FORHUMANITY

ForHumanity's Audit Manual 1.5 For Independent Audit of AI Systems

ForHumanity's Audit Manual for

Independent Audit of AI Systems

This Document is designed to enable Certification Bodies (CB) to perform audits and issue certification when criteria are satisfied based upon ForHumanity's Independent Audit of AI Systems. It covers explanations of requirements that will satisfy compliance, as well as tools and resources to determine sufficiency and maturity of compliance. All normative criteria can be found in ForHumanity's Certification Scheme Criteria Catalogues.

Audit Manual for

Independent Audit of AI Systems v1.5

Introduction

ForHumanity (https://forhumanity.center/) is a 501(c)(3) non profit organisation and ForHumanity Europe is a French 1901 Association, dedicated to addressing risk associated with Ethics, Bias, Privacy, Trust, and Cybersecurity in artificial intelligence, algorithmic and autonomous systems.

ForHumanity uses an open and transparent process that draws from a pool of over 1500+ international contributors to construct audit criteria, certification schemes, and educational programs for legal and compliance professionals, educators, auditors, developers, and legislators to mitigate bias, enhance ethics, protect privacy, build trust, improve cybersecurity, and drive accountability and transparency in AI, algorithmic and autonomous (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 AI and autonomous 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*

Data subjects and the use of their Personal Data in AI, Algorithmic, and Autonomous systems (AAA Systems) fit squarely into the centre of that mission. AAA Systems using Personal Data have been placed on the market with insufficient governance, oversight, and accountability including failures of technical, ethical, and organisational controls. ForHumanity has developed a systematic risk mitigation process to ensure that these failures are mitigated and risk to humans are minimised – this system is called Independent Audit of AI Systems (IAAIS). ForHumanity believes that a binary (compliant/non-compliant) set of criteria, approved by the duly authorised government agencies (e.gInformation Commissioner's Office) and verified for compliance independently by certifying bodies, can create an infrastructure of trust for the public.

Founded in 2016, ForHumanity first wrote about Independent Audit of AI Systems in 2017 and it has been our primary focus since that time (Appendix A contains a list of linked reports that all support the ecosystem). We advocate for mandatory independent audits and the establishment of an 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, for more than three years, ForHumanity has drafted audit criteria for AAA Systems in the context of new legislation such as, the General Data Protection Regulation (GDPR), Children's Code and the EU Artificial Intelligence Act. ForHumanity believes that a binary (compliant/non-compliant) set of criteria, approved by the duly elected democratic legislatures or subsequent oversight bodies, and verified for compliance independently by private certifying bodies, can recreate the success of financial audit's infrastructure of trust for AAA Systems that ensures compliance with this body of audit requirements and fosters trust for individuals.

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.

For Humanity's system is grounded on four core tenets:

1. ForHumanity produces accessible, binary (compliant / not compliant) certification criteria that transparently and inclusively aligns to public requirements, (e.g. GDPR, EU AI Act, Children's Code, NYC AEDT Bias Audit) 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 maximising risk mitigations to humans (ideally criteria is approved and mandated by governments or regulatory bodies)

2. Individuals are trained and certified as experts on the knowledge of audit process and criteria. They are individually held to a high standard of behaviour and professionalism as described in the ForHumanity Code of Ethics and Professional Conduct - they are ForHumanity Certified Auditors (FHCAs). Certifications are issued by ForHumanity University following rigorous study and examinations.

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 assure 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 and ForHumanity through the licensing program.

4. Corporations use the criteria to operationalise governance, oversight and accountability for their AAA System that helps them to satisfy certification compliance comprehensively. Comprehensive compliance 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

Any company (public or private) or government organisation wishing to ensure compliance with certification schemes in a specific instance of a AAA System would be able to seek independent, third party assurance.

Laws are reactive and designed to encourage compliance, but they do not assure it. Independent audits performed by third parties which apply criteria required by statute, regulation, or industry custom, such as the Generally Accepted Accounting Principles (GAAP) or International Financial Reporting Standards (IFRS), create a system that encourages proactive compliance. ForHumanity believes this system represents a more trustworthy environment for the processing of personal data and use of AAA Systems and emerging technologies.

1.0 Scope

ForHumanity designs certification schemes for Providers, Deployers, Processors, and Controllers (Auditees) of any size. Certifications are offered for AAA Systems in the context of AAA System, data protection, equality, accessibility, digital services, and children's laws. ForHumanity also provides certification schemes for specific aspects of compliance, such as Top Management and Oversight Bodies, Ethics Committees, Algorithmic Risk Committees, Risk management, and Cybersecurity.

The Target of Evaluation, as identified in section 1.3, must include a AAA System or component and may include other supporting systems and infrastructure to ensure compliance with the scope of the certification scheme. Each certification scheme specifies its own scope.

1.1 Concurrent Certification Scheme Requirements

Frequently, ForHumanity requires organisations to hold multiple certification scheme assurances concurrently. This requirement is to ensure that all applicable laws related to an AAA System are compliant. For example, the EU AI Act requires conformity assessments for high-risk AAA Systems. However, the EU also has the General Data Protection Regulation (GDPR) and it is nonsensical to consider compliance with one law and not the other, especially when that AAA System uses Personal Data. Therefore, ForHumanity requires concurrent compliance with both certification schemes during the 12-month period. Each certification scheme specifies all required concurrent certifications.

