated in advance to determine the success or failure of an algorithmic model to achieve its purposes
Key Regulated Product Indicators (Digital Services Act)	<p>Parameterised content, where the content regardless of medium(e.g., AR/VR, audio, images, video, profile/comments, etc), is related to a product or service and is determined to be any of the following:</p> <ul style="list-style-type: none">A. Illegal Content (e.g., Terrorism, Child Sex Abuse Material, Trafficking)B. Fraudulent, or infringing of a copyright or intellectual propertyC. Regulated Goods, sold or displayed improperly (e.g., weapons, alcohol, tobacco, pharmaceuticals, illicit drugs)D. Regulated Services (e.g., Financial products)E. Adult Content and age-restricted sales of goods and



Defined Term	Definition
	<p>services</p> <p>F. Regulated Goods biologics (e.g., bacteria, virus, fungus, livestock, plants and seeds, birds, fish and sea creatures)</p> <p>G. Illegal cultural appropriation</p> <p>H. Regulated Military or Defence industry items</p> <p>I. Regulated or illicit services</p> <p>J. Monetary items and assets</p> <p>K. Regulated electronics, code, or technology (e.g., software or hardware)</p> <p>L. Online gambling</p>
Key Risk Indicators (KRIs)	<p>Measurements and thresholds of model health and fitness that identify any of the following:</p> <p>A. A realised deviation based upon any of the following:</p> <ol style="list-style-type: none">Pipeline data that fails to conform to the data schemeExceptions Interpretability outputs identifying anomalies, outliers, or exceptionsAAA System output that exceeds thresholdsAdverse Incident Reports that exceed thresholds, <p>B. A new, Emergent Risk</p>
Knowledge, Skills, and Abilities (KSA)	<p>In the context of different sectors, job categories and positions, KSAs (e.g., ONET, ESCO) are pre-defined descriptions of traits/attributes that are relevant or necessary for the successful performance of a job or occupation and are used to assess (e.g., hiring, performance measurement, training & development) candidates, employees, contractors, or gig-workers in the workplace</p>
Making Available on the Market	<p>Any supply of an AI system for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge</p>
Market Surveillance Authority	<p>The national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020</p>



Defined Term	Definition
Metadata	Information about a datum (e.g. location, owner, date, time)
Model Drift	Any change (degradation or improvement) in the predictive performance of a model that results in a change to the scope, nature, context, and purpose of the model resulting in misalignment
Monitoring Lead	An expert accountable for continuous and post market monitoring of the AAA System
National Competent Authority	Means any of the following, the national supervisory authority, the notifying authority and the Market Surveillance Authority. As regards AI systems put into service or used by EU institutions, agencies, offices and bodies, the European Data Protection Supervisor shall fulfil the responsibilities that in the Member States are entrusted to the national competent authority and, as relevant, any reference to national competent authorities or National Competent Authority in this Regulation shall be understood as referring to the European Data Protection Supervisor
National Supervisory Authority	The authority to which a Member State assigns the responsibility for the implementation and application of this Regulation, for coordinating the activities entrusted to that Member State, for acting as the single contact point for the Commission, and for representing the Member State at the European Artificial Intelligence Board
Nature	The forces and processes that influence and control the variables and features (e.g., foreseeable conditions, input variables)
Necessity Assessment	Produced by the Algorithmic Risk Committee in consultation with the Ethics Committee , who are guided by the Code of Ethics and principles portion of the Code of Data Ethics , to determine whether an AAA System is the only or best solution, considering a comprehensive set of



Defined Term	Definition
	stakeholders, in the context of the legal basis. Additionally, it analyses and determines whether the inclusion of each Personal Datum collected and processed by AAA System is vital.
Notified Body	A conformity assessment body designated in accordance with this Regulation and other relevant Union harmonisation legislation
Novel	Having the characteristics of being one of the following: 1) unique, 2) unprecedented, or 3) innovative and therefore possessing insufficient comparables or industry standards resulting in an unknowable risk profile
Nudge (Nudging)	Design, interfaces and notifications of an AAA System that leverage concepts found in behavioural economics, political theory, and behavioural sciences, to reinforce, suggest, or influence (consciously or subconsciously) the behaviour, actions, or decision-making of individuals or groups
Penetration Testing	Testing technique aiming to exploit security vulnerabilities (known or unknown) to gain unauthorised access
Persona	Persona 1 = Users (non-employees) Persona 2 = Employees impacted by the AI System Persona 3 = Employees* working on the AI System directly Persona 4 = Top Management and Oversight Bodies Persona 5 = AI Leaders, decision-makers for the AI System
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 specialised terms such as Inferences, Proxy Variables, and Special Category Data



Defined Term	Definition
Place(ing) on the Market	The first making available of an AI system on the Union market
Pipeline Data	Inputs to an operational AAA System from external sources (including natural persons) via a predetermined collection mechanism
Pipeline Quality	The nature of the live data input into an operating (live) AAA System, including the manner in which the data matches to the data schema
Post-market Monitoring	All activities carried out by providers of AI systems to proactively collect and review experience gained from the use of AI systems they Place on the Market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions
Profiling Decline	A Deployer or AI Subject interface that allows the Deployer or AI Subject to opt out of recommendation engines or other content moderation through the use of Profiling
Profile Reset	A Deployer or AI Subject interface that allows the Deployer or AI Subject to zero-out or completely reset the profile created by the Provider of the system for the Deployers or AI Subject interface with the AAA System
Profile Re-engage	A Deployer or AI Subject interface that allows the Deployer or AI Subject to reapply their Profile to the AAA System after a period of Profiling Decline or Profiling Reset
Profiling	Any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour location or movements



Defined Term	Definition
Proportionality Study	Conducted prior to a DPIA , it is a documented study conducted by the Ethics Committee to assess tensions and Tradeoffs between risks to and sacrifices of the rights and freedoms of individuals or groups, balanced against the potential benefits and gains to an individual or group in the context of the Relevant Legal Frameworks
Protected Category(ies)	Defined under law or regulation by Jurisdiction, may include race, age, gender, religion, ability/disability, sexual orientation, creed, colour, nation of origin, socioeconomic class etc
Provenance	The history and traceability of the supply chain especially when documented or authenticated
Provider	A natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge
Pseudonymisation	Processing of personal data in such a manner that the personal data can no longer be attributed to a specific Data Subject without the use of additional information
Publicly	Refers to something that is broadly available to a wide range of people outside a particular individual, company, or select group (e.g., a public-facing website, public regulatory filing, public announcement, report, advertisement, or consumer-facing document)
Publicly Accessible Space	Referring to any physical space that is accessible to an undetermined number of natural persons, and irrespective of whether the space in question is privately or publicly owned, irrespective of the activity for which the space may be used or regardless of potential capacity or security restrictions, access is subject to certain predetermined conditions which can be fulfilled by an undetermined number of persons



Defined Term	Definition
Purpose	The aim or goal of a system (e.g., limitations, variants)
Putting into Service	The supply of an AI system for first use directly to the Deployer or for own use on the Union market for its intended Purpose
QMS Audit Report	Generated by the Quality Management Lead in the context of the Quality Management Policy it documents the validation of quality objectives, controls and assurance processes
Quality Management Lead	An expert accountable for quality functions (e.g., control, assurance, validation) for a designated AAA System
Quality Management System	A system that captures all policies, procedures and written guidance for compliance with Chapter 2 of the Act, including policies, guidance, instructions, user guides, metrics, thresholds, technical specifications, data management and required documentation. It also includes an operations manual for the risk management system, regulatory compliance, record-keeping, post-market monitoring and Adverse Incident Reporting Systems, communications with National and EU authorities
Reasonably Foreseeable Misuse	The use of an AAA System in a way that is not in accordance with its intended Purpose , but which may result from interaction with other systems or identified by human accessors for potentially negative impacts beyond the intended Scope, Nature, Context, and Purpose
Recall of an AI Systems	Any measure aimed at achieving the return to the Provider of an AAA System made available to Deployers
Relevance	The appropriateness and meaningfulness of each datum, feature, and Causal Hypothesis to the Scope, Nature, Context, and Purpose of the AAA System



Defined Term	Definition
Relevant Legal Frameworks	The collection of applicable law such as the laws that govern an entity or organisation, that govern the rights, freedoms, and privileges of a Data Subject or AI Subject , that restrict the activities and behaviors or put positive obligations upon a Provider or Deployer
Reliability	Degree to AAA System performs specified functions under specified conditions for a specified period of time. [SOURCE - ISO 25000]
Remote Biometric Identification System	An AAA System for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AAA System whether the person will be present and can be identified
Representativeness	Describes a measurement of the AAA System dataset, especially for a Protected Category , Intersectionality , and Vulnerable Populations , that it has comparable statistical characteristics between the training, validation, and testing datasets related to at least two different benchmarks (within a reasonable confidence level), 1) general population and 2) a reasonable explanation of the source, sample, and pipeline (target) population, with the aim of the AAA System dataset being reasonably similar
Residual Risk	The documented sum of all unmitigated risk pertaining a AAA System
Resilience	In the context of a major disruption, the ability of the system to withstand and recover. The speed and capability to return to a sufficient level of function in accordance with the system's intended operation.
Risk Appetite	The type, amount and threshold of risk that an organisation is prepared to accept in pursuit of its strategic objectives and business plan.



Defined Term	Definition
Risk Tolerance	The acceptable level of variation relative to the achievement of objectives. In setting-specific risk tolerances, management considers the relative importance of related objectives and aligns risk tolerance with risk appetite.
Robustness	Degree to which an AAA System can maintain its level of functional correctness under any circumstances [SOURCE: ISO/IEC 25059:2023]
Safety Component of a Product or System	A component of a product or of a system which fulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property
Scope	The boundaries of a system, what is covered, what is not covered (i.e, in scope, out-of-scope)
Service Provider	Third-party contracted provider who is supplying critical infrastructure and services to the organisation
Social Scoring	An AAA System that evaluates or classifies natural persons or groups thereof on the basis of multiple data points related to their social behaviour in multiple contexts or known, inferred or predicted personal or personality characteristics over certain periods of time - paraphrase from Recital 31 of (EU) 2024/1689
Source Data	Set of inputs gathered from outside the model environment
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: (EU) 2016/679)
Statistical Bias	Systematic and repeatable errors in a computer system that create unfair outcomes, applied specifically to Protected



Defined Term	Definition
	Categories, Intersectionalities and Vulnerable Populations resulting in discriminatory outcomes
Substantial Modification	A change to the AAA System following its placing on the market or putting into service which affects the compliance of the AAA System with the requirements set out in Title III, Chapter 2 of this Regulation or results in a modification to the intended Purpose for which the AAA System has been assessed
Synthetic Data	Artificial data, without Provenance, Authority, or Authenticity , (not include data anonymization techniques e.g., masking) that is generated from original Source Data and represents characteristics of the original Source Data
System Architecture Report	Document the overall, top-level blueprint of conceptual/logical/physical structure of the system including relevant frameworks (e.g., TOGAF, Zachman) and applicable standards (e.g., ISO, CEN/CENELEC, IEEE)
System Design Report	Documents the design of the system and its design choices and associated rationale, notably in the areas of human interactions with the system, including pros and cons, tensions and Trade-offs amongst choices, especially in the context of Protected Categories and Vulnerable Populations and log design choices of the overall system at various levels of granularity based upon the complexity of the system
System Development Report	Document the development process followed in building the system including approach, phases, methods (CRISP-DM,



Defined Term	Definition
	SDLC), techniques, procedures, and tools
Systemic Societal Impact Analysis	A study designed to consider, track and measure the importance (risk and/or potential negative impact), authority, saturation, and dependency of socio-technical systems to individuals, communities, nation-states or society-at-large in order to signal shifting levels of risk that likely require risk reassessment
Technology Barrier Bias	Also known as Non-Response Bias, a phenomenon in which the availability, accessibility, and usability of the technology used to gather data or interface with the AAA System results in certain participants having reduced ability to participate which affects their representativeness in the dataset, potentially resulting in biased estimates and discriminatory outcomes
Integration Test Completion Report	report that provides a summary of the testing that was performed across the end-to-end system including test procedures, metrics, measurements, and thresholds, testing artefacts, and model/system test types. [SOURCE: ISO/IEC/IEEE 29119-3:2021, 3.9]
Test Data	A set of data required to evaluate the Integration Test Plan objectives (e.g., inputs, outputs, ground truth)
Test Item	Work product to be tested
Test Lead	An expert accountable for the Integration Test Plan and Integration Test Completion Report for an AAA System








Defined Term	Definition
Test Objective	Reason for performing testing [SOURCE: ISO/IEC/IEEE 29119-2:2021, 3.55]
Testing Data	data used for providing an independent evaluation of the trained and validated AI system in order to confirm the expected performance of that system before its placing on the market or putting into service
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
Trade-offs	Decision-making actions that select from various requirements and alternative solutions on the basis of net benefit to the stakeholders [SOURCE: ISO/IEC/IEEE 15288]
Training Data	data used for training an AI system through fitting its learnable parameters, including the weights of a neural network
Usability	A type of user acceptance testing that identifies barriers to usage by considering the needs of impacted stakeholders and Vulnerable Populations , including people with a variety of disabilities (e.g., physical, sensory, cognitive, etc.), and assessing the Scope, Nature, Context, and Purpose of the AAA System in terms of use cases, foreseeable scenarios, languages, use of Assistive Technologies, and key modalities of the AAA System
Validation Data	Data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process, among other things, in order to prevent overfitting



Defined Term	Definition
Validity	The extent to which the results really measure what they are supposed to measure (intended Purpose) presently and as time passes distinct from the concept of a (validation) dataset as it relates to training and testing data.
Version Control and Change Log	Collects all human deliberative changes, combined with alterations to Pipeline , outcomes, and Architectural Inputs across the lifecycle of the AAA System (Annex IV.6) A description of any change made to the system through its lifecycle; including changes required by a Notified Body
Vulnerable Populations (People in vulnerable situations)	Persons who often experience exclusion, insufficient accessibility resulting from geopolitical, social, socioeconomic, and cultural inequitable power distribution including but not limited to: children, persons with disabilities, ethnic minorities, and people made vulnerable by an imbalance of power in relation to knowledge, economic or social circumstances, or age
Withdrawal of an AI Systems	Any measure aimed at preventing the distribution, display and offer of an AI system

3.1 Policies, Plans, and Assessments

Policy, Plan, or Assessment	 File Link
Algorithmic Risk Assessment	 ForHumanity CORE AAA System Governance Prov...
Bias Mitigation Policy	 ForHumanity CORE AAA System Governance Prov...
Business Continuity Plan	 ForHumanity Cybersecurity Certification Scheme
Change Management Impact Assessment	 ForHumanity CORE AAA System Governance Prov...



Change Management Plan	ForHumanity CORE AAA System Governance Prov...
Committee Governance Assessment	ForHumanity CORE AAA System Governance Prov...
Contingency Plan	ForHumanity Cybersecurity Certification Scheme
Cybersecurity Risk Management Policy	ForHumanity Cybersecurity Certification Scheme
Data Management and Governance Policy	ForHumanity CORE AAA System Governance Prov...
Data Protection Impact Assessment	ForHumanity CORE AAA System Governance Prov...
Data Protection Policy	ForHumanity's EU GDPR Controller Certification ...
Data Security Policy	ForHumanity's EU GDPR Controller Certification ...
Decommissioning Policy	ForHumanity CORE AAA System Governance Prov...
Ethical Risk Assessment	ForHumanity CORE AAA System Governance Prov...
Fundamental Rights Impact Assessment	ForHumanity CORE AAA System Governance Prov...
Human Interactions Policy	ForHumanity CORE AAA System Governance Prov...
Incident Response Policy	ForHumanity CORE AAA System Governance Prov...
Inclusivity Risk Assessment	ForHumanity CORE AAA System Governance Prov...
Monitoring Policy	ForHumanity CORE AAA System Governance Prov...
Necessity Assessment	ForHumanity CORE AAA System Governance Prov...
Restoration Prioritization Plan	ForHumanity Cybersecurity Certification Scheme
Quality Management Policy	ForHumanity CORE AAA System Governance Prov...
Real-time Biometric Identification Policy	EU Artificial Intelligence Act Provider-only v1.5



Real World Integration Test Plan	EU Artificial Intelligence Act Provider-only v1.5
Risk Management Policy	ForHumanity CORE AAA System Governance Prov...
Security Policy	ForHumanity Cybersecurity Certification Scheme
Integration Test Plan	ForHumanity CORE AAA System Governance Prov...
Vendor Due Diligence and Procurement Policy	ForHumanity CORE AAA System Governance Prov...
Vendor Procurement Plan	ForHumanity CORE AAA System Governance Prov...

4.0 General Requirements for Accreditation

4.1 Interoperability with Standards

ForHumanity's work is designed primarily to ensure an ecosystem called Independent Audit of AI Systems. This ecosystem establishes an infrastructure of trust, predicated on third party, independent assurance of compliance with rules that are either approved by governments and regulators or accepted in the marketplace. This assurance is "at-risk", meaning the independent auditor can be held liable for "false assurance of compliance". As a result of this high standard of behaviour, auditors seek maximum, binary clarity on the criteria that determines compliance and non-compliance.

The goal of maximising the binary (compliant/non-compliant) nature of each audit criteria can be incompatible with industry-led, consensus driven standards from Standards Development Organisations (SDOs). As a result of traditional SDO processes, consensus outcomes sometimes do not reach adequate risk control, treatment, and mitigation for humanity.

Additionally, while some SDOs and their specific standards are accepted widely, some critical national and regional divides occur (such as NIST versus ISO adoption of cybersecurity or risk management in artificial intelligence). This divide makes compliance challenging for corporations acting globally. ForHumanity drafts certification schemes (collection of audit criteria) that are jurisdictionally-sensitive and globally harmonised.

Finally, SDOs are typically industry-led and only recently have begun to factor in a wider perspective of stakeholders. The historical result is that the focus has been on organisational



risk management and compliance rather than the risks to the user/AI subject/natural person. ForHumanity's mission is to examine and analyse downside risk associated with the ubiquitous advance of AI, algorithmic and autonomous systems and where possible to engage in risk mitigation to maximise the benefits of these systems... ForHumanity. Therefore, when ForHumanity draft our audit criteria and certification schemes, our different perspective leads us to different human-centric audit criteria.

