CARIBBEAN AI RISK MANAGEMENT COUNCIL

CARIBBEAN AI RISK MANAGEMENT STANDARD

First Edition — February 2026

A Comprehensive Framework for AI Governance, Risk Assessment, and Regulatory Alignment in the Caribbean Region



CONSULTATION DRAFT

Prepared by: Caribbean AI Risk Management Council (CAIRMC)

Date: February 2026
Status: Draft for Stakeholder Consultation
Reference: CAIRMC-STD-2026-001

Important Notice

This document is a consultation draft issued by the Caribbean AI Risk Management Council (CAIRMC). It has not been formally adopted or endorsed by the Caribbean Community (CARICOM) or any CARICOM member state. It does not constitute binding law unless and until adopted by a CARICOM member state through national legislation. It is published to facilitate public consultation, stakeholder engagement, and regional policy dialogue.

CAIRMC invites written submissions from governments, private sector organisations, civil society, academic institutions, and individuals across the Caribbean region. Submissions should be directed to info@caribbeanairisk.com with the subject line “Caribbean AI Risk Management Standard — Consultation Submission” by 31 December 2026.

Table of Content

Important Notice 2
PART I: GENERAL PROVISIONS 9
Chapter 1: Purpose, Scope, and Definitions 9
Article 1 — Purpose 9
Article 2 — Scope 9
Article 3 — Definitions 10
Article 4 — AI Literacy 14
PART II: RISK CLASSIFICATION 15
Chapter 2: AI Risk Tier System 15
Article 5 — The Four-Tier Risk Classification 15
Article 6 — Tier 1: Prohibited AI Practices 15
Article 7 — Tier 2: High-Risk AI Systems 17
7.1.1 — Critical Infrastructure 17
7.1.2 — Education and Employment 17
7.1.3 — Essential Private Services 17
7.1.4 — Public Services and Benefits 17
7.1.5 — Healthcare 18
7.1.6 — Law Enforcement 18
7.1.7 — Migration, Asylum, and Border Control 18
7.1.8 — Democratic Processes 18
7.1.9 — AI Agents and Autonomous Systems 18
Article 8 — Tier 3: Limited Risk AI Systems 19
Article 9 — Tier 4: Minimal Risk and Voluntary Codes of Conduct 19
PART III: OBLIGATIONS FOR HIGH-RISK AI SYSTEMS 20
Chapter 3: Provider Obligations 20
Article 10 — Quality Management Systems 20
Article 11 — Data and Data Governance 20
Article 12 — Technical Documentation 21
Article 13 — Transparency and Provision of Information 21
Article 14 — Human Oversight 22
Article 15 — Accuracy, Robustness, and Cybersecurity 22
Article 16 — Automatic Logging 23
Chapter 4: Deployer Obligations 23
Article 17 — Responsibilities of Deployers 23

Article 18 — Fundamental Rights Impact Assessment for Public Sector Deployers 24
Article 19 — Importer Obligations 24
Article 20 — Distributor Obligations 25
Article 21 — Authorised Representatives 25
Article 22 — Obligations Along the AI Value Chain 25
PART IV: CARIBBEAN AI RISK ASSESSMENT (CARA) 27
Chapter 5: The CARA Methodology 27
Article 23 — Purpose and Scope of CARA 27
Article 24 — CARA Assessment Dimensions 27
Article 25 — CARA Process 27
PART V: TRANSPARENCY AND GENERAL-PURPOSE AI 29
Chapter 6: Transparency Obligations 29
Article 26 — Transparency for Limited Risk AI Systems 29
Article 27 — Deep Fake Provisions 29
Chapter 7: General-Purpose AI Systems 29
Article 28 — Obligations for GPAI System Providers 30
Article 29 — GPAI Systems with Systemic Risk 30
Article 30 — Codes of Practice for GPAI 31
PART VI: CONFORMITY ASSESSMENT AND CERTIFICATION 32
Chapter 8: Conformity Assessment 32
Article 31 — Conformity Assessment for High-Risk AI Systems 32
Article 32 — Caribbean AI Conformity Mark 32
Article 33 — Conformity Assessment Bodies 32
Chapter 9: QAIRP Certification 33
Article 34 — The Qualified AI Risk Professional Programme 33
PART VII: GOVERNANCE AND ENFORCEMENT 34
Chapter 10: The Caribbean AI Registry 34
Article 35 — Establishment of the Caribbean AI Registry 34
Article 36 — Registration Obligations 34
Chapter 11: Competent Authorities and CAIRMC's Role 35
Article 37 — National Competent Authorities 35
Article 38 — CAIRMC as Regional Coordinating Body 35
Article 39 — Caribbean AI Advisory Forum 36
Article 40 — Caribbean AI Scientific Panel 36
Chapter 12: Market Surveillance and Post-Market Monitoring 36
Article 41 — Post-Market Monitoring by Providers 36
Article 42 — Market Surveillance by Competent Authorities 37

Article 43 — Serious Incident Reporting 37
Chapter 13: Sanctions and Remedies 38
Article 44 — Administrative Sanctions 38
Article 45 — Periodic Penalty Payments 38
Article 46 — Individual Rights and Remedies 39
Article 47 — Whistleblower Protections 39
Article 48 — Right to a Human Alternative 39
PART VIII: REGULATORY SANDBOXES AND INNOVATION 41
Chapter 14: AI Regulatory Sandboxes 41
Article 49 — Establishment of Regulatory Sandboxes 41
Article 50 — Sandbox Conditions and Safeguards 41
Article 51 — Sandboxes for Small Island Developing States 41
Chapter 15: Confidentiality and Trade Secrets 42
Article 52 — Confidentiality of Information 42
PART IX: SECTOR-SPECIFIC AI GOVERNANCE 43
Chapter 16: AI in Tourism 43
Article 53 — AI in Tourism and Hospitality 43
Chapter 17: AI in Financial Services 43
Article 54 — AI in Financial Services 43
Chapter 18: AI in Healthcare 44
Article 55 — AI in Healthcare 44
Chapter 19: AI in Agriculture and Food Security 44
Article 56 — AI in Agriculture 44
Chapter 20: AI in Education 45
Article 57 — AI in Education 45
PART X: ENVIRONMENTAL AND CLIMATE AI GOVERNANCE 46
Chapter 21: Climate and Environmental Impact 46
Article 58 — Environmental Principles for AI 46
Article 59 — Climate Impact Assessment 46
Article 60 — AI for Climate Resilience 46
PART XI: LIABILITY AND INSURANCE 48
Chapter 22: AI Liability 48
Article 61 — Liability of Providers 48
Article 62 — Presumption of Causation 48
Article 63 — Mandatory AI Liability Insurance 48
PART XII: ACCESSIBILITY AND INCLUSION 50
Chapter 23: Accessibility Requirements 50

Article 64 — Accessibility for Persons with Disabilities 50
Article 65 — Digital Inclusion and the Digital Divide 50
PART XIII: SUPPLY CHAIN DUE DILIGENCE 51
Chapter 24: Due Diligence in the AI Value Chain 51
Article 66 — Supply Chain Due Diligence Obligations 51
Article 67 — Open-Source AI Components 51
PART XIV: AI AGENTS, MULTI-AGENT SYSTEMS, AND FRONTIER AI 52
Chapter 25: AI Agents and Autonomous AI Systems 52
Article 68 — Classification and Governance of AI Agents 52
Article 69 — Multi-Agent Systems and Agent Swarms 52
Article 70 — Frontier AI Models and Artificial General Intelligence 53
PART XV: ETHICAL FRAMEWORK FOR AI IN THE CARIBBEAN 55
Chapter 26: Caribbean Ethical AI Principles 55
Article 71 — Purpose and Status of the Ethical Framework 55
Article 72 — The Principles 55
Article 73 — Ethical Review for High-Risk AI Systems 57
PART XVI: IMPLEMENTATION AND TRANSITIONAL PROVISIONS 58
Chapter 27: Phased Implementation 58
Article 74 — Implementation Timeline 58
Article 75 — Support for Small Island Developing States 58
Article 76 — Relationship with Existing Law 59
Article 77 — International Cooperation and Mutual Recognition 59
Article 78 — Review and Amendment 59
Article 79 — Delegated and Implementing Powers 60
PART XVII: FINAL PROVISIONS 61
Article 80 — Effective Date 61
Article 81 — Authoritative Texts 61
Article 82 — Custodian 61
ANNEX I — Caribbean AI Risk Taxonomy 62
ANNEX II — Framework Alignment Table 64
ANNEX III — CAIRMC AI Governance Maturity Model 65
ANNEX IV — Sector-Specific High-Risk AI Applications (Caribbean) 66
Signature 68

Preamble

The Caribbean AI Risk Management Council (CAIRMC), established in January 2024 as the foremost body for AI governance across the Caribbean region, issues this Caribbean AI Risk Management Standard (hereinafter "the Standard" or "this Standard") as a proposed regional framework for the responsible development, deployment, and governance of artificial intelligence systems.

This Act draws its foundational architecture from Regulation (EU) 2024/1689 of the European Parliament and of the Council (the EU AI Act), adapted to reflect the legal, economic, institutional, and socio-cultural context of Caribbean nations. It integrates obligations and principles from the General Data Protection Regulation (EU) 2016/679 (GDPR), the NIST Artificial Intelligence Risk Management Framework (NIST AI RMF, 2023), ISO/IEC 42001:2023 (AI Management Systems), the COSO Enterprise Risk Management Framework (2017), relevant Basel Committee guidance on AI in financial services, ISO/IEC 27001:2022 (Information Security Management), and ISO 31000:2018 (Risk Management).