Upstream/downstream supply chains also require concurrent certifications such as this requirement from the UK GDPR certification scheme:

Controllers seeking this certification using a Processor to provide any AAA System component for the target of evaluation are required to document that the AAA System component, from the Processor, is certified separately and independently under any of the following schemes:

1) *If the Processor previously acted as a Controller when developing the AAA System component, as evidenced by the use of Personal Data of UK Data Subjects, then the Processor's certification must be under the ForHumanity's UK GDPR - Controller Certification Scheme for AI, Algorithmic and Autonomous System (this scheme)*

2) *If the Processor developed their AAA System component without the use of Personal Data of UK Data Subjects, then the Processor's certification must be under the ForHumanity's UK GDPR - Processor (standalone) Certification Scheme for AI, Algorithmic and Autonomous Systems*

3) *If the Processor developed their AAA System component with, on behalf of, or under contract with the Controller, then the Processor's certification must be under the ForHumanity's UK GDPR - Processor (integrated) Certification Scheme for AI, Algorithmic and Autonomous Systems*

This requirement is critical to ensure holistic compliance with the certification scheme and, by proxy, for the law, regulation, or best practice upon which the certification scheme is anchored.

1.2 Out of Scope

Systems or Data Processes that do not contain an AAA System or component. Each certification scheme will also have further stipulation for out of scope systems, data processing, or AAA Systems. These stipulations are often stated in the law or regulation upon which the certification scheme is based. An example of out of scope exemptions are listed below from the UK's Data Protection Act of 2018.

Domestic purposes (e.g., Personal Data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity) and processing of Personal Data by competent authorities for law enforcement purpose that is subject to Part 3 of the DPA 2018, Intelligence Services processing (i.e., personal data processed by the intelligence services (MI5) and their processors subject to Part 4 of the DPA 2018) are out of scope.

1.3 Target of Evaluation Determination Process

The Target of Evaluation (ToE) shall be defined by the organisation in a contract with the certifying body. The organisation will provide all information required by the certifying body for a Certification Plan. Each certification scheme may vary the specific requirements required to establish the ToE. Furthermore, the contract between Certifying Body/Auditor and Auditee must establish a clear ToE. Below is an example of ToE determination process - please note that this process is defined specifically for each certification scheme:

A. Name/identifier of the ToE, specifically noting the all inputs and outputs of **Personal Data** associated with an **AAA System** across controller, joint controller, **Processor**, and sub-**Processor** relationships including databases, processing, flow and movements, pipeline, data collection, UX interfaces, and location/**Jurisdiction (Data Flow Diagram)**
B. Beginnings and Ends of the Data Processing(s) where Personal Data is processed (including a visual representation - Data Flow Diagram)

C. Systems or organisations expected to be "in" or "out" of scope (including a visual representation as appropriate). "In" and "out" of scope applies to Joint Controllers and data Processors under contract (Processors are required to have their own separate certification if they are providing the AAA System component).
D. The AI, Algorithmic or Autonomous component of the data processing will be specifically identified including its scope, nature, context, purpose, and position in the data processing (as represented in the Data Flow Diagram). For "out" of scope adjacent or interdependent processing or systems shown in the Data Flow Diagram, the organisation shall document and justify "out" of scope boundaries for those adjacent or interdependent processing or systems
E. Description of the legal basis for processing, as well as the scope, nature, context, and purpose
F. 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)
G. Specify if the data processing falls into a category that is covered by Appendix A, High Risk Data Processing as referred to in EDPB guidelines WP248rev01.
H. Specify where the processing of personal data happens in terms of physical location, including whether or not there are transfers to third countries or international organisations.

The target of evaluation shall be defined in such a way that it is not misleading or likely to be misinterpreted by data subjects or other third parties.

The ToE may include additional elements that are NOT AAA Systems themselves but are necessary to ensure that the data processing, AAA System or component functions correctly and compliantly.

1.4 Territorial Scope

ForHumanity establishes the territorial scope of all certification schemes based upon the Jurisdiction of the certification scheme and the applicable law or regulation. This scope may include elements of extraterritoriality when the underlying law or regulations permits such enforcement.

1.5 Jurisdictional Sensitivity

ForHumanity chooses to uphold the laws and shared moral framework of the Jurisdiction under which our certification scheme is produced above all other factors. Under Independent Audit of AI Systems, nation-states or regional unions retain their authority. Audit criteria are jurisdictionally sensitive, drawing upon local law and regulations to

specify such details as, for example, Protected Categories. By focusing on local regulations, the audit avoids "legislating" compliance but instead leaves these governance questions in the hands of elected officials.

> *Under IAAIS, proactive compliance can be achieved through the certification process - an evidentiary based proof-statement, independently verified by an objective, third-party auditor working for the public good.*

An example of this jurisdictional sensitivity can be found in Protected Category variables. Bias, in itself, is a statistical term describing a characteristic of a data set. However, when society then dictates that certain activities shall not be biased in their execution, it becomes something we need to account for in our systems. In the case of Protected Category Variables, each jurisdiction may be different. In Scotland, for example, socioeconomic status is a Protected Characteristic, but that is not true of law in the United States. Another example distinguishes ForHumanity's shared moral framework which is subservient to the shared moral framework of jurisdictions where our certification schemes may be used, for example, ForHumanity upholds gender equality, but will draft audit criteria that do not include gender equality when the nation-state or regional union does not hold that principle in its own shared moral framework. ForHumanity certification schemes permit each jurisdiction the ability to establish its own shared moral framework provided those principles do not conflict with core tenents of Independent Audit of AI Systems, such as governance, oversight, accountability, and transparency.

Each jurisdiction's laws will be considered in the adaptation of the audit rules.

1.6 Relevant Legal Frameworks

ForHumanity uses the term "Relevant Legal Frameworks" to require that organisations seeking certification are attentive to applicable laws in the jurisdiction. These Relevant Legal Frameworks may include any of the following examples or more (e.g., equality, nondiscrimination, fair trade and commercial, protection for children, data retention, reporting, governance, consumer protection, and human rights laws). It is the duty of the organisation, especially top management and oversight bodies to ensure that all applicable laws are considered when establishing regulatory compliance structures, especially for audit certification. The use of Relevant Legal Framework terminology allows ForHumanity to create binary audit criteria that are adaptable to multiple jurisdictions, especially regional governments. Furthermore, it avoids making the audit criteria too brittle and

susceptible to a multitude of changes in the law with a frequency that is too difficult to monitor at the global level.