It is in these three challenges of the SDO process that ForHumanity finds its role. Our primary work is to provide human-centric, binary and globally harmonised audit criteria in support of Independent Auditors and the second-order benefit of facilitating compliance.

As a result of this mission, ForHumanity make the following declarations:

1. In upholding its mission, ForHumanity will ensure that our perspective remains human-centric in our output of audit criteria and certification schemes
2. ForHumanity fully supports the work of SDOs
 - a. ForHumanity participates in many SDOs and will continue to expand our efforts to support the development of standards
 - b. ForHumanity offers its own crowdsourced, transparent, and expert work in creating binary audit standards that support the development of traditional standards
 - c. ForHumanity's audit criteria will always reference accepted, published standards, relevant and consistent with ForHumanity's scope of AI, Algorithmic, and Autonomous (AAA) Systems
3. ForHumanity will ensure that our audit criteria:
 - a. Are aligned to accepted, published standards that are legally binding, relevant and consistent with ForHumanity's scope of AI, Algorithmic, and Autonomous (AAA) Systems
 - b. Are binary (compliant/non-compliant), implementable, and measurable to accepted forms of evaluation methods for third party independent auditors such as (but not limited to) procedure manuals, published codes, correspondence, physical testing, official filings, pictures/graphics, and contracts
 - c. Maximise global harmony, as applicable to facilitate compliance for multi jurisdictional companies

4.2 Normative Criteria explanation

Normative criteria take one of three forms shall/should/may and each are described below including how each term is satisfied in the audit certification scheme. All criteria require documentary evidence, including "may" criterion as they indicate a choice leading to further criteria or disclosures.



SHALL - is a requirement. There is no compliance without sufficient satisfaction with the requirements of the criterion. A criterion is a SHALL because it is a legal requirement, a regulatory requirement, or a non-negotiable imperative for the protection of an individual or management/mitigation of a risk to individuals, and has been determined feasible to comply. Strictly from a risk perspective, failure to comply with a SHALL criterion absolutely and unequivocally exposes the organisation to risk and non-compliance with the certification scheme.

SHOULD - is a recommendation. It is within the power and judgement of an organisation to decide if it will comply or not. However, SHOULD identifies the recommended option. Therefore, if the organisation makes the choice to not comply, it must recognize and acknowledge that a risk is present and has been accepted. Therefore, audit compliance for a SHOULD statement can take one of two forms. Either documented compliance with the SHOULD statement or documented acceptance of the risk taken, “why” the risk is tolerable, and non-compliance with the criterion is accepted. From a risk perspective, the choice to not comply with a SHOULD statement exposes the organisation to risk, but the organisation may determine the subsequent risk to be tolerable, unlikely to occur, or mitigated in some other fashion. The assessment and associated mitigations are to be documented.

MAY - is a choice without prejudice to the options. It has been determined that compliance or non-compliance with the criterion by itself is neither positive nor negative for humanity inherently. MAY statements will often lead to documented risks that will lead to further compliance requirements based upon the choice. MAY statements exist to clarify for the organisation that it does, in fact, have a choice. For audit compliance purposes, the target of evaluation should document the choice it makes. This documentation must also reflect the pros and cons of the choice. Audit compliance is satisfied by this documentation. The choice made in response to a MAY question does NOT mean there is no inherent risk. Each choice has risks associated with it and they should be assessed and documented in the risk assessment process.

4.3 Documentation of Assessments and Certification

Certifications may only be conducted by ForHumanity Certified Auditors (FHCA) under contract with accredited entities as established by local accreditation authorities. Certification is available for individuals who demonstrate sufficient knowledge of the scheme and achieve a passing grade on the certification exam.

The following documents shall be produced by the certifying body in order to ensure that the certification is rigorous, transparent, and itself auditable.



A. Certification Plan, including:

- i. Opening meeting where:
 1. The scope is verified
 2. Organisations and individuals, including their roles, are documented
- ii. Confirmation of the authorisation of the Certification Body to award the certification, and their impartiality
- iii. Description of the ToE (as documented in the contract)
- iv. Documentation of the Relevant Legal Framework (according to criteria #6) applicable to the AAA System and associated ecosystem including the role of the Auditee (e.g., Controller/Processor, Provider/Deployer)
- v. Expected documentary evidence
- vi. Physical testing scheduling
- vii. Any expected deviations from the evaluation methods detailed in the certification criteria
- viii. Any site or network access required, and any special requirements for that access (e.g. permission to conduct intrusive network scanning)
- ix. Closing meeting for presentation of Certification Report, issuance of Certification, or issuance of Non-Compliance Letter

B. Certification Report that has two versions, a Public version based upon Relevant Legal Framework requirements and a private version for the auditee, including:

Public

- i. Public disclaimer including description of the Scope, Nature, Context, and Purpose of the AAA System (Public)
- ii. The specific dates of inspections (Public)
- iii. Intended users of the certification report (e.g., investors, clients, regulatory compliance) (Public)
- iv. Whether a certification is awarded, and its duration (Public)

Private

- v. Explanation of the scope, including Beginnings and Ends, agreed in the Audit Engagement Letter (private)
- vi. Any deviations from the Certification Plan (private)
- vii. Process narratives, walkthroughs, flowcharts, diagrams, control descriptions, codes, policies (Management Representations) (private, unless required under criteria)
- viii. The specific software and hardware versions and assets inspected including third-party assets, as applicable (private)
- ix. A list of documentation and assets that will be retained as audit evidence, and explanation of deviations (private)
- x. A duly authorised signatory (private, but at the auditee's discretion)



- xi. A list of deficiencies if certification will not be issued (private)
- xii. If included in the Audit Engagement Letter, a determination of sufficient/mature levels of compliance (private, but at the auditee's discretion)
- xiii. A process for resolving disputes (private)
- xiv. A list of non-compliance issues for consideration (private)
- xv. That auditee has met all public disclosure requirements as logged by the auditor (private)
- xvi. Sufficient, robust, and resilient ongoing monitoring systems and explicit statement that systemic failures of ongoing monitoring systems will preclude future certification, including next date of expected certification (private)
- xvii. Statement of auditor independence and quality management (private)
- xviii. Statement of understanding that this certification scheme does not represent complete protection from enforcement of the law by National Supervisory Authorities (private)

4.4 Evaluation Methodology

Each of the scheme criteria identifies an evaluation method type. The certifying body may vary the evaluation method type where it provides additional assurance, but not so that it provides less. The following types are listed:

1. *Contract* - An executed contract that can be examined and demonstrates compliance with the criteria.
2. *Correspondence (Internal or External)* - Historical correspondence is available that demonstrates compliance with the criteria.
3. *Employee Handbook* - In the context of an employment contract, an internal document that comprehensively describes an employee's duties, obligations, responsibilities, guidelines, rights, benefits, and available resources.
4. *Internal log, register or database* - Internal, systemic records with proof of authenticity that can be examined by the certifying body and that demonstrate compliance.
5. *Internal procedure manual* - Internal policy and procedure documentation that can be shown to the certifying body to demonstrate compliance with the criteria. These may include, but are not limited to, documents, notifications, interfaces, assessments, studies, rosters, and meeting minutes. All evidence should be of sufficient detail to show that they are up-to-date, implemented, and complete.
6. *Picture/Graphic* - Includes diagrams and technical drawings.
7. *Public disclosure document* - Contains all legal obligations and elements as described by the specific audit criteria. The document must meet the definition of Public (as found in Section 3.0).



8. *Physical testing* - At the certifying body's discretion, this can refer to documentation of any of the following:
- Interviews with authorized personnel
 - Inspection of current events, interfaces, and/or notifications
 - Technical testing including metrics, measurements, and thresholds

Copies of all evidence obtained during the evaluation should be stored in encrypted form by the certifying body, except where the evidence includes personal data and does not comply with the principle of data minimisation.

5.0 Use of the term “Algorithmic Lifecycle”

ForHumanity uses the terminology “algorithmic lifecycle” in our Provider and Deployer schemes. It should be noted that this term represents differing stages for Providers and Deployers, for example:

- Provider Algorithmic lifecycle: 1) Design 2) Development 3) Deployment 4) Monitoring 5) Decommissioning
- Deployer Algorithmic Lifecycle: 1) Procurement 2) Implementation 3) Deployment 4) Monitoring 5) Decommissioning

5.1 Criteria catalog

Column 1 = ForHumanity unique identifier (FHUI)

Column 2 = CORE Classification description

Column 3 = Audit criteria

Column 4 = Evaluation method

	<u>Categories</u>	<u>Audit Criteria</u>	<u>Evaluation Method</u>
Expert Oversight			
	Expert Oversight	The Deployer shall have a duly designated team of experts trained in understanding the following specific and multi-disciplinary risks	Internal log, register, or database



		<p>associated with the deployment of the AAA System in regards to:</p> <ul style="list-style-type: none">A. Risk(s) to Fundamental Rights of AI Subjects (especially Vulnerable Populations), including associated legal risks such as equality, nondiscrimination, transparency, and fairnessB. Risk(s) of poor data management and governance, including failure to deliver privacy-by-design and data protection for Pipeline Data and to uphold Data Subject rights, especially in the areas of Special Category Data (e.g., race, gender, age, biometric facial mapping, retinal scan, DNA)C. Risk(s) associated with insufficient risk management processes in regards to:<ul style="list-style-type: none">i. Managing risk associated with the AAA System deployment:<ul style="list-style-type: none">a. Ineffective risk controls, treatments, and mitigationsb. Ineffective feedback loopsc. Failure to identify incidentsd. Failure to identify and include all stakeholders in risk assessment (need to ensure the inclusion of Diverse Inputs and Multi Stakeholder Feedback)D. Risk(s) associated with due diligence of the Provider's AAA System including:<ul style="list-style-type: none">i. Risk Managementii. Data Management and Governanceiii. Regulatory compliance	
--	--	--	--



		<p>E. Risk(s) associated with insufficient disclosure, transparency and operating protocols for the AAA System deployment including detailing Residual Risk</p> <p>F. Risk(s) associated with integration and deployment choices regarding machine autonomy, human oversight and interactions</p> <p>G. Risk(s) associated with unmitigated Cognitive Bias and Technology Barrier Bias in regards to deployment choices</p> <p>H. Risk(s) of insufficient oversight of AAA System deployment and ongoing health and fitness for purpose</p> <p>I. Risk(s) associated with inadequate security and cybersecurity, including risks associated with insufficiently robust, reliable, and resilient operations</p> <p><i>Note - The duly designated team of experts are hereafter referred to as the Algorithmic Risk Committee for the purposes of ease of reference.</i></p>	
	Expert Oversight	<p>The Deployer shall have a duly designated team of experts trained in understanding the following specific and multi-disciplinary risks associated with Algorithm Ethics and Ethical Choices associated with AAA System deployment such as:</p> <p>A. Adjudicating instances of Ethical Choice, and analyzing, evaluating, and treating Ethical Risk including:</p> <p>i. Human oversight and interactions of the AAA System deployment as documented in the Human</p>	Internal log, register, or database



		<ul style="list-style-type: none">Interactions Reportii. Controllabilityiii. Necessityiv. Explainability and Explainability+ <p>B. Compiling the shared moral framework of the organization as applicable to AAA System deployment, including:</p> <ul style="list-style-type: none">i. Identification of applicable Relevant Legal Frameworksii. Documenting the shared moral framework in a Code of Ethics and the principles portion of the Code of Data Ethicsiii. Managing changes to the shared moral frameworkiv. Establishing an operational definition of diversity, especially for Diverse Input and Multi Stakeholder Feedback <p>C. Managing risks to health, safety and fundamental rights of AI Subjects, including:</p> <ul style="list-style-type: none">i. Conducting a Fundamental Rights Impact Assessmentii. Assessing and implementing Proportionalityiii. Assessing the AAA System deployment to determine during procurement whether it is an:<ul style="list-style-type: none">a. Emotional recognition systemb. Social scoring system <p>D. Implementing fairness in:</p> <ul style="list-style-type: none">i. Testing processes, procedures, metrics, measurements, and thresholdsii. Residual Risk Public	
--	--	---	--



		<p>disclosures</p> <p>iii. Integration of the AAA System with the current version of deployment</p> <p>iv. Evaluating UX/UI interfaces and AAA System deployment for:</p> <ul style="list-style-type: none">a. Detrimental Nudges,b. Deceptive design,c. Dark patternsd. Subliminal techniques or other material impacts that distort AI Subjects' behavior <p>E. Identifying and mitigating Cognitive Bias in the AAA System and associated ecosystem deployment</p> <p>F. Establishing guardrails for the deployment of the AAA System to identify:</p> <ul style="list-style-type: none">i. Deviations from the agreed upon Scope, Nature, Context, and Purposeii. Process and procedures to monitor the risk of Model, Data, and Concept Drift (e.g., periodic audits of the Provider) <p>G. If applicable, establishing content moderation metrics, measurements, and thresholds to the AAA System deployment including:</p> <ul style="list-style-type: none">i. If applicable, Key Detrimental Indicators for Content Moderationii. If applicable, Key Regulated Product Indicators for illegal or harmful product moderationiii. If applicable, Key Language Indicators for AAA Systems	
--	--	--	--



		<p>using LLM, LMM or questionnaires</p> <p>H. Establishing metrics, measurements and thresholds to control, treat, and mitigate Ethical Risks (e.g., vendors, inputs products, services), including the health, safety, and well-being of human interactors</p> <p>I. Assessing systemic riskiness of the AAA System deployment and associated metrics, measurement, and thresholds</p> <p>J. Establishing metrics, measurements, and thresholds to identify and classify Novel deployments and Emergent Risk</p> <p><i>Note 2 - The duly designated team of experts is hereafter referred to as the Ethics Committee for ease of reference. The controller may refer to this team in any manner they see fit.</i></p>	
Top Management and Oversight Bodies			
	Top Management and Oversight Bodies	<p>Top Management and Oversight Bodies shall ensure that the following governance, oversight, and accountability functions for the AAA System deployment are operational, including:</p> <p>A. LEADERSHIP AND GOVERNANCE - Demonstrating leadership and commitment to ethical and risk management by establishing standing and empowered Ethics Committee, Algorithmic Risk Committee, and all applicable specialty committees (e.g., Children’s Data Oversight, Disability Inclusion & Accessibility, Digital</p>	Correspondence (Internal or External)



		<p>Services Content)</p> <p>B. ACCOUNTABILITY - Delineating roles and responsibilities of the operational teams responsible for organizational-wide compliance and oversight, including proportionate applications of:</p> <ul style="list-style-type: none">i. Quality management systems (e.g., internal audit)ii. Legal and regulatory compliance,iii. Enterprise risk management, and their interactions with the AAA System deployment <p>C. RISK MANAGEMENT - Using a currently updated cAIRE Report, ensuring that the Algorithmic Risk Committee and/or applicable specialty committees are governing and accountable for the risk management process for the AAA System, associated ecosystem and deployment, including:</p> <ul style="list-style-type: none">i. Identifying specific and unique risksii. Ensuring the implementation of risk controls, treatments, and mitigationsiii. Monitoring the effectiveness of risk controls, treatments, and mitigationsiv. Ensuring that risk management process is conducted over the lifecycle of the AAA System deployment and kept current <p>D. REGULATORY COMPLIANCE - Ensuring that the Algorithmic Risk Committee works in conjunction with the appropriate AAA System expert legal consultation to determine the</p>	
--	--	--	--



		<p>applicable Relevant Legal Frameworks and document a plan for initial and ongoing regulatory compliance for the AAA System deployment, including assigning an AI Compliance Lead</p> <p>E. RESOURCE ALLOCATION - Ensuring that the necessary resources are allocated to manage governance, oversight, accountability, risk, and quality (e.g., people, budget, infrastructure)</p> <p>F. OVERSIGHT - Assigning authority, responsibility, and accountability at appropriate levels within the organization documented in the Committee Governance Assessment (conducted by a third line of defense, such as internal audit or enterprise risk management) and ensuring delivery of the assessment to the Algorithmic Risk Committee</p> <p>G. DUTY OF CARE FOR VULNERABLE POPULATIONS - Assess stakeholders to identify Vulnerable Populations, and then ensure that teams with expertise are established to oversee specific and unique risks to Vulnerable Populations (e.g., Children, Persons with Disabilities) including the provision of Accommodations as applicable.</p> <p>H. STATEMENT OF PRINCIPLES - Endorse:</p> <ul style="list-style-type: none">i. A public Code of Ethicsii. The principles portion of the Code of Data Ethicsiii. A commitment to uphold the	
--	--	--	--



		<p>applicable Relevant Legal Framework(s)</p> <p>I. DEFINE STAKEHOLDERS - Ensuring that stakeholders are considered from a holistic perspective of impacted groups, including both direct stakeholders that may be internal (e.g., employees, shareholders) or external (e.g., customers, agents, communities) and indirect stakeholders (e.g., society, the environment)</p> <p>J. DUTY TO STAKEHOLDERS - Ensuring the inclusion of Diverse Inputs and Multi Stakeholder Feedback throughout the risk assessment process across the development lifecycle of the AAA System deployment, including endorsing the definition of diversity in the Code of Ethics</p> <p>K. HUMAN OVERSIGHT - Ensuring that:</p> <ul style="list-style-type: none">i. Humans are in-the-loop, on-the-loop, in-Command, or available for post hoc review of outputs of the AAA System deployment as appropriate and that they are duly trained, authorized, and empowered to execute their dutiesii. The AAA System deployment always has human ownership and direct legal and professional accountability <p>L. VENDOR MANAGEMENT - Endorsing a policy established by the Algorithmic Risk Committee that delineates compliance specifications and liability management requirements for all upstream and downstream suppliers</p>	
--	--	---	--