This Act also gives effect to and builds upon the following existing Caribbean instruments:

- The Jamaica Data Protection Act 2020
- The Trinidad and Tobago Data Protection Act 2011
- The Barbados Data Protection Act 2019
- The OECS Model Data Protection Bill
- The Guyana Data Protection Act 2023
- The Cayman Islands Data Protection Act 2017 (as amended)
- The CARICOM Digital Economy Strategy
- Applicable national Electronic Transactions Acts across CARICOM member states
- The Revised Treaty of Chaguaramas establishing the Caribbean Community including the CARICOM Single Market and Economy (CSME)
- The Inter-American Convention on Human Rights (Pact of San José)
- The Caribbean Court of Justice (CCJ) jurisprudence on fundamental rights and regional economic integration

CAIRMC recognises that the Caribbean region comprises Small Island Developing States (SIDS) with distinct regulatory capacity constraints, emerging data protection regimes, and significant dependence on digital technology across sectors including tourism, financial services, agriculture, healthcare, and public administration. This Act is calibrated to those realities.

CAIRMC further acknowledges the responsible AI principles published by leading AI developers including Google (PAIR Principles), OpenAI (System Card methodology), Anthropic (Responsible Scaling Policy), Microsoft (Responsible AI Standard v2), and IBM (AI Ethics Board principles). These industry commitments, while not binding, inform and complement the obligations set out in this Standard.

This Standard goes beyond existing international frameworks in several material respects. It introduces binding AI literacy obligations, mandatory climate and environmental impact assessment, sector-specific governance for the Caribbean's most economically significant

industries, a right to a human alternative in high-stakes decisions, mandatory AI liability insurance, regulatory sandboxes designed for small economies, supply chain due diligence obligations for AI built on general-purpose models, dedicated governance of AI agents and multi-agent systems (agent swarms), precautionary provisions for frontier AI and artificial general intelligence, and a binding ethical framework grounded in Caribbean constitutional values and cultural identity. These provisions reflect the position that Caribbean AI governance must not merely replicate Global North regulation but address the particular vulnerabilities, opportunities, and development priorities of the region.

PART I: GENERAL PROVISIONS

Chapter 1: Purpose, Scope, and Definitions

Article 1 — Purpose

The purpose of this Standard is to:

1. Establish a common framework for the classification, assessment, and governance of artificial intelligence systems developed or deployed within the Caribbean region.
2. Protect the fundamental rights, dignity, safety, and economic interests of individuals and organisations across Caribbean nations from harms arising from AI systems.
3. Promote trust, transparency, accountability, and human oversight in AI deployment across public and private sectors.
4. Support regional alignment with international AI governance standards while recognising the specific regulatory capacity and development context of Caribbean member states.
5. Provide a basis for CARICOM adoption, bilateral implementation agreements, and national legislation among member states.
6. Advance AI literacy across all levels of Caribbean society, from schoolchildren to senior public officials and corporate directors.
7. Safeguard Caribbean environmental and climate resilience from AI-related risks while supporting AI applications that strengthen climate adaptation.
8. Promote responsible AI innovation through regulatory sandboxes and capacity-building programmes designed for small economies.
9. Establish clear liability rules and insurance requirements for AI-caused harm, so that affected persons have practical redress.

Article 2 — Scope

2.1. This Act applies to:

(a) Providers that place or put into service AI systems in the Caribbean region, regardless of whether they are established in a Caribbean member state.

(b) Deployers of AI systems located in the Caribbean region.

(c) Importers and distributors of AI systems that are made available in the Caribbean region.

(d) Product manufacturers that place AI systems on the market as part of a physical product.

(e) Authorised representatives of providers established outside the Caribbean region.

(f) Any person who places on the market or puts into service a general-purpose AI system, regardless of where that person is established, where the output of that system is used within the Caribbean region.

2.2. This Act does not apply to:

(g) AI systems developed or used exclusively for military, national security, or intelligence purposes by a sovereign Caribbean member state.

(h) AI systems used solely for scientific research that does not involve deployment to end users or decisions affecting natural persons.

(i) Free and open-source AI components, except where they are incorporated into a high-risk AI system placed on the market or put into service, or where they are themselves general-purpose AI systems with systemic risk.

(j) Personal, non-professional use of AI systems by natural persons.

Article 3 — Definitions

For the purposes of this Standard, the following definitions apply:

Artificial Intelligence System (AI System): A machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers from the inputs it receives how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Provider: A natural or legal person, public authority, agency, or other body that develops or has an AI system developed and places it on the market or puts it into service in the Caribbean region under its own name or trademark, whether for payment or free of charge.

Deployer: A natural or legal person, public authority, agency, or other body that uses an AI system under its authority, except where the AI system is used in the course of personal non-professional activity.

Importer: A natural or legal person located in the Caribbean region that places on the market an AI system bearing the name or trademark of a provider established outside the Caribbean region.

Distributor: A natural or legal person in the supply chain, other than the provider or importer, that makes an AI system available on the Caribbean market.

Authorised Representative: A natural or legal person located in the Caribbean region that has received and accepted a written mandate from a provider of an AI system to carry out the obligations and procedures established by this Standard on behalf of that provider.

Operator: The provider, deployer, importer, distributor, product manufacturer, or authorised representative of an AI system.

Product Manufacturer: A manufacturer within the meaning of applicable Caribbean consumer protection legislation that places a product on the market with an AI system integrated into it.

High-Risk AI System: An AI system that poses significant risk to the health, safety, or fundamental rights of persons, as classified in Articles 6 and 7 of this Standard.

General-Purpose AI System (GPAI): An AI system that is based on a general-purpose AI model and can be used for a range of purposes, both for direct use and for integration into other AI systems.

General-Purpose AI Model: An AI model, including where trained using a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market.

Systemic Risk: A risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant effect on the Caribbean market due to its reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or Caribbean society as a whole, and that can be propagated at scale across the value chain.

Caribbean AI Risk Assessment (CARA): The proprietary assessment methodology of CAIRMC for evaluating AI systems across technical, ethical, legal, and societal risk dimensions in the Caribbean context.

AI Risk Tier: One of four risk classification levels (Tier 1: Unacceptable; Tier 2: High; Tier 3: Limited; Tier 4: Minimal) assigned to an AI system under this Standard.

Caribbean AI Risk Taxonomy: CAIRMC's structured classification of AI risk types specific to the Caribbean context, as set out in Annex I.

Placing on the Market: The first making available of an AI system on the Caribbean market, whether for payment or free of charge.

Putting into Service: The supply of an AI system for first use directly to the deployer or for own use in the Caribbean region for its intended purpose.

Intended Purpose: The use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the technical documentation and instructions for use.

Reasonably Foreseeable Misuse: The use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems.

Substantial Modification: A change to the AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment and which affects the compliance of the AI system with this Standard or results in a modification to the intended purpose.

Fundamental Rights: Rights established under applicable national constitutions of Caribbean member states, the American Convention on Human Rights, the Inter-American Commission on Human Rights instruments, and universally recognised under the Universal Declaration of Human Rights.

Competent Authority: The national body designated by a Caribbean member state to supervise and enforce this Standard within that jurisdiction. CAIRMC may serve as a regional Competent Authority by agreement among member states.

Personal Data: Any information relating to an identified or identifiable natural person, consistent with the definition in applicable national data protection legislation including the Jamaica Data Protection Act 2020, the Trinidad and Tobago Data Protection Act 2011, and equivalent instruments.

Sensitive Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for unique identification, health data, data on sexual orientation, and criminal conviction data, as defined in applicable Caribbean data protection legislation.

Biometric Data: Personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, including facial images and fingerprint data.

Real-Time Remote Biometric Identification System: An AI system for the purpose of identifying natural persons at a distance through the comparison of biometric data with data in a reference database, where the capture, comparison, and identification occur without significant delay and in real time.

Post-Remote Biometric Identification System: An AI system that identifies natural persons from biometric data that was previously captured, and where comparison and identification do not occur in real time.

Emotion Recognition System: An AI system that identifies or infers emotions, intentions, or mental states of natural persons on the basis of their biometric data.

Deep Fake: AI-generated or AI-manipulated image, audio, or video content that falsely appears to be authentic and that depicts a person appearing to say or do something they did not say or do, or that depicts events that did not occur.

Serious Incident: An incident or malfunction of an AI system that directly or indirectly leads to: (a) the death of a person or serious damage to health; (b) a serious and irreversible disruption of the management and operation of critical infrastructure; (c) a breach of obligations under Caribbean law intended to protect fundamental rights; or (d) serious damage to property or the environment.

AI Literacy: The skills, knowledge, and understanding that allow providers, deployers, and affected persons to make informed decisions regarding AI systems, taking into account the rights and obligations of all parties and the risks and benefits of AI.

Regulatory Sandbox: A controlled environment established by a Competent Authority or CAIRMC that facilitates the development, testing, and validation of innovative AI systems for a limited time before placement on the market or putting into service, under regulatory oversight and with specific safeguards.

Free and Open-Source AI Component: An AI system or AI model whose source code, model weights, training methodology, and evaluation results are made publicly available under a licence that permits use, modification, and distribution, whether or not for commercial purposes.