2.0 Roles and Responsibilities under ForHumanity's Infrastructure of Trust

2.1 ForHumanity

ForHumanity is the certification scheme provider. Our duty is to establish the certification scheme and ensure that the scheme is acceptable to regulatory authorities, in the case of the UK that includes the Information Commissioner's Office for UK GDPR. Once the scheme is approved, by the ICO (in their sole discretion), then ForHumanity plays three additional roles:

1. We licence the certification scheme to all entities that would seek to commercialise the certification scheme for teaching, training, pre-audit services, audit services, or to build technological solutions to facilitate any/all of the aforementioned tasks. The criteria to be eligible to receive a licence are covered in Section 8.5.
2. We educate, train, and certify individuals to be qualified to issue certification from a duly accredited certification body. These persons are known as ForHumanity Certified Auditors (FHCAs). For more information about FHCAs please see Section 2.4
3. We assist National Accreditation Bodies to know which entities have been duly licenced, for which schemes they are duly licenced and which individuals are certified FHCAs qualified to issue certificates upon completion of the audit.

2.2 ForHumanity University

ForHumanity University is the trade name used by ForHumanity to educate, train, and certify individuals as ForHumanity Certified Auditors (FHCAs) or experts in certain specialities (e.g., Risk Management and Algorithm Ethics). It is an online platform where individuals from around the world can register to take courses. Each course is offered initially live online, where recordings occur for posterity. Recordings are uploaded to Youtube (or an equivalent platform). Each recording is accompanied by a quiz (typically 10 questions) designed to ensure knowledge transfer. Students can access video lectures, quizzes and associated slides and content in each individual classroom. Certification requires the payment of fees.

Foundations of Independent Audit of AI Systems is a required course for all certifications. Once completed, students may elect any course. Those that complete all quizzes with a 70% passing grade are eligible to sit in a ForHumanity Exam Window, offered most Fridays at varying times. The exam window offers all ForHumanity University course final exams in a password-protected, proctored, closed-book exam. Students that pass their exams earn their expert certificates or become FHCAs.

2.3 Certification Body (CB) Responsibilities

CB's play a special role as a proxy for the public. In their sole discretion, CBs have the responsibility to determine compliance with the approved scheme criteria. CBs will use their experience, training as ForHumanity Certified Auditors (FHCA), ForHumanity's Body of Knowledge and the specific certification scheme criteria to determine compliance with each normative statement and when compliant issue certifications. CB's must be duly licensed by ForHumanity to use all ForHumanity certification schemes for commercial purposes.

CB's are required to be accredited, as applicable, according to each jurisdiction and their requirements under their National Accreditation Service. A CB will ensure that it is duly licensed with ForHumanity and that on staff there are FHCAs, in good standing, who can issue certifications if earned by the auditee.

2.4 Auditee Responsibilities

Auditees choose to initiate certification and thus are expected to provide willful compliance with the audit criteria. These responsibilities include providing transparency and documentary evidence to satisfy each of the criteria found in the Certification Scheme Catalogue. The Auditee is required to identify duly authorised individuals qualified to represent the organisation to satisfy accountability, governance and oversight requirements. Documentary evidence may include internal procedure manuals, databases, logs, registers, employee handbooks in addition to certain public disclosures. The auditee shall determine the data process (ToE), including the "beginnings"and "ends".

The Auditee signs the Audit Engagement Letter and agrees to timely satisfaction of audit criteria and then to use certification marks according to the predetermined use standards as well as the associated disclaimer.

2.5 ForHumanity Certified Auditors (FHCA)

ForHumanity Certified Auditors are individuals who have completed certificates at ForHumanity University on Foundations of Independent Audit of AI Systems as well as one or more FHCA course (GDPR, Children's Code, Disability Inclusion and Accessibility, NYC AEDT Bias Audit, or EU AI Act).

FHCAs also agree to remain current on the law, regulatory guidance, best practices and industry standards associated with audit compliance with the certifications they have earned. This includes continuing education requirements on both ForHumanity audit criteria and changes in the relevant legal frameworks.

FHCAs also agree to abide by ForHumanity's Code of Ethics and Professional Conduct. They are regularly trained on the Code and ForHumanity ensures that FHCAs remain in good standing. As the field progresses, we can imagine further requirements include post-secondary degrees and apprenticeship time with existing FHCAs.

3.0 Certification Roles and Responsibilities

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)[1]

- 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)

[1] Bullet points and image - excerpted from ForHumanity's Infrastructure of Trust for AI - Guide to Entity Roles and Responsibilities v2.0

