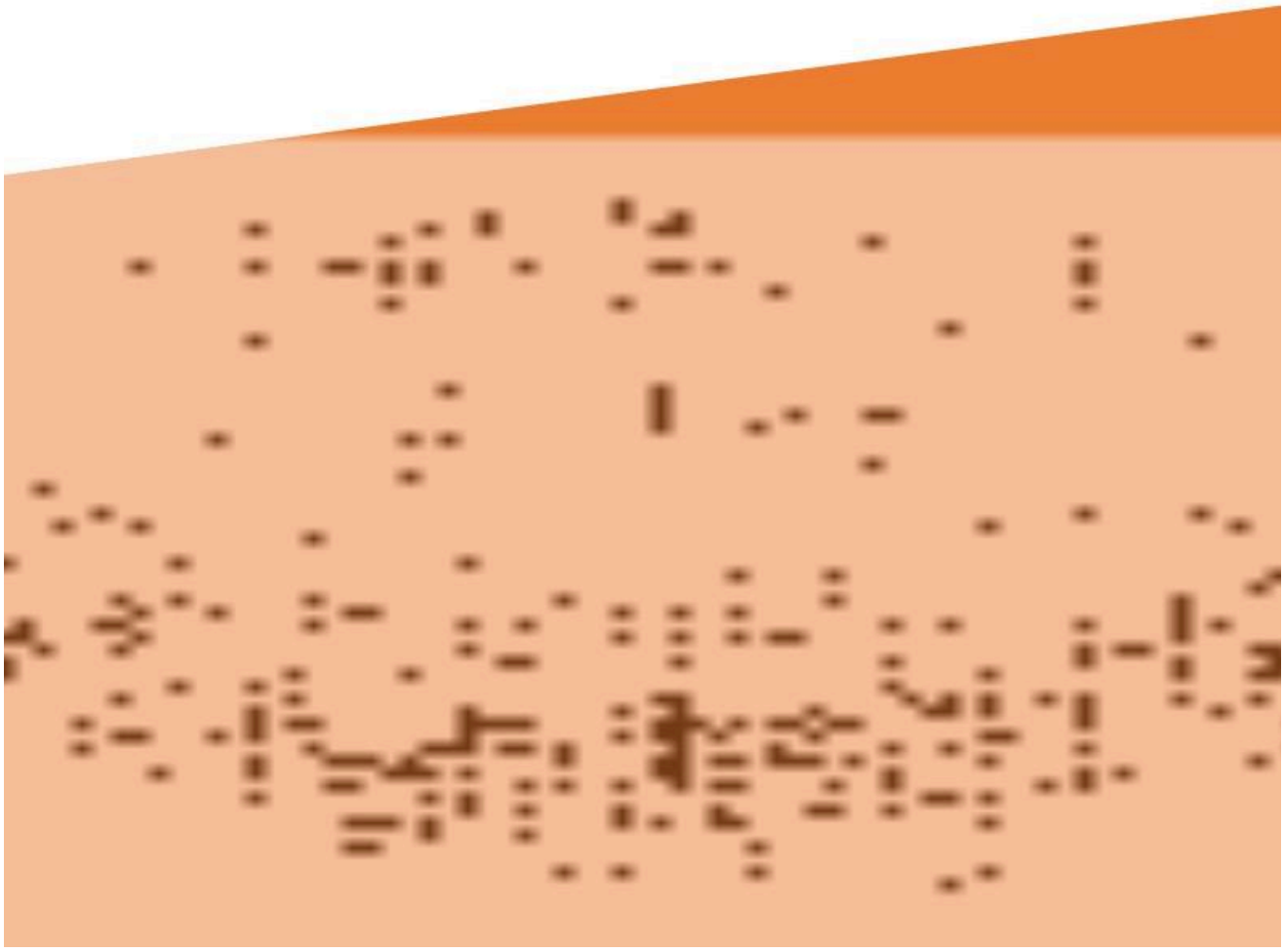
FORHUMANITY
980 Broadway #506 Thornwood, NY 10594
(+1) 9146028663
ryan@forhumanity.center
www.forhumanity.center

FORHUMANITY EUROPE
12 rue Frederic Petit
80000 Amines, France

FORHUMANITY

Model Risk Management

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



Introduction

ForHumanity (https://forhumanity.center/) is a 501(c)(3) non profit Regulated 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 2900+ 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 analyze downside risk associated with the ubiquitous advance of AI, algorithmic and autonomous systems and where possible to engage in risk mitigation to maximize the benefits of these systems… ForHumanity*

With the passage of the European Union's Artificial Intelligence Act, certain applications of artificial intelligence in finance have been deemed high risk (those regarding the evaluation of an individual's creditworthiness). Further, anyone experiencing the financial crisis of 2009 would be likely to argue that financial applications of all kinds, including those using AAA Systems, are high-risk applications whether they directly or indirectly impact AI Subjects. This form of systemic risk resulting from the economy-wide impact of financial sector stability has resulted in robust (albeit imperfect) risk management practices stemming from oversight from BASEL III and country-specific regulatory oversight such as the US Federal Reserve and European Central Bank (Model Risk Management) implemented as far back as 1987. The result is a sector-wide pervasive risk management culture that provides a strong, but insufficient foundation for governance, oversight, and accountability of the ever-expanding adoption of AAA Systems inside financial institutions. This certification scheme is designed to augment existing model risk management approaches by addressing the specific and unique risks associated with AAA Systems in the financial sector. The ForHumanity Model Risk Management certification scheme integrates existing model risk management process and procedure infrastructure with the emerging global requirements and standards for robust governance, oversight, and accountability of financial sector AAA Systems.

Background

In response to the systemic risk posed by financial institutions around the world. The BASEL Framework (currently BASEL III) represents a consensus view on strength and stability and establishes minimum standards for regulation, supervision, and risk management. These voluntary standards are weighed by organizations as they consider the scope and nature of

business conducted with each financial institution. BASEL III standards help to establish a culture of risk management.

Additionally, in 2011, the US Federal Reserve and the Office of the Controller of the Currency (OCC) jointly issued the supervisory guidance on Model Risk Management for banking organizations and supervisors (SR11-7/OCC-2011-12). Subsequently, in 2021, the Federal Reserve, Department of Treasury (OCC), Federal Deposit Insurance Corporation (FDIC), Bureau of AI Subject Financial Protection (CFPB), and National Credit Union Administration (NCUA) (hereafter referred to as "Federal Regulators") all called for comments on the use of artificial intelligence in financial institutions. The scope was clear, all banking organizations (banks) and financial institutions under supervision from these regulators were being scrutinized for the manner in which AAA Systems are being deployed. Factors being assessed include but are not limited to, size, scope, and complexity. Further OCC Guidance on Managing Outsourcing Risk, SR13-19 extended SR11-7 to third-party vendor-provided AAA Systems.

SR11-7 called for banks to be attentive to adverse consequences of decisions based on models that are incorrect or misused. Further, banks should engage in active model risk management that includes:

1. Effective model risk management frameworks
2. Robust model development implementation and use
3. Effective validation
4. Sound governance, policies and controls

The ForHumanity Model Risk Management certification scheme adapts these obligations (BASEL III, SR11-7, SR13-19,) applied to AAA Systems, to establish audit criteria that can be made available to both internal audit functions at banking organizations as well as independent third-party auditors for assurance.