Conformity Assessment: The process of verifying whether an AI system, before its placing on the market or putting into service, satisfies the requirements set out in this Standard.

Post-Market Monitoring: All activities carried out by providers to proactively collect and review experience gained from AI systems placed on the market or put into service, for the purpose of identifying any need to apply corrective or preventive actions.

Qualified AI Risk Professional (QAIRP): An individual who has obtained CAIRMC's professional certification demonstrating competence in AI risk assessment, AI governance, and the application of this Standard.

CAIRMC AI Governance Maturity Model: CAIRMC's five-level maturity framework for assessing an organisation's AI governance readiness, ranging from Level 1 (Ad Hoc) to Level 5 (Optimised).

AI Value Chain: The sequence of activities from AI model training through integration, deployment, and post-market monitoring, including all operators involved at each stage.

Climate Impact Assessment: An evaluation of the energy consumption, carbon emissions, electronic waste, and broader environmental effects of an AI system across its lifecycle, including training, inference, and hardware.

Human Alternative: A meaningful option for a natural person to obtain a decision, service, or outcome from a human decision-maker rather than from an AI system, without undue delay, additional cost, or disadvantage.

Supply Chain Due Diligence: The process by which a deployer or provider that integrates a general-purpose AI model into a downstream AI system verifies the compliance of the upstream model with applicable obligations under this Standard.

AI Agent: An AI system designed to pursue goals or complete tasks with a degree of autonomy, capable of planning, executing multi-step actions, interacting with external tools or services, and adapting its behaviour based on environmental feedback, with limited or no human intervention between steps.

Autonomous AI System: An AI system that operates and makes decisions without concurrent human oversight, where the system's actions have direct effects in the physical or digital world and cannot be reversed or halted by a human operator before execution.

Multi-Agent System (Agent Swarm): A system comprising two or more AI agents that communicate, coordinate, or collaborate to achieve shared or individual goals, including architectures where agents delegate tasks to other agents, negotiate resource allocation, or produce emergent collective behaviours not explicitly programmed by the provider.

Artificial General Intelligence (AGI): A hypothetical AI system that matches or exceeds human cognitive ability across the full range of intellectual tasks, including reasoning, learning, perception, creativity, and social intelligence, without being limited to a narrow domain.

Frontier AI Model: A general-purpose AI model that represents the current boundary of AI capability as measured by standardised benchmarks, compute thresholds, or demonstrated capability in high-risk domains, and whose capabilities are sufficiently novel that their full risk profile cannot be reliably predicted from prior models.

Agentic AI Application: An AI application in which one or more AI agents are orchestrated to carry out a workflow that involves sequential decision-making, tool use, and real-world or digital actions on behalf of a natural person or organisation, including but not limited to code execution, financial transactions, communications, and data retrieval.

Human-in-the-Loop: A system design in which a human decision-maker must approve or authorise each action or decision before the AI system executes it.

Human-on-the-Loop: A system design in which a human overseer monitors the AI system's actions in real time or near-real time and retains the ability to intervene, override, or halt operations, but does not approve each individual action.

Human-out-of-the-Loop: A system design in which the AI system operates without concurrent human oversight and takes actions that are not reviewed by a human before execution. This design is prohibited for Tier 2 AI systems under this Standard unless specific conditions in Article 14 are met.

Caribbean Ethical AI Principles: The set of ethical principles established in Part XVI of this Standard, grounded in Caribbean constitutional values, cultural norms, and the lived experience of Caribbean peoples, that must guide the development, deployment, and governance of AI systems in the region.

Article 4 — AI Literacy

4.1. Providers and deployers of AI systems must take measures to ensure a sufficient level of AI literacy among their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education, and training, as well as the context in which the AI systems are to be used and the persons or groups on which the AI systems are to be used.

4.2. Each Caribbean member state that adopts this Standard shall, within two years of adoption, establish a national AI literacy strategy that addresses:

I. Integration of AI literacy into national education curricula at primary, secondary, and tertiary levels.

II. Professional development programmes for public sector officials who procure, deploy, or oversee AI systems.

III. Public awareness campaigns on AI rights, risks, and responsible use, delivered in languages accessible to the population including English, French, Dutch, Spanish, and relevant Creole languages.

IV. Targeted training for judges, magistrates, and legal professionals who adjudicate matters involving AI systems.

4.3. CAIRMC shall publish AI literacy frameworks, curricula, and training materials suitable for Caribbean contexts and make them freely available to member states.

4.4. Organisations deploying Tier 2 (High-Risk) AI systems must demonstrate that personnel responsible for human oversight of those systems have completed AI literacy training appropriate to their role. Records of such training must be maintained and made available to Competent Authorities on request.

PART II: RISK CLASSIFICATION

Chapter 2: AI Risk Tier System

Article 5 — The Four-Tier Risk Classification

All AI systems subject to this Standard must be classified into one of four AI Risk Tiers. Classification determines the compliance obligations applicable to the provider and deployer.

Risk Tier	Classification	Threshold	Primary Obligation
Tier 1	Unacceptable Risk	AI systems that pose a clear threat to safety, livelihoods, or fundamental rights	Prohibition — may not be placed on market or put into service
Tier 2	High Risk	AI systems deployed in critical sectors or with significant impact on persons	Full compliance: registration, CARA, conformity assessment, transparency, human oversight, insurance
Tier 3	Limited Risk	AI systems with specific transparency risks, including generative AI content	Transparency obligations: disclosure of AI nature, content labelling, deep fake marking
Tier 4	Minimal Risk	All other AI systems	Voluntary codes of conduct; AI literacy recommended

5.2. Where an AI system falls within multiple tiers, the highest applicable tier governs.

5.3. Providers may apply to the relevant Competent Authority or CAIRMC for a reasoned re-classification of an AI system where they can demonstrate that, despite falling within a listed category, the system does not in fact pose a significant risk to health, safety, or fundamental rights. CAIRMC shall publish guidance on the re-classification procedure within six months of this Standard's adoption.

Article 6 — Tier 1: Prohibited AI Practices

The following AI practices are prohibited within the Caribbean region:

1. AI systems that deploy subliminal techniques beyond a person's consciousness, or purposefully manipulative or deceptive techniques, to materially distort behaviour in a manner that causes or is likely to cause physical or psychological harm.
2. AI systems that exploit vulnerabilities of specific groups—including children, persons with disabilities, persons in economic hardship, or elderly persons—in a manner likely to cause harm.
3. Biometric categorisation systems that classify individuals based on sensitive attributes including race, ethnicity, religion, political opinion, or sexual orientation, except for

lawful labelling or filtering of biometric datasets acquired in the context of law enforcement.

4. Real-time remote biometric identification systems in publicly accessible spaces, except where expressly authorised by judicial or equivalent oversight for the prevention of a specific, substantial, and imminent threat to life, and subject to the safeguards set out in Article 6.2.
5. Social scoring systems operated by public authorities or on behalf of public authorities that evaluate or classify natural persons based on social behaviour, inferred personality characteristics, or socioeconomic status, where such scoring leads to detrimental or unfavourable treatment unrelated to the context in which the data was generated.
6. AI systems used to predict criminal offending based solely on profiling, personality traits, or physical characteristics without objective, verifiable indicators of criminal activity.
7. AI systems that create facial recognition databases through untargeted scraping of facial images from the internet or CCTV footage.
8. AI systems used to infer emotions of natural persons in the workplace or educational institutions, except where the system is intended for medical or safety purposes and the affected person has given explicit, informed consent.
9. Autonomous AI agents or multi-agent systems that execute financial transactions, enter into contracts, or take legally binding actions on behalf of natural persons without explicit, informed, per-transaction authorisation from that person.
10. AI systems that autonomously generate and disseminate political content, deepfake political advertising, or synthetic media depicting Caribbean public officials or electoral candidates without clear, prominent disclosure, particularly during election periods as defined by national electoral legislation in each Caribbean member state.
11. The deployment of an artificial general intelligence (AGI) system, or any AI system assessed by CAIRMC or a Competent Authority as exhibiting AGI-equivalent capabilities, without prior authorisation from CAIRMC following a comprehensive safety assessment, an independent red-team evaluation, and publication of a public safety case. This prohibition applies regardless of where the AGI system was developed.

6.2. The exception in paragraph (d) for real-time remote biometric identification is subject to the following cumulative conditions:

I. Authorisation is granted by a judicial authority or an independent administrative authority of the relevant Caribbean member state.

II. The authorisation is limited in time and geographic scope to what is strictly necessary.

III. Use is limited to the targeted search for specific potential victims of crime, the prevention of a specific and imminent threat to life or physical safety, or the detection of a suspect of a criminal offence punishable by imprisonment of four or more years under applicable national law.

IV. A fundamental rights impact assessment has been completed prior to deployment.

V. The relevant Competent Authority is notified within 24 hours and the use is registered in the Caribbean AI Registry.

Article 7 — Tier 2: High-Risk AI Systems

7.1. The following categories of AI systems are classified as high-risk under this Standard:

7.1.1 — Critical Infrastructure

- AI systems used in the management and operation of electrical grids, water treatment, telecommunications networks, transportation systems, and port or airport operations.
- AI systems embedded in financial market infrastructure including payment clearing, settlement systems, and systemic financial institution operations.
- AI components of digital infrastructure providing essential internet, cloud computing, or data centre services.