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

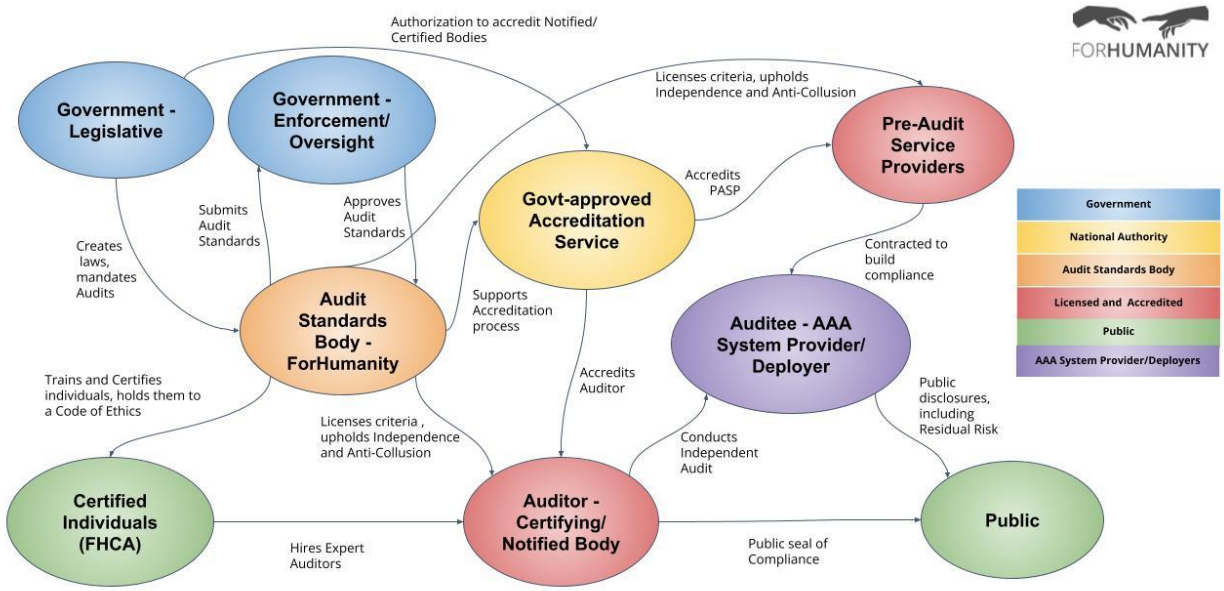
- Trains and certifies individual practitioners on all criteria in support of uniformity of audit assurance process
- Maintains a transparent repository of use cases and knowledge stores in support of Auditors/Auditees to facilitate compliance
- Licences criteria to all qualified Certifying Bodies/Notified 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



Roles and Responsibilities - Independent Audit - Infrastructure of Trust

4.0 Rules Governing the Certification Process

4.1 Governance, oversight, and accountability of organisations seeking certification, including small and medium enterprises

Specific segregation of duties, expertise and accountability are a hallmark of the ForHumanity's Independent Audit of AI Systems. The certification schemes require an Algorithm Risk Committee and an Ethics Committee and occasionally, as the risk warrants it, specialty committees. These committees exist to mitigate specific risks for the organisation:

1. Single point of failure risk/continuity/overlapping functions
2. Peer oversight, accountability and governance
3. Insufficient expertise, training and current knowledge
4. Increased inclusivity

Further, committees protect individuals in two specific ways:

1. Team responsibility, backups, transition management
2. Diversity of thought and opinion

With regards to committee requirements, it would be impractical for all entities, at all stages of maturity to implement this best-practice from the outset. Therefore, the ForHumanity Certification schemes provide for entities to have a committee or equivalent. Entities seeking certification should ensure they can evidence sufficient safeguards (expertise, knowledge and training), in the form of competency, procedures and guidelines. Entities should document residual risk that arises from equivalencies to committees. Procedures should still be clear, documented, consistently implemented and enforced. These alternative arrangements will be reviewed by the CB.

All criteria designated as the responsibility of a committee may be satisfied by a duly designated officer of the organisation. For example, a criteria assigned to the Algorithm Risk Committee may be satisfied by the Chief AI Officer or a Chief Risk Officer, so long as they directly report to the highest management level of the organisation, as recommended for the position of Data Protection Officer[2] as referenced in the GDPR .

The CB may treat this as adequate compliance when the organisation has duly assigned the responsibilities held by committees to a specific individual. This is accomplished with a **Duty Designation Letter** for each committee to be replaced by an individual. A **Duty Designation Letter**, prepared by the CB and executed by the Board, CEO and designated officer, explicitly enumerates the certification scheme's specific criteria formerly belonging to a committee as stated in that scheme, will now be the responsibility of the designated officer. A **Duty Designation Letter** may be used to assign the responsibility to any of the following committees: Ethics Committee, Algorithm Risk Committee, and/or specialty committees. Upon execution of a **Duty Designation Letter**, the **Certification Report** should note that, from a risk-based approach, this change increases the risks related to the data process and would be considered less mature. When individuals replace the responsibilities of a committee, all disclosures must document this risk.

The merit of the committee structure is widely understood, providing a set of diverse inputs to the governance. When members are well chosen the diversification of thought and imagination can reduce the risk of volatility of compliance and decision making. Outlier thoughts, myopia, and personal biases are mitigated in a committee structure naturally reducing decision making risk. Committees supply continuity during transitions as individuals come and go, the knowledge of the team remains inside the committee. Maintaining current knowledge on regulations, law and best-practises can be an overwhelming task. The committee structure allows for specialisation and allocation of responsibility amongst the team members. Additionally, fraud, malfeasance, mismanagement, confirmation bias and sunk cost bias are mitigated with a committee structure. Committees are not a panacea, instead they are a risk mitigation tool demonstrating a maturity of process.

[2] EDPB Guidelines on Data Protection Officers ('DPOs') WP243 Rev.01 https://ec.europa.eu/newsroom/article29/items/612048

The committee structure allows for greater support for its individual members since working in isolation creates enormous pressures when a person does not have peers and colleagues with whom to discuss, consider and thoughtfully review ideas, decisions and documentary evidence for compliance.

Committee structures do not provide guarantees either. They are insufficiently large to consider all perspectives and to achieve true diversity. Committees can be dominated by an individual and populated by personalities who create an echo chamber of support when critique may be necessary. However, the point of the committee structure and ForHumanity's requirement for the committee is to maximise governance, accountability, and oversight.

4.2 Documentary evidence of specific words

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, 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.

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 and "why" the risk was tolerable and non-compliance with the criterion accepted. Strictly from a risk perspective, the choice to not comply with a SHOULD statement likely 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. This subsequent risk assessment must 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. Both choices likely have risks associated with them, therefore regardless of the choice, the organisation will need to manage risks stemming from that choice.