As a result of lawmaking and Federal Regulator guidance, the following Relevant Legal Frameworks apply to this specific certification scheme:

1. SR11-7
2. SR13-19 (Guidance on Managing Outsourcing Risk)
3. Unfair, Deceptive, and Abusive Practices

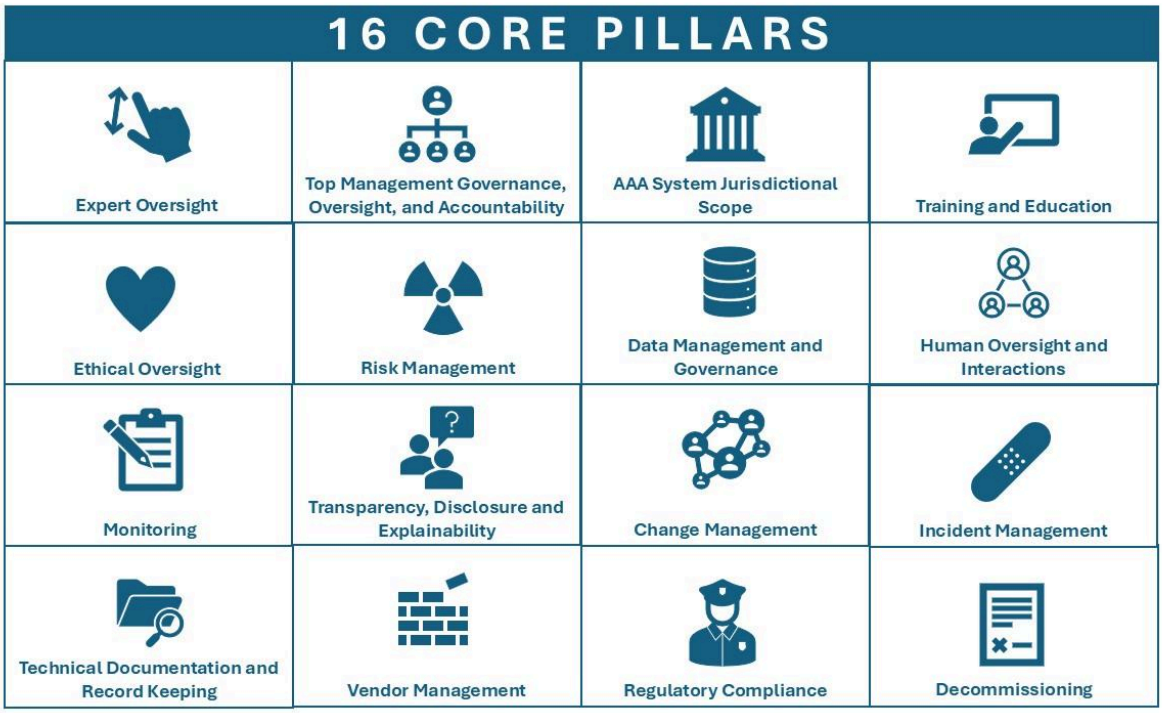
The scheme covers organizations known as "Regulated Financial Institutions". Regulated Financial Institutions include any organizations that are subject to BASEL II, the Federal Reserve or OCC.

Modularity of ForHumanity Certification Schemes

CORE AAA System Governance

The CORE AAA Governance certification scheme describes the foundational elements necessary for robust governance, oversight, and accountability of AAA Systems (regardless of economic sector of AAA System use case) required by burgeoning legal frameworks and standards as well as the crowdsourced identification of implementable best practices necessary to mitigate risk to humans from AAA Systems.

AAA Systems are (often complex) socio-technical tools. As a result, the CORE AAA System Governance certification scheme is designed to ensure that globally-recognised, minimum requirements for robust AAA System governance are established and operational. This certification scheme is the cornerstone to ForHumanity's global, modular certification program. Critical compliance-by-design infrastructure is necessary for responsible and trustworthy usage of AAA Systems by corporations and the public sector regardless of jurisdiction. These elements of governance, oversight, and accountability are applicable to all AAA System operations:



Modular Approach to Jurisdictional Compliance

To facilitate implementation of AAA System governance, oversight, and accountability. ForHumanity has established certification schemes that are modular. The Model Risk Management certification scheme relies upon the CORE AAA Governance (CORE) certification scheme. The CORE is applicable for all AAA Systems that are not low risk and it represents the non-negotiable foundational requirements necessary to engage in responsible use of AAA Systems. The elements established as a result of compliance with the CORE certification scheme are fully integrated with all ForHumanity modular certification schemes, such as GDPR, EU AI Act, Unfair, Deceptive, or Abusive Practices, Cybersecurity, or the Children's Code and most importantly, Model Risk Management.

As a result of this modular process, for any given AAA System, multiple certification schemes may be applicable to assure the auditee of compliance with all Relevant Legal Frameworks and certification schemes.

Assurance will be granted to an auditee based upon the certification scheme for which they are currently compliant, according to an assurance contract, as assured by their third-party independent auditor. An auditee, at the initial phases of building certification under the

ForHumanity process, might find itself certified only under the CORE scheme, while they are conducting their compliance audits on additional modular schemes. The auditee is entitled to disclose all Independent Audit of AI Systems certification scheme seals (and associated disclaimers) for which it is currently compliant.

Infrastructure of Trust - replicating financial audit for AAA Systems

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 ensures compliance with this body of regulations.

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, in the US, (e.g. CCPA, UDEP, Title VII) 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 organizations 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 where applicable and ForHumanity.

4. Corporations and public sector Providers and Deployers of AAA Systems can use the criteria to operationalize 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.

Any bank wishing to ensure conformity under the law or to document compliance with SR11-7 obligations that may be shared with potential Deployers of the AAA System as the most robust evidence of meeting the obligations of the law, regulations, and guidance.

Existing Model Risk Management in the context of Independent of AI Systems

Independent Audit of AI Systems uses two specific terminologies, Algorithmic Risk Committee and Top Management and Oversight Bodies. The Algorithmic Risk Committee is a team of experts trained to understand the specific and unique risk associated with AAA Systems. This team sits beside traditional model development teams to augment their process with robust risk and data management practices unique to AAA Systems. Under this certification scheme the Algorithmic Risk Committee is responsible for the production of all compliance at the model ownership level.

The term "Top Management and Oversight Bodies" encompasses all C-suite and enterprise wide teams, including Internal Audit, Model Risk Committee, and Model Validation/Governance. Top Management and Oversight Bodies have specific audit criteria for which they are accountable, such as Conceptual Soundness validation, prior to first usage in production (distinct from testing and sandboxes) of an AAA System.

1.0 Scope

ForHumanity designed this certification scheme for Regulated Financial Institutions acting as Providers or Deployers (Auditees), of any size, who are using AAA Systems to produce outcomes that are governed by BASEL II, and US Federal Regulators. The scheme may be applied to one or more specific AAA Systems (including General Purpose AI), however it may not be used for AAA Systems that are prohibited under the EU AI Act, Federal or State laws. Certification is valid for 12 months unless significant changes occur (see section 1.0.1 for the Audit Period of Validity).

Establishing "if" the AAA System is in scope for this certification scheme is the first step. The scope assessment goes through the following steps to determine applicability:

1) Assess whether the Target of Evaluation (as defined in Section 1.2) falls under the definition of AAA Systems (definitions found in section 3.0)
2) Is the organization seeking certification a Regulated Financial Institutions
3) Is the Regulated Financial Institutions acting as a Provider or Deployer of the AAA System?
4) Assess whether the AAA System is subject to any Relevant Legal Frameworks

1.0.1 ForHumanity Modular Certification Requirements

ForHumanity certification schemes are built with modularity. This enables global harmonization and implementable compliance-by-design. For this certification scheme, a Regulated Financial Institution requires the following pre-requisite certification scheme(s):

1. ForHumanity CORE AAA Governance certification scheme (Provider/Deployer)

1.0.2 Audit Period of Validity

A certification is good for one year. 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 significant change which requires 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

1.1 Out of Scope Systems

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

1.2 Target of Evaluation Determination Process

The Regulated Financial Institution 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 Bank. The certification is valid for a maximum of 12 months, dependent upon the risk classification of the Target of Evaluation, from the date certification is issued by the certifying body, but shall include risk-based, periodic validation of certain interim measurements appropriate to the scope, nature, context, and purpose of the Target of Evaluation.