		<p>including the AAA System itself, data and associated services, networking, storage, and technical infrastructure</p> <p>M. TECHNICAL REQUIREMENTS - Endorsing technical infrastructure investment that is appropriate and proportional to the risk of the AAA System deployment to ensure robust, reliable, and resilient function that aligns to all Relevant Legal Frameworks and industry standards including:</p> <ul style="list-style-type: none">i. Quality Management System, if applicableii. Risk Management Framework <p>N. PURPOSE INTEGRITY - Ensuring that the AAA System deployment remains consistent with agreed upon contractually stipulated Purpose(s) and Acceptable Use third parties, including AI Subjects, by engaging in the following:</p> <ul style="list-style-type: none">i. Continuous and post-market monitoringii. Monitoring and managing Model, Data, and Concept Driftiii. Auditing usage by contracted parties <p>O. SYSTEM INTEGRITY - Documenting, in a Code of Data Ethics, a commitment to robust AAA System deployment that has</p> <ul style="list-style-type: none">i. Data that are:<ul style="list-style-type: none">i. Relevantii. High qualityii. Architectural Inputs that have:<ul style="list-style-type: none">i. Construct validityiii. Outputs that are	
--	--	---	--



		<ul style="list-style-type: none">i. Validated by Ground Truth orii. Disclosed in Residual Risk and Explainability Statements as inferential conclusions <p>P. TRANSPARENCY - Ensuring the public display of all of the following:</p> <ul style="list-style-type: none">i. Residual Riskii. A Data Transparency Documentiii. Public portions of the Ethical Risk Assessmentiv. Privacy Policy, if applicablev. Explainability Statements to AI Subjects <p>Q. TRAINING AND EDUCATION - Ensuring that all employees, including Top Management and Oversight Bodies, and AI Subjects are proportionately trained and educated, as applicable and according to the Scope, Nature, Context, and Purpose of the AAA System deployment and the nature of their interactions, on all of the following:</p> <ul style="list-style-type: none">i. AI Literacyii. Risk Management, including Residual Risk and potential harmsiii. Operating instructionsiv. Terms and conditionsv. Acceptable Usevi. Incident identification and reporting proceduresvii. Quality control and assurance standards <p>R. CHANGE MANAGEMENT - Endorse and communicate a Change</p>	
--	--	--	--



		<p>Management Plan as recommended by the Algorithmic Risk Committee</p> <p>S. CONFLICT RESOLUTION - Ensuring that, in all matters where committees (including specialty committees) or delegated persons interact, there is a procedure outlined in the Code of Ethics to adjudicate any conflict</p> <p>T. DECOMMISSIONING - Deciding and documenting the decision to decommission the AAA System deployment, in consideration of recommendations from the Algorithmic Risk Committee</p>	
	Top Management and Oversight Bodies	<p>Top Management and Oversight Bodies shall ensure that a Committee Governance Assessment is conducted including the following:</p> <p>A. Collect all Terms of Reference, reports, logs, assessments, and the cAIRE Report with Traceability from the Ethics Committee, the Algorithmic Risk Committee, and any specialty committees (e.g., Children’s Data Oversight Committee, Disability Inclusion and Accessibility Committee)</p> <p>B. Log all Duty Designation Letters</p> <p>C. Assess gaps, inconsistencies, or issues associated with the alignment to the mandates for the specific committees and/or duty designation letters including controls, treatments, and mitigations for identified problems</p> <p>D. Delineating roles and responsibilities between and amongst committees (e.g., Algorithmic Risk, Ethics Committee)</p>	Correspondence (Internal or External)



		<p>and leads (e.g., AAA Cybersecurity, AI Compliance, Quality Management)</p> <p>E. Identify all audit criteria that transit from one committee or duly designated officer to another committee or duly designated officer</p> <p>F. Assessing cross communications, sharing of risk inputs, consultations with specific committees including Ethics Committee, and/or all specialty committees (e.g., Children’s Data Oversight Committee) and gaps that exist in such communications or interactions including controls, treatments, and mitigations for identified shortcomings</p> <p>G. Ensuring that user interfaces and Accommodations Rights Requests, in regards to the AAA System, are integrated, coordinated, and documented with the organization’s established accommodation requests process</p> <p>H. Assessing all committees for:</p> <ul style="list-style-type: none">i. Sufficient diversityii. Sufficient expertise,iii. Conflicts of interest (or duty) to determine disclosure and/or recusaliv. Inclusion of experts (internal or external) from specialty committees onto the Ethics Committee and Algorithmic Risk Committee for assessments of the specific and unique risks associated with those specialty committees <p>and remediate any shortcomings or conflicts documenting the risk control, treatment, and/or mitigation</p>	
--	--	---	--



		<ul style="list-style-type: none">I. Record all risk controls, treatments, mitigations, and Residual Risk in the cAIRE reportJ. Endorse the accepted Residual RiskK. Endorsing the Decommissioning Policy, processes and procedures	
	Top Management and Oversight Bodies	<p>In consideration of:</p> <ul style="list-style-type: none">1. The cAIRE Report, including:<ul style="list-style-type: none">i. Current Residual Riskii. The advised metrics, measurements and thresholds applicable to Risk Appetite and Risk Tolerance associated with the AAA System2. Organisational Risk Appetite and Risk Tolerance <p>Top Management and Oversight Bodies shall execute the following steps to establish the accepted Residual Risk:</p> <ul style="list-style-type: none">A. Assess to determine whether additional risk controls, treatments, and mitigations for the AAA System deployment are to be implementedB. Assess to determine whether external risk treatment options are to be implementedC. Assess to determine the current Residual Risk is accepted with Traceability	Correspondence (Internal or External)
	Top Management and Oversight Bodies	<p>The Top Management and Oversight Bodies shall ensure, with Traceability, that all logs, records, and assessments related to risk (e.g., Algorithmic Risk Assessment, Ethical Risk Assessment) are documented in the cAIRE Report and provided to enterprise or organisational risk management logs, registers, or databases</p>	Correspondence (Internal or External)



	Top Management and Oversight Bodies	Top Management and Oversight Bodies shall ensure that a person educated on Ethical Choice and Algorithm Ethics , or equivalent, from the Ethics Committee is duly designated to assist the Algorithmic Risk Committee in managing the risks from AAA System deployment	Internal procedure manual
Relevant Legal Framework and Modular Assurance Assessments			
	Relevant Legal Framework	In consultation with expert legal counsel (internal or external), the Algorithmic Risk Committee shall assess and determine whether the AAA System is in scope of the EU Artificial Intelligence Act (EU) 2024/1689 and document, in the AAA Systems List , whether conformity with the Act is mandatory or voluntary	Internal logs, registers or databases
	Relevant Legal Framework	The Algorithmic Risk Committee shall assess the deployment of the AAA System to determine all applicable Jurisdictions in which the AAA System is deployed and document those Jurisdictions in the AAA Systems List	Internal log, register, or database
	Relevant Legal Framework	If the ToE is classified as an Annex III (1) AAA System , then the AI Compliance Lead shall ensure that the conformity assessment is conducted by a duly authorised notified body with Traceability	Correspondence (Internal or External)
	Relevant Legal Framework	For each Jurisdiction in which the ToE operates and in the context of its Scope, Nature, Context, and Purpose , and in consultation with the legal team (internal and/or	Internal log, register, or database



		<p>external), the Algorithmic Risk Committee, shall regularly or as needed (e.g., changes to laws, regulatory guidance or jurisprudence) assess the AAA System deployment for applicable legal obligations including, but not limited to, the following sectors of law:</p> <ul style="list-style-type: none">A. Data Protection and Privacy LawB. Fundamental RightsC. Legal/Lawful basisD. Data collection, protection and retentionE. Equality and nondiscriminationF. Access to goods and servicesG. Market and competition lawH. National SecurityI. Prohibited SystemsJ. Sector-specific law (e.g., health, security)K. Protection for Vulnerable Populations (e.g., Elderly, Children, Persons with Disabilities)L. Employment law <p>and document the following details in the Relevant Legal Framework log:</p> <ul style="list-style-type: none">1. Applicable legal obligations as Relevant Legal Frameworks2. A conclusion, from the legal expert, that the ToE is compliant with applicable legal obligations, prior to deploying the AAA System3. Legal expertise of the person providing the legal opinion, including certification from oversight bodies where applicable	
	Modular Assurance Assessment	The Deployer shall stipulate that the Provider will meet its legal obligations and document separate assurance under the ForHumanity EU AI Act Provider-only Certification scheme, conformity assessment, or	Contract/ Internal log, register, or database



		equivalent	
	Modular Assurance Assessment	In consideration of: 1. Relevant Legal Frameworks 2. Jurisdictions of operation, The Algorithmic Risk Committee shall assess the ToE to determine whether Personal Data is processed and document the conclusion in the AAA Systems List	Internal log, register, or database
	Modular Assurance Assessment	In consideration of: 1. Relevant Legal Frameworks 2. Jurisdictions of operation, and in consultation with the Ethics Committee and legal experts (internal or external), the Algorithmic Risk Committee shall assess the AAA System deployment to determine if Children are AI Subjects and document the conclusion in the AAA Systems List	Internal log, register, or database
	Modular Assurance Assessment	In consideration of: 1. Relevant Legal Frameworks 2. Jurisdictions of operation, And in consultation with the AAA Cybersecurity Lead and legal experts (internal or external), the Algorithmic Risk Committee shall assess the AAA System deployment to determine whether there are legal obligations pertaining to security and/or cybersecurity and document the conclusion in the AAA Systems List	Internal log, register, or database
	Modular Assurance Assessment	In consideration of: 1. Relevant Legal Frameworks 2. Jurisdictions of operation, in consultation with: 1. the Disability Inclusion and Accessibility Committee	



		prior to deploying the high risk AAA System, the Algorithmic Risk Committee shall demonstrate conformity of the AAA System deployment with (EU) 2019/882 by receiving assurance such as ForHumanity's Global Disability Inclusion and Accessibility certificate or equivalent	
	Modular Assurance Assessment	In consideration of: 1. Relevant Legal Frameworks 2. Jurisdictions of operation, And in consultation with the Ethics Committee and legal experts (internal or external), the Algorithmic Risk Committee shall assess the AAA System to determine whether there are applicable use case or industry specific: A. Legal obligations B. Standards (e.g., harmonised standards, common specifications) C. Voluntary Standards (e.g., ForHumanity certification schemes) and document the conclusion in the AAA Systems List	Internal log, register, or database
	Modular Assurance Assessment	The Algorithmic Risk Committee shall assess the AAA System to determine whether the AAA System is an Information Society Service and subject to Regulation (EU) 2022/2065 (Digital Services Act) and then document this legal obligation in the Relevant Legal Framework log and ensure conformity within the same 12 month period of assurance with this scheme	Internal Procedure Manual
Organisational Controls			
EU-EU -DR-O C-AC-0	Organisational Controls	The Algorithmic Risk Committee shall	Internal logs, register or database



01-2508		<p>maintain and keep current an AAA Systems List including:</p> <ul style="list-style-type: none">A. Jurisdictions of operationB. Scope, Nature, Context and Purpose,C. Legal basisD. Descriptions and presence of Personal DataE. Classes of dataF. Source of data and expected number of AI SubjectsG. Status of Usability and accessibility conformance (e.g., Accessibility Conformance Report)H. The presence of Accommodations and processes to supply themI. Whether the AAA System deployment has been assessed as a “High-Risk AI”J. Whether Children are impactedK. Whether cybersecurity obligations existL. Whether use case or industry specific standards are being applied	
	Organisational Controls	<p>The Deployer shall be insured in a manner related to the risk associated with cybersecurity and data breaches according to the Scope, Nature, Context, and Purpose of the AAA System deployment</p>	Contract
	Organisational Controls	<p>In consideration of:</p> <ul style="list-style-type: none">1. Relevant Legal Frameworks2. Jurisdictions of operation, <p>Top management and oversight bodies shall ensure that procedures are established to handle and record government or law enforcement requests for information including the following:</p> <ul style="list-style-type: none">a. Designating employees to process	Internal procedure manual



		<p>requests</p> <p>b. Documenting what constitutes lawful government and law enforcement requests</p>	
	Organisational Controls	<p>Top Management and Oversight Bodies shall maintain a log, register, or database of employee, contractor, or gig-worker raised questions, concerns, or negative impacts on the fundamental rights of AI Subjects relating to the AAA System deployment</p>	Internal log, register or Database
	Organisational Contract	<p>In consideration of:</p> <ol style="list-style-type: none"> 1. The Code of Ethics 2. The database of employee raised questions <p>And in consultation with the Ethics Committee, the Algorithmic Risk Committee shall implement a Just-in-Time notification that affirms the employee, contractor, and gig-worker is free from retaliation associated with the inquiry</p>	Physical Testing
<h2>Training and Education (AI Literacy)</h2>			
	Training and Education	<p>Top Management and Oversight Bodies shall train and educate Persona #3-5 on the legal obligation(s) to align the Scope, Nature, Context, and Purpose of any AAA System deployment to the contracted range of approved usage as described in the contract with the Provider and document the training in the Training and Education log</p>	Internal log, register, or database
	Training and Education	<p>In support of general AI Literacy, the Algorithmic Risk Committee shall ensure</p>	Internal log, register, or



		<p>that the following groups (not mutually exclusive):</p> <ol style="list-style-type: none">1. AI Subjects as users or impacted stakeholders of the AAA System deployment, not including any employees, contractors, or gig-workers (Persona 1)2. Employees, contractors, or gig-workers as impacted stakeholders only, but not interacting with the AAA System for professional individual or corporate purposes (Persona 2)3. Employee, contractors, or gig-workers that are interacting with the AAA System deployment for individual or corporate professional purposes (Persona 3)4. Top Management and Oversight Bodies (Persona 4)5. Employees (AI Leaders) who are the decision-makers in regards to the AAA System deployment (Persona 5) <p>are proportionately trained and educated appropriately and proportionately according to their knowledge, expertise, impact, usage, and/or responsibility associated with the Scope, Nature, Context, and Purpose of the AAA System deployment, on the following learning objectives:</p> <p>A. Persona 1 learner</p> <ol style="list-style-type: none">i. Should be able to define the AAA Systemii. State the primary Purpose of the AAA System deploymentiii. Describe how their actions affect the output of the AAA System deploymentiv. Give examples of what can go wrong when using the toolv. Describe the process for reporting	database
--	--	--	----------



		<p>concerns about the tool and for seeking help, and opting-out of tool usage, if applicable</p> <p>B. Persona 2 learning objectives include all of Persona 1 learning objectives and:</p> <ul style="list-style-type: none">i. General AI Safety Knowledgeii. Corporate Governance and Organisational Policiesiii. Approved Tool Training for individual productivity and informationiv. Employees as Impacted Stakeholders <p>and log the results in the Training and Education log</p> <p><i>*Note - see ForHumanity Body of Knowledge for AI Literacy learning objectives and supporting research and documentation</i></p>	
	Training and Education	Top Management and Oversight Bodies shall ensure that the Persona 2 training and education is included in the learning objectives for Personas #3-5 and log the results in the Training and Education log	Internal log, register or database
	Training and Education	Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers are proportionately trained and educated when onboarding (and then no less than annually afterwards), on the internal process for raising questions, concerns, or negative impacts on the human rights and freedoms of AI Subjects in regards to the AAA System deployment and log the results in the Training and Education log	Internal log, register or database
	Training and Education	Top Management and Oversight Bodies shall ensure that Persona #3-5 employees, contractors, and gig-workers are proportionately	Internal logs, register or database



		<p>trained and educated on the following AAA System oriented curricula (or equivalent):</p> <ul style="list-style-type: none">A. Ethical Choice CurriculumB. Nudge and Deceptive Pattern AwarenessC. Automation BiasD. Disability Inclusion and Accessibility Awareness <p>and log the results in the Training and Education log</p> <p><i>*Note - see ForHumanity Body of Knowledge for each curriculum for learning objectives and supporting research and documentation</i></p>	
	Training and Education	<p>In consideration of the learning objectives from the Risk Management Policy, the Algorithmic Risk Committee shall ensure that Diverse Input and Multi Stakeholder Feedback human risk assessors, including domain experts and direct and indirect stakeholders, are proportionately trained and educated on the following:</p> <ul style="list-style-type: none">A. AAA System deployment, including Scope, Nature, Context, and PurposeB. Code of Conduct, Code of Ethics, Code of Data EthicsC. ConfidentialityD. Security AwarenessE. Risk management:<ul style="list-style-type: none">i. Processes,ii. Procedures,iii. Metrics, measurements, and thresholdsiv. Risk categories and taxonomyv. Scales of severity and likelihood <p>And log the results in the Training and Education log</p>	Internal logs, register or database
	Training and Education	<p>In consideration of the following:</p> <ul style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System	Internal log, register or database



		<ol style="list-style-type: none">2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the Ethics Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standards, current governance on Algorithm Ethics and Ethical Choices in AAA Systems, and best practices and log the results in the Training and Education log</p>	
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. The Provider's Risk Management in regards to:<ol style="list-style-type: none">i. Residual Riskii. Adverse Incident Reporting Systemiii. Any other risk management contractual duties2. Scope, Nature, Context, and Purpose of the AAA System3. Delineated roles and responsibilities of the learners4. Learning objectives identified in the applicable policy or plan documentation <p>In consultation with the Algorithmic Risk Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on the AAA System deployment in regards to:</p> <ol style="list-style-type: none">A. The risk management techniques and/or assigned duties and responsibilities from the Provider	Internal log, register or database



		<p>B. Industry standards,</p> <p>C. The Deployer's current risk management techniques, and best practices</p> <p>and log the results in the Training and Education log</p>	
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System deployment2. Delineated roles and responsibilities of the learners3. Learning objectives identified in the applicable policy or plan documentation <p>In consultation with the Ethics Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standards, current governance and best practices on Algorithm Ethics and Ethical Choices in the AAA System deployment, and log the results in the Training and Education log</p>	Internal log, register or database
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. The Provider's Risk Management in regards to:<ol style="list-style-type: none">i. Residual Riskii. Adverse Incident Reporting Systemiii. Any other risk management contractual duties2. Scope, Nature, Context, and Purpose of the AAA System deployment3. Delineated roles and responsibilities of the learners	Internal log, register or database