All ForHumanity certification schemes require the certified body to document assessments and decision-making processes. Independent Audit of AI Systems asserts that robust governance, oversight and accountability comes from ethical, fair, unbiased, transparent, risk-based, and implementable processes and controls. Documentary evidence of process execution is required to satisfy audit compliance and examples are covered below of satisfactory evidence:

Organisations are required to seek out knowledge and ensure understanding of the issue at hand, including consideration for **Relevant Legal Frameworks**. Independent Audit of AI Systems does not require perfect knowledge and understanding, but it also does not allow the organisation to neglect necessary work to gather information and educate decision-makers.

The following bullet points demonstrate audit satisfaction of the information gathering process. It must be able to:

1. identify and provide documentary evidence, at a minimum, pros and cons and if the issue is two-sided or multi-faceted;
2. Make decision-makers aware of the tensions and 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] for each side of the issue with documentary evidence;
3. Present those tensions and Trade-offs in an unbiased manner; and,
4. Provide documentary evidence of the tensions and Trade-offs in correspondence or internal procedure manuals for audit compliance.

Organisations are required to document "how" decisions are reached. Decision-makers are expected to debate and reach a conclusion on how the issue will be resolved. Independent Audit of AI Systems does not prescribe the process, but it requires satisfaction of the process. When an issue is considered, previously established compliance resources ought to guide the discussion, such as Code of Ethics, Code of Data Ethics, diversity policies, Security Policies, Risk Analysis. These frameworks should help to guide the debate and ensure thorough knowledgeable evaluation.

The following bullet points demonstrate audit satisfaction of decision-making processes:

1. Meeting minutes outlining the debate;
2. Supporting documentary evidence weighing the tensions and Trade-offs;
3. Correspondence or internal procedure manuals designed to document the conclusion reached; and,
4. Level of accepted Residual Risk associated with the conclusion reached.

Organisation that make decisions must ensure implementation with methods such as Traceability. Independent Audit of AI Systems does not prescribe what actions to take, beyond those required for compliance with audit criteria. However, the audit requires documentary evidence of the action and or associated execution plan. For example, when risks and risk mitigations are identified, it is never sufficient to stop at the identification step. Risk Mitigations discussed and left idle are rendered meaningless without deployment.

The following bullet points demonstrate audit satisfaction of Traceability or other documentation of implementation:

1. Correspondence or internal procedure manuals describing the action to be taken;
2. Correspondence or internal procedure manual response upon effective completion with traceability; and,
3. Correspondence or internal procedure manuals designed to document ongoing monitoring or post-deployment considerations.

Many of the required audit criteria are also required to be made public. Public(ly): 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).

The following bullet points demonstrate audit satisfaction of "Publicly Document":

1. A display and release that meets the requirements of *Publicly*
2. Maintenance of that display with updates on an "as needed" basis

"Accountability is further enhanced when the process requires and fosters greater transparency. Now, not only is someone watching, and checking, but the whole world is able to see the work, to review and critique crucial elements of disclosure and compliance. Transparency and disclosure create a feedback loop. Once information is Publicly Documented, critics can provide constructive critique into the process and facilitate future

improvements. Accountability combined with transparency creates a virtuous circle of improvement and development." [3]

5.0 Audit Documentation

5.1 Documentation of Assessments and Certification

Audits may only be conducted by ForHumanity Certified Auditors (FHCA) under contract with a CB as accredited by local accreditation authorities. The following documents shall be produced by the certifying body in order to ensure that the certification is rigorous, transparent, and itself auditable.

- Certification Plan, including:
    - Opening meeting where the scope is verified and the names of organisations and individuals participating, and their roles;
    - Confirmation of the authorisation of the Certification Body to award the certification, and their impartiality;
    - The ToE (as documented in the contract);
    - The Relevant Legal Framework applicable to the AAA System and associated ecosystem including the role of the Auditee(e.g., Controller/Processor, Provider/Deployer);
    - Expected documentary evidence
    - Physical testing scheduling
    - any expected deviations from the evaluation methods detailed in the certification criteria; and,
    - Any site or network access required, and any special requirements for that access (e.g. permission to conduct intrusive network scanning); and,
    - Closing meeting for presentation of Certification Report, issuance of Certification or issuance of Non-Compliance Letter
- Certification Report that has two versions, a public version based upon Relevant Legal Framework requirements and a Private version for the auditee, including:
    - Clear explanation of the scope, including Beginnings and Ends, agreed in the Audit Engagement Letter and also expressed in the disclaimer
    - any deviations from the plan;
    - Process narratives, walkthroughs, flowcharts, diagrams, control descriptions, codes, policies (Management Representations)

[3] Rise of the Ethics Committee, by Ryan Carrier Apr 2021 https://static1.squarespace.com/static/5ff3865d3fe4fe33db92ffdc/t/60767acef0d59e782d2af79b/1618377424910/The+Rise+of+the+Ethics+Committee.pdf

- The specific software and hardware versions and assets inspected including third-party assets, as applicable;
- the actual dates of inspections;
- A list of documentation and assets that will be retained as audit evidence, and explanation of deviations;
- A duly authorised signatory;
- A list of deficiencies if certification will not be issued;
- If included in the Audit Engagement Letter, a determination of sufficient/mature levels of compliance;
- A process for resolving disputes
- a list of issues for consideration;
- whether a certification is awarded, and its duration; and,
- Sufficient deliverable for disclosure requirements; and,
- Sufficient, robust and resilient ongoing monitoring systems and explicit statement that systemic failures of ongoing monitoring systems will preclude future certification

This Report will be provided to the Auditee. A copy will be retained by the Certification Body for a period of 7 years or as may be lawfully required by the Relevant Legal Framework. Further copies may be required by ForHumanity and National Accreditation Body per licence agreement and Accreditation requirements respectively.