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., SR11-7) 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 Regulated Financial Institution 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 Regulated Financial Institution 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 Sensitive Data that may be present (including Inferences and/or potential Proxy Variables)
5) Identify all applicable jurisdictions in which the **AAA System** processes data in order to determine additional applicable legal obligations called **Relevant Legal Frameworks**.

The certifying body will only perform an audit of the documented scope. The Regulated Financial Institution 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.

1.3 Territorial/Regulatory Scope

Applicable to all Regulated Financial Institutions governed by the Federal Reserve, and OCC, regardless of state or territory.

2.0 Normative References

No Normative references

3.0 Terms and Definitions

Defined terms are bolded and capitalised throughout this document.

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)
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**
AAA System Deployer Guide	A digital documentation that intends to enable and empower the Deployer with information about the **AAA Systems** from the **Provider** that is necessary to successfully operate the **AAA System**.
AAA Systems List	A list, either by name or other identifier that tracks all distinct AI, Algorithmic or Autonomous Systems

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
Accredited Investor (Individual)	Financial requirements -Net worth over $1 million, excluding primary residence (individually or with spouse or partner) or Income over $200,000 (individually) or $300,000 (with spouse or partner) in each of the prior two years, and reasonably expects the same for the current year Or Professional requirements that include 1. Investment professionals in good standing holding the general securities representative license (Series 7), 2. the investment adviser representative license (Series 65), or 3. the private securities offerings representative license (Series 82) 4. Directors, executive officers, or general partners (GP) of the company selling the securities (or of a GP of that company) 5. Any "family client" of a "family office" that qualifies as an accredited investor For investments in a private fund, "knowledgeable employees" of the fund
Accredited Investor (Entity)	An entity with any of the following attributes: 1. Entities owning investments in excess of $5 million 2. The following entities with assets in excess of $5 million: corporations, partnerships, LLCs, trusts, 501(c)(3) organizations, employee benefit plans, "family office" and any "family client" of that office

	3. Entities where all equity owners are accredited investors 4. Investment advisers (SEC- or state-registered or exempt reporting advisers) and SEC-registered broker-dealers 5. A bank, savings and loan association, insurance company, registered investment company, business development company, or small business investment company or rural business investment company
AI Subject	A natural person who is impacted by the outcomes of a AAA System
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
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 human rights and freedoms
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, T&E At-Risk Report, Ethical Risk Assessment, and an Committee Governance Assessment
Capital Risk	The risk that a bank may not have enough capital to cover its losses, which can lead to insolvency - SOURCE BASEL III
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
Choice Architecture	The inputs to a recommender system that may be controlled or modified by the **AI Subject**
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 Legal Frameworks, providing context to instances of Ethical Choice, diversity and anti-discrimination
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
Concentration Risk	The potential for significant losses due to excessive exposure to a single counterparty, sector, or geographic area within a financial institution's portfolio - SOURCE BASEL III
Conceptual Soundness	Includes descriptions of Scope, Nature, Context, Purpose, Construct Validity and Causal Hypothesis explanations and Ground Truth validation where appropriate and applicable

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
Content Moderation	The activities, whether automated or not, undertaken by providers of intermediary services or online platforms, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account
Context	The circumstances in which an event occurs; including jurisdiction and/or location, behavior and functional inputs to an **AAA System** that are appropriate (e.g. domain, operating environment)
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]
Credit Risk	the potential for loss due to a borrower's failure to repay a loan or meet contractual obligations - SOURCE BASEL III
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

Deployer (EU)	any natural or legal person, including a public authority, agency or other body under whose authority the system is used, except where the AI system is used in the course of a personal non-professional activity - SOURCE EU AI Act
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**)
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
Ethics Committee	A group of persons trained in Algorithm Ethics and Ethical Choice, guided by the **Code of Ethics** and Code of Data Ethics, which they create and maintain on behalf of the organization. The Ethics Committee is responsible for all instances 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**.

Exceptions Interpretability	timely interface designed for human oversight during the period in which the **AAA System** is in use for identification of: A. Anomalies, B. Dysfunctions, C. Exceptions, D. Expected foreseeable misuse, E. False positive and false negative F. **Key Risk Indicators** (KRIs) to enable and empower a **Human-in-Command to** stop, pause, disregard, override, and reverse the **AAA System**
Explainability Statement	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 human 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)
Explainability+	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
Fiduciary	A person or entity that holds a legal or ethical relationship of trust with another party, typically managing money or assets for the benefit of that party. This relationship requires the Fiduciary to act in the best interest of the beneficiary, maintaining loyalty and avoiding conflicts of interest
Ground Truth	Information ascertainable as real or true through observation or experience
Human Interactions Report	This report tracks all human interactions, their effectiveness and impact on a **AAA System**
Information Quality	Data that is fit 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
Jurisdiction	a defined geographic area over which a particular legal authority may lawfully exercise control
Key Detrimental Indicators	Parameterized 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, Non-Consensual Intimate Visual Depiction)** B. Harmful or negatively impacting to the well-being of users, including **Vulnerable Populations,** such as: a. **Adult Content** b. **Bullying** c. Defamatory/Slander/Libellous content d. Misrepresentation and identity fraud e. indications of self-harm, suicide, violence, and disorders 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) C. **Disinformation** D. restricted by guidelines and codes of practice E. Breach of copyright and other intellectual property rights where the parameters are subsequently deployed for monitoring and measuring in order to censor, filter or restrict the content in the online service
Key Regulated Product Indicators	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:

	A. **Illegal Content (e.g., Terrorism, Child Sex Abuse Material, Trafficking)** B. Fraudulent, or infringing of a copyright or intellectual property C. 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 services F. Regulated Goods biologics (e.g., bacteria, virus, fungus, livestock, plants and seeds, birds, fish and sea creatures) G. Illegal cultural appropriation H. Regulated Military or Defence industry items I. Regulated or illicit services J. Monetary items and assets K. Regulated electronics, code, or technology (e.g., software or hardware) L. Online gambling
Liquidity Risk	The risk that a financial institution will not be able to meet its short-term financial obligations due to an inability to convert assets into cash without incurring significant losses - SOURCE BASEL III
Market Risk	The risk of losses arising from movements in market prices, including factors such as interest rates, foreign exchange rates, equity prices, and commodity prices - SOURCE BASEL III
Model Risk Validation Report	Generated by the **Model Risk Management Lead** in the context of the Model Risk Management Policy it documents the validation of quality objectives, controls and assurance processes