		<p>4. Learning objectives identified in the applicable policy or plan documentation</p> <p>In consultation with the Algorithmic Risk Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on the AAA System deployment in regards to:</p> <ul style="list-style-type: none">A. The risk management techniques and/or assigned duties and responsibilities from the ProviderB. Industry standards,C. The Deployer's current risk management techniques, and best practices <p>and log the results in the Training and Education log</p>	
	Training and Education	<p>In consideration of the following:</p> <ul style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System deployment2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with Data Lead, Top Management and Oversight Bodies shall proportionately, based upon the volume and complexity of deployment data, train and educate employees, contractors, and gig-workers (Persona 3) on industry standards, current data management and governance techniques, and best practices in regards to the AAA System deployment and log the results in the Training and Education log</p>	Internal log, register or database
	Training and Education	<p>In consideration of the following:</p> <ul style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System	Internal log, register, or database



		<ol style="list-style-type: none">2. Delineated roles and responsibilities of the learners3. Learning objectives identified in the bias mitigation policy <p>In consultation with the Algorithmic Risk Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on the bias mitigation policy including industry standard techniques and best practices for the mitigation of Statistical Bias, Cognitive Bias and Technology Barrier Bias on the AAA System including roles, responsibilities, and duties according to the policy</p>	
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the Test Lead, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standard and best practice tools, techniques and procedures to be applied in the Integration Test Plan for the AAA System and and log the results in the Training and Education log</p>	Internal log, register or database
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation	Internal log, register or database



		In consultation with the AI Compliance Lead , Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standards and best practice tools in regards to Technical Documentation applicable to the AAA System and and log the results in the Training and Education log	
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the Algorithmic Risk Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standards and best practice tools in regards to record-keeping and Event log generation applicable to the AAA System and and log the results in the Training and Education log</p>	Internal log, register or database
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the Algorithmic Risk Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standards and best practices for transparency documentation,</p>	Internal log, register or database



		AI Subject Guides applicable to the AAA System and and log the results in the Training and Education log	
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the Algorithmic Risk Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers who are human-in-the-loop, human-on-the-loop, Human-in-Command or post hoc human reviewers associated with the AAA System are proportionately trained and educated on the human interactions learning objectives and log the results in the Training and Education log</p>	Internal log, register, or database
	Training and Education	<p>If the Deployer is supplying the human oversight for the AAA System, then Top Management and Oversight Bodies shall train and educate the person(s) responsible for overseeing the AAA System deployment on all of the following:</p> <ol style="list-style-type: none">A. The Capacity and limitations of the AAA SystemB. Automation Bias CurriculumC. How to use the Exceptions Interpretability interfaceD. How to decide, based upon outputs from Exceptions Interpretability on how to stop, pause, disregard, override, and reverse the AAA SystemE. Delineation of roles and responsibilities for the Human-in-CommandF. When to refer cases to the Provider's	Internal log, register or database



		<p>Accommodation process as applicable And log the results in the Training and Education log (TE-TM-0015)</p>	
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none"> 1. Provider's security and cybersecurity learning objectives 2. Scope, Nature, Context, and Purpose of the AAA System 3. Delineated roles and responsibilities of the learners 4. Learning objectives identified in the applicable policy or plan documentation 5. Deployer security and cybersecurity protocols <p>In consultation with the AAA Cybersecurity Lead, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on</p> <ol style="list-style-type: none"> A. The Provider's security and cybersecurity policies and protocols B. Industry standards and best practices regarding security and cybersecurity of the AAA System deployment and log the results in the Training and Education log 	Internal logs, register or database
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none"> 1. Scope, Nature, Context, and Purpose of the AAA System 2. Delineated roles and responsibilities of the learners 3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the Monitoring Lead, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standards and best</p>	Internal logs, register or database



		practices regarding monitoring of the AAA System and log the results in the Training and Education log	
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the Algorithmic Risk Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standards, best practices and incident response processes, procedures and plans of the AAA System and log the results in the Training and Education log</p>	Internal logs, register or database
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the Algorithmic Risk Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standards, best practices and change management processes, procedures and plans applicable to the AAA System and log the results in the Training and Education log</p>	Internal logs, register or database
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System	Internal logs, register or database



		<ol style="list-style-type: none">2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the Algorithmic Risk Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standards, best practices vendor management processes, procedures applicable to the AAA System and log the results in the Training and Education log</p>	
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the Algorithmic Risk Committee, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standards, best practices and system development processes and procedures applicable to the AAA System and log the results in the Training and Education log</p>	Internal logs, register or database
	Training and Education	<p>In consideration of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the Quality Management Lead, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately</p>	Internal logs, register or database



		trained and educated on industry standards, best practices and the organization's Quality Management System applicable to the AAA System and log the results in the Training and Education log	
	Training and Education	<p>In consideration of all of the following:</p> <ol style="list-style-type: none">1. Scope, Nature, Context, and Purpose of the AAA System2. Delineated roles and responsibilities of the learners3. Learning Objectives identified in the applicable policy or plan documentation <p>In consultation with the AI Compliance Lead, Top Management and Oversight Bodies shall ensure that employees, contractors, and gig-workers (Persona 3) are proportionately trained and educated on industry standards, best practices, and the organisations Regulatory Compliance processes and procedures applicable to the AAA System and log the results in the Training and Education log</p>	Internal logs, register or database
	Training and Education	<p>Top Management and Oversight Bodies shall ensure that Top Management and Oversight Bodies personnel (Persona 4), including members of the Board of Directors, are proportionately trained and educated regarding all of the following enterprise-wide learning objectives for AAA Systems:</p> <ol style="list-style-type: none">A. Establishing expert oversight for AAA SystemsB. Establishing ethical oversightC. Risk management policyD. Data management and governance policyE. Integration Testing and Evaluation processes and proceduresF. Transparency and documentation processes and proceduresG. Monitoring policy	Internal logs, register or database



		<p>H. Change management processes and procedures</p> <p>I. Incident response processes and procedures</p> <p>J. Vendor management processes and procedures</p> <p>K. System development processes and procedures</p> <p>L. Quality management policy</p> <p>M. Decommissioning Policy</p> <p>And log the results in the Training and Education log</p>	
	Training and Education	<p>In regards to the AAA System, Top Management and Oversight Bodies shall ensure that the following personnel (Persona 5):</p> <ol style="list-style-type: none">1. Members of the Algorithmic Risk Committee,2. Members of the Ethics Committee3. Applicable members of any specialty committees,4. Data Lead5. Test Lead6. AAA Cyberseceurity Lead7. Monitoring Lead8. Quality Management Lead9. AI Compliance Lead <p>are trained and educated appropriately and proportionately according to their knowledge, expertise, impact, usage, and/or responsibility associated with the Scope, Nature, Context, and Purpose of the AAA System in regards to the following learning objectives as appropriate and applicable to the learner:</p> <ol style="list-style-type: none">A. Understanding of direct and indirect stakeholdersB. Current awareness of risks and harms applicable to the AAA SystemC. State-of-the-art awareness of risk	Internal logs, register or database



		<p>controls, treatments, and mitigations</p> <p>D. Understanding of potential systemic risk</p> <p>E. Establishing expert oversight for AAA Systems</p> <p>F. Establishing ethical oversight</p> <p>G. Risk Management policy</p> <p>H. Data Management and Governance policy</p> <p>I. Integration Testing and Evaluation processes and procedures</p> <p>J. Transparency and Documentation processes and procedures</p> <p>K. Monitoring Policy</p> <p>L. Change Management processes and procedures</p> <p>M. Incident Response processes and procedures</p> <p>N. Vendor Management processes and procedures</p> <p>O. System Development processes and procedures</p> <p>P. Quality Management policy</p> <p>Q. Decommissioning Policy</p> <p>And log the results in the Training and Education log</p>	
	Training and Education	<p>In consideration of:</p> <ol style="list-style-type: none">1. Relevant Legal Frameworks2. Jurisdictions of operation, <p>Top Management and Oversight Bodies shall train and educate employees, contractors, and gig-workers when onboarding, and then no less than annually afterwards, on:</p> <ol style="list-style-type: none">A. Whistleblower rightsB. Processes and procedures to handle and comply with lawful government or law enforcement requests <p>and log the results in the Training and Education log</p>	Internal logs, register or database



	Training and Education	<p>In consultation with the:</p> <ol style="list-style-type: none">1. Algorithmic Risk Committee2. Ethics Committee3. Data Lead4. Monitoring Lead5. Testing Lead6. AAA Cybersecurity Lead7. Quality Management Lead8. AI Compliance Lead <p>Top Management and Oversight Bodies shall regularly (no less than annually) assess training and education applicable to the AAA System to determine whether the training and education remains fit for purpose with Traceability to the person or team responsible for the training</p>	Correspondence (Internal or External)
Specialty Committees			
	Specialty Committees	<p>In consideration of stakeholders who have been identified as Vulnerable Population, the Algorithmic Risk Committee shall designate a team of experts (specialty committee) charged with a duty of care to assess the specific and unique risks to that population resulting from the AAA System deployment including all of the following duties:</p> <ol style="list-style-type: none">A. Establishing the Terms of Reference for the specialty committeeB. Identification of the specific and unique risks including risk controls, treatments, and mitigation across ethics, bias, privacy, trust and cybersecurityC. Identification of the fundamental rights	Internal Procedure Manual



		<p>and freedoms of AI Subjects to be upheld on behalf of the Vulnerable Population</p> <p>D. Inclusion of experts in regards to identifying, analysing, evaluating, and treating risks related to the health and safety of Vulnerable Population</p>	
	Specialty Committees	<p>In consideration of:</p> <ol style="list-style-type: none">1. the European Accessibility Act of 2019 (EU) 2019/8822. Persons with Disabilities always being impacted stakeholders of the AAA System deployment and considered a Vulnerable Population, <p>The Deployer shall have a duly designated team of experts (hereafter referred to as the Disability Inclusion and Accessibility Committee, to augment the Algorithmic Risk Committee and Ethics Committee, ever present during deliberations regarding Persons with Disabilities and the risks associated with AAA Systems), trained in understanding the following specific and multi-disciplinary AAA System's risks taking such as:</p> <ol style="list-style-type: none">A. Risks to health, safety, and fundamental rights and freedoms of Persons With DisabilitiesB. Risks associated with Persons with Disabilities and the associated accessibility and accommodations controls, treatments, and mitigationsC. Risk associated with Persons with Disabilities and inclusion of a range of modalities that may be impacted by the design and development choices of the AAA System deployment (in Diverse	Public disclosure document



		<p>Input and Multi Stakeholder Feedback)</p> <p><i>Note 1</i> - The duly designated team of experts is hereafter referred to as the Disability Inclusion and Accessibility Committee for ease of reference. The organisation may refer to this team in any manner they see fit.</p>	
	Specialty Committees	<p>In support of the benefits of lived experience, Top Management and Oversight Bodies should ensure that a Person with a Disability is a member of the Disability Inclusion and Accessibility Committee</p> <p><i>Note - it is not necessary to disclose the disability</i></p>	Internal Procedure Manual
	Specialty Committees	<p>If the AAA System deployment may be accessed by Children, then the Deployer shall have a duly designated team of experts (<i>with membership on the Algorithmic Risk Committee and Ethics Committee, ever present during deliberations regarding Children and the risks associated with AAA Systems</i>) trained in understanding the following specific and multi-disciplinary AAA System's risks taking account of Children and their unique needs and vulnerabilities such as:</p> <ul style="list-style-type: none">A. Risk(s) of failure to uphold the fundamental rights and freedoms of AI Subjects that are Children (e.g., the UNCRC Rights of the Child)B. Risk(s) of failure to support for the Best Interests of the ChildC. Risk of failure to implement an Age-Appropriate and	Public disclosure document



		<p>Child-Friendly design</p> <p>D. Risk of discrimination or unfairness, including guidance on the subconscious impact of design interfaces</p> <p>E. Risk of Bias, Model, Data and Concept Drift in the AAA System deployment</p> <p>F. Risk of insufficient transparency and need for Diverse Inputs and Multi Stakeholder Feedback risk assessment to assure the health, safety, and well-being of the Child</p> <p>G. Risk to data privacy and protections afforded by the Relevant Legal Frameworks (e.g., Children's Code), especially in the areas of Sensitive Data, Biometric Data, Geolocation, and Profiling</p> <p>H. Risk of insufficient security and cybersecurity solutions unique to Children</p> <p>I. Risk of failure to provide specialized design and controls of AAA System deployment</p> <p>J. Risk of failure to disclose Residual Risk in an Age-Appropriate and Child-Friendly manner</p> <p><i>Note</i> - The duly designated team of experts is hereafter referred to as the Children's Data Oversight Committee for ease of reference. The organization may refer to this team in any manner they see fit.</p>	
--	--	---	--



Prohibited System - Article 5

5.1.c	Prohibited Systems	<p>In consultation with:</p> <ol style="list-style-type: none">1. An expert legal team (internal or external) <p>In consideration of all of the following:</p> <ol style="list-style-type: none">1. The Proportionality Study2. The Necessity Assessment3. The Causal Hypothesis, Construct Validity and Ground Truth availability4. Design choices <p>the Ethics Committee shall assess and document in the Ethical Risk Assessment whether the AAA System deploys prohibited applications and usage according to Article 5 including:</p> <ol style="list-style-type: none">A. Engaging in Nudges, Deceptive Design, or other subliminal techniques that produce significant harms to health, safety, and fundamental rights either physically or psychologically to the AI SubjectB. Exploiting any Vulnerable Populations, with the objective to materially distort or having the effect of materially distorting an AI Subject's behaviour (or another person) that produces significant harms to health, safety, and fundamental right either physically or psychologicallyC. Evaluating or classifying of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:<ol style="list-style-type: none">i. Detrimental or unfavourable treatment of certain natural	Public Disclosure Document
-------	--------------------	---	----------------------------



		<p>persons or whole groups thereof in social contexts which are unrelated to the context in which the data was originally generated or collected;</p> <p>ii. Detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity</p> <p>D. Natural persons and the likelihood of their offending or to predict the occurrence of an actual or potential criminal offence based solely on Profiling them or on assessing their personality traits and characteristics</p> <p>E. Using AAA Systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage</p> <p>F. Use of AAA Systems intended to be used to detect the emotional state of individuals in situations related to the workplace, education and all other applications where the health, safety, and fundamental rights of Protected Categories, Intersectionalities, or Vulnerable Populations are compromised, except for medical or safety reasons, such as systems intended for therapeutic use, documenting the exception with justification in the Ethical Risk Assessment</p>	
--	--	---	--



	Prohibited Systems	<p>The Ethics Committee shall assess the AAA System deployment to determine whether it deduces or infers any conclusions from the following list:</p> <ul style="list-style-type: none">A. Race,B. Political opinions,C. Trade union membership,D. Religious or philosophical beliefs,E. Sex lifeF. Sexual orientation <p>and ensure that the AAA System deployment is not Placed on the market or Put into service and document the conclusion in the Ethical Risk Assessment</p>	Internal Procedure Manual
	Prohibited Systems	<p>The Ethics Committee shall ensure that the AAA System deployment is not prohibited by the EU Artificial Intelligence Act and document in the Ethical Risk Assessment and communicate the conclusion to the Algorithmic Risk Committee and applicable legal team</p>	Correspondence (Internal or External)
	Prohibited System	<p>In consultation with:</p> <ul style="list-style-type: none">1. The Ethics Committee,2. The expert legal team (internal or external), <p>In regards to a “real-time” biometric identification system used in Publicly Accessible Spaces by law enforcement and the Algorithmic Risk Committee shall establish metrics, measurements, and thresholds documented in a real-time biometric identification policy and appended to the Monitoring Policy to assess whether the legal conditions found in criteria PS-AC-002 (I), (II), (III) have been met</p>	Internal Procedure Manual
EU-EU-DR-PS-AC-002-2508	Prohibited Systems 5.1.h Recital 40 Recital 41	<p>If:</p> <ul style="list-style-type: none">1. The AAA System deployment is used by law enforcement (or on their behalf) in Publicly Accessible Spaces	Internal log register or database



		<p>2. If the biometric identification of natural persons by law enforcement in Publicly Accessible Spaces is being deployed in Ireland or Denmark and is used for activities in the field of police cooperation and judicial cooperation in criminal matters</p> <p>3. At least one the following conditions are met:</p> <ul style="list-style-type: none">i. That there is a targeted search for specific victims of:<ul style="list-style-type: none">a. Abduction,b. Trafficking in human beings orc. Sexual exploitation of human beings,d. Search for missing personsii. The prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attackiii. The localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years <p>then the Algorithmic Risk Committee, in consultation with the expert legal team (internal or external) shall document, in the AAA Systems List, the legal opinion affirming</p>	
--	--	--	--



		whether the metrics, measurements, and thresholds for use of a real-time biometric identification AAA System deployment have been met and document the conclusions in the Event Log	
	Prohibited Systems 5.2	<p>If the AAA System engages in real-time biometric identification of natural persons in Publicly Accessible Spaces for the purposes of law enforcement, then the Ethics Committee shall assess the proportionality of the deployed AAA System in consideration of the following:</p> <ul style="list-style-type: none">A. the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm that would be caused if the system were not used;B. the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences <p>And append the conclusions to the Proportionality Study</p>	Internal Procedure Manual
	Prohibited Systems 5.2	<p>If the AAA System engages in real-time biometric identification of natural persons in Publicly Accessible Spaces for the purposes of law enforcement and in consideration of Relevant Legal Frameworks, the Algorithmic Risk Committee shall ensure that all necessary and proportionate safeguards and conditions in relation to the use are in accordance with the Relevant Legal Frameworks authorising the use thereof, in particular as regards the temporal, geographic and personal limitations</p>	Internal Procedure Manual
	Prohibited Systems 5.2 and	<p>In consultation with:</p> <ol style="list-style-type: none">1. The Ethics Committee	Internal Procedure