7.1.2 — Education and Employment

- AI systems used to determine access to educational institutions, evaluate academic performance, or certify professional qualifications.
- AI systems used in recruitment, selection, promotion, task allocation, performance evaluation, or termination of employment relationships.
- AI systems used to monitor or evaluate the performance of workers, including through emotion recognition or activity tracking.

7.1.3 — Essential Private Services

- AI systems used in the assessment of creditworthiness or establishment of credit scores, including those deployed by commercial banks, credit unions, and microfinance institutions.
- AI systems used in insurance risk assessment, underwriting, pricing, or claims processing that affect policyholders' access to coverage or premium levels.
- AI systems used to evaluate eligibility for private housing, rental, or mortgage applications.

7.1.4 — Public Services and Benefits

- AI systems used by public authorities to determine eligibility for and access to government benefits, social services, healthcare, or housing assistance.
- AI systems used in the administration of justice, including sentencing, bail, and parole decisions.
- AI systems used in border control, immigration status determination, visa processing, or asylum applications.
- AI systems used in the dispatch or prioritisation of emergency services.

7.1.5 — Healthcare

- AI systems used as medical devices or for clinical decision support in diagnosis, treatment recommendation, or patient monitoring.
- AI systems used in the management of patient records where output directly informs clinical decisions.
- AI systems used in pharmaceutical research, drug interactions, or public health surveillance that influence decisions affecting individual or population health.

7.1.6 — Law Enforcement

- AI systems used by law enforcement authorities for individual risk assessment, including recidivism risk.
- AI systems used as polygraphs or to detect deception.
- Post-remote biometric identification systems used by law enforcement.
- AI systems used for crime analytics regarding natural persons, allowing law enforcement to search or analyse large and complex datasets to identify unknown patterns or discover hidden relationships.

7.1.7 — Migration, Asylum, and Border Control

- AI systems used to assess security risks posed by natural persons entering the Caribbean region.
- AI systems used to assist Competent Authorities in the examination of applications for asylum, visa, or residence permits.
- AI systems used for the detection, recognition, or identification of natural persons in the context of migration management.

7.1.8 — Democratic Processes

- AI systems intended to influence the outcome of an election or referendum, or the voting behaviour of natural persons in the exercise of their right to vote, including AI systems used for micro-targeting of political messages based on psychological profiling.

7.1.9 — AI Agents and Autonomous Systems

- AI agents that autonomously execute tasks with real-world consequences, including code execution on production systems, financial transactions, procurement decisions, or communications sent on behalf of an organisation or natural person.
- Multi-agent systems (agent swarms) deployed in any Tier 2 sector listed in this Article, regardless of whether any individual agent in the system would independently qualify as high-risk.
- AI agents that interact with members of the public on behalf of a government agency, financial institution, healthcare provider, or educational institution, where the interaction could reasonably be mistaken for communication with a human official.

– Agentic AI applications that chain together multiple AI models, tools, or data sources to execute workflows involving personal data, financial data, health data, or data protected under applicable Caribbean data protection legislation.

7.2. An AI system referred to in paragraph 7.1 is not considered high-risk if it does not pose a significant risk of harm to the health, safety, or fundamental rights of natural persons, including by not materially influencing the outcome of decision-making. The provider bears the burden of demonstrating this. A provider that considers its AI system is not high-risk under this exception must document its assessment and notify the relevant Competent Authority before placing the system on the market.

Article 8 — Tier 3: Limited Risk AI Systems

The following AI systems carry limited risk and are subject to transparency obligations set out in Part V:

1. Conversational AI systems (chatbots, virtual assistants) that interact with natural persons and could be mistaken for a human by a reasonable user.
2. AI systems that generate or manipulate synthetic audio, video, image, or text content (generative AI), including deep fakes, where such content is presented to a recipient.
3. AI systems used for emotion recognition or biometric categorisation that do not fall within Tier 1 or Tier 2.
4. AI systems that generate or manipulate text published for the purpose of informing the public on matters of public interest, unless the text is subject to human editorial review and the human has editorial responsibility for the published content.

Article 9 — Tier 4: Minimal Risk and Voluntary Codes of Conduct

9.1. AI systems that do not fall within Tiers 1, 2, or 3 are classified as Tier 4 (Minimal Risk). No mandatory obligations apply to Tier 4 AI systems under this Standard.

9.2. CAIRMC and national Competent Authorities shall encourage and facilitate the drawing up of voluntary codes of conduct intended to foster the application of requirements set out for Tier 2 systems on a voluntary basis to Tier 4 AI systems, including in relation to:

I. Environmental sustainability, including energy efficiency and resource consumption.

II. AI literacy for persons dealing with AI.

III. Inclusive design and accessibility for persons with disabilities.

IV. Diversity, non-discrimination, and fairness in the design and use of AI.

V. Stakeholder participation in the design and development of AI systems.

9.3. CAIRMC shall maintain a public register of organisations that have voluntarily adopted codes of conduct under this Article.

PART III: OBLIGATIONS FOR HIGH-RISK AI SYSTEMS

Chapter 3: Provider Obligations

Article 10 — Quality Management Systems

Providers of high-risk AI systems must establish, implement, and maintain a quality management system that addresses at minimum:

1. A documented AI risk management policy aligned to ISO/IEC 42001:2023 and the NIST AI RMF GOVERN function.
2. Procedures for the design, development, and validation of AI systems including data governance protocols consistent with applicable Caribbean data protection legislation.
3. Processes for post-market monitoring, incident reporting, and corrective action.
4. Internal controls aligned to the COSO Enterprise Risk Management Framework (2017) covering risk identification, assessment, response, and monitoring for AI-related risks.
5. A strategy for regulatory compliance, including procedures for conformity assessments and registration in the Caribbean AI Registry.
6. Resource management procedures, including specifications for the competence, training, and AI literacy of staff involved in AI system development and oversight.
7. An accountability framework specifying the natural person or persons within the provider's organisation with overall responsibility for AI governance.
8. Data management protocols, including data collection, storage, validation, labelling, and retention procedures.
9. A record-keeping system to maintain documentation generated under this Standard for a period of not less than ten (10) years after the AI system is placed on the market or put into service.

Article 11 — Data and Data Governance

11.1. Training, validation, and testing data used for high-risk AI systems must meet the following requirements:

1. Data governance practices must comply with all applicable national data protection legislation in the Caribbean, including the Jamaica Data Protection Act 2020, the Trinidad and Tobago Data Protection Act 2011, the Barbados Data Protection Act 2019, and the OECS Model Data Protection Bill where enacted.
2. Training datasets must be subject to appropriate data quality protocols addressing representativeness, completeness, and freedom from discriminatory bias, with specific attention to the representation of Caribbean demographic groups.
3. Data collection, processing, and storage must be lawful under applicable national law, consistent with the data minimisation and purpose limitation principles of the GDPR where Caribbean operators process data of persons in GDPR-covered territories.

4. Data lineage must be documented to permit audit and traceability, using metadata standards consistent with ISO 8000 (Data Quality).

11.2. Providers must conduct and document a bias assessment of training data, examining at minimum racial, ethnic, gender, age, socioeconomic, and geographic bias. Where bias is detected, providers must document the steps taken to mitigate it and the residual bias remaining.

11.3. Where training data includes personal data of Caribbean nationals or residents, the provider must maintain a record of the lawful basis for processing, the categories of data subjects, and the retention period.

Article 12 — Technical Documentation

Before placing a high-risk AI system on the Caribbean market, providers must prepare technical documentation that includes:

1. A general description of the AI system, its intended purpose, the provider's identity, and the version of the system.
2. A detailed description of the elements of the AI system, including the system's design architecture, algorithms, computational logic, and data processing mechanisms.
3. A description of the training methodology and datasets used, including data provenance and representativeness assessments.
4. Assessment of known and foreseeable risks, conducted in accordance with ISO 31000:2018 risk assessment requirements.
5. The measures taken to address identified risks, including accuracy, robustness, and cybersecurity measures consistent with ISO/IEC 27001:2022.
6. Results of all testing conducted prior to deployment, including test datasets, evaluation metrics, and performance benchmarks disaggregated by relevant demographic groups.
7. A completed Caribbean AI Risk Assessment (CARA) as specified in Part IV of this Standard.
8. A description of the system for post-market monitoring and the plan for updates and corrective action.
9. A climate impact assessment as specified in Article 62 of this Standard.
10. Evidence of the conformity assessment conducted under Part VIII of this Standard.

Article 13 — Transparency and Provision of Information

High-risk AI systems must be accompanied by instructions for use that provide deployers with clear information on:

1. The identity and contact details of the provider and, where applicable, the authorised representative.

2. The capabilities and limitations of the AI system, including its level of accuracy, robustness, and cybersecurity, along with any known or foreseeable circumstances that may lead to risks.
3. The data the AI system has been trained on and the extent to which it may perform differently across demographic groups, with specific reference to Caribbean populations.
4. Any circumstances in which the AI system should not be used or requires human oversight, including foreseeable misuse scenarios.
5. Technical specifications for input data and any requirements for the data quality needed in operation.
6. Details of post-market monitoring requirements and the procedure for reporting malfunctions to the provider.
7. The human oversight measures built into the system and the qualifications or training recommended for persons exercising oversight.
8. The expected lifetime of the system and any planned maintenance, update, or decommissioning schedule.