Nature	The forces and processes that influence and control the variables and features (e.g., foreseeable conditions, input variables)
Operational Risk	The risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events - SOURCE BASEL III
Personal Data	Any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity. Personal Data may be a collective term encompassing specialized terms such as Inferences, Proxy Variables, Personally Identifiable Information, Personal Information, Sensitive Data, and Special Category Data
Pipeline Data	Inputs to an operational **AAA System** from external sources (including natural persons) via a predetermined collection mechanism
Purpose	The aim or goal of a system (e.g., limitations, variants)
Regulated Financial Organisation	Corporations that fall under the regulatory oversight of the the US Federal Reserve and/or the OCC
Relevance	The appropriateness and meaningfulness of each datum, feature and causal hypothesis to the Scope, Nature, Context, and Purpose of the AAA System
Relevant Legal Frameworks	The collection of applicable law such as the laws that govern an entity or organization, that govern the rights, freedoms, and privileges of a Data Subject or AI Subject, that restrict the activities and behaviors of a Provider, or put positive obligations upon an entity
Residual Risk	The documented sum, Publicly disclosed, of all unmitigated risk pertaining a AAA System

Risk Appetite	The type, amount and threshold of risk that an organization is prepared to accept in pursuit of its strategic objectives and business plan.
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.
Scope	The boundaries of a system, what is covered, what is not covered (i.e, in scope, out-of-scope)
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)
Terms of Reference	define the purpose and structures of a project, committee, meeting, negotiation, or any similar collection of people who have agreed to work together to accomplish a shared goal (SOURCE: Institute of Project Management)
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
Version Control and Change Log	Collects all human deliberative changes, combined with alterations to Pipeline, outcomes, and Architectural Inputs across the lifecycle of the system. A description of any change made to the system through its lifecycle; including changes required by a Notified Body
Vulnerable Populations (People	Persons who often experience exclusion, insufficient accessibility resulting from geopolitical, social, socioeconomic, and cultural inequitable power distribution including but not

in vulnerable situations)	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

3.1 Policies, Plans, and Assessments

Policy, Plan, or Assessment	File Bookmark Link
Algorithmic Risk Assessment	ForHumanity CORE AAA System Governance Prov…
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…
Decommissioning Policy	ForHumanity CORE AAA System Governance Prov…
Ethical Risk Assessment	ForHumanity CORE AAA System Governance Prov…
Human Interactions Policy	ForHumanity CORE AAA System Governance Prov…
Monitoring Policy	ForHumanity CORE AAA System Governance Prov…
Risk Management Policy	ForHumanity CORE AAA System Governance Prov…
System Development Life Cycle Policy	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 behavior, auditors seek maximum, binary clarity on the criteria that determines compliance and non-compliance.

The goal of maximizing the binary (compliant/non-compliant) nature of each audit criteria can be incompatible with industry-led, consensus-driven standards from Standards Development Regulated 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 harmonized.

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 organizational risk management and compliance rather than the risks to the user/AI subject/natural person. *ForHumanity's mission is to examine and analyze downside risk associated with the ubiquitous advance of AI, algorithmic and autonomous systems and where possible to engage in risk mitigation to maximize the benefits of these systems… ForHumanity*. Therefore, when ForHumanity drafts 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 harmonized audit criteria in support of Independent Auditors and the second-order benefit of facilitating compliance.

As a result of this mission, ForHumanity makes 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. Maximize 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 natural persons or management/mitigation of a risk to natural persons, and has been determined feasible to comply. Strictly from a risk perspective, failure to comply with a SHALL criterion absolutely and unequivocally exposes the organization to risk.

SHOULD - is a recommendation. It is within the power and judgment of an organization to decide if it will comply or not. However, SHOULD identifies the recommended option. Therefore, if the organization 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 organization to risk, but the organization may determine that 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 Regulated 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.

- Certification Plan, including:
    - Opening meeting where:
        - The scope is verified
        - The organization and individuals, including their roles, are documented
    - Confirmation of the authorisation of the Certification Body to award the certification, and their impartiality
    - Description of the ToE (as documented in the contract)
    - 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)
    - Expected documentary evidence
    - Physical testing scheduling

- Any expected deviations from the evaluation methods detailed in the certification criteria
- Any site or network access required, and any special requirements for that access (e.g. permission to conduct intrusive network scanning)
- 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:

Public

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

Private

- Explanation of the scope, including Beginnings and Ends, agreed in the Audit Engagement Letter (Private)
- Any deviations from the Certification Plan (Private)
- Process narratives, walkthroughs, flowcharts, diagrams, control descriptions, codes, policies (Management Representations) (Private, unless required under criteria)
- The specific software and hardware versions and assets inspected including third-party assets, as applicable (Private)
- A list of documentation and assets that will be retained as audit evidence, and explanation of deviations (Private)
- A duly authorized signatory (Private, but at the auditee's discretion)
- A list of deficiencies if certification will not be issued (Private)
- If included in the Audit Engagement Letter, a determination of sufficient/mature levels of compliance (private, but at the auditee's discretion)
- A process for resolving disputes (Private)
- A list of non-compliance issues for consideration (Private)
- That auditee has met all public disclosure requirements as logged by the auditor (Private)
- 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)
- Statement of auditor independence and quality management (Private)

- Statement of understanding that this certification scheme does not represent complete protection from enforcement of the law by National Supervisory Authorities (Private)

4.3 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 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 drawing
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:
    a. Interviews with authorized personnel
    b. Inspection of current events, interfaces, and/or notifications
    c. 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 Criteria catalog

Column 1 = ForHumanity Unique Identifier
Column 2 = Category
Column 3 = Audit criteria
Column 4 = Evaluation method

	Categories	**Audit Criteria**	Evaluation Method
		Expert Oversight	
	Expert Oversight	The **Regulated Financial Organization** shall augment the **Algorithmic Risk Committee** with experts trained in understanding the following specific and multi-disciplinary risks associated with Model Risk Management and the **AAA System** in regards to: A. Experience with extreme, unexpected non-normal distribution events (e.g., Tail-risk, Systemic Risk, Black Swans, Financial Crisis) B. Behaviors of all of the following: a. Markets, b. Trading and Execution c. Asset class behaviors and risk profiles d. Market practices and infrastructure e. Global payments and financial settlements C. Financial crime and associated cybersecurity *Note - The duly designated team of experts are appended to as the*	Public disclosure document

		Algorithmic Risk Committee *for the purposes of ease of reference.*	
	Expert Oversight	The **Regulated Financial Organization** should have experts trained in understanding the specific and multi-disciplinary risks associated with **AAA Systems** and financial markets, demonstrated by participation in organizations that seek best practice advancement and/or continuing education in regards to those specific and multi-disciplinary risks (e.g., AIMR, FINRA, ISO, IEEE, National Standards Bodies, IAPP)	Internal log, register or database
Top Management and Oversight Bodies			
	Top Management and Oversight Bodies	Top Management and Oversight Bodies shall ensure that the following governance, oversight, and accountability functions for the **AAA System** are operational, including: A. LEADERSHIP AND GOVERNANCE - Demonstrating leadership by establishing standing and empowered **Ethics Committee, Algorithmic Risk Committee,** and integrating them with existing Model Risk Management governance B. ACCOUNTABILITY - Delineating roles and responsibilities of the operational teams responsible for organizational-wide compliance and oversight, including model risk management, quality management system, legal, compliance, enterprise risk management, and internal audit, and	Correspondence (Internal or External)

		their interactions with **AAA System** specific operations (e.g., the **Algorithmic Risk Committee** and the **Ethics Committee)** C. RISK MANAGEMENT - integrating **AAA System** risk management, including a 360 degree perspective of stakeholders and the inclusion of **Diverse Inputs and Multi Stakeholder Feedback** with existing Model Risk Management processes and procedures to minimize overlap and duplication D. REGULATORY COMPLIANCE - in regards to regulatory requirements on capital reserves take into account the risk of noncompliance with **Relevant Legal Frameworks** E. OVERSIGHT - by: i. 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 and/or enterprise risk management) ii. Integrating members of the Model Risk Management team with **Algorithmic and Ethics Committees**, as appropriate with delineated duties, responsibilities, and accountabilities F. DUTY OF CARE FOR VULNERABLE POPULATIONS - Assess and append **AI Subject's** vulnerabilities associated with financial transactions	