	5.3	<p>In consideration of</p> <p>1. Relevant Legal Frameworks</p> <p>If the AAA System engages in real-time biometric identification of natural persons in Publicly Accessible Spaces for the purposes of law enforcement and, then the Algorithmic Risk Committee shall establish policies and procedures governing the real-time biometric identification of natural persons that:</p> <p>A. Ensures that the Ethics Committee conducts a specific, situational, and context-driven Fundamental Right Impact Assessment, Proportionality Study and Necessity Assessment for the explicit Scope, Nature, Context, and Purpose of the AAA System</p> <p>B. Establishes a procedure to ensure receipt of prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law</p> <p>C. Deploys the system without authority, in a duly justified situation of urgency, but is subject to the following validation procedures:</p> <p>i. Provided that, such authorisation shall be requested without undue delay, including an explanation of the reason for delay requesting authorisation, during its use of the AAA System and not later than within 24 hrs</p> <p>ii. If such authorisation is rejected in (i), the AAA System's use shall be stopped with immediate effect and all applicable data is to be</p>	Manual
--	-----	---	--------



		immediately Destroyed	
	Prohibited Systems 5.4 5.6	The AI Compliance Lead shall notify the National Competent Authority and National Data Protection Authority of each use of Biometric Identification of Natural Persons in Publicly Accessible Spaces according to the template established by the EU Commission and register the AAA System deployment in the EU Database according to Article 49	Official Filing
	Prohibited Systems	The Algorithmic Risk Committee shall ensure that the risk controls, treatments, and mitigations identified in the real-time biometric identification policy, Fundamental Rights Impact Assessment, Necessity Assessment, and Proportionality Study are implemented with Traceability provided to the Ethics Committee	Correspondence (Internal or External), Internal Log
	Prohibited Systems	The Algorithmic Risk Committee shall establish a monitoring system that tracks the metrics, measurements, and thresholds described in the real-time biometric identification policy, for inputs from all relevant lawful authorities that identify scenarios described in criteria PS-AC-002 (I), (II), (III)	Physical Testing
	Prohibited Systems	In consideration of: <ol style="list-style-type: none">1. The Scope, Nature, Context, and Purpose of the AAA System2. Relevant Legal Frameworks3. Necessity Assessment4. Data Protection Policy the Algorithmic Risk Committee shall ensure that data retention associated with real-time biometric identification of natural persons is: <ol style="list-style-type: none">A. Retained according to the Relevant Legal Framework associated with the scenario and documented in the metadata occurring in criteria PS-AC-002 (I), (II), (III)	Physical Testing



		<p>B. Pseudonymised and/or encrypted</p> <p>C. Secure and archived according to the Deployer’s Data Protection Policy, Data Security, and Security Policy</p>	
	Prohibited Systems	In consideration of the Scope, Nature, Context, and Purpose of the AAA System deployment, the Ethics Committee shall define and document in the Ethical Risk Assessment , “a certain period of time” during which social behaviour is considered relevant for risk assessment	Public Disclosure Document
	Prohibited Systems	<p>In consideration of:</p> <ol style="list-style-type: none">1. The Necessity Assessment2. A “certain period of time” <p>the Ethics Committee shall assess the data used in the AAA System deployment and report to the Algorithmic Risk Committee all of the following:</p> <ol style="list-style-type: none">A. Whether the data used for the AAA System deployment is relevant based upon the Scope, Nature, Context, and PurposeB. If data is determined to be “not” relevant, then documentation of removal from the dataset and inputs to the AAA System deployment with Traceability that includes:<ol style="list-style-type: none">i. A process for Deletion/Destruction of the “not” relevant data if possibleii. A process for terminating collection of the data in the future if possibleC. That inferences are not treated as facts and documented as such with Traceability	Correspondence (Internal or External)
	Prohibited Systems	<p>In consideration of:</p> <ol style="list-style-type: none">3. The Necessity Assessment	Correspondence (Internal or



		<p>4. A “certain period of time”</p> <p>the Ethics Committee shall assess the data used in the AAA System deployment and ensure that the Algorithmic Risk Committee removes with Traceability all measurements, Proxy Variables, or Inferences of social behaviour or scoring that are:</p> <ul style="list-style-type: none">A. Unjustified or disproportionate to an AI Subject’s social behaviourB. Detrimental or resulting in unfavourable treatment to the AI Subject in the Context of the original dataC. Determined to be insufficiently relevant to the Causal Hypothesis and Construct Validity of the AAA System deployment	External)
	Prohibited Systems	The Ethics Committee shall assess the AAA System deployment using Diverse Inputs and Multi Stakeholder Feedback , including domain experts to to determine whether the AAA System deployment engages in subliminal techniques to materially distort a person’s behaviour that causes physical or psychological harms and document the conclusion in the Ethical Risk Assessment	Internal Procedure Manual
Excluded AI Systems (Recital 53-60)			
Article 6.3 Recital 53	Excluded AI Systems	In consideration of the Scope, Nature, Context, and Purpose of the AAA System , the Ethics Committee shall assess the AAA System deployment to determine whether the deployment does not engage in automated decision making including Profiling and any of the following conditions for exclusion from the requirements associated with high risk AI Systems applies to the AAA System deployment:	Internal Procedure Document/ Official Filing



		<p>A. That performs a narrow procedural task (e.g., transforms unstructured data into structured data, classifies incoming documents into categories or to detect duplicates among a large number of applications) that poses no discernible impact unto itself to the health, safety, and fundamental rights to EU Citizen</p> <p>B. That the task performed by the deployment is intended to improve the result of a previously completed human activity (e.g., spell checking, grammar checking previously drafted content)</p> <p>C. That the deployment is intended to detect human decision-making patterns or deviations from prior human decision-making patterns to assist the same human in ensuring their own consistency</p> <p>D. That the deployment is intended to perform a task that is only preparatory to an assessment relevant for the purposes of a larger AAA System deployment that requires a conformity assessment unto itself (e.g., smart solutions for file handling, which include various functions from indexing, searching, text and speech processing or linking data to other data sources, or AI systems used for translation of initial documents)</p> <p>Then prior to deploying the AAA System, the AI Compliance Lead shall:</p> <ol style="list-style-type: none">1. Document the assessment of exclusion from above in the Ethical Risk Assessment2. Register the AAA System deployment with the EU Database based upon the Article 49 assessment of registration as	
--	--	--	--



		excluded	
Recital 54	Excluded AI Systems	<p>In consideration of the Scope, Nature, Context, and Purpose of the AAA System deployment , the Ethics Committee shall assess the deployment using Biometric identification to determine whether any of the following deployments are true:</p> <ul style="list-style-type: none">A. The deployment is used exclusively for security verification of identity by an employerB. The deployment is used exclusively for security verification of identity for the sole purpose of having access to a service, unlocking a device or having secure access to premises by a duly authorised individualC. The deployment is used exclusively for enabling cybersecurity or personal data protection <p>And document the conclusion in the AAA Systems List as excluded</p>	Internal Procedure Manual
Recital 58	Excluded AI Systems	<p>In consideration of the Scope, Nature, Context, and Purpose of the AAA System, the Ethics Committee shall assess the AAA System deployment to determine whether the purpose of the deployment is to:</p> <ul style="list-style-type: none">A. Detect fraud in the offering of financial servicesB. For prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements, <p>If either is true, then document the conclusion in the AAA Systems List as excluded</p>	Internal Procedure Manual
Recital 59	Excluded AI Systems	<p>In consideration of:</p> <ul style="list-style-type: none">1. the Scope, Nature, Context, and Purpose of the AAA System deployment <p>If the organisation is a tax or customs authority or a financial intelligence unit, then the Ethics</p>	Internal Procedure Manual



		Committee shall assess the AAA System deployment to determine whether the Purpose of the deployment is for carrying out administrative tasks analysing information pursuant to Union anti-money laundering law, and if true, then document the conclusion in the AAA Systems List as excluded	
Recital 60	Excluded AI Systems	In consideration of: 1. The Scope, Nature, Context , and Purpose of the AAA System , the Ethics Committee shall assess the AAA System deployment to determine whether the purpose of the deployment is the verification of travel documents, and if true, then document the conclusion in the AAA Systems List as excluded	Internal Procedure Manual
Recital 61	Excluded AI Systems	In consideration of: 1. The Scope, Nature, Context , and Purpose of the AAA System , the Ethics Committee shall assess the AAA System deployment to determine whether the purpose of the deployment is for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, (e.g., anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, administrative tasks), and if true, then document the conclusion in the AAA Systems List as excluded	Internal Procedure Manual
Recital 62	Excluded AI Systems	In consideration of: 1. The Scope, Nature, Context , and Purpose of the AAA System , the Ethics Committee shall assess the AAA System to determine whether the purpose of the deployment is to organise, optimise and structure political campaigns from an administrative and logistical point of view and not to influence the outcome of an election or	Internal Procedure Manual



		referendum or the voting behaviour of natural persons, and if true, then document the conclusion in the AAA Systems List as excluded	
Business Rationale			
	Business Rationale	<p>The Deployer shall document, in the AAA Systems List and in the Business Rationale Report, the following for the AAA System deployment:</p> <ul style="list-style-type: none">A. Definition of a reasonable and defensible Causal Hypothesis and Construct ValidityB. Definition of the system logicC. Business objectives, including expected Functional Correctness and feature RelevanceD. Intended resultsE. Business benefitsF. Planned Scope, Nature, Context, and Purpose	Internal Log, register or Database
	Business Rationale	The Deployer shall document in the Contracts Log all contractual relationships by which it intends to deploy the AAA System to AI Subjects	Internal log, register, or database
General-Purpose AI Determination			
	General Purpose AI Determination	<p>The Algorithmic Risk Committee shall assess the AAA System deployment and associated AI model to determine whether the deployment is classified as a General-Purpose AI System (with or without systemic risk) using the following considerations:</p> <ul style="list-style-type: none">A. Scope, Nature, Context, and PurposeB. Does the AI model have generality and the capability to competently perform a	Internal Log, register, or database



		<p>wide range of distinct tasks? (Recital 97)</p> <p>C. Does the AI model have at least a billion parameters and is trained with a large amount of data using self-supervision at scale and is considered to display significant generality and to competently perform a wide range of distinctive tasks? (Recital 98)</p> <p>D. Is it a large generative AI model and does it allow for flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks? (Recital 99)</p> <p>E. Does the AAA System deployment incorporate any aspect of a General-Purpose AI model (as classified as general purpose under the Act? (Recital 100)</p> <p>And document the conclusion in the AAA Systems List</p>	
Ethical Oversight			
	Ethical Oversight	<p>The Deployer shall have an Ethics Committee that has responsibility for assessing all instances of Ethical Choice associated with the AAA System deployment and that documents its conclusions in the Ethical Risk Assessment</p>	Internal procedure manual
	Ethical Oversight	<p>In regards to specialty committees as established by Top Management and Oversight Bodies, the Ethics Committee shall establish a procedure to ensure that the specialty committees (e.g., Children’s Data Oversight, Disability Inclusion and Accessibility, Digital Service Content) have a duly designated member on the Ethics Committee</p>	Correspondence (Internal or External)



		trained in Ethical Choice and Algorithm Ethics (or equivalent) with Traceability	
	Ethical Oversight	<p>The Ethics Committee shall document, in the employee handbook, keep current, and Publicly display a Code of Ethics and the principles portion of a Code of Data Ethics that includes all of the following:</p> <ul style="list-style-type: none">A. The shared moral framework for the organisation, especially those related to AI Subject's fundamental rights and freedoms, nondiscrimination, equality, access to goods and services, children's law, laws regarding AI/data processingB. Definition of diversity as having perspectives (e.g., diversity of thought and lived experiences) from people such as, but not limited to:<ul style="list-style-type: none">i. Impacted stakeholders, either direct or indirectii. Domain expertsiii. Persons with a range of disabilities (e.g., physical, sensory, cognitive, etc)iv. Persons with varying ages, as appropriate to the AAA System deployment (e.g., Children or the elderly)v. Varying Protected Category and Vulnerable Population representationC. Identification of applicable Relevant Legal FrameworksD. The organisation's metrics, measurements, and thresholds for public disclosure of Residual Risk and instances of Ethical Choice, in	Employee handbook/ Public Disclosure Document



		<p>consideration of Relevant Legal Frameworks</p> <p>E. The organisation’s metrics, measurement, and thresholds for sufficiency of diversity of human risk assessors providing Diverse Inputs and Multi Stakeholder Feedback</p> <p>F. Context to Ethical Choice as it relates to AAA System deployment’s Scope, Nature, Context, and Purpose</p> <p>G. A framework or set of procedures providing guidance as to when/what kinds of instances of Ethical Choice are to be brought to the Ethics Committee</p> <p>H. A guide for employees to gauge when they are nearing an ethical boundary</p> <p>I. A commitment to uphold Article 4(3) of Directive (EU) 2019/790 in support of intellectual property rights of rights holders</p>	
6.1.a	Ethical Oversight	<p>In consultation with:</p> <ol style="list-style-type: none">1. The Algorithmic Risk Committee2. AI Compliance Lead, <p>the Ethics Committee shall assess the AAA System deployment to determine whether any of the following apply:</p> <ol style="list-style-type: none">A. The AAA System deployment has a significant impact on the health, safety, and fundamental rights of EU Citizens (e.g., considering severity and likelihood)B. The AAA System deployment is a safety component or a product unto itself that is governed by Union harmonisation legislation referenced in either section of Annex I <p>Then if (A) or (B) apply, document the conclusion and the associated harmonisation legislation(s) in the AAA Systems List</p>	Internal Procedure Manual



6.3	Ethical Oversight	<p>In consideration of the Scope, Nature, Context, Purpose of the AAA System, the Ethics Committee shall assess to determine whether the AAA System deployment meets the standard of “purely accessory” (<i>and therefore unnecessary for the AAA System deployment to undergo a conformity assessment</i>), including all of the following considerations:</p> <ul style="list-style-type: none">A. Whether the AAA System deployment supports the decision or relevant action, including providing expertiseB. Whether the AAA System deployment impacts health, safety, or fundamental rights <p>and document the conclusions in the Ethical Risk Assessment</p>	Internal Procedure Manual
	Ethical Oversight	<p>In consideration of all of the following:</p> <ul style="list-style-type: none">1. The documented Scope, Nature, Context, and Purpose in the terms and conditions2. Jurisdiction(s) of deployment3. Fundamental Rights Impact Assessment from the Provider <p>In consultation with:</p> <ul style="list-style-type: none">1. The organisation’s expert legal team (internal or external)2. Impacted stakeholders direct or indirect <p>Prior to deploying the AAA System, the Ethics Committee shall conduct a Fundamental Rights Impact Assessment that documents the following:</p> <ul style="list-style-type: none">A. The Provider’s Fundamental Rights Impact AssessmentB. A description of the Scope, Nature, Context, and Purpose (including the frequency of interaction with the AAA System) including the expected life of the AAA System deployment	Public Disclosure Document



		<ul style="list-style-type: none">C. An assessment of the inclusion of Personal Data in the AAA System deployment and if Personal Data is present, include the Data Protection Impact Assessment in the Fundamental Rights Impact AssessmentD. An assessment and identification of categories of groups and natural persons likely to be impactedE. A verification of upholding Relevant Legal Frameworks according to deployed Jurisdiction(s)F. A log (in the risk log) of reasonably foreseeable impact and/or harms on natural persons, especially Protected Categories, Intersectionalities, and Vulnerable Populations using Diverse Input and Multi Stakeholder Feedback from human risk assessorsG. A log (in the risk log) of negative impacts to the environment using Diverse Input and Multi Stakeholder Feedback from human risk assessorsH. An identification of risk controls, treatments, and mitigation for logged negative impacts to Fundamental rights and freedoms with TraceabilityI. A description of the governance and monitoring system for risk controls, treatments, and mitigations identified in (G)J. Metrics, measurements, and thresholds for governance and monitoring of (H)K. A frequency for reassessment of any impact to fundamental rights and freedomsL. A process to share the Fundamental Rights Impact Assessment with AI	
--	--	--	--



		Subjects in the AAA System AI Subject's Guide	
	Ethical Oversight	<p>In consideration of the Fundamental Rights Impact Assessment, the Ethics Committee shall conduct, a Proportionality Study that considers:</p> <ol style="list-style-type: none">1. Tensions and Trade-offs2. Pros and cons3. Risk controls, treatments, and mitigations <p>To balance and maximize the objectives of AAA System deployment with impacts to AI Subject's well-being in regards to:</p> <ol style="list-style-type: none">A. The design and operation of the AAA System deploymentB. Data management and governance associated with the deploymentC. Risk management of the AAA System deploymentD. Public disclosures including the Explainability Statement, and if applicable the Explainability+ Statement <p>and document the conclusions in the Ethical Risk Assessment</p>	Internal procedure manual
	Ethical Oversight	<p>In the context of maximizing risk controls, treatments, and mitigation on behalf of Persons with Disabilities (e.g., Accommodations, Accessibility, Inclusion, Usability), and in collaboration with the Disability Inclusion and Accessibility Committee, the Ethics Committee should ensure that diversity for Diverse Inputs and Multi Stakeholder Feedback includes range</p>	Internal procedure manual



		of modalities and types of Persons with Disabilities in the pool of human risk assessors and document the conclusions in the Ethical Risk Assessment	
	Ethical Oversight	<p>In consideration of:</p> <ol style="list-style-type: none">1. Relevant Legal Frameworks,2. The Code of Ethics3. The Code of Data Ethics, <p>the Ethics Committee shall assess all instances of Ethical Choice to determine whether the choice is to be disclosed Publicly and document in the Ethical Risk Assessment the conclusion for disclosure in Residual Risk</p>	Public Disclosure Document/Internal Procedure Manual
	Ethical Oversight	<p>The Ethics Committee shall conduct an Ethical Risk Assessment for all instances of Ethical Choice found in the Deployer's algorithmic lifecycle (procurement, integration, deployment, monitoring, decommissioning) and document the following:</p> <ol style="list-style-type: none">a. Identification of the nature of the decision (e.g., binary or multi-faceted)b. An unbiased display of pros and cons for each side of the choice and supporting evidencec. An unbiased display of tensions and Trade-offs for each side of the choice and supporting evidenced. Decision reachede. Residual Risk associated with the choicef. Traceability of the deployment of the choiceg. Receipt of Traceability when the deployment is satisfied	Internal Procedure Manual / Correspondence (Internal or External)