Article 14 — Human Oversight

14.1. High-risk AI systems must be designed and developed to allow effective human oversight during their operation. Providers must ensure that AI systems include:

I. The ability for natural persons assigned to oversight to fully understand the AI system's capabilities, limitations, and known failure modes.

II. Clear mechanisms for natural persons to intervene in, override, or halt the operation of the AI system at any time.

III. The ability to correctly interpret the AI system's output, including clear confidence indicators and explanations of the factors contributing to decisions.

IV. The ability to decide, in any particular case, not to use the AI system or to disregard, override, or reverse a decision by the AI system.

V. Automatic escalation mechanisms that alert human overseers when the AI system encounters inputs outside its validated operating conditions or when confidence levels fall below defined thresholds.

14.2. For AI systems making decisions about natural persons in the areas listed in Article 7.1, the level of human oversight must be proportionate to the severity and reversibility of the decision. Decisions that are both severe and irreversible require human approval before execution.

Article 15 — Accuracy, Robustness, and Cybersecurity

15.1. High-risk AI systems must achieve appropriate levels of accuracy, robustness, and cybersecurity consistent with their intended purpose. These levels must be declared in the technical documentation and verified through testing.

15.2. Accuracy levels must be measured and documented with respect to the AI system's performance across Caribbean demographic groups, including but not limited to racial, ethnic, gender, age, and socioeconomic dimensions. Where accuracy varies materially across groups, the provider must disclose this variation and the measures taken to address it.

15.3. High-risk AI systems must be resilient against errors, faults, and inconsistencies that may occur within the system or the environment in which the system operates. Technical redundancy solutions, including backup and fail-safe plans, must be in place.

15.4. High-risk AI systems must be resilient against attempts by unauthorised third parties to alter their use, outputs, or performance by exploiting system vulnerabilities. Cybersecurity measures must be proportionate to the risk and consistent with ISO/IEC 27001:2022 and applicable Basel Committee guidance for AI systems in financial services.

15.5. Providers must conduct adversarial testing appropriate to the risk level, including testing against data poisoning, model evasion, model extraction, and prompt injection attacks where applicable.

Article 16 — Automatic Logging

16.1. High-risk AI systems must be designed with automatic logging capabilities that record:

I. The date and time of each use of the system and the identity of the deployer or natural person activating the system.

II. The input data provided to the system for each use, or a reference sufficient to identify that input data.

III. The output or decision produced by the system.

IV. Any instance in which a human overseer intervened to override or reverse the system's output.

V. Any instance in which the system's automatic escalation mechanism was triggered.

16.2. Logs must be retained for a period appropriate to the intended purpose of the high-risk AI system, and in any event for not less than three (3) years. Logs must be accessible to the relevant Competent Authority upon request.

Chapter 4: Deployer Obligations

Article 17 — Responsibilities of Deployers

Deployers of high-risk AI systems operating in the Caribbean region must:

1. Verify that the AI system they deploy is registered in the Caribbean AI Registry as required under Article 41 of this Standard.
2. Implement the human oversight measures specified by the provider in the system's technical documentation and instructions for use.

3. Ensure that input data used in operation is relevant, complete, sufficiently representative, and appropriate for the system's intended purpose.
4. Inform the relevant Competent Authority of any serious incident within seventy-two (72) hours of becoming aware of it, and report any lesser malfunction within thirty (30) days.
5. Maintain records of the AI system's operation and output for a period of not less than three (3) years, consistent with data retention obligations under applicable Caribbean data protection legislation.
6. Where the deployer processes personal data in operating the AI system, comply with all obligations under applicable national data protection legislation.
7. Suspend use of the AI system where they have reason to believe it presents a risk to health, safety, or fundamental rights, and notify the provider and Competent Authority.
8. Ensure that natural persons affected by the AI system's decisions are informed that they have been subject to AI-assisted decision-making and of their right to a human alternative where applicable under Article 48.

Article 18 — Fundamental Rights Impact Assessment for Public Sector Deployers

18.1. Public authorities deploying high-risk AI systems must conduct a fundamental rights impact assessment prior to deployment. The assessment must evaluate the potential impact of the AI system on:

I. The right to non-discrimination and equal treatment under national constitutional provisions and international human rights instruments.

II. The right to privacy and data protection under applicable national legislation.

III. Access to justice and due process where the AI system informs or replaces administrative or judicial decision-making.

IV. Economic rights and access to services, with specific attention to vulnerable populations in Caribbean member states including low-income households, the elderly, persons with disabilities, and rural communities.

V. Children's rights, including the best interests of the child as a primary consideration.

VI. Cultural rights and community identity, with attention to the diverse cultural heritage of the Caribbean.

18.2. The impact assessment must be made publicly available prior to deployment. CAIRMC will publish a standardised template for this assessment.

18.3. Where the impact assessment identifies a high risk to fundamental rights, the deploying authority must demonstrate the measures taken to mitigate that risk and explain why AI deployment remains justified despite the identified risks.

Article 19 — Importer Obligations

19.1. Before placing a high-risk AI system on the Caribbean market, importers must ensure that:

I. The provider of the AI system has carried out the conformity assessment procedure required under Part VIII.

II. The provider has drawn up the technical documentation required under Article 12.

III. The AI system bears the required conformity marking and is accompanied by the required documentation and instructions for use.

IV. The provider has appointed an authorised representative in the Caribbean region where required under Article 21.

19.2. Where an importer considers or has reason to consider that a high-risk AI system is not in conformity with this Standard, the importer must not place that system on the market until it has been brought into conformity and must inform the provider and the relevant Competent Authority.

19.3. Importers must indicate their name, registered trade name or trademark, and contact address on the AI system or its documentation.

Article 20 — Distributor Obligations

20.1. Before making a high-risk AI system available on the Caribbean market, distributors must verify that the system bears the required conformity marking and is accompanied by the documentation and instructions for use required under this Standard.

20.2. Where a distributor considers or has reason to consider that a high-risk AI system is not in conformity with this Standard, the distributor must not make that system available until it has been brought into conformity, and must inform the provider or importer and the relevant Competent Authority.

Article 21 — Authorised Representatives

21.1. Before making a high-risk AI system available on the Caribbean market, providers established outside the Caribbean region must, by written mandate, appoint an authorised representative established in the Caribbean.

21.2. The authorised representative shall perform the tasks specified in the mandate received from the provider, which must as a minimum include:

I. Keeping a copy of the conformity assessment documentation and technical documentation available for national Competent Authorities.

II. Providing a Competent Authority, upon reasoned request, with all information and documentation necessary to demonstrate conformity.

III. Cooperating with Competent Authorities on any action they take in relation to the AI system.

Article 22 — Obligations Along the AI Value Chain

22.1. Any distributor, importer, deployer, or other third party is considered a provider of a high-risk AI system for the purposes of this Standard and is subject to the provider obligations if that third party:

I. Puts its own name or trademark on a high-risk AI system already placed on the market or put into service.

II. Makes a substantial modification to a high-risk AI system that is already placed on the market or put into service.

III. Modifies the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk, in a manner that makes it high-risk under Article 7.

22.2. Where the circumstances described in paragraph 22.1 occur, the original provider is no longer considered the provider for purposes of the relevant AI system, subject to appropriate cooperation obligations and information-sharing between the original and new provider.

PART IV: CARIBBEAN AI RISK ASSESSMENT (CARA)

Chapter 5: The CARA Methodology

Article 23 — Purpose and Scope of CARA

The Caribbean AI Risk Assessment (CARA) is CAIRMC's proprietary assessment methodology for evaluating AI systems across four risk dimensions in the Caribbean context. CARA is mandatory for all Tier 2 (High-Risk) AI systems and recommended for Tier 3 systems. CARA results form part of the technical documentation required under Article 12.

Article 24 — CARA Assessment Dimensions

A CARA evaluation addresses the following four dimensions:

Dimension	Key Assessment Areas
Technical Risk	System accuracy and reliability; training data quality and bias; cybersecurity and resilience; explainability and interpretability; performance across Caribbean demographic groups; failure modes and adversarial robustness; model drift monitoring
Ethical Risk	Fairness and non-discrimination; privacy and dignity; transparency to affected persons; alignment with Caribbean cultural values and norms; consent and autonomy; potential for manipulation or deception; impact on children and vulnerable groups
Legal Risk	Compliance with applicable Caribbean data protection legislation; alignment with EU AI Act for operators with EU nexus; intellectual property rights including copyright in training data; consumer protection; sector-specific regulation; liability allocation; cross-border regulatory obligations
Societal Risk	Impact on Caribbean labour markets and livelihoods; access to essential services; digital divide and inclusion; environmental and climate impact; impact on public trust in institutions; effects on democratic processes; cultural and linguistic impacts; concentration of economic power

Article 25 — CARA Process

The CARA process comprises the following stages:

I. Scope definition: identification of the AI system, its intended purpose, affected persons, operating environment, and the Caribbean jurisdictions in which it will operate.

II. Risk identification: mapping of potential harms across the four CARA dimensions using the Caribbean AI Risk Taxonomy (Annex I).

III. Risk assessment: evaluation of likelihood and severity of identified risks, applying COSO ERM risk quantification principles and CAIRMC's published risk scoring methodology.

IV. Control identification: documentation of existing technical, operational, and governance controls and their effectiveness.

V. Residual risk determination: assessment of risk remaining after controls, with comparison against the organisation's AI risk appetite and CAIRMC's published residual risk thresholds.