		G. STATEMENT OF PRINCIPLES -Append to the Code of Ethics: i. **Relevant Legal Frameworks** impact on key terminology (e.g., "fair") H. DEFINE STAKEHOLDERS - Ensuring that markets and exchanges are appended to the list of stakeholders I. DUTY TO STAKEHOLDERS - Append to the duty, a commitment to the proper function of markets and exchanges and a commitment to "fair" dealing J. TRAINING AND EDUCATION - Ensuring that members of the **Algorithmic Risk Committee,** Model Risk Management and Top Management and Oversight Bodies are trained on the specific and unique risks associated with **AAA Systems** and AI Literacy K. CONFLICT RESOLUTION - Ensuring that, in all matters where committees (including specialty committees and pre-existing model risk management governance) or delegated persons interact, there is a procedure outlined in the **Code of Ethics** to adjudicate any conflict L. DECOMMISSIONING - Deciding and documenting the decision to **Decommission** the **AAA System**, in consideration of recommendations from the **Algorithmic Risk Committee** and Model Risk Management	
	Top Management and Oversight Bodies	Top Management and Oversight Bodies shall ensure that a **Committee Governance Assessment** is conducted including the following:	Correspondence (Internal or External)

		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 including Model Risk Management B. Assess cross communications, sharing of risk inputs, consultations with specific committees including Model Risk Management, **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 C. Assess all committees for: i. Sufficient diversity ii. Sufficient expertise, iii. Conflicts of interest (or duty) to determine disclosure and/or recusal iv. Inclusion of experts (internal or external) from specialty committees and Model Risk Management onto the **Ethics Committee** and **Algorithmic Risk Committee** for assessments of the specific and unique risks associated with those specialty committees and remediate any shortcomings or conflicts documenting the risk control, treatment, and/or mitigation	
	Top Management and Oversight Bodies	Using the **cAIRE Report** and **Residual Risk** as provided by the **Algorithmic Risk Committee**, Top Management and Oversight	Correspondence (Internal or External)

		Bodies shall execute the following steps to establish the accepted **Residual Risk**: A. Assess and determine whether additional risk controls, treatments, and mitigations for the **AAA System** are to be implemented B. Assess and determine whether external risk treatment options are to be implemented C. Using enterprise **Risk Appetite, Tolerance**, and management procedures, document the accepted **Residual Risk** with **Traceability**	
	Top Management and Oversight Bodies	The Top Management and Oversight Bodies shall ensure, with **Traceability**, that all logs, registers, databases and assessments related to risk (e.g., **Algorithmic Risk Assessment**, **Ethical Risk Assessment**) are documented in the **cAIRE Report** and provided to enterprise or organizational risk management logs, registers, or databases	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** duly designated to assist the **Algorithmic Risk Committee** in managing the risks from **AAA System**	Internal procedure manual
	Top Management and Oversight Bodies	Prior to first use in production (excluding regulatory sandboxes or internal playgrounds) of the **AAA System** and in consultation with the **Ethics Committee** and all other applicable specialty committees, the **Algorithmic Risk Committee**, shall append, to the **Business Rationale Report,** the endorsement by Top Management and Oversight Bodies (e.g., **Model Risk Management** committee)	Correspondence (Internal or External)

Relevant Legal Framework and Modular Assurance Assessments			
	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	For each **Jurisdiction** in which the target of evaluation operates and in the context of its **Scope, Nature, Context,** and **Purpose,** and in consultation with the legal team (internal and/or external), the **Algorithmic Risk Committee,** shall regularly or as needed (e.g., as laws or jurisprudence change) assess the **AAA System** for applicable legal obligations including, but not limited to, the following sectors of law: A. Central Bank and/or Regulatory Guidance B. Banking and Financial Services law and document the following details in the **Relevant Legal Framework** log: 1. Append the applicable legal obligations as **Relevant Legal Frameworks log** 2. A conclusion, from the legal expert, that the target of evaluation is compliant with applicable legal obligations, prior to placing the **AAA System** on market 3. Legal expertise of the person providing the legal opinion, including certification from oversight bodies where applicable	Internal log, register, or database

Training and Education			
	Training and Education	In support of general AI Literacy, the **Algorithmic Risk Committee** shall augment employee training (including Top Management and Oversight Bodies), according to their knowledge, expertise, and responsibility in understanding the following topics associated with Model Risk Management and the **AAA Systems**: A. Governance, oversight, and accountability B. Risks associated with the integration of AAA Systems and Model Risk Management processes and procedure, C. Regulatory oversight and applicable guidance D. Model Risk Management unique and specific risks such as: i. **Market Risk** ii. **Concentration Risk** iii. **Credit Risk** iv. **Capital Risk** v. **Liquidity Risk** vi. **Operational Risk** vii. Model Risk Management viii. Organizational Risk ix. System Development Lifecycle risk x. Model Risk Management objectives , controls, and assurance for: i. Materiality ii. Conceptual Soundness iii. Effective Challenge E. Policies and procedures for: i. Model validation, Conceptual soundness, Process verification and benchmark comparison ii. Data Management and	Internal log, register, or database

		Governance iii. Model limitations and applicable controls iv. Roles, responsibilities, and limitations on employees, contractors, and gig workers v. Decommissioning thresholds and procedures and log the results in the Training and Education log	
	Training and Education	The Top Management and Oversight Bodies shall ensure that ethics officers are trained on current regulatory guidance for National Supervisory Authorities in regards to **AAA System**	Internal Procedure Manual
	Training and Education	In support of general AI Literacy, the **Algorithmic Risk Committee** shall ensure that employees (including Top Management and Oversight Bodies), are trained appropriately and proportionately according to their knowledge, expertise, and responsibility in understanding the governance, oversight, and accountability frameworks applicable to the **AAA System,** and existing Model Risk Management processes and procedures and log the results in the Training and Education log	Internal log, register, or database
Business Rationale			
	Business Rationale	The **Algorithmic Risk Committee** shall append the **AAA Systems List** and document in the **Business Rationale Report,** the following determinations for the **AAA System**: A. Business objectives i. Does the **AAA System** impact **AI Subjects**? ii. If the **AAA System** serves **AI**	Internal Log, register or Database

		Subjects, are they retail or Accredited Investors? iii. Does the **AAA System** allocate the capital of the firm? iv. Does the **AAA System** impact compliance and regulatory obligations B. Business Rationale i. **Causal Hypothesis** ii. **Construct Validity** iii. The Fundamental Rights Impact Assessment	
		Ethical Oversight	
	Ethical Oversight	The **Ethics Committee** shall append to the **Code of Ethics** with all of the following: A. A commitment to model validation B. A commitment to effective challenge of **AAA Systems** by duly empowered and incentivized experts C. A commitment to maintain and regularly assess the proportionality of the **AAA System** risk and quality management systems D. A commitment to independence of model validation from model development	Public Disclosure Document
	Ethical Oversight	In the context of the **Code of Ethics** and maximizing risk controls, treatments, and mitigation, the **Ethics Committee** shall append the definition of diversity for **Diverse Inputs and Multi Stakeholder Feedback** to include all of the following, if applicable, in the pool of human risk assessors: A. Market experts	Internal procedure manual