5.2 Evaluation Methods

Each of the scheme criteria identifies an evaluation method type. The CB 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 can be examined and demonstrates compliance with the criteria.
2. *Correspondence*. Historical correspondence is available that demonstrates compliance with the criteria.
3. *Internal log, register or database*. Internal records and reports or systems with proof of authenticity can be examined by the CB, and demonstrate compliance.
4. *Internal procedure manual*. Internal procedural documentation can be shown to the CB that demonstrates compliance with the criteria. Note that these procedures should be of sufficient detail to show that they are up-to-date, implemented, operational and complete. High-level policies are not sufficient to demonstrate implementation.
5. *Public disclosure document*. A publicly disclosed document will demonstrate compliance. This may include comparison to other evaluation types.

6. *Physical testing*. This can refer to any of the following, at the CB's discretion:
    a. *Records of previous events that can be examined*. For example, if there is a clear audit trail demonstrating the response to prior Data Subject Access Request, the CB can review this audit trail to gain confidence that the organisation can comply with the criteria.
    b. *Witnessing current events*. For example, to ensure that an organisation can restore from backup, the organisation can demonstrate its ability to do so to the CB.
    c. *Technical testing*. For example, to demonstrate that network traffic is encrypted, the CB may inspect the traffic.

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

5.3 Appeals Process and Requests for Audit Changes/Updates

CBs and Auditees may appeal directly to the executive team of ForHumanity if there is a belief that an audit criteria needs to be amended or should be suspended.

The ForHumanity Executive Director will respond to all requests for appeal. The Executive Director may form a small expert committee of ForHumanity Fellows to discuss and review the appeal. No conflicts of interest will be permitted in consideration of the appeal. The considerations for the appeal will be based on the following criteria:

1) What is the best interest of humanity with regards to the appeal?
2) What maximises the ability of the auditee to mitigate their risks?
3) What maximises the ability of the Certification Body to minimise their risk associated with assurance?

Appeals will be noted in writing to the entity which has requested the appeal. CBs and Auditees will be notified and ForHumanity may choose to apply the appeal to all aspects of the audit until it can be amended through the formal audit update process.

Appeals will be held in effect for one year. Any extension to an appeal resides in the sole discretion of ForHumanity.

6.0 Applying Audit Criteria

6.1 Definitions

Defined terms (bolded and capitalised) are used, like in contract law, to make the interpretation easier and to reduce ambiguity. They are purposefully defined to incorporate key concepts and often aspects of law that are required for compliance. The certification scheme is built on the foundation of a common lexicon.

6.2 Protected Categories

When a jurisdiction takes legal steps to protect certain groups of people or aspects of a person's innate characteristics, from discrimination and/or bias, the audit describes these aspects or classes as Protected Categories and exist in varied forms such as Protected Categories, Protected Variables, and Proxy Variables.

The use of Protected Category variables indicates that the associated data process must go through bias remediation. Further, the use of Protected Category variables may also indicate the need for Special data process rules such as further lawful basis assurance or a higher degree of cybersecurity.

6.3 Committee experts

Independent Audit of AI Systems requires experts in the special and unique risks to humans found in AAA Systems. These experts are organised into committees for accountability, governance, and oversight purposes associated with binary audit criteria. The required expertise varies depending on the scope, nature, context, and purpose of the AAA system, theToE, and applicable Relevant Legal Framework. Examples include, but are not limited to the following:

Algorithmic Risk Committee

a. Risks to rights and freedoms of **Data Subjects**, including associated legal risks
b. Considerations and concerns regarding fairness, **Bias**, **Concept Drift**, transparency, and the need for **Diverse Inputs and Multi Stakeholder Feedback**
c. Implications to data privacy and protections, especially in the areas of **Special Category Data** and **Biometric Data**
d. Process and associated challenges of model validation
e. Unique security and cybersecurity risks
f. Specialised controls of **AAA Systems**

g. Risk management and the detailing of **Residual Risk**

Ethics Committee

a. **Algorithm Ethics**, human rights, how to identify a moral situation and adjudicate instances of **Ethical Choice**
b. Possess diversity in thought, lived experience and protected categories-ness
c. Committed to support the organisation's shared moral framework even when it might not be aligned in each aspect with their own personal moral framework
d. Understanding and considering fundamental rights according to the **Relevant Legal Frameworks** under which they operate

Specialty Committees

a. risks to rights and freedoms of **People With Disabilities,** including associated legal risks
b. uphold the **UNCRC Rights of the Child**,
c. support for the Best Interests of the **Child**
d. provide **Age-Appropriate** and **Child-Friendly** design
e. assess fairness, including guidance on the subconscious impact of design interfaces
f. assess of **Bias**, **Concept Drift**, transparency and need for **Diverse Inputs and Multi Stakeholder Feedback** assuring the health and well-being of the **Child**
g. assess data privacy and protections afforded by the Children's Code, especially in the areas of **Special Category Data, Biometric Data, geolocation,** and **profiling**
h. Provide security and cybersecurity solutions to mitigate risks associated with **Children**
i. provide specialised design and controls of **AAA Systems**
j. provide unique risk management and the detailing of **Residual Risk** in an **Age-Appropriate** and **Child-Friendly** manner

ForHumanity's certification schemes specify the required training and expertise required for these teams of expertise to govern, oversee and be accountable for the AAA Systems being certified. The organisation holds the responsibility at the Top Management and Oversight Bodies level to ensure that these experts are present, duly organised with assigned roles and responsibilities, and sufficiently trained and funded to carry out their duties.

6.4 Awareness Curriculum

ForHumanity requires a specific awareness education for all members of the design and development teams including Ethics Committees, Algorithm Risk Committees, specialty committees and members of Top Management and Oversight Bodies Committees. This

curriculum focuses on raising awareness in these team members about specific areas where awareness is lacking, risk is present, and the organisation is taking measures to mitigate these risks.