	Ethical Oversight	The Ethics Committee shall define, in the Code of Ethics , sufficient diversity of human risk assessors providing Diverse Inputs and Multi Stakeholder Feedback	Public Disclosure Document
	Ethical Oversight	The Ethics Committee shall ensure and document that each instance of Diverse Inputs and Multi Stakeholder Feedback meets diversity standards as defined in the Code of Ethics	Correspondence (Internal or External)
	Ethical Oversight	In regards to employee questions and concerns related: <ol style="list-style-type: none">1. Risks to fundamental rights of AI Subjects2. Other risks of the AAA System, the Ethics Committee shall assess to determine whether the question or concern requires immediate action and document the conclusion in the Ethical Risk Assessment	Internal Procedure Manual
	Ethical Oversight	In consideration of: <ol style="list-style-type: none">1. The Code of Ethics2. Relevant Legal Frameworks3. Incidents reported in the Adverse Incident Reporting System4. Employee raised questions or concerns5. The following guidance:<ol style="list-style-type: none">i. Incidents or malfunctioning leading to death or serious damage to health,ii. Serious and irreversible disruption of the management and operation of critical infrastructure,iii. Infringements of obligations under Union law intended to protect fundamental rightsiv. Serious damage to property or the	Internal Procedure Manual



		<p>environment.</p> <p>the Ethics Committee shall establish metrics, measurements, and thresholds to determine and classify an incident as any of the following:</p> <ul style="list-style-type: none">A. Serious or not seriousB. Reportable or not reportableC. Requiring or not requiring immediate action <p>and document them in the Monitoring Policy</p>	
13.3.b.I V	Ethical Oversight	<p>In consideration of Protected Categories, Intersectionalities, and Vulnerable Populations, the Ethics Committee shall assess the AAA System deployment to determine whether the performance of the deployment might impact any specific group with a meaningful deviation from expected performance and document the conclusion in the Ethical Risk Assessment</p>	Public Disclosure Document
	Ethical Oversight	<p>If the parameterisation of content is the duty of the Deployer, then</p> <p>In consideration of:</p> <ul style="list-style-type: none">1. The contract between the Provider and the Deployer2. Training, education and consultation from the Provider <p>the Ethics Committee shall establish the following:</p> <ul style="list-style-type: none">A. Key Performance Indicators (KPI) for the risk of Model Drift, Data Drift, and Concept DriftB. If applicable, Key Risk Indicators (KRI) for Exceptions InterpretabilityC. If applicable, Key Detrimental Indicators for Content ModerationD. If applicable, Key Regulated Product Indicators for illegal or harmful product	Internal Procedure Manual



		moderation E. If applicable, Key Language Indicators for AAA Systems using LLM, LMM or questionnaires and document them in the Ethical Risk Assessment	
	Ethical Oversight	The Ethics Committee shall assess if the AAA System deployment is Novel to determine if there are sufficient industry standards and comparables for risk assessment and documenting the result in the Ethical Risk Assessment	Internal Procedure Manual
	Ethical Oversight	In consideration of: 1. The contract with the Provider for the AAA System In consultation with: 1. The expert legal team (internal or external) The Ethics Committee shall establish metrics, measurements, and thresholds for the following instances of Ethical Choice in the AAA System deployment: A. The alignment of the Scope, Nature, Context, and Purpose of the AAA System deployment to the Provider's contractual description of acceptable use B. Human oversight and interactions as documented in the Human Interactions Report C. Controllability D. Fairness and document them in the Ethical Risk Assessment	Internal Procedure Manual
	Ethical Oversight	In regards to the Integration Test Plan , the Ethics Committee shall establish metrics, measurements, and thresholds applicable to instances of Ethical Choice for the AAA	Internal Procedure Manual/ Correspondence



		System deployment and document the conclusions in Ethical Risk Assessment with Traceability to Test Lead	(Internal or External)
	Ethical Oversight	<p>In regards to establishing metrics, measurements, and thresholds for instances of Ethical Choice for the Ethics Committee, the Algorithmic Risk Committee shall ensure that the Ethics Committee has access to risk inputs and indicators from all of the following processes with Traceability:</p> <ul style="list-style-type: none">A. Monitoring processesB. Adverse Incident Reporting Systems, (not to include Personal Data)C. Employee questions and concerns (not to include Personal Data)D. Incident databasesE. MediaF. Deployed advertising, promotions, and sales materials	Correspondence (Internal or External)
	Ethical Oversight	<p>In consideration of:</p> <ul style="list-style-type: none">1. The Code of Ethics2. The Code of Data Ethics, <p>the Ethics Committee shall assess all instances of Ethical Choice associated with human oversight and interactions in the AAA System deployment as identified in the Human Interactions Report and complete the following actions:</p> <ul style="list-style-type: none">A. Decide the Ethical ChoiceB. Document the choice and associated processes, procedures, risk controls, treatments, or mitigations with TraceabilityC. Communicate the choice and associated outcomes from (B) to the Human-in-Command or applicable human oversight with Traceability	Correspondence (Internal or External)



	Ethical Oversight	<p>In consideration of:</p> <ol style="list-style-type: none">1. The Necessity Assessment,2. Proportionality Study,3. The Code of Ethics, <p>if the Integration Test Plan or Integration Test Completion Report for the AAA System deployment does not validate the original metrics, measurements, and thresholds for testing and evaluation, then the Ethics Committee shall assess the recommended changes to determine whether the basis for the changes upholds the Integrity of testing and the intent of the shared moral framework of the organisation because one of the following thresholds is met:</p> <ol style="list-style-type: none">A. The original metrics, measurements, and thresholds proved insufficient or invalidB. The new metrics, measurements, and thresholds provide an improved validationC. The new metrics, measurements, and thresholds increase support for the health, safety, and fundamental rights of AI Subjects	Correspondence (Internal or External)
	Ethical Oversight	<p>In consideration of:</p> <ol style="list-style-type: none">1. The Code of Ethics2. The principles portion of the Code of Data Ethics, <p>In regards to the AAA System deployment, the Ethics Committee shall assess and determine the metrics, measurements, and thresholds that identify ethical risk (e.g., financial, reputational, legal, strategic) to the organisation from the following:</p> <ol style="list-style-type: none">A. Each vendor associated with the supply chainB. Each input, product, or service being acquired <p>And document the conclusions in the Vendor</p>	Internal Procedure Manual



		Procurement Plan	
	Ethical Oversight	In regards to the AAA System deployment and in consideration of the Vendor Due Diligence and Procurement policy, the Ethics Committee shall assess each vendor for ethical risks to determine whether the vendor is acceptable and document the decision in the Ethical Risk Assessment	Internal Procedure Manual
	Ethical Oversight	<p>In consideration of all of the following:</p> <ol style="list-style-type: none">1. Relevant Legal Frameworks2. Regulatory guidance3. Code of Ethics4. Scope, Nature, Context, and Purpose of the AAA System deployment <p>The Ethics Committee shall assess each unmitigated risk's severity and likelihood in regards to meaningful negative impact on:</p> <ol style="list-style-type: none">A. AI SubjectsB. Indirect stakeholders (e.g., environment, society, markets)C. Protected Categories, Intersectionalities, and Vulnerable Populations <p>to determine applicable thresholds of negative impact that require Public disclosure of the unmitigated risk and document the conclusion in the Ethical Risk Assessment</p>	Internal Procedure Manual
	Ethical Oversight	<p>In regards to any Public Disclosure Documents associated with the AAA System deployment, the Ethics Committee shall do any of the following that are applicable:</p> <ol style="list-style-type: none">1. Validate and pass through the Provider's Public Disclosure Documents2. Keep current and publish the Deployer's Public Disclosure Documents with a range of accessible modalities	Internal Procedure Manual



	Ethical Oversight	In regards to any logs, recording keeping, and associated private documentation with the AAA System deployment, the Ethics Committee should implement, keep current, and store them with a range of accessible modalities	Internal Procedure Manual
	Ethical Oversight	In consideration of: 1. The Code of Ethics , 2. Relevant Legal Frameworks the Ethics Committee shall assess the metrics, measurements, and thresholds associated with AAA System deployment to determine whether the inferences concluded are fair, balanced, and relevant to the applicable Purpose and document the conclusion in the Ethical Risk Assessment	Internal Procedure Manual
Consumer Protection			
	Consumer Protection	In consideration of: 1. The Deployer's sales, marketing and promotional materials, including training, associated with AAA System deployment 2. Relevant Legal Frameworks and in consultation with the expert legal team (internal or external), the Ethics Committee shall assess to determine whether the materials for the AAA System deployment do any of the following: A. Exaggerate B. Mislead C. Falsify And document the controls, treatments, and mitigations in the Ethical Risk Assessment	Internal Procedure Manual
	Consumer Protection	If the organisation offers free trials or limited	Physical Testing



		period discounted contracts for the use of the AAA System deployment, then the organisation shall provide explicit and Just-in-Time notification to the AI Subject of the end of the trial or limited period and the need for additional Consent to contract for services at the end of that period	
	Consumer Protection	<p>In regards to Nudges and Deceptive Design, the Ethics Committee shall assess the deployment of the AAA System in the following areas:</p> <ol style="list-style-type: none">1. Design2. Interfaces3. Advertising4. Community policies and standards5. Terms and conditions6. Notifications <p>and determine whether the use of Nudges and/or Deceptive Designs in the AAA System deployment are in support of the best interest of the AI Subject by:</p> <p>A. Encouraging Nudges and design that:</p> <ol style="list-style-type: none">i. Lead the AI Subject to make higher privacy selectionsii. Support health and well-beingiii. Encourage robust securityiv. Follow signposts to seek the advice of parents, carers or Guardiansv. Balance the best interests of the Child with the need for the Child to learn how to make their own choices <p>and if the use of Nudges and/or Deceptive Designs in the AAA System deployment are</p>	Internal procedure manual



		<p>NOT in support of the best interest of the AI Subject, then:</p> <p>B. Identify any Nudges and/or Deceptive Designs that are likely to:</p> <ul style="list-style-type: none">i. Violate the Human Rights and Freedoms of the AI Subjectii. Result in economic harm or damagesiii. Result in inaccessible terms or conditionsiv. Foster addiction through rewards that are provided for regular access without a commensurate warning as to the risks (e.g., creating experiences that depict/resemble gambling without appropriate warnings)v. Persuade an AI Subject to lower data privacy settings and/or to frequently reassess those settings (e.g., access to contacts or phonebook)vi. Persuade an AI Subject to provide more Personal Data, including to keep Geolocation “on” when it is not necessary for the performance of the AAA System deploymentvii. Persuade an AI Subject to lie or to select the incorrect age rangeviii. Persuade an AI Subject to elect personalization tools (e.g., cookies, trackers, push notifications) and/or direct marketingix. Persuade an AI Subject to provide excessively precise Geolocation	
--	--	---	--



		<ul style="list-style-type: none">x. Mislead and/or deceive an AI Subject by using high-pressure business terms and/or tactics (e.g., hidden or unconnected offers and associated cost, delayed terminations)xi. Mislead and/or deceive an AI Subject by using false or misleading calls to action, UX/UI interfaces, and notificationsxii. Mislead and/or deceive an AI Subject by using asymmetry in Choice Architecture (e.g., yes/no, opt-in/opt-out)xiii. Mislead and/or deceive an AI Subject regarding the impact of online interactions on data rates or data usagexiv. Mislead and/or deceive an AI Subject with UX/UI interfaces that trap or forces the AI Subject into certain choices (e.g., unnecessary run-time permission requests)xv. Mislead and/or deceive an AI Subject with Choice Architecture that guides towards a single choice for account management (e.g., pause-only or delete-only)xvi. Mislead and/or deceive an AI Subject with UX/UI interfaces that guides towards choices that benefit the organisation by replacing expected standard functionalityxvii. Mislead and/or deceive an AI Subject with false or misleading	
--	--	--	--



		<p>terms and conditions in apps or subscriptions (e.g., size of app, technical requirements, age restrictions, requiring Personal Data)</p> <p>C. Prohibit identified detrimental Nudges and Deceptive Design controlled by the Deployer</p> <p>D. Notify the Provider of identified detrimental Nudges or Deceptive Designs</p> <p>E. Document any applicable changes, risk controls, treatments, or mitigations in the Ethical Risk Assessment</p>	
	Consumer Protection	In regards to Nudges and in consultation with the Ethics Committee , the Algorithmic Risk Committee shall implement all changes, risk controls, treatments, and mitigations with Traceability , as identified in the Ethical Risk Assessment	Physical Testing
	Consumer Protection	<p>In consultation with the Ethics Committee, the Algorithmic Risk Committee shall notify the AI Subject of all of the following regarding the deployment of the AAA System including:</p> <p>A. Establishing a Code of Conduct, if applicable</p> <p>B. Descriptions of what data is monitored, collected, or used and the associated purpose</p> <p>C. How the Personal Data is used</p> <p>D. What are the metrics, measurements, and thresholds used to determine boundary conditions for acceptable and unacceptable use</p> <p>E. How the AI Subject can validate inferences determined by the AAA</p>	Correspondence (Internal or External)



		System and challenge and/or Delete/Destroy unfair inferences	
Data Privacy and Protection			
	Data Privacy and Protection	<p>In consideration of:</p> <ol style="list-style-type: none">1. Vendor Procurement Plan2. Vendor due diligence <p>The Algorithmic Risk Committee shall assess the Provider's AAA System Source Data to determine whether the Source Data was unstructured and subsequently, during structuring, introduced Personal Data in the metadata and document the conclusion in the AAA Systems List that Personal Data is present</p>	Internal log, register, or database
	Data Privacy and Protection	<p>If the AAA System deployment collects, processes, or uses Personal Data then</p> <p>In consideration of:</p> <ol style="list-style-type: none">1. Relevant Legal Frameworks2. The Jurisdiction(s) of operation for the AAA System <p>the Deployer shall have current assurance upholding applicable GDPR Article 42 certification and demonstrating data privacy and protection conformity by documenting one of the following:</p> <ol style="list-style-type: none">A. Certification with a ForHumanity or equivalent Personal Data certification scheme(s) applicable to all Personal Data in the AAA System deployment	Public Disclosure Document



	Data Privacy and Protection	If Personal Data is processed in the AAA System deployment, then the Algorithmic Risk Committee shall assess and determine the organisation's responsibility for the Personal Data as a Controller or Processor and document the conclusion in the AAA Systems List	Internal Procedure Manual
	Data Privacy and Protection	If the Controller/Processor assessment concludes that the AAA System deployment is a Processor of Personal Data , then the Algorithmic Risk Committee shall assess the AAA System to determine if the AAA System is integrated or standalone and subsequently certified under the applicable ForHumanity EU GDPR Processor Certification scheme or equivalent	Internal Procedure Manual
AAA System Procurement			
	AAA System Procurement	<p>In consideration of:</p> <ol style="list-style-type: none">1. Code of Ethics2. Code of Data Ethics, <p>And in consultation with:</p> <ol style="list-style-type: none">1. The Ethics Committee, <p>the Algorithmic Risk Committee shall conduct and keep current a Necessity Assessment for the AAA System design, development, and deployment that includes:</p> <ol style="list-style-type: none">A. Documents the problem statementB. Default to the simplest possible technological implementationC. Identify precise specifications and requirements for the AAA System design, development and deploymentD. Ensuring that the design, development and deployment of the AAA System deployment is auditable	Internal Procedure Manual



	AAA System Procurement	<p>In consideration of:</p> <ol style="list-style-type: none">1. The Code of Ethics2. The Code of Data Ethics,3. The design and development of the AAA System deployment4. Relevant Legal Frameworks5. Quality Management Policy <p>And in consultation with:</p> <ol style="list-style-type: none">1. The Ethics Committee,2. The expert legal team (internal or external)3. Top Management and Oversight Bodies, if applicable4. AAA Cybersecurity Lead <p>the Algorithmic Risk Committee shall document a AAA System Procurement Plan that includes all of the following:</p> <ol style="list-style-type: none">A. A description of the specifications and requirements of the Provider and the AAA System that are necessary to fulfil the legal obligations of the Deployer in regards to the AAA System deployment, including an assessment of the riskiness of the AAA System deploymentB. Metrics, measurements, and thresholds in regards to the specifications and requirements of the AAA System for:<ol style="list-style-type: none">i. Scope, Nature, Context, and Purpose of the AAA System<ol style="list-style-type: none">a. Characteristics and featuresb. Licensing and terms and conditionsc. Limitations and out of Scope boundariesii. AAA System embedded governance, oversight, and accountability (e.g., monitoring, human	Internal Procedure Manual
--	---------------------------	--	---------------------------------



		<ul style="list-style-type: none">interaction)iii. Functional Correctness, Robustness, resilienceiv. Ethical considerationsv. Data privacy, security, and protectionvi. Bill of Materials and/or System of Records, as appropriate and applicable to the AAA Systemvii. Acquisition or interface standardsviii. Security and cybersecurityix. Accessibility, Usability, and Accommodationsx. Quality objectivesxi. Conformity or third-party assurance assessments, if applicablexii. Environmental and sustainability impactsxiii. Legal and regulatory obligations (e.g., representations, warranties, indemnifications), including required disclosures, transparency, and Explainability <p>C. Metrics, measurements, and thresholds of the AAA System Provider for:</p> <ul style="list-style-type: none">i. Ethics standards and oversight (e.g., Provider's Code of Ethics, Code of Data Ethics)ii. Robustness and resilienceiii. Security and technical requirementsiv. Data privacy and protection safeguards (e.g., GDPR, CCPA, DPDPA certifications)v. Record-keeping tools (e.g., Event logs), and technical documentation provisionvi. Vendor quality control	
--	--	---	--