		B. Trading expertise C. Model validation and document the conclusions in the **Ethical Risk Assessment**	
	Ethical Oversight	The **Ethics Committee** shall append: A. If applicable, **Key Detrimental Indicators** for **Content Moderation** i. Language determined to be an indicator of market abuse, insider trading, fraud or malfeasance ii. Language and product offerings that are only applicable to certain qualified persons or organization B. If applicable, **Key Regulated Product Indicators** i. To monitor product offerings being made available only to certain qualified persons or organizations ii. To monitor trading asset access to ensure that access is made available only to authorized employees or contractors	Internal Procedure Manual
	Ethical Oversight	The **Ethics Committee** shall establish metrics, measurements, and thresholds for the following instances of **Ethical Choice**: A. Human oversight and interactions of the **AAA System** as documented in the **Human Interactions Report** B. **Controllability** C. Fairness metrics and document them in the **Ethical Risk Assessment**	Internal Procedure Manual
	Ethical Oversight	In consideration of: 1. **Relevant Legal Frameworks** (e.g., fairness laws) **2. Code of Ethics**	Internal log, register, or database

		3. Duty of Care for **Vulnerable Populations** 4. Fairness metrics, measurements, and thresholds The **Ethics Committee** shall assess outcomes of the **AAA System** to determine whether the outcomes are NOT fair and exceed fairness thresholds and document the conclusion as a risk input or indicator and log the results in the **Ethical Risk Assessment**	
	Ethical Oversight	In regards an **AAA System** and measuring the systemic riskiness to the organization and/or others spheres of influence, the **Ethics Committee** shall: A. Augment the Community Sphere of influence to monitor across the following distinctions: i. Markets ii. Asset Classes iii. Portfolio management/ Capital Allocation iv. Technology-assisted decision making B. Determine whether the the following variables are to be measured: i. Importance (e.g., customer/client demand) ii. Saturation iii. Dependency (e.g., % of profitability) iv. Authority (e.g., reliance as a trusted input) C. Determine the thresholds for the following variables when any single sphere of influence (or combination) has achieved a meaningful change in systemic riskiness:	Internal Procedure Manual

		i. Importance ii. Saturation iii. Dependency iv. Authority D. Recommend processes and procedures for risk reassessment when measurements exceed thresholds And document the metrics, measurements, and thresholds in the Risk Management Policy	
Consumer Protection			
	Consumer Protection	In the context of sales, marketing and promotional materials, including training, associated with **AAA System** and in consideration of the **Relevant Legal Frameworks** and in consultation with the expert legal team (internal or external), the **Ethics Committee** shall document an Accredited Investor Policy or appended to that document suitability metrics, measurements, and thresholds (e.g., Accredited Investors) that define eligibility to receive financial or investment offerings	Internal Procedure Manual
	Consumer Protection	In consideration of the Accredited Investor Policy, the **Algorithmic Risk Committee** shall implement an assessment of individuals to determine whether the individual is suitable to receive the marketing, sales, and promotional materials	Internal Procedure Manual
	Consumer Protection	In consideration of **Relevant Legal Frameworks**, and in consultation with the	Public Disclosure

		expert legal team (internal or external), the **Algorithmic Risk Committee** shall augment the **AAA System Deployer's Guide** or **AI Subject's Guide** with all applicable legal disclaimers	Document
Data Privacy and Protection			
	Data Privacy and Protection	In regards to **Accredited Investor** status, the **Algorithmic Risk Committee** shall ensure that all applicable suitability data is treated as **Personal Data**	Internal log, register, or database
Risk Management			
	Risk Management	In consideration of: 1. The Algorithmic Risk Assessment, the **Algorithmic Risk Committee** shall augment the Risk Management Policy with metrics, measurements, and thresholds for: A. Materiality and Reliance (e.g., Scope, Nature, Context, Purpose, Impact, Capital requirements) B. Complexity (e.g., number of variables, amount of source data, interactions of parameters) C. Uncertainty (e.g., confidence associated with estimates and controls)	Internal Procedure Manual
	Risk Management	In consideration of: 1. The Algorithmic Risk Assessment, the **Algorithmic Risk Committee** shall assess: A. Materiality and Reliance (e.g., Scope,	Internal log, register, or database

		Nature, Context, Purpose, Impact, Capital requirements) B. Complexity (e.g., number of variables, amount of source data, interactions of parameters) C. Uncertainty (e.g., confidence associated with estimates and controls) And append risk inputs and indicators to the risk log	
	Risk Management	In consideration of: 1. The **Scope, Nature, Context, and Purpose** of the **AAA System,** the **Algorithmic Risk Committee** shall augment risk inputs and indicators with the following risk identifications as applicable: 1. **Market Risk** 2. **Concentration Risk** 3. **Credit Risk** 4. **Capital Risk** 5. **Liquidity Risk** 6. **Operational Risk** 7. Model Risk 8. Strategy Risk And log the inputs and indicators in the Risk log	Internal log, register or database
	Risk Management	In regards to **AAA System** risk management, the Top Management and Oversight Bodies shall augment the **Algorithmic Risk Committee** with individuals from all of the following disciplines: 1. **Market Risk** 2. **Concentration Risk** 3. **Credit Risk** 4. **Capital Risk** 5. **Liquidity Risk** 6. **Operational Risk** 7. Model Risk Management 8. Organizational Risk And document the inclusion of expertise with **Traceability**	Internal Procedure Manual/ Correspondence (Internal or External)

	Risk Management	In regards to **AAA System** risk management, the **Algorithmic Risk Committee** shall include individuals from all of the following disciplines: 1. **Market Risk** 2. **Concentration Risk** 3. **Credit Risk** 4. **Capital Risk** 5. **Liquidity Risk** 6. **Operational Risk** 7. Model Risk Management 8. Organizational Risk 9. System Development Lifecycle risk in **Diverse Input and Multi Stakeholder Feedback** human risk assessors as domain experts	Internal Procedure Manual
	Risk Management	In consultation with: 1. New product approval team, if applicable 2. The expert legal team (internal or external) If the **AAA System:** A. May be used by an **AI Subject** and B. Requires a determination of AI Subject status (e.g., Accredited Investor) then the **Algorithmic Risk Committee** shall implement the necessary **Accredited Investor (entity)** qualification process or procedure to ensure that the **AAA System** outputs are suitable for the **AI Subject**	Physical Testing
	Risk Management	If the AAA System may be used by an **Accredited Investor (entity)**, then **Algorithmic Risk Committee** shall log documents from the **Accredited Investor (entity)** to verify their investor status	Internal log, register, or database
Data Management and Governance			