These curriculum are short form, amounting to roughly two to three hours per annum, at a minimum. Their tailored design completes two critical functions:

A. To help all impacted employees to be more aware of risks and mitigations associated with the AAA System
B. To explain and operationalise the organisation's specify process for handling the risks and mitigations described when they manifest

ForHumanity produces the learning objectives for this curriculum and providers offer learning management systems that enable compliance with this audit requirement. This learning must be traceable for compliance for all members of the team for compliance.

These curricula are individual audit requirements and are included in normative criteria as applicable. They are briefly summarised in the sub-sections below.

6.4.1 Ethical Choice

ForHumanity identified a common flaw in algorithm development - organisation's regularly have failed to incorporate experts in ethics in the creation of socio-technical systems, like artificial intelligence. These systems are often filled with instances of ethical choice, ranging from benchmarking for data representativeness to threshold levels for key performance indicators measuring learning algorithms for concept drift.

6.4.1 Automation Bias

The EU AI Act requires that human oversight be trained in how to overcome Automation Bias. ForHumanity agrees with the sentiment and requires that humans-in-the-loop, humans-on-the-loop, humans-in-command, and other affiliated humans are trained to be aware of the commonly found problem of Automation Bias. This body of work is designed to raise awareness and personal susceptibility to the problem. It further provides tools to identify and overcome Automation Bias to produce a health balance of appropriate scepticism and validate trust.

6.4.1 Nudge and Deceptive Pattern Awareness

Our online interactions require user interfaces and user experiences (UI/UX) which has resulted in critical analysis of UI/UX to design, develop, and deploy processes that produce better results, sometimes consciously and obviously while other instances are subconscious and hidden, for the organisation or the individual. As a result, some nudges and deceptive

patterns are deemed negative or detrimental. This curriculum is designed to increase the awareness of the presence of nudges and deceptive patterns, and to determine who they benefit and who they may harm. The curriculum also establishes the organisation's preferred method for reporting such instances and how they may be remediated.

6.4.1 Disability Inclusion & Accessibility

This curriculum is designed to raise awareness about inclusion and accessibility for persons with Disabilities. There are statistical processes that automatically exclude persons with disabilities from AAA Systems. They can be treated as outliers, anomalies, or excluded based on accessibility. Not only is this harmful, but in many cases it may be illegal. The curriculum raises awareness around Relevant Legal Frameworks associated with persons with disabilities, inclusion, accessibility, and usability. It raises the awareness of these issues for mission-critical persons including providing basic methods to improve inclusion, reduce issues of accessibility, and reduce the risks in AAA Systems for persons with disabilities. The course then teaches how the organisation handles issues brought forward including the provision of accommodations when applicable.

7.0 Audit Governance and Accountability

7.1 Top Management and Oversight Bodies Audit

There are audit criteria dedicated to "Top Management and Oversight Bodies" and which must be answered according to the required audit documentary evidence. This term may include the CEO and other offices, oversight bodies and a Board of Directors.

It is not expected that "Top Management and Oversight Bodies" will have day-to-day responsibilities associated with audit compliance, however, they are accountable for systemic failures of governance, oversight and accountability systems. Audit criteria are designed to ensure culpability. These are designed to ensure that "top management" has adequate knowledge and governance of key elements of the audit process. Notably, the requirement to establish an Algorithmic Risk Committee and the Ethics Committee.

7.2 Body of Knowledge - Knowledge Stores

The Body of Knowledge and its specific Knowledge Stores provide templates, notes, and guidance for Auditors, to be applied when examining items of compliance sufficiency and maturity. They do not represent normative criteria. Instead they reflect measures, tools, guidance, templates, and thresholds that help an Auditor understand if the documentary evidence is sufficient or sometimes even reaching a mature level of compliance. Further,

the knowledge stores will often highlight frequent insufficiencies related to documentary compliance evidence designed to draw attention to common mistakes with sufficiency. The Body of Knowledge - Knowledge Stores can be found HERE.

8.0 Auditor Accreditation, Licensing, Professional Ethics, and Responsibility

8.1 Accredited Certification Bodies

ForHumanity assists National Accreditation Bodies at their discretion to determine the process for the accreditation of certifying bodies. CBs must be duly licensed with ForHumanity for use of the criteria and have sufficient knowledge and expertise in performing the audits, represented by auditors accredited as ForHumanity Certified Auditors (FHCA). CB must have sufficient staff employed who are individually accredited ForHumanity Certified Auditors (FHCA). UKAS in other accreditations has provided an excellent guide for good-functioning, independent CBs, including:

1. Ensure impartiality - Any service provided by the Licensee (including its employees, officers, contractors, subcontractors, and other agents) to any particular client during a 12-month period related to the Authored Work shall relate either to that of an independent CB or a pre-audit service provider (including, but not limited to, assessment, remediation, or other services designed to aid or enable audit compliance). A Licensee shall not provide both auditing and pre-auditing services to the same client in a 12-month period but may be engaged in the business of both auditing and pre-audit compliance so long as it does not provide the same services to any one client within a 12-month period. A CB may provide no additional services of any kind to an audit client.
2. Ensure competence - demonstrate adequate expertise to perform audits for each client, including having ForHumanity Certified Auditors performing/managing the audits.
3. Ensure robust reporting and satisfaction of criteria - demonstrate the ability to complete audits and provide reasonable, timely and accurate assessments for the clients and other stakeholders, such as ForHumanity.
4. Management and avoidance of conflict of interest.
5. Ensure rightful certification/Quality control management - submit periodically to inspections of audit reports and underlying working papers, chosen by ForHumanity.