		<ul style="list-style-type: none">vii. Accessibility, Usability, and Accommodations provisions, if applicableviii. Applicable training and education provisionix. Financial stabilityx. Environmental sustainability practicesxi. Legal and regulatory compliance and Deployer support (e.g., representations, warranties, indemnifications) <p>D. For each of the above applicable metrics, measurements, and thresholds a list of acceptable validation for the Provider's response</p> <p>E. A risk-based assessment (due diligence) of the Provider's ability to meet all contractual requirements including identifying according to the criticality of the Provider's and the AAA System:</p> <ul style="list-style-type: none">i. Audit targets to determine the necessary audit level and frequencyii. Integration Testing and Evaluation of the the interface with the Provider's and the integration of AAA System	
	AAA System Procurement	<p>In consideration of:</p> <ul style="list-style-type: none">1. Relevant Legal Framework2. Regulatory guidance, as appropriate and applicable3. AAA System Procurement Plan <p>And in consultation with the expert legal team (internal or external), the Algorithmic Risk Committee shall ensure that all of the following clauses are stipulated in the contract with the Provider:</p> <p>A. List of technical specifications required</p>	Contract



		<p>for contracting in regards to:</p> <ul style="list-style-type: none">i. The AAA Systemii. The vendor <p>B. Representations and warranties in regards to:</p> <ul style="list-style-type: none">i. The AAA System being acquiredii. Intellectual property rightsiii. Certification, if applicableiv. Cybersecurity measuresv. Compliance with Relevant Legal Frameworks, consent decree, and/or judicial/legal decisionsvi. Personal Data storagevii. Personal Data breaches <p>C. Delineation of duties between the Deployer and the Provider (e.g., human interactions, monitoring)</p> <p>D. Right to audit, as applicable</p> <p>E. Termination rights and process</p>	
	AAA System Procurement	<p>In consideration of the AAA System Procurement Plan and in consultation with the Algorithmic Risk Committee, Top Management and Oversight Bodies shall assess the contract with the Provider to determine completeness and document the decision with Traceability</p>	Correspondence (Internal or External)
	AAA System Procurement	<p>In consideration of:</p> <ul style="list-style-type: none">1. The Monitoring Policy,2. The AAA System Procurement Plan3. The contract with the Provider4. Quality Management Policy <p>And in consultation with the Quality Management Lead, the Monitoring Lead shall establish processes and procedure to monitor the AAA System and the Provider, including audits, using the technical specification identified in the AAA System</p>	Internal Log, register, or database



		Procurement Plan to determine whether the AAA System and the Provider remain within specifications and document the conclusion in the Monitoring log and the QMS Audit Report	
Risk Management - Article 9			
	Risk Management	<p>In consideration of:</p> <ol style="list-style-type: none">1. Maximizing risk controls, treatments, and mitigation on behalf of both direct and indirect stakeholders2. Duty of Care to Protected Categories, Intersectionalities, and Vulnerable Populations3. AAA System Procurement Plan specifications and requirements <p>In consultation with:</p> <ol style="list-style-type: none">1. All applicable specialty committees, the Algorithmic Risk Committee shall assess the Provider's AAA System to determine whether the AAA System meets specifications and requirements for risk management by:<ol style="list-style-type: none">A. Examining the Provider's risk management processes and procedures<ol style="list-style-type: none">i. Identifying impacts on direct and indirect stakeholders in the context of the AAA System deploymentii. The Provider's Residual Risks are acceptableB. Determine whether the Provider has included an Adverse Incidents Reporting System <p><u>In regards to the AAA System deployment</u></p> <ol style="list-style-type: none">C. Identify risk controls, treatments, and mitigations for each Algorithmic RiskD. Implement risk controls, treatments, and	Internal Procedure Manual



		<p>mitigations identified in the studies, analyses, or assessments (e.g. Necessity, Proportionality, Algorithmic Risk, Ethical Risk) for the AAA System deployment with Traceability</p> <p>E. Conduct Integration Testing and Evaluation for the AAA System and deployment including,</p> <ul style="list-style-type: none">i. Approving the Integration Test Plan and Integration Test Completion Reportii. Providing specialist testing resources including an expert in Integration Testing and Evaluation, designated as the Test Lead <p>F. Include the Test Lead as a member of the Algorithmic Risk Committee</p> <p>G. Ensure that the committee members remain trained on current Integration Testing and Evaluation methods, outputs, and reports in order to properly assess the Integration Test Plan and Integration Test Completion Report</p> <p>H. Ensure Integration Testing and Evaluation includes foreseeable scenarios, capabilities, and expertise aligned and documented appropriate to the Integration Test Plan</p> <p>I. Ensure proportionate, based upon the risk of the AAA System deployment, continuous and post-market monitoring including regularly evaluating the risk controls, treatments, and mitigations for effectiveness</p> <p>J. Establish a remediation process or procedure, with Traceability, for when:</p> <ul style="list-style-type: none">i. Continuous or post-market	
--	--	--	--



		<p>monitoring identifies deviations from acceptable monitoring thresholds</p> <p>ii. Adverse Incidents Reporting Systems identify a new or changed risk input or indicator</p> <p>K. Publicly document Residual Risk according to Relevant Legal Frameworks, regulatory guidance, the Ethical Risk Assessment, and industry standards</p> <p>L. Ensure the production of the cAIRE Report and delivery to Top Management and Oversight Bodies</p> <p>And document the conclusions in the Algorithmic Risk Assessment</p>	
	Risk Management	<p>In consultation with:</p> <ol style="list-style-type: none">1. The Enterprise/Organizational Risk Management (Chief Risk Officer)2. The Ethics Committee3. Any applicable Specialty Committees <p>and in consideration of:</p> <ol style="list-style-type: none">1. the Code of Ethics2. and Code of Data Ethics, <p>the Algorithmic Risk Committee shall establish and document a Risk Management Policy for the AAA System deployment that includes all of the following by establishing:</p> <p>A. The AAA System deployment risk management framework, processes, and procedures including:</p> <ol style="list-style-type: none">i. Establishing a culture and process of constant risk assessment by all persons associated with the AAA System deploymentii. Establishing a process to identify	Internal Procedure Manual



		<p>direct and indirect stakeholders (to satisfy the requirement for Diverse Input and Multi Stakeholder Feedback) involved in the AAA System deployment who are responsible for risk identification</p> <p>iii. Establishing a risk taxonomy and risk categories</p> <p>iv. Establishing guidance for identifying risk inputs and indicators negatively impacting the health, safety, and fundamental rights associated with the AAA System deployment, including:</p> <ul style="list-style-type: none">a. Ground Truth Availabilityb. Functional Correctnessc. Human Interactionsd. Fairness and nondiscriminatione. Robustnessf. Systemic Riskiness (e.g., Systemic Societal Impact)g. Effectiveness of embedding Ethics, Governance or Accountability structures to oversee risks <p>v. Establishing a process for the evaluation of risk inputs and indicators including metrics and measurements for severity and likelihood</p> <p>vi. Establishing a risk evaluation process that does all of the following:</p>	
--	--	--	--



		<ul style="list-style-type: none">a. Examines existing incident reporting systems and industry-standard mitigationsb. Examines risk indicators to identify root cause and negative impacts to health, safety, and fundamental rightsc. Examines risk inputs to consider a range of potential controls, treatments, and mitigationsd. Examines and tests the effectiveness of potential risk controls, treatments, and mitigationse. Identifies metrics, measurements, and thresholds for monitoring an Adverse Incident Reporting System to define an Emergent Risk and establish processes and procedures to begin immediate risk assessment <p>vii. Establishing a process for assessing and implementing risk controls, treatments, and mitigations.</p> <p>viii. Compiling Residual Risks from all risk assessments associated with the AAA System deployment and document them in the cAIRE Report</p> <p>B. Metrics, measurements, and thresholds to identify excessive Residual Risk</p>	
--	--	---	--



		<ul style="list-style-type: none">C. The risk logD. The frequency for risk assessment, including by Diverse Input and Multi Stakeholder Feedback pool of human risk assessors in the context of the lifecycle of the AAA System deploymentE. Metrics, measurements, and thresholds for the following:<ul style="list-style-type: none">i. Severityii. Likelihoodiii. Human Interactionsiv. To advise Top Management and Oversight Bodies regarding the assessment of Residual Risk in the context of Risk Appetite and Risk ToleranceF. Metrics, measurements, and thresholds in regards to the frequency of risk reassessment:<ul style="list-style-type: none">i. In response to a change in Risk Input, Indicator, Severity, or Likelihoodii. In response to inadequate risk categories, taxonomies, scales (Severity and Likelihood)iii. In response to a change in Residual Risk (comprehensive)G. A process or procedure to reassess (Identify, Analyze, Evaluate, Treat) any of the (E.i - iii) in response to an exceeded threshold and compile a new Residual RiskH. Learning objectives in regards to risk management for the AAA System including roles, responsibilities, and duties in the context of the AAA System deployment for all impacted employees, contractors, or gig-workers (e.g., human	
--	--	--	--



		<p>risk assessors)</p> <ul style="list-style-type: none">I. The frequency of review of the Risk Management PolicyJ. The process for amending risk inputs and indicators based upon feedback from continuous and post-market monitoring, including the Adverse Incident Reporting SystemK. Metrics, measurements, thresholds for existing and newly identified risk controls, treatments, and mitigations, to determine effectivenessL. The frequency of update to Enterprise/operational risk management with the cAIRE Report for the AAA System deploymentM. A process to receive input from the Ethical Risk Assessment to determine whether any Residual Risk is to be disclosed <p><i>Note 3 -</i> https://forhumanity.center/bok/risk-management/ <i>provides guidance and templates for all elements of the ForHumanity Risk Management Framework</i></p>	
	Risk Management	<p>The Algorithmic Risk Committee shall conduct and keep current an Algorithmic Risk Assessment that:</p> <ul style="list-style-type: none">A. Logs the Residual Risk from the Provider's AAA System as identified during due diligenceB. Includes Diverse Inputs and Multi Stakeholder Feedback from human risk assessorsC. Establishes a risk logD. Conducts regular reviews across the	Internal log, register, or database



		<p>lifecycle of the AAA System deployment (e.g., procurement, integration, deployment, monitoring, and decommissioning)</p> <p>E. Identifies risk inputs and risk indicators as negative impacts to health, safety, and fundamental rights and freedoms including</p> <ul style="list-style-type: none">i. Reasonably foreseeable misusesii. Insufficiencies associated with:<ul style="list-style-type: none">a. Accessibilityb. Usability <p>F. Conducts Failure Mode and Effect Analysis (FMEA)</p> <p>G. Analyzes risk, including identifying severity and likelihood</p> <p>H. Evaluates risk to identify:</p> <ul style="list-style-type: none">i. Risk controls, treatments, and mitigations, with Traceability of deploymentii. If applicable and appropriate, minor incident response processes and/or procedures,iii. If applicable and appropriate, major incident plans <p>I. Compiles Residual Risk</p> <p>J. Classifies Residual Risk as public or confidential</p> <p>K. If the AAA System deployment has Personal Data, then compiles a separate Data Protection Impact Assessment</p> <p>L. Implements specific metrics, measurements, and thresholds for risk reassessment</p> <p>M. Implements procedures for identifying deviations from acceptable monitoring thresholds, Key Performance</p>	
--	--	---	--



		Indicators, and Key Risk Indicators	
	Risk Management	<p>The Algorithmic Risk Committee shall establish and keep current a risk log (as established in the Algorithmic Risk Assessment) for all of the following:</p> <ul style="list-style-type: none">A. Risk inputsB. Risk indicatorsC. Risk controls, treatments, and mitigations,D. Residual Risk, including the category of disclosure (i.e., Public, confidential, or internal) <p>as determined in the Algorithmic Risk Assessment</p>	Internal log, register or database
	Risk Management	<p>If the AAA System deployment collects, processes, or uses Personal Data, then the Algorithmic Risk Committee shall compile a Data Protection Impact Assessment that contains all of the following elements:</p> <p><u>Describe the AAA System</u></p> <ul style="list-style-type: none">A. The Scope, Nature, Context, and Purpose of the AAA SystemB. Data Flow DiagramC. Bias mitigation policyD. Data Protection PolicyE. Assess requirement for specialty committees in regards to Vulnerable PopulationsF. Data Subject Rights Request provisionG. Privacy policyH. Data security policyI. Security policy <p><u>Identify and Include Stakeholders</u></p>	Internal Procedure Manual



		<p>K. Diverse Input and Multi Stakeholder Feedback (DI&MSF) throughout the AAA System lifecycle</p> <p>L. DI&MSF in the Algorithmic Risk Assessment, including Bias Mitigation</p> <p>M. DI&MSF in the Ethical Risk Assessment</p> <p>N. Ethics Committee definition of diversity</p> <p>O. Ethics Committee assess pools of human risk assessors for diversity</p> <p>P. Contractual obligations of Processors</p> <p><u>Assess Necessity and Proportionality</u></p> <p>Q. Necessity Assessment</p> <p>R. Proportionality Study</p> <p>S. AAA Systems List (for legal basis)</p> <p>T. Model, Data, Concept Drift monitoring</p> <p>U. Data and Information Quality assessment</p> <p>V. bias mitigation</p> <p>W. Transfer Impact Assessment</p> <p><u>Identify and Analyze Risk</u></p> <p>X. Risk management policy</p> <p>Y. Implementation of risk management framework</p> <p>Z. Algorithmic Risk Assessment</p> <p><u>Evaluate and Treat Risk</u></p> <p>AA. Implement all Algorithmic Risk Assessment risk controls, treatments, and mitigations</p> <p>BB. Implement all Cybersecurity Risk Assessment controls, treatments, and mitigation</p> <p>CC. Implement post-market and continuous monitoring</p> <p><u>Signoff and Record Outcomes</u></p> <p>DD. Residual Risk approval</p> <p>EE. DPO identified and advice provided</p>	
--	--	--	--



		FF. DPO advice justified or overruled with Traceability GG. DPIA owner identified and all approvals logged	
	Risk Management	The Algorithmic Risk Committee shall ensure that, in a timely manner throughout the deployment lifecycle of the AAA System (e.g., procurement, integration, deployment, monitoring, decommissioning), all risk inputs and indicators are collected and logged, in the risk log, from the following workflows: A. Risk Management, B. Data Management and Governance, C. Integration Testing and Evaluation, D. Technical Documentation E. Monitoring, F. Human Oversight G. Vendor Management H. Change Management I. Incident Management J. Quality Management System, including quality controls and objectives K. Adverse Incident Reporting Systems L. Real world testing (Article 60), if applicable	Internal log, register, or database
	Risk Management	In consideration of Residual Risk , the Algorithmic Risk Committee shall implement processes and procedures to determine whether the Residual Risk of the AAA System deployment is excessive and recommend decommissioning and document the conclusion in the cAIRE Report	Internal Procedure Manual
	Risk Management	In consultation with: 1. The Ethics Committee 2. All applicable specialty committees	Correspondence (Internal or External)



		<p>Prior to acquiring the AAA System, the Algorithmic Risk Committee, shall document in the Business Rationale Report:</p> <ul style="list-style-type: none">A. The Provider's description of the Causal HypothesisB. The Residual Risk to fundamental human rights, as identified in the fundamental rights impact assessment	
	Risk Management	<p>In consideration of:</p> <ul style="list-style-type: none">1. The Scope, Nature, Context, and Purpose of the AAA System,2. Relevant Legal Frameworks3. Deployed Jurisdictions <p>the Algorithmic Risk Committee shall log, in the risk log, a list of applicable requirements identified from the relevant EU Harmonised Standards and Common Specifications found in Annex I Section A or B applicable to the AAA System deployment</p>	Internal log, register or database
	Risk Management	<p>In consideration of relevant EU harmonised standards and common specification aligned to the Scope, Nature, Context and Purpose of the AAA System, the Algorithmic Risk Committee documents, in the Risk Log, risk inputs and indicators associated with conformance to the standards and specifications across the entire lifecycle of the AAA System deployment (e.g., procurement, integration, deployment, monitoring, decommissioning)</p>	Internal log, register or database
9.2.b	Risk Management	<p>The Algorithmic Risk Committee shall implement all risk controls, treatments, and mitigations with Traceability as documented in the Algorithmic Risk Assessment</p>	Internal Procedure Manual
	Risk Management	<p>In consideration of the Deployer's Fundamental Rights Impact Assessment, the</p>	Correspondence (Internal or



		Algorithmic Risk Committee shall implement all identified risk controls, treatments, and mitigations with Traceability	External)
	Risk Management	The Algorithmic Risk Committee shall implement all risk controls, treatments, and mitigations identified in the Deployer's Proportionality Study with Traceability	Correspondence (Internal or External)
	Risk Management	The Algorithmic Risk Committee shall implement all risk controls, treatments, mitigations and/or Ethical Choice decisions documented in the Ethical Risk Assessment with Traceability	Internal procedure manual
	Risk Management	In consideration of: <ol style="list-style-type: none">Integration Integration Testing and EvaluationThe Algorithmic Risk AssessmentThe Fundamental Rights Impact AssessmentRelevant Legal Frameworks, if any assessment identified that the AAA System deployment may have a discriminatory impact on any individual, group or population, then the Algorithmic Risk Committee shall reject the AAA System and document the conclusions in the AAA System Procurement Plan	Internal Procedure Manual
9.2.b	Risk Management	If Diverse Inputs and Multi Stakeholder Feedback human risk assessors identify potential misuses of the AAA System deployment, then the Algorithmic Risk Committee shall log them as risk inputs in the risk log	Internal log, register, or database