	Data Management and Governance	In consideration of: 1. The **Scope, Nature, Context, and Purpose** 2. **Relevant Legal Frameworks** 3. Applicable collective bargaining agreements 4. Applicable Employment contracts 5. Applicable Market Data (and/or Exchange Data) contracts 6. **Code of Ethics** 7. Code of Conduct If **Personal Data** is present in the **AAA System**, then the **Ethics Committee** shall assess the following **Pipeline Data** and inferences processed by the **AAA System** to determine all of the following: A. The significance and envisaged consequences of the **AAA System** on the **AI Subject** in an **Explainability Statement** B. The contents of the **Explainability+ Statement** C. That **Pipeline Data** and inferential outcomes are disclosed to the **AI Subject** with a clear and conspicuous digital process or procedure including all of the following tasks: i. Notifications associated with any change in the output from the **AAA System** ii. The ability to exercise rights in regards to **Personal Data** and **Relevant Legal Frameworks** such as, but not limited to**:** a. Access b. Rectification c. Objection d. Erasure e. Accounting of disclosures to other **AAA Systems** and/or	Physical Testing

		organizations iii. Manage notification preferences iv. See any other **AAA Systems** that receive the data v. See categories of recipients of the data vi. See how the data is used (e.g., **Purpose**) vii. **Choice Architecture** and ability to alter the **AAA System** viii. A dispute mechanism D. That the **Pipeline Data** allows for appropriate and applicable **Accommodations** and is fairly implemented by the **Architectural Inputs** of the **AAA System** in generating outcomes E. That the UX/UI interface, notifications, and nudges are in support of the well-being of the individual And document the conclusions in the **Ethical Risk Assessment**	
Explainability			
	Explainability	If **Personal Data** is deployed in the **AAA System** then, the **Algorithmic Risk Committee** shall produce an **Explainability+ Statement** to the **AI Subject** with **Traceability** to the **Ethics Committee**	Correspondence (Internal or External)
Transparency and Information to AI Subjects			
	Transparency and Information Provision to Deployers	In consideration of: 1. **Relevant Legal Frameworks** In consultation with: 1. The expert legal team (internal or	Internal log, register, or database

		external) The **Algorithmic Risk** shall augment the **AAA System AI Subject Guide** with all appropriate and applicable legal disclaimers	
Control			
	Control	The **Algorithmic Risk Committee** shall augment **Intervenability** with controls, treatments, and mitigations that include all of the following: A. The Model Risk Management team acts as a post hoc human oversight for the **AAA System**, including periodic assessment and ongoing monitoring B. Market-based rules applicable to the **AAA System** operations (e.g., circuit breakers, market-making duties, spoofing) And document the controls, treatments, and mitigations in the **Algorithmic Risk Assessment** and the risk log	Internal log, register, or database
	Control	If the **AAA System** output materially impacts the organization's: i. Capital allocation ii. Liquidity iii. Valuation iv. Maximum market exposure and limits Then the **Algorithmic Risk Committee** shall augment the **AAA System** risk management with additional controls, treatments, or mitigations designed to manage model specific risk or limitations (e.g., time, valuation quality, insufficient data) and log the controls,	Internal log, register, or database

		treatments, and mitigations in the risk log	
Human Oversight and Interaction			
	Human Oversight and Interaction	Prior to deploying the **AAA System** and in consideration of the **Scope, Nature, Context, and Purpose**, the **Algorithmic Risk Committee** shall augment a Human Interactions Policy to include all of the following: A. A description of the expected human oversight in regards to any applicable **Fiduciary** duty B. A commitment to put the interests of client above the interests of the organization C. A minimum oversight of human-on-the-loop who can stop, pause, disregard, override, and/or reverse the **AAA System** D. Establishing learning objectives for all employees acting as a **Fiduciary** in regards to the **AAA System** and their human oversight duties E. Establishing metrics, measurements, and thresholds for effective **Fiduciary** human oversight as applicable to the **AAA System** ***Note -*** *consider how and when to share these metrics, measurements, and thresholds with the human interactor during operation to avoid confirmation bias*	Internal Procedure Manual
	Human Oversight and Interaction	**T**he **Algorithmic Risk Committee** shall authorize and empower the **Fiduciary** human oversight to implement the prescribed responses when **Exceptions Interpretability** metrics exceed predetermined thresholds as identified in the **Monitoring** policy	Correspondence (Internal or External)

		AAA System Procurement	
	AAA System Procurement	In consultation with: 1. The expert legal team (internal or external) In consideration of: 1. The AAA System Procurement Plan The **Algorithmic Risk Committee** shall augment the AAA System Procurement plan with the following: A. Financial Stability, including credit department validation B. Contractual Contingency Plan for the **AAA System** continuous operation and continuity C. Contractual Contingency Plan for the **AAA System** backup plan	Contract
		Change Management	
	Change Management	In regards to a deployed **AAA System** and associated ecosystem, if a potential change has NOT been predetermined, documented, tested, and approved, then the **Algorithmic Risk Committee** shall augment a **Change Management Impact Assessment,** including assessing the metrics, measurements, and thresholds, in the following areas: A. **Market Risk** B. **Concentration Risk** C. **Credit Risk** D. **Capital Risk** E. **Liquidity Risk** F. **Operational Risk** G. Model Risk Management H. Organizational Risk	Internal Procedure Manual

		I. System Development Lifecycle risk J. Model Risk Management objectives , controls, and assurance for: i. Materiality ii. Conceptual Soundness iii. Effective Challenge	
	Change Management	In consideration of the: 1. Change Management Plan, the **Algorithmic Risk Committee** shall augment the Change Management Plan to consider Impact to: A. Model Risk Management B. Model validation And document the conclusion in the Change Management Plan and the **Version Control and Change Log**	Internal Procedure Manual/ Internal log, register, and database
	Change Management	In consideration of: 1. The Change Management Plan, 2. The updated Test Plan or Integration Test Plan and Completion Report the **Algorithmic Risk Committee** shall augment notifications to include the responsible and accountable party (ies) in Model Risk Management of their associated duties and responsibility with **Traceability**	Correspondence (Internal or External)
	Change Management	In consideration of: 1. The Change Management Plan, 2. The updated Test Plan and Completion Report The accountable and responsible party(ies) in Model Risk Management shall implement the approved changes applicable to their delineated accountability and notify the **Algorithmic Risk Committee** with **Traceability**	Correspondence (Internal or External)
System Development Lifecycle			

	System Development Lifecycle	In regards to the System Development Lifecycle Policy for the **AAA System** and associated deployment, the **Algorithmic Risk Committee** shall augment considerations with the Model Risk Management Policy for **AAA Systems** and augment consultation to include the **Model Risk Management Lead** with **Traceability**	Correspondence (Internal or External)
		Model Risk Management	
	Model Risk Management	In consideration of: 1. The **cAIRE Report** 2. The determination of systemic riskiness, Prior to deploying the **AAA System**, Top Management and Oversight Bodies shall establish **Model Risk Management** oversight based upon: A. Materiality B. Complexity C. Uncertainty D. Reliance	Internal Procedure Manual
	Model Risk Management	Prior to placing the **AAA System** into use, the **Algorithmic Risk Committee** shall document in the **AAA Systems List** all of the following elements of **Conceptual Soundness:** A. **Scope, Nature, Context, and Purpose** B. **Casual Hypothesis** C. **Construct Validity** D. Whether **Ground Truth** validation was available and applicable	Internal log, register, or database
	Model Risk Management	Top Management and Oversight Bodies shall endorse the **Model Risk Management** team as	Correspondence (Internal or

		accountable and responsible for the **AAA System** by assigning the **Model Risk Management Lead** with **Traceability**	External)
	Model Risk Management	In consideration of: 1. Enterprise-wide Model Risk Management Policy 2. Enterprise-wide **AAA System** Risk Management Top Management and Oversight Bodies shall assign a **Model Risk Management Lead** who has the following responsibilities: A. Establishing the Model Risk Management Policy applicable to the **AAA System** or deployment B. Implementing model risk activities (e.g., targets, controls, assurance) C. Ensuring that model risk assurance record storage and retention processes and procedures are in conformity with **Relevant Legal Frameworks** and regulatory guidance D. Implement model risk assurance metrics, measurement and thresholds E. Implement learning objectives activities in regards to the model risk management policy F. Establish the **Model Risk Validation Report**	Correspondence (Internal or External)
	Model Risk Management	In consideration of: 1. Existing enterprise-wide Model Risk Management frameworks 2. The **cAIRE Report**, 3. Data Management and Governance Policy, 4. Test Plan	Internal Procedure Manual/ Internal log, register, or database