VI. Remediation planning: development of time-bound actions to reduce residual risk to acceptable levels, with identified owners and reporting milestones.

VII. Independent review: for Tier 2 systems, the CARA must be reviewed by a Qualified AI Risk Professional (QAIRP) who was not involved in the system's development.

VIII. CAIRMC registration: submission of the completed CARA to CAIRMC for registration in the Caribbean AI Registry and, for Tier 2 systems, third-party verification.

CARA assessments must be updated whenever a substantial modification is made to the AI system, when the operating context changes materially, or at intervals of not more than two (2) years, whichever comes first.

PART V: TRANSPARENCY AND GENERAL-PURPOSE AI

Chapter 6: Transparency Obligations

Article 26 — Transparency for Limited Risk AI Systems

26.1. Providers and deployers of Tier 3 (Limited Risk) AI systems must ensure that:

I. Natural persons who interact with a conversational AI system are informed clearly and at the earliest opportunity that they are interacting with an AI system, unless the AI nature is evident from the circumstances.

II. Synthetic content generated by AI systems—including text, images, audio, and video—is labelled as AI-generated in a clear and prominent manner accessible to the recipient. Machine-readable metadata must also be embedded in the content where technically feasible.

III. Persons subject to AI-based emotion recognition or biometric categorisation are informed of such assessment before or at the time of the assessment, unless it is incompatible with a lawful purpose established by national legislation.

IV. Labels and disclosures required under this Article must be presented in a language accessible to the intended recipient, taking into account the multilingual context of the Caribbean including English, French, Dutch, Spanish, and relevant Creole languages.

Article 27 — Deep Fake Provisions

27.1. Providers of AI systems that generate or manipulate image, audio, or video content that appreciably resembles existing persons, objects, places, or events and would falsely appear to a person to be authentic (deep fakes) must:

I. Label the content as artificially generated or manipulated, using both a visible disclosure and machine-readable metadata.

II. Deploy technical measures, where technically feasible, to watermark or fingerprint the output in a manner that is robust against common editing and format conversion.

27.2. Deployers who publish or distribute deep fake content must disclose that the content has been artificially generated or manipulated, in a manner that is clear, prominent, and proximate to the content.

27.3. The obligations in paragraphs 27.1 and 27.2 do not apply where the use is part of a manifestly artistic, satirical, or fictional work that does not present the content as factual, provided the work is clearly identified as such.

Chapter 7: General-Purpose AI Systems

Article 28 — Obligations for GPAI System Providers

28.1. Providers of general-purpose AI systems that are made available for use in the Caribbean region must:

1. Maintain and make available technical documentation describing the model's training process, capabilities, limitations, and known risks, sufficient to allow downstream providers to understand and comply with their obligations under this Standard.
2. Comply with applicable copyright and data protection law when processing Caribbean-origin content in training, and maintain a sufficiently detailed summary of training data sources.
3. Establish a policy for respecting copyright and related rights, including through the identification and compliance with reservations of rights expressed by rights holders.
4. Publish a sufficiently detailed summary of training data used, following a CAIRMC-provided template, to support transparency and trust without requiring disclosure of trade secrets.
5. Provide downstream AI system providers with sufficient information and documentation to enable those providers to comply with their own obligations under this Standard, including for conducting CARA assessments.

Article 29 — GPAI Systems with Systemic Risk

29.1. A general-purpose AI system presents a systemic risk where:

I. It has high-impact capabilities assessed on the basis of appropriate technical tools and methodologies, including through model evaluation and benchmarking.

II. It was trained using a total computing power of more than 10^{25} floating point operations, measured in FP32 equivalents or equivalent computation.

III. CAIRMC or a national Competent Authority designates it as presenting systemic risk based on criteria including: the number of registered users in the Caribbean, the degree to which it is integrated into critical infrastructure, the scale of its use in high-risk applications, or evidence of prior serious incidents.

29.2. Providers of GPAI systems with systemic risk must, in addition to the obligations in Article 28:

1. Conduct and publish an adversarial testing report (red-teaming) before deployment in the Caribbean region, covering at minimum: dangerous content generation, biosecurity, cybersecurity, radiological and nuclear risks, and discrimination.
2. Assess and mitigate systemic risks at the Caribbean regional level, including foreseeable risks of use in the Caribbean's specific economic and social context.
3. Track, document, and report to CAIRMC any serious incidents involving the system in the Caribbean, without undue delay.
4. Ensure adequate cybersecurity protection for the model and its physical infrastructure.

5. Make available to CAIRMC, upon request, model weights, training data summaries, and evaluation results for audit purposes, subject to the confidentiality protections in Article 52.

Article 30 — Codes of Practice for GPAI

30.1. CAIRMC shall facilitate the drawing up of codes of practice at the regional level to contribute to the proper application of Articles 28 and 29, taking into account international approaches.

30.2. GPAI system providers may rely on adherence to a code of practice to demonstrate compliance with the corresponding obligations. Where a provider does not adhere to a code of practice, it must demonstrate alternative adequate means of compliance.

PART VI: CONFORMITY ASSESSMENT AND CERTIFICATION

Chapter 8: Conformity Assessment

Article 31 — Conformity Assessment for High-Risk AI Systems

31.1. Before placing a high-risk AI system on the Caribbean market or putting it into service, the provider must carry out a conformity assessment to demonstrate that the system meets the requirements of this Standard.

31.2. For high-risk AI systems listed in Article 7.1.4 (public services and benefits) and Article 7.1.6 (law enforcement), the conformity assessment must be carried out by a third-party conformity assessment body accredited under Article 33.

31.3. For all other high-risk AI systems, the provider may carry out the conformity assessment through internal procedures, provided that the provider's quality management system has been verified by a conformity assessment body within the preceding three years.

31.4. Where a high-risk AI system is substantially modified after its initial conformity assessment, a new conformity assessment must be carried out with respect to the modification.

Article 32 — Caribbean AI Conformity Mark

32.1. CAIRMC shall establish a Caribbean AI Conformity Mark (the "CAI Mark") to be affixed to high-risk AI systems that have undergone a successful conformity assessment.

32.2. The CAI Mark shall be affixed visibly, legibly, and indelibly to the AI system or its documentation. Where that is not possible due to the nature of the system, it must be affixed to the accompanying documentation and instructions for use.

32.3. CAIRMC shall publish detailed specifications for the design, format, and affixing of the CAI Mark within one year of this Standard's adoption.

32.4. The CAI Mark is without prejudice to conformity marks required under sector-specific Caribbean or international regulation.

Article 33 — Conformity Assessment Bodies

33.1. Conformity assessment bodies must be accredited by a national accreditation body in a Caribbean member state, or by CAIRMC where no national accreditation body exists, to perform conformity assessments under this Standard.

33.2. To be accredited, a conformity assessment body must demonstrate:

I. Independence from AI system providers and deployers, with no conflicts of interest.

II. Sufficient technical competence, including staff with expertise in AI systems, data governance, risk management, and the relevant sector.

III. Organisational integrity, including adequate professional liability insurance.

IV. Compliance with ISO/IEC 17065 (Conformity Assessment) or equivalent standards.

33.3. CAIRMC shall maintain a public register of accredited conformity assessment bodies and facilitate mutual recognition of conformity assessments across member states.

Chapter 9: QAIRP Certification

Article 34 — The Qualified AI Risk Professional Programme

34.1. CAIRMC administers the Qualified AI Risk Professional (QAIRP) certification programme, which certifies individuals as competent to:

I. Conduct and review Caribbean AI Risk Assessments (CARA).

II. Advise organisations on compliance with this Standard.

III. Serve as independent reviewers for conformity assessment purposes.

IV. Support national Competent Authorities in supervisory and enforcement activities.

34.2. CAIRMC shall publish the QAIRP certification standards, examination requirements, continuing professional development obligations, and ethical code within one year of this Standard's adoption.

34.3. CAIRMC shall maintain a public register of certified QAIRPs.

PART VII: GOVERNANCE AND ENFORCEMENT

Chapter 10: The Caribbean AI Registry

Article 35 — Establishment of the Caribbean AI Registry

35.1. CAIRMC shall establish and maintain the Caribbean AI Registry, a publicly accessible database of AI systems deployed in the Caribbean region. The Registry serves as the primary transparency instrument of this Standard.

35.2. The Registry shall include separate sections for:

I. High-risk AI systems registered by providers.

II. High-risk AI systems registered by public sector deployers.

III. General-purpose AI systems with systemic risk.

IV. Regulatory sandbox participants.

35.3. The Registry must be accessible free of charge through a user-friendly web interface and must support searches by provider, sector, risk tier, jurisdiction, and CARA residual risk rating.

Article 36 — Registration Obligations

36.1. Prior to deployment of any Tier 2 (High-Risk) AI system, the provider or, where applicable, the authorised representative must register the system in the Caribbean AI Registry. Registration requires submission of:

1. The provider's identity, contact information, and authorised representative details.
2. A summary of the AI system's intended purpose, the sectors in which it will operate, and the Caribbean jurisdictions of deployment.
3. The AI Risk Tier classification and the basis for that classification.
4. A summary of the completed CARA, including overall and dimension-level residual risk ratings.
5. A summary of the conformity assessment conducted and the identity of the conformity assessment body where applicable.
6. The human oversight measures in place and the qualifications of oversight personnel.
7. A contact point for queries from affected persons and Competent Authorities.
8. The status of the system (active, suspended, or withdrawn from market).