8.2 Independence

A legal term defined by The Sarbanes-Oxley Act of 2001 that requires a CB to receive no other remuneration from an Auditee beyond reasonable audit fees. In its licence agreements, ForHumanity further stipulates that a licence holder cannot be an CB and an Pre-Audit Service Provider/Assessor/Consultant (or provide any other form of service) to the same Auditee within a 12-month period. ForHumanity has adopted this rule and determination into the licensing agreements for CB and their staff who abided by the FHCA Code of Ethics and Professional Conduct.

Independence and independent audit increases compliance with established laws and regulations. Time and again, human nature has proven that self-assessment is useful but insufficient, thus requiring the need for further enforcement mechanisms. However, government and regulatory enforcement requires resources to examine societal compliance. Enforcement bodies can mandate uniform criteria that satisfies compliance (e.g. the Securities and Exchange Commission mandating adherence to Generally Accepted Accounting Principles GAAP for publicly traded companies in 1975). Then, Independent Audit when mandated by governmental enforcement agencies creates a leveraged, overarching compliance mechanism - examining and assuring compliance - accomplished by third-party trained practitioners, accredited robustly (and equally overseen - "watching the watchers"), using uniform rules, regularly assure compliance, at their own risk of false assurance of compliance. Under this ecosystem, conflicts are mitigated, objectivity is maximised, and trust is built.

More details on specific examples of Independence can be found in **ForHumanity's Certified Auditor Code of Ethics and Professional Conduct v1.0.**

8.3 Anti-Collusion

Independence is further enforced through licensing requirements enforcing anti-collusion amongst CBs and pre-auditors. As the market for data auditing matures and grows, it is impermissible for pre-audit service providers andCBs to regularly guide clients to each other excessively. This prevents pre-auditors andCBs from becoming overly comfortable with each other's processes/expectations and failing to deliver the maximum diligence and objectivity owed to the client and the public. Anti-collusion requirements ensure maximum mitigation of risk to humans and implement complete compliance.

8.4 Code of Ethics and Professional Conduct

See **ForHumanity Certified Auditor Code of Ethics and Professional Conduct v1.0** for a detailed description of the shared moral framework and professional responsibilities that FHCAs are held to in their role as an Auditor or Pre-Audit Service provider.

8.5 Licensing

ForHumanity provides four types of licences:

A. Auditor/Certification Body and Pre-Audit Service Provider
B. Platform, technology, or SaaS tools
C. Teaching (for commercial purposes)
D. 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 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.

8.6 Audit Period of Validity

Certification is valid for 12 months, however the period of validity may be subject to Relevant Legal Frameworks that may override the basic length of the certification period. Compliance should be renewed each year and an auditee is expected to maintain compliance with the current version of the certification scheme. In any areas where the audit has been changed, the auditee will have until the next annual audit to bring their systems into compliance.

Significant changes in the scope, nature, context, and purpose of an AAA system will require an updated certification for that specific system. Significant changes to an AAA

system may jeopardise the certification status of the previous system. Some examples which may require recertification to maintain status are:

1. Acquisition/Change in Control
2. Complaint
3. Regulatory intervention
4. ForHumanity's Cause for Concern

8.7 Certification Warning/Certification At-risk

The CB may issue a write warning to an auditee that they are not compliant with the terms of the Audit Engagement Letter. This written warning shall include a timestamp, remediation period, and the expected remedy. Failure to satisfy may result in the withdrawal of certification. Potential warnings could be required for any of the following concerns:

1. Misuse or misrepresentations in use of certification mark and their stated purpose;
2. Contravention to any of the contractual clauses for certification;
3. Failure to maintain documentary evidence related to the certification;
4. Failure to maintain post market, robust and ongoing monitoring on the data process;
5. Failure to uphold agreed and documented thresholds, Key Performance Indicators on the data process;
6. Concept drift and deviations from scope, nature, context or purpose of the data processing;
7. At the launch of an investigation based upon a report or complaint by the FHCA highlighting potential misrepresentation, falsification or fraud associated with information provided for audit; or
8. Reported data privacy breaches.

Warnings and at-risk certification may or may not lead to withdrawal of certification based upon this guidance and failures to remediate in a timely fashion at the discretion of the CB.

8.8 Withdrawal of Certification

Certification may be withdrawn for any of the following reasons:

1. Regulatory action related to the data process;
2. Successful civil litigation of a case directly pertaining to the data process certified;
3. Failure to maintain documentary evidence related to the certification;
4. Failure to maintain post market, robust and ongoing monitoring on the data process;

5. Failure to uphold agreed and documented thresholds, Key Performance Indicators on the data process;
6. Concept drift and deviations from scope, nature, context or purpose of the data processing;
7. Material change in organisational governance, accountability, oversights or controls related to the data process;
8. Reported data privacy breach;
9. Fraud, misrepresentation or malfeasance associated with material information related to the certification

The Auditor will notify the Auditee that certification has been withdrawn with a Letter of Withdrawn Certification and will be required to provide the auditee with the associated reason for the withdrawn certification from the list above. This may be done at their sole discretion according to the Audit Engagement Letter for any reasons listed above.

8.9 Material and Non-material changes to Certification Criteria

Any changes to the criteria are at the sole discretion of the government or regulator that approved the criteria. In cases where the criteria is not government or regulator approved, then ForHumanity will signal the date of implementation and allow for adoption of the changes at the next applicable certification date.

ForHumanity maintains a robust dialogue, inspection and interaction with the marketplace to ensure that the criteria are current and up to the standards of the law, regulations, and known best practices. As needed, ForHumanity will submit changes to the government or regulator for their considerations for adoption. This deliberation process is clear and transparent at the ForHumanity level. Changes are shared immediately and directly with all FHCAs and Licensees.

It is the duty of the Auditee to be aware of changes that would lead to re-certification. The CB may choose to assist the Auditee with notification and compliance guidance.