9.2.b	Risk Management	<p>In consideration of the Relevant Legal Frameworks, the Ethics Committee shall assess instances of Ethical Choice in the AAA System deployment:</p> <ul style="list-style-type: none">A. To determine which misuses of the AAA System deployment are reasonably foreseeableB. To document reasonably foreseeable misuses in an Ethical Risk AssessmentC. To communicate the reasonably foreseeable misuses to the Algorithmic Risk Committee	Internal Procedure Manual
	Risk Management	<p>If the Provider does not supply an Adverse Incident Reporting System, then the Algorithmic Risk Committee shall implement an Adverse Incident Reporting System for the AAA System deployment</p>	Physical
9.2.c	Risk Management	<p>In consideration of:</p> <ul style="list-style-type: none">1. Continuous and post-market monitoring2. The Adverse Incident Reporting System, <p>the Algorithmic Risk Committee shall assess each incident identified as risks (either as a risk input or indicator) to:</p> <ul style="list-style-type: none">A. Classify it as security or algorithmic riskB. Log it as risk inputs or indicators in the Cybersecurity Risk Log or the Algorithmic Risk Log as applicableC. Analyse, evaluate and treat it according to the applicable policy	Internal Log, Register, or Database
9.2.c	Risk Management	<p>In consideration of:</p> <ul style="list-style-type: none">1. Continuous and post-market monitoring2. Adverse Incident Reporting System,3. Key Risk Indicators (KRIs) <p>The Algorithmic Risk Committee shall assess incidents and newly identified risks (either as a risk input or indicator) to determine whether</p>	Internal procedure Manual



		they exceed established thresholds indicating a full risk reassessment, and document the conclusion in the Algorithmic Risk Assessment , including lessons learned from exceeded KRIs .	
9.2.c	Risk Management	If the root cause of a risk indicator can be identified through analysis and evaluation of the risk by the Algorithmic Risk Committee then the risk indicator shall be changed to a risk input and treated accordingly else, the failure to determine a root cause shall be included in the Residual Risk and the risk indicator shall be treated accordingly	Internal Procedure Manual
9.2.d	Risk Management	The Algorithmic Risk Committee shall: A. Assess all risk inputs and indicator to determine the most effective risk controls, treatments, and mitigations that collectively minimises Residual Risk B. Implement the risk controls, treatments, and mitigations with Traceability C. Implement a monitoring process with metrics, measurements, and thresholds for each risk control, treatment, and mitigations to determine continued effectiveness	Internal Procedure Manual
	Risk Management	In consideration of the: 1. Integration Integration Test Completion Report 2. Algorithmic Risk Assessment 3. Ethical Risk Assessment 4. Data Procurement Report 5. Relevant Legal Frameworks 6. Deployer's Risk Appetite and Risk Tolerance , the Algorithmic Risk Committee shall accept and compile all individual unmitigated risks in the following manner: A. In manner that meets all legal obligations	Internal Procedure Manual



		<p>B. A risk controlled, treated, or partially mitigated but not entirely eliminated establishes an individual unmitigated risk</p> <p>C. Each individual unmitigated risk must be documented and accepted by the Algorithmic Risk Committee or the Ethics Committee (for instances of Ethical Choice)</p> <p>D. All individual unmitigated risks must be combined to establish the AAA System's Residual Risk</p> <p>and document the conclusions in the cAIRE Report</p>	
	Risk Management	<p>In consideration of:</p> <ol style="list-style-type: none">1. The established thresholds for public disclosure found in the Ethical Risk Assessment,2. Relevant Legal Frameworks3. Harmonized Standards and Common Specifications, if applicable <p>the Algorithmic Risk Committee shall establish a procedure to assess whether the unmitigated risk exceeds the thresholds to determine if the unmitigated risk is to be disclosed Publicly and document the conclusion in the cAIRE Report</p>	Physical Testing
	Risk Management	<p>In consideration of:</p> <ol style="list-style-type: none">1. Relevant Legal Frameworks2. Regulatory Guidance3. The threshold(s) for confidential disclosure to National Supervisory Authorities <p>In regards to each unmitigated risk, the Algorithmic Risk Committee shall assess to determine whether the unmitigated risk exceeds the thresholds indicating that the risk is to be</p>	Physical Testing



		disclosed confidentially to National Supervisory Authorities and document the conclusion in the cAIRE Report	
	Risk Management	<p>In consideration:</p> <ol style="list-style-type: none"> 1. The Residual Risk conclusion in the correspondence from Top Management and Oversight Bodies 2. Relevant Legal Frameworks 3. Regulatory guidance <p>the Algorithmic Risk Committee shall assess the Residual Risks to be disclosed Publicly to determine the language and medium in which they are to be compiled, documented, and displayed</p>	Public Disclosure Document
EU-DE -EU-R M-AC- 025-04 25	Risk Management	<p>In consideration of:</p> <ol style="list-style-type: none"> 1. The accepted Residual Risk 2. The Algorithmic Risk Assessment, <p>the Algorithmic Risk Committee shall assess the severity and likelihood of each individual Residual Risks to determine which individual risks are to to be disclosed in the Just-in-Time notification or the terms and conditions and document conclusions in the Algorithmic Risk Assessment</p>	Internal Procedure Manual
	Risk Management	<p>Based upon the assessment in Criteria (RM-AC-025), the Algorithmic Risk Committee shall ensure that the public disclosure of Residual Risk is disclosed in a Just-in-Time notification using clear and plain language containing all of the following:</p> <ol style="list-style-type: none"> A. Specific unmitigated individual risks based upon a risk-based assessment of severity and likelihood to AI Subjects B. That the AI Subject is interacting with an AAA System C. The known level of Functional Correctness along with Explainability and if applicable, Explainability+ 	Physical Testing



		<p>Statement</p> <p>D. An adequate disclaimer for Adverse Impacts and directions on how to access the Adverse Incident Reporting Systems for AI Subjects</p> <p>E. An opportunity for AI Subjects to opt-out as far as feasible</p> <p>F. A conspicuous link to the terms and conditions</p>	
	Risk Management	Based upon the assessment in Criteria (RM-AC-025), the Algorithmic Risk Committee shall document public Residual Risk in the terms and conditions	Physical Testing
	Risk Management	<p>If the Ethics Committee assesses the AAA System deployment to be Novel, then the Algorithmic Risk Committee shall ensure all of the following:</p> <p>A. Specific disclosure in the Residual Risk that the AAA System deployment is Novel documented in the risk log with Traceability</p> <p>B. Augment training to sales, marketing and promotional teams, with Traceability, on the added risks associated with a Novel deployment to avoid false, misleading or exaggerated claims</p> <p>C. Augment disclosures in the AAA System AI Subject's Guide stating the lack of industry standards and sufficient comparables</p>	Correspondence (Internal or External)
	Risk Management	<p>In consideration of:</p> <ol style="list-style-type: none">1. The Ethical Risk Assessment2. The metrics, measurements, and thresholds provided by the Ethics Committee in regard to the health, safety, and well-being of human interactors,	Correspondence (Internal or External)



		the Algorithmic Risk Committee shall establish a process or procedure to measure and monitor human interactors with Traceability to the Ethics Committee	
	Risk Management	The Algorithmic Risk Committee shall log all risk inputs and indicators identified by: A. The due diligence and contracting with the Provider of the AAA System B. Vendor Procurement Plan And implement contractual duties and document risk inputs and/or indicators in the risk log	Internal Log, register or database
	Risk Management	In consideration of the Scope, Nature, Context, and Purpose and the technical infrastructure of the AAA System deployment, the Algorithmic Risk Committee shall establish the expected lifetime of the system and document it in the AAA Systems List , and the AAA System AI Subject Guide	Internal Procedure Manual

Appendix A - Infrastructure of Trust for AI - Guide to Entity Roles and Responsibilities

ForHumanity promotes this certification scheme to all entities that wish to provide advice, guidance, consulting and assurance or organisation both outside and within the European Union. ForHumanity licences entities to offer the scheme and a list of licensed entities can be found [here](#).

ForHumanity also trains individuals to become ForHumanity Certified Auditors (FHCAs). Earning this certification is the ultimate assurance of knowledge of this certification scheme and the process by which certification is achieved for organisations. ForHumanity offers online, asynchronous training in this certification scheme through its training platform – [ForHumanity University](#).

ForHumanity promotes this and many other certification schemes to organisations, governments, regulators, national accreditation bodies, professionals and the public by social



media, conference speeches, university lectures, online presence, and execution of our mission statement to specific support an infrastructure of trust with a wide range of participants from society.

Describing the roles in an [infrastructure of trust](#) for AI, Algorithmic and Autonomous (AAA) Systems - we have a model with a long track record of success. ForHumanity is adapting that model to AAA Systems.

Background on Independent Audit

In 1973, the accounting industry came together and formed The Financial Accounting Standards Board (FASB) which created the Generally Accepted Accounting Principles (GAAP) which still govern financial accounting today. Eventually, the US Securities and Exchange Commission, and other extranational regulatory agencies, required adherence to the GAAP standard for all publicly listed companies. This clarity and uniformity significantly improved the financial world. An infrastructure of trust has been built over the past 50 years because of critical features such as independence, certified practitioners, and third-party rules that are compliant with the law and best practices.

Adapting to AI and Autonomous Systems

ForHumanity has advocated for the adoption of this infrastructure of trust and explained how it can be adapted and adopted for the Governance, Accountability, and Oversight of AI and Autonomous Systems. We support the creation and mandate of Independent Audit of AI Systems (IAAIS). IAAIS provides a comprehensive solution grounded in the same fundamental principles as Independent Financial Audit. ForHumanity develops and maintains audit and certification criteria designed for a range of industries and jurisdictions.

The proposed system replicates the distributed oversight, accountability and governance needed for AI, Algorithmic, and Autonomous (AAA) systems in the same manner as financial audit, through audit and pre-audit service providers. These entities will employ certified practitioners to prepare for an eventual independent audit performed by other certified practitioners. The audit criteria are crowdsourced and presented transparently to maximise an entity's ability to achieve compliance. Advancements in systems technology allow many of these processes to be automated for entities such as with the Treadway Commissions' Committee of Sponsoring Organization (COSO) framework for internal risk, audit and controls. The result is a fully-integrated, compliance-by-design infrastructure that embeds human agency, transparency, disclosure and compliance from design to decommission.

Role on Independent Audit of AI and Autonomous Systems

The audit criteria are applied in two vectors: 1) Top-down accountability, governance and oversight 2) laterally, AI system by AI system. The top-down approach creates accountability systems for ethics, bias, privacy, trust, and cybersecurity for the Board of Directors, Chief Executive Officer, and Chief Data Officer. Committee structures are required such as an Algorithmic Risk, Ethics and specialty committees to manage the audit/compliance responsibilities, as a second line of defence. All of these top-down criteria apply to every AI and every autonomous system in the organisation. The system-specific audit criteria are designed to ensure legal and best practice compliance tailored to the specific impact of each system on humans. This comprehensive approach ensures consistency across the organisation combined with complete risk management coverage of each unique system.



Participants in the System

The roles largely remain the same in Independent Audit of AI Systems as described in [Taxonomy](#). There are six distinct roles in most jurisdictions. Each player performs their function and the rules are executed in the same conflict-free manner, ensuring the highest integrity.

Certifying Bodies/Notified Bodies/Auditors (Auditors)

- An Auditor engages in 3-party contract party contracts, with the Target of Evaluation (ToE) and on behalf of the public or intended users.
- The auditor deploys certified practitioners to conduct the audits.
- The auditor itself is certified by the Government Accreditation Service.
- When audits are conducted there is no feedback loop to the company and the audit is compliant or non-compliant.
- Audits are publicly disclosed according to the rules of the jurisdiction.
- The Auditor is liable for false assertions of compliance
- An Auditor is licensed for use of certification criteria
- The Auditor shall not provide Pre-audit services to Audit clients
- An Auditor may provide Pre-Audit services to non-Audit ToEs (may require accreditation)

Pre-Audit Service Providers/Consultants/Advisors (PASP)

- PASP engages in a 2-party contract directly with the Target of Evaluation
- There is a direct feedback loop between the ToE and PASP
- The PASP may or may not deploy certified practitioners per local jurisdiction rules
- The PASP may or may not be accredited by the Government Accreditation Service
- The PASP offers no certification or guarantee of audit compliance
- The PASP works are private, on behalf of the ToE
- The PASP is not liable for failed compliance or false assertions of compliance
- The PASP may or may not be licensed for use of certification criteria, but must be licensed if the service offered is related to or designed to satisfy certification requirements
- The PASP shall not be the auditor for a PASP client
- A PASP may offer Audit service to non-PASP clients (must be accredited)
- A PASP may deploy compliance-in-a-box solutions for criteria compliance

Entities seeking Certification/Providers/Deployers (Auditee)

- Auditee may engage PASP
- Auditee shall have an Auditor if required by the Relevant Legal Framework
- Auditee pledges that all components, systems and relevant, supporting infrastructure to be certified will be disclosed to the Auditor, failure in this regard is the responsibility of the ToE
- Auditee dealings with PASP shall be confidential and non-public audit compliance may be confidential with an Auditor
- Auditee shall maintain compliance structures, such as Algorithmic Risk Committee, Children's Data Oversight Committee, and Ethics Committee



- Auditee shall build and maintain internal controls and systems to aid in compliance with audit requirements and foster robust risk management, monitoring, and regulatory compliance
- Auditee shall be responsible for all public disclosures

Third-Party Criteria creation, maintenance, and individual certifier (ForHumanity)

- Non-profit organisation
- Independent of Auditors and PASP
- Transparent and inclusive of input and critique from all participants
- Criteria designed to uphold human well-being
- Conflict-free of undue Auditee influence
- Submits to the authority of the jurisdiction for certified criteria
- Iterates and maintains criteria consistent with the law and best practices in a binary and auditable fashion
- Trains and certifies individual practitioners on all criteria in support of uniformity of audit assurance process
- Maintains a transparent repository of use cases and knowledge stores in support of Auditors/Auditees to facilitate compliance
- Licences criteria to all qualified Certifying Bodies/Notified Bodies/Auditors/PASP
- Provides standard contract clauses for Auditors and PASP
- Engages in distributed education system to maximise availability and certified individuals
- Maintains a system of Continuing Education (CE)
- Maintains a searchable, registration system of Accredited Individuals and holds them to a Code of Ethics and Professional Conduct
- Ensures Independence and anti-collusion amongst of Certifying Bodies/Notified Bodies/Auditors/PASP
- Maximises global harmony amongst audit criteria while ensuring jurisdictional sensitivity

Government-approved Accreditation Service

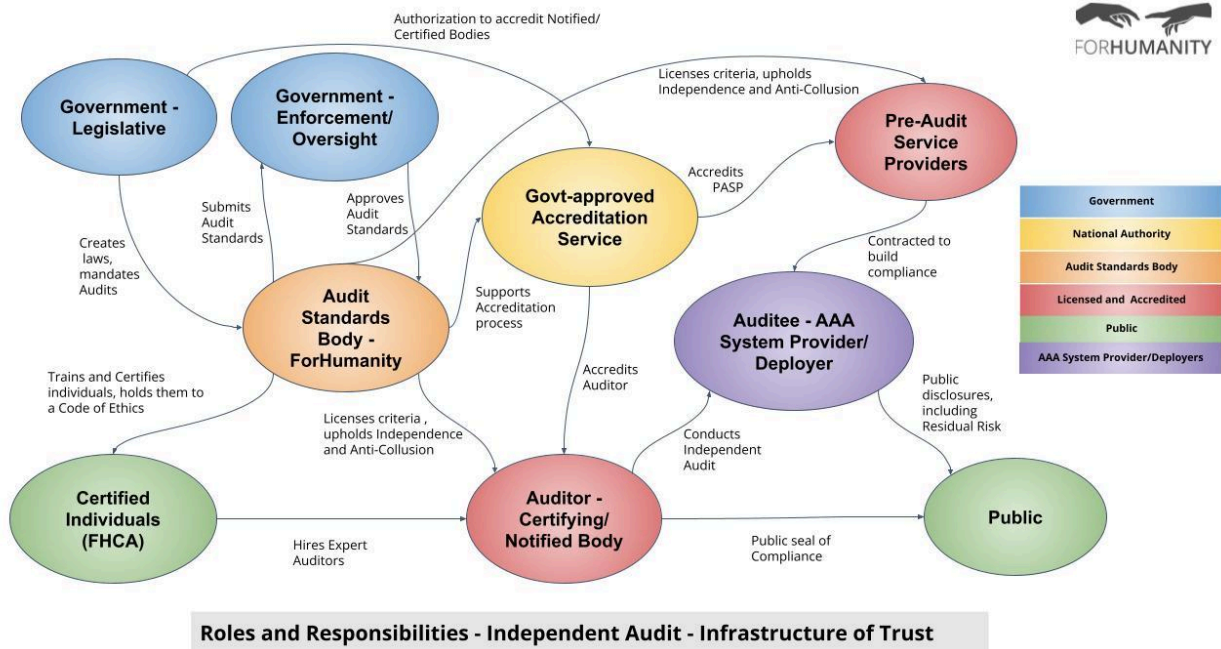
- Creates trust and confidence in products and services
- Assures that Certified/Notified/Accredited Bodies have sufficient talent, skill, scope, and financial foundation to provide certification
- Regular review of accreditation standards
- Regular review of Certified/Notified/Accredited Bodies
- Regular review of Third-party Criteria provider and individual certification
- Determines form and elements of Post Audit Compliance Report
- Maintains an accessible list of Certified/Notified/Accredited Bodies
- Maintains an accessible list of sanctioned or suspended Certified/Notified/Accredited Bodies

Governments/Regulators or similar Law-making/enforcement body

- Democratically, elected body
- Legislative responsibilities
- Executive or enforcement responsibilities
- Establishes prohibited AAA Systems



- Establishes low risk and exclusionary criteria from mandatory Independent Audit
- Regularly meets to review laws and best-practices
- Establishes a panel of experts to reviews and accredits (or rejects) submitted criteria
- Engages in enforcement actions for non-compliance with the law
- Handles concerns and issues brought by the Public



Licensing

ForHumanity provides four types of licences:

- Auditor/Certification Body and Pre-Audit Service Provider
- Platform, technology, or SaaS tools
- Teaching (for commercial purposes)
- University (for academic and research purposes) as well as commercial use of certification course

Any entity that uses the certification scheme as the basis of their business relationship (generating revenue or a similar quid pro quo - commercial purposes) with a client must be duly licensed. Any organisation may be licensed by ForHumanity, but they must also have FHCAs on staff in good standing to issue certificates or provide services using the intellectual property.

Audit fees are owed upon receipt of revenue by a licensee. The licence fees allow ForHumanity to maintain the certification schemes and training individuals as experts or ForHumanity



Certification Scheme for:
EU AI Act - Deployer v1.5

Certified Auditors (FHCA). Trademarks, certification marks, audit criteria, and services marks of ForHumanity are provided in licensing agreements and must be used in adherence with the terms of service found in the licence agreement. All licence agreements contain identical terms and conditions as relatable across use cases and are non-negotiable to ensure uniformity.