36.2. Deployers in the public sector must separately register their use of high-risk AI systems, including the specific deployment context, the fundamental rights impact assessment, and the designated human oversight officer.

Chapter 11: Competent Authorities and CAIRMC's Role

Article 37 — National Competent Authorities

37.1. Each Caribbean member state that adopts this Standard shall designate one or more national Competent Authorities responsible for supervision and enforcement. Where a member state has an existing data protection authority or digital economy regulator, that body may serve as the national Competent Authority subject to appropriate resourcing and mandate expansion.

37.2. National Competent Authorities shall have the power to:

1. Access the Caribbean AI Registry and all documentation submitted by providers and deployers.
2. Conduct investigations and audits of AI systems deployed within their jurisdiction, including on-site inspections.
3. Request and obtain access to logs, technical documentation, and source code where necessary for enforcement, subject to the confidentiality provisions of Article 52.
4. Issue compliance orders, warnings, and corrective action notices.
5. Impose administrative sanctions in accordance with Article 44.
6. Order the withdrawal, recall, or disabling of an AI system that poses a risk to health, safety, or fundamental rights.

37.3. National Competent Authorities must be provided with adequate financial and human resources to fulfil their functions. CAIRMC shall publish recommended minimum resourcing benchmarks.

Article 38 — CAIRMC as Regional Coordinating Body

CAIRMC shall serve as the regional coordinating body for implementation of this Standard. CAIRMC's functions include:

1. Maintaining and operating the Caribbean AI Registry and the CARA methodology.
2. Publishing guidance, codes of practice, interpretive notices, and model templates to support national Competent Authorities and obligated entities.
3. Facilitating mutual recognition of AI conformity assessments, QAIRP certifications, and regulatory sandbox outcomes across member states.
4. Representing the Caribbean region in international AI governance forums, including within CARICOM, before global standards bodies, and in bilateral and multilateral AI governance negotiations.
5. Administering the QAIRP certification programme.
6. Establishing and overseeing the Caribbean AI Advisory Forum and the Caribbean AI Scientific Panel as described in Articles 39 and 40.
7. Publishing an annual State of AI Risk in the Caribbean report summarising registry data, incident trends, compliance rates, and emerging risks.

8. Managing the Caribbean AI Governance Support Fund.

Article 39 — Caribbean AI Advisory Forum

39.1. CAIRMC shall establish a Caribbean AI Advisory Forum comprising representatives of:

1. National Competent Authorities from each adopting member state.
2. Industry associations and technology companies operating in the Caribbean.
3. Civil society organisations, including consumer protection and digital rights groups.
4. Academic and research institutions.
5. Caribbean financial regulatory bodies and insurance supervisors.
6. Representatives of affected communities and marginalised groups.

39.2. The Advisory Forum shall advise CAIRMC on the implementation and evolution of this Standard, provide input on draft guidance and codes of practice, and serve as a channel for stakeholder feedback. The Forum shall meet at least twice per year.

Article 40 — Caribbean AI Scientific Panel

40.1. CAIRMC shall convene a Caribbean AI Scientific Panel of independent experts in AI technology, AI safety, data science, ethics, law, and relevant domain areas.

40.2. The Scientific Panel shall:

1. Advise CAIRMC on the classification of GPAI models with systemic risk.
2. Support the development and updating of the CARA methodology and Caribbean AI Risk Taxonomy.
3. Provide technical opinions on emerging AI risks and capabilities.
4. Assist with the design of regulatory sandbox programmes and evaluation criteria.
5. Review and advise on the 10^{25} FLOPS threshold for systemic risk designation and recommend adjustments as technology evolves.

Chapter 12: Market Surveillance and Post-Market Monitoring

Article 41 — Post-Market Monitoring by Providers

41.1. Providers of high-risk AI systems must establish and document a post-market monitoring system proportionate to the nature of the AI system and the risks it presents.

41.2. The post-market monitoring system must actively and systematically collect, document, and analyse data on the AI system's performance throughout its lifetime, including:

1. Performance metrics tracked against the levels declared in the technical documentation.
2. Feedback from deployers and end users.

3. Incidents, near-misses, and complaints.
4. Changes in the operating environment that may affect the system's risk profile.
5. Evidence of bias, drift, or degradation in accuracy over time, particularly across Caribbean demographic groups.

41.3. Where post-market monitoring reveals that the AI system presents a risk not anticipated in the initial risk assessment, the provider must take corrective action, update the technical documentation and CARA, and notify the relevant Competent Authority.

Article 42 — Market Surveillance by Competent Authorities

42.1. National Competent Authorities shall conduct market surveillance activities to ensure that AI systems on the Caribbean market comply with this Standard.

42.2. Market surveillance shall include:

1. Reviewing information in the Caribbean AI Registry.
2. Conducting random and risk-based inspections and audits.
3. Testing AI systems, including through the use of simulated data and test purchases.
4. Investigating complaints received from affected persons, deployers, and other stakeholders.
5. Monitoring serious incident reports.

42.3. Where a Competent Authority finds that an AI system does not comply with this Standard, it shall require the provider to bring the system into compliance within a reasonable timeframe. Where non-compliance persists or where the system presents a serious risk, the Competent Authority may order the withdrawal or recall of the system and impose sanctions under Article 44.

Article 43 — Serious Incident Reporting

43.1. Providers and deployers of high-risk AI systems must report serious incidents to the relevant national Competent Authority and to CAIRMC:

1. Within twenty-four (24) hours: an initial notification where the incident involves death, serious injury, or serious and irreversible disruption to critical infrastructure.
2. Within seventy-two (72) hours: a detailed report for all other serious incidents, including the cause, the persons affected, and the corrective actions taken or planned.

43.2. CAIRMC shall publish a standardised serious incident reporting template and maintain a regional serious incident database, with anonymised summaries published annually as part of the State of AI Risk in the Caribbean report.

Chapter 13: Sanctions and Remedies

Article 44 — Administrative Sanctions

44.1. Member states adopting this Standard shall provide for administrative sanctions commensurate with the following guidance:

Violation Category	Recommended Maximum Penalty
Deployment of a Tier 1 (Prohibited) AI system	Up to USD $35 million or 7% of global annual turnover (whichever is greater)
Non-compliance with Tier 2 (High-Risk) obligations	Up to USD $15 million or 3% of global annual turnover (whichever is greater)
Non-compliance with GPAI obligations (Articles 28–30)	Up to USD $15 million or 3% of global annual turnover (whichever is greater)
Failure to report a serious incident within required timeframes	Up to USD $10 million or 2% of global annual turnover (whichever is greater)
Provision of incorrect, incomplete, or misleading information to a Competent Authority or in the Caribbean AI Registry	Up to USD $7.5 million or 1.5% of global annual turnover (whichever is greater)
Non-compliance with transparency obligations (Tier 3)	Up to USD $2 million or 0.5% of global annual turnover (whichever is greater)

44.2. Sanctions must be effective, proportionate, and dissuasive. In setting sanctions, Competent Authorities must consider:

1. The nature, gravity, and duration of the infringement and its consequences.
2. Whether the provider or deployer has taken corrective action.
3. Previous infringements by the same operator.
4. The size and market share of the operator, with specific accommodation for micro, small, and medium enterprises and local Caribbean businesses.
5. Any other aggravating or mitigating circumstances, including financial benefit gained from the infringement.

44.3. For micro, small, and medium enterprises, Competent Authorities shall apply proportionate sanctions that do not threaten the viability of the enterprise. CAIRMC shall publish guidance on proportionate sanctions for SMEs.

Article 45 — Periodic Penalty Payments

National Competent Authorities may impose periodic penalty payments for ongoing non-compliance, at a daily rate of up to 1% of the average daily worldwide turnover of the preceding financial year, for each day that the non-compliance continues following the date set in the compliance order.

Article 46 — Individual Rights and Remedies

46.1. Any person who considers they have been adversely affected by an AI system subject to this Standard has the right to:

1. Lodge a complaint with the relevant national Competent Authority, which must acknowledge receipt within fourteen (14) days and provide a substantive response within ninety (90) days.
2. Receive a clear, meaningful, and personalised explanation of any decision taken by a Tier 2 AI system that significantly affects their interests, including the main parameters of the decision and the role of AI in reaching it.
3. Seek review of AI-assisted decisions made by public authorities through existing administrative review and judicial review mechanisms.
4. Request the intervention of a human decision-maker to review any AI-assisted decision that significantly affects the person's legal rights or economic interests.

46.2. The right to explanation under this Article applies regardless of whether the AI system has produced a legally binding decision and regardless of whether the person's data was processed as part of the decision.

Article 47 — Whistleblower Protections

47.1. Persons who report breaches of this Standard to a Competent Authority or to CAIRMC shall be protected from retaliation in accordance with applicable national whistleblower protection legislation.

47.2. Where a Caribbean member state does not have whistleblower protection legislation, CAIRMC shall encourage the member state to adopt such legislation and shall, in the interim, establish a confidential reporting mechanism that protects the identity of the reporting person.

Article 48 — Right to a Human Alternative

48.1. In the following circumstances, a natural person has the right to obtain a decision, service, or outcome from a human decision-maker rather than from an AI system, without undue delay, additional cost, or disadvantage:

I. Decisions by public authorities regarding access to government benefits, social services, healthcare, housing, or other essential services.