		5. Monitoring Policy, 6. Risk Management Policy 7. Cybersecurity Risk Management Policy 8. **Business Rationale Report** 9. **Relevant Legal Frameworks** 10. Regulatory Guidance and in consultation with the: 1. **AI Compliance Lead**, 2. **AAA Cybersecurity Lead**, 3. **Data Lead** 4. **Test Lead** 5. **Monitoring Lead** 6. **Algorithmic Risk Committee** The **Model Risk Management Lead** shall establish a Model Risk Management Policy in regards to the **AAA System** that: A. Establishes the rules governing the creation and storage of model risk objectives, controls and assurance records in conformity with **Relevant Legal Frameworks** and regulatory guidance B. Establishes a process to identify **AAA System** regulatory compliance obligations i. Legal obligations identified in the **Relevant Legal Framework** ii. If applicable common specifications, iii. If applicable harmonized standards iv. Regulatory guidance C. Identifies model risk objectives (e.g., targets), controls, and assurance process or procedures including metrics, measurement and thresholds that validate and assure: i. That the **AAA System** is fit for	

		purpose (e.g., **Data Quality**, **Information Quality**, Model health and fitness, monitoring, software) ii. Specific quality objectives (e.g., control, assurance) in regards to: a. Design (control and verification) b. Development c. Deployment d. Risk Management e. Change Management f. Monitoring g. Decommissioning D. Establishes, in accordance with **Relevant Legal Frameworks,** a frequency of model risk validation of the effectiveness of: i. Model risk controls ii. Risk management iii. Regulatory compliance E. In consideration of each employee's role, responsibilities, and duties, establish proportionate learning objectives that raise awareness of the **AAA System's** model risk management policy in regards to: i. Design, Design control, verification ii. Examination, testing and evaluation procedures iii. Technical specifications, including metrics, measurements, and thresholds if appropriate iv. Systems and Procedures for record-keeping v. Resource management F. Establishes a **Model Risk Validation**	

		Report that logs validation of policies, processes, and procedures based upon model risk objectives regarding: i. Vendor Management ii. Change Management iii. System Development iv. Cybersecurity v. AI Compliance vi. Risk Management vii. Data Management and Governance viii. Testing and Evaluation ix. Monitoring x. Record Keeping xi. Human Oversight	
	Model Risk Management	Top Management and Oversight bodies shall endorse the Model Risk Management Policy for the **AAA System** with **Traceability** to the **Model Risk Management Lead** and **AI Compliance Lead**	Correspondence (Internal or External)
	Model Risk Management	In consideration of the **AAA Systems List**, Model Risk Management shall validate the **AAA System** for **Conceptual Soundness** with **Traceability**	Correspondence (Internal or External)
	Model Risk Management	In consideration of all of the following: 1. The **Scope, Nature, Context, and Purpose** of the **AAA System** 2. The Model Risk Management Policy 3. Algorithmic Risk Assessment and **Residual Risk** 4. **Testing and Evaluation** 5. Harmonized standards and common specifications, if applicable 6. Existing Model Risk objectives 7. Business objectives and strategy	Internal Procedure Manual

		8. Relevant Legal Frameworks 9. Regulatory Guidance and in consultation with the **Algorithmic Risk Committee,** the **Model Risk Management Lead** shall establish the following metrics, measurements, thresholds, processes and/or procedures: A. Model risk targets and controls for: i. Design (Control and Verification) ii. Development iii. Deployment iv. Change Management v. Monitoring vi. Decommissioning B. Identify model risk assurance metrics, measurement and thresholds that validate and assure: i. That the **AAA System** is fit for purpose (e.g., **Data Quality**, **Information Quality**, Model health and fitness, monitoring, software) ii. That requirements, specifications, guidelines, characteristics, metrics, measurements, and thresholds are appropriate to the **AAA System,** classification of materiality and systemic riskiness, and the **Residual Risk** And document the conclusions in the **Model Risk Management Plan**	
	Model Risk Management	The **Model Risk Management Lead** shall validate that the **AAA System** has been supplied with the necessary resources (e.g., people, budget, infrastructure) to achieve model risk objectives such as: A. The assignment of appropriate leads and	Correspondence (Internal or External)/ Internal Procedure Manual

		the rostering of expert oversight B. The **Test Completion Report** has been accepted by the **Algorithmic Risk Committee**	
	Model Risk Management	In consideration of the **Model Risk Management Plan**, each of the the following accountable parties: 1. **Algorithmic Risk Committee** 2. **Ethics Committee** 3. **AAA Cybersecurity Lead** 4. **Data Lead** 5. **Test Lead** 6. **Monitoring Lead** **7. AI Compliance Lead** shall ensure the **AAA System** meets all applicable quality objectives with **Traceability**	Correspondence (Internal or External)
	Model Risk Management	In consideration of: 1. The Model Risk Management Policy 2. The Model Risk Management Plan The **Model Risk Management Lead** shall validate all of the following in regards to **AAA System** risk management: A. That there is a process to: i. Identify risk ii. Analyze risk iii. Evaluate risk iv. Treat risk v. Report risk to Top Management and Oversight Bodies in the **cAIRE Report,** including **Residual Risk** vi. Establish and review metrics, measurements, and thresholds in regards to frequency of review and risk reassessment	Internal Log, register, and database / Correspondence (Internal or External)

		vii. Reevaluate systemic riskiness, including assessment of the appropriate frequency B. That **Diverse Input and Multi Stakeholder Feedback** human risk assessors were included and found to be sufficiently diverse by the **Ethics Committee** and document the conclusion to the **Model Risk Validation Report** with **Traceability** to the **Algorithmic Risk Committee**	
	Model Risk Management	In consideration of the Model Risk Management Policy and Plan, the **Model Risk Management Lead** shall validate: A. Risk Management B. Data Management and Governance C. Technical Documentation D. Record Keeping and Logs E. Transparency requirements for Deployers and AI Subject, if applicable F. Human oversight G. Testing and Evaluation H. Security and Cybersecurity I. Monitoring J. Incident Response K. Vendor Management L. Change Management M. System Development N. Regulatory Compliance To determine whether the **AAA System** meets model risk objectives, controls, and assurance metrics, measurements and thresholds and document the conclusions in the **Model Risk Validation Report** including notification to the accountable party of any shortfalls	Internal log, register, and database / Correspondence (Internal or External)

	Model Risk Management	In consideration of: 1. **Model Risk Management Policy** 2. **Relevant Legal Frameworks** 3. **Model Risk Validation Report**, the **Model Risk Management Lead** shall validate the **AAA System** and document the conclusion in the **AAA Systems List** prior to deployment	Internal log, register, or database
	Model Risk Management	In consideration of **Model Risk Validation Report** and **AAA Cybersecurity Lead** responses to findings, Top Management and Oversight Bodies shall endorse the **Model Risk Validation Report** as complete in the **AAA System List** prior to deployment	Correspondence (Internal or External)
Decommissioning			
	Decommissioning	In consideration of: 1. The Algorithmic Risk Assessment 2. Monitoring policy, the **Algorithmic Risk Committee** shall append to the **Decommissioning Policy** all criteria and associated metrics, measurements, and thresholds necessary to determine when the **AAA System** is to be decommissioned including: A. Increased complexity and risks associated with **AAA System** that cannot be sufficiently mitigated B. Sufficiently granularity of measurements of risk (e.g., volatility, concentration, liquidity) C. A process to reassess the frequency of measurements	Internal Procedure Manual