II. Decisions significantly affecting a person's legal rights, including immigration, criminal justice, employment, and education decisions.

III. Credit decisions, insurance decisions, or other financial service decisions made by AI systems where the person requests human review.

48.2. Deployers of AI systems in the areas listed in paragraph 48.1 must clearly inform affected persons of their right to a human alternative and provide a simple, accessible mechanism to exercise that right.

48.3. The human decision-maker exercising the human alternative must have the authority, competence, and access to information necessary to make an independent decision.

PART VIII: REGULATORY SANDBOXES AND INNOVATION

Chapter 14: AI Regulatory Sandboxes

Article 49 — Establishment of Regulatory Sandboxes

49.1. National Competent Authorities, individually or jointly with CAIRMC, may establish AI regulatory sandboxes to facilitate the development, testing, and validation of innovative AI systems before their placement on the Caribbean market or putting into service.

49.2. Regulatory sandboxes shall provide a controlled environment with regulatory oversight and specific safeguards, allowing participants to:

I. Test AI systems that do not yet fully comply with this Standard under agreed conditions and for a limited period.

II. Receive guidance from Competent Authorities on compliance requirements.

III. Develop evidence for the conformity assessment of their AI systems.

49.3. Participation in a regulatory sandbox does not exempt participants from liability for harm caused to third parties during the testing period.

Article 50 — Sandbox Conditions and Safeguards

50.1. Regulatory sandbox plans must specify:

I. The participants and their AI systems.

II. The duration of the sandbox period, which must not exceed twenty-four (24) months, extendable once by twelve (12) months.

III. The scope of testing, including the data, sectors, and jurisdictions involved.

IV. The safeguards for affected persons, including informed consent, data protection measures, and exit procedures.

V. The reporting obligations of participants, including interim and final reports to the Competent Authority.

50.2. Natural persons participating in sandbox testing as subjects or users must provide informed consent and must be able to withdraw at any time without disadvantage.

50.3. CAIRMC shall publish model sandbox terms of reference and application templates.

Article 51 — Sandboxes for Small Island Developing States

51.1. CAIRMC shall operate a regional sandbox programme specifically designed for SIDS member states that may lack the capacity to establish their own national sandboxes.

51.2. The regional sandbox shall offer reduced fees or fee waivers for micro, small, and medium enterprises and public sector agencies in SIDS.

51.3. Sandbox outcomes achieved in the regional programme shall be recognised by all participating member states for the purpose of national conformity assessments.

Chapter 15: Confidentiality and Trade Secrets

Article 52 — Confidentiality of Information

52.1. All parties involved in the application of this Standard—including Competent Authorities, conformity assessment bodies, and CAIRMC staff—must respect the confidentiality of information and data obtained in the exercise of their functions.

52.2. Information exchanged between national Competent Authorities and CAIRMC under this Standard shall be subject to professional secrecy obligations.

52.3. Nothing in this Standard requires providers to disclose trade secrets, proprietary algorithms, or model weights to the public. Where Competent Authorities require access to such information for supervisory or enforcement purposes, they must ensure that information is handled under strict confidentiality safeguards, accessed only by authorised personnel with relevant expertise, and used solely for the purposes of this Standard.

52.4. The confidentiality protections in this Article do not override the transparency obligations owed to affected persons under Articles 13, 26, and 46.

PART IX: SECTOR-SPECIFIC AI GOVERNANCE

Chapter 16: AI in Tourism

Article 53 — AI in Tourism and Hospitality

53.1. Given the importance of tourism to the Caribbean economy, AI systems deployed in the following tourism-related applications are subject to the sector-specific obligations in this Article in addition to any applicable Tier obligations:

I. Dynamic pricing systems for accommodation, transportation, and tourism services that may result in price discrimination based on the nationality, country of origin, or inferred economic status of the customer.

II. AI-powered guest profiling systems used by hotels, resorts, or cruise lines that process personal data including health data, dietary preferences, or behavioural patterns.

III. Automated decision-making systems for visa-on-arrival or tourism entry permissions.

IV. AI systems used to manage, direct, or restrict tourist access to natural sites, heritage sites, or public spaces.

V. 53.2. Providers and deployers of AI systems listed in 53.1 must:

VI. Ensure that dynamic pricing algorithms do not engage in unfair discrimination based on nationality or national origin.

VII. Provide clear disclosure to tourists when AI is used to personalise pricing or services.

VIII. Conduct a CARA that includes an assessment of the impact on the tourism sector's reputation, visitor trust, and the economic interests of local tourism workers.

Chapter 17: AI in Financial Services

Article 54 — AI in Financial Services

54.1. AI systems deployed in financial services in the Caribbean are subject to the following additional obligations, which complement applicable financial regulation and Basel Committee guidance:

I. Financial institutions must integrate AI risk into their enterprise risk management frameworks, with AI risk reported to the board of directors at least quarterly.

II. AI model risk management must follow the three-lines-of-defence model: the first line (business unit) owns the AI model, the second line (risk management) validates and monitors it, and the third line (internal audit) provides independent assurance.

III. Credit scoring and loan approval AI systems must be subject to annual validation and recalibration using data that includes the relevant Caribbean population.

IV. Financial regulators in each Caribbean member state shall have access to the methodology, training data, and validation results of AI systems used in regulatory reporting, capital adequacy calculations, or systemic risk monitoring.

54.2. CAIRMC shall coordinate with the Caribbean Group of Banking Supervisors (CGBS) and regional insurance supervisors to ensure alignment between this Standard and sector-specific financial regulation.

Chapter 18: AI in Healthcare

Article 55 — AI in Healthcare

55.1. In addition to the general high-risk obligations, AI systems deployed in healthcare in the Caribbean must:

I. Be validated on datasets that include Caribbean demographic groups, disease prevalence rates, and genetic profiles, before deployment in a Caribbean healthcare setting.

II. Carry a clear indication of the system's validated clinical context and the populations for which it has been validated, so that clinicians can assess its applicability.

III. Be subject to ongoing clinical performance monitoring, with results reported to the relevant national health authority and CAIRMC.

IV. Include fail-safe mechanisms that default to human clinical judgement where the system encounters inputs outside its validated parameters.

55.2. AI systems used in public health surveillance, epidemic prediction, or disaster health response in the Caribbean must be registered in the Caribbean AI Registry and must include provisions for data sharing across Caribbean member states, subject to data protection safeguards.

Chapter 19: AI in Agriculture and Food Security

Article 56 — AI in Agriculture

56.1. AI systems deployed in the Caribbean agricultural sector must be designed and validated with attention to the region's specific agricultural conditions, including tropical crop varieties, climate variability, and smallholder farming structures.

56.2. AI systems that make recommendations regarding crop management, pesticide application, water allocation, or market pricing for agricultural commodities that could materially affect the livelihoods of farmers are classified as Tier 2 if their output directly determines the allocation of resources or access to markets without human review.

56.3. Providers of agricultural AI systems deployed in the Caribbean must make the system's training data sources and validation methodology available to the relevant national agricultural authority upon request.

Chapter 20: AI in Education

Article 57 — AI in Education

57.1. AI systems used in Caribbean educational settings must be subject to the following additional provisions:

I. AI systems that assess, evaluate, or profile students must not be used as the sole basis for decisions that affect a student's educational trajectory, including grade assignment, admission, or disciplinary action.

II. AI-generated educational content must be reviewed by a qualified human educator before deployment in a formal educational programme.

III. AI-powered student monitoring or proctoring systems must comply with the transparency obligations in Article 26 and must not process biometric data of minors without the explicit consent of a parent or legal guardian.

IV. The use of emotion recognition AI on students is prohibited except where explicitly authorised for the student's health or safety and with parental consent.

PART X: ENVIRONMENTAL AND CLIMATE AI GOVERNANCE

Chapter 21: Climate and Environmental Impact

Article 58 — Environmental Principles for AI

58.1. AI governance in the Caribbean must take into account the region's acute vulnerability to climate change, rising sea levels, and extreme weather events. AI systems must not exacerbate environmental harm, and where possible should contribute to climate adaptation and resilience.

58.2. The environmental principles of this Standard are:

I. Proportionality: The energy consumption and environmental footprint of an AI system must be proportionate to its societal benefit.

II. Transparency: Providers must disclose the environmental impact of AI system training and operation.

III. Sustainability: AI systems should be designed to minimise energy consumption, electronic waste, and carbon emissions throughout their lifecycle.

Article 59 — Climate Impact Assessment

59.1. Providers of Tier 2 (High-Risk) AI systems and GPAI systems with systemic risk must include a climate impact assessment as part of their technical documentation. The assessment must cover:

I. The estimated energy consumption for training the AI model, expressed in kilowatt-hours and equivalent carbon emissions.

II. The estimated energy consumption per unit of inference or operation.

III. The hardware used, including the location and energy source of training data centres.

IV. The electronic waste implications of the hardware lifecycle.

V. Any measures taken to reduce the system's environmental footprint, including model compression, efficient architectures, or use of renewable energy.

59.2. CAIRMC shall publish a Climate Impact Assessment template and methodology within one year of this Standard's adoption.

59.3. Where a climate impact assessment reveals that an AI system's environmental footprint is disproportionate to its societal benefit, the Competent Authority may require the provider to implement efficiency improvements or offset measures before the system may be placed on the Caribbean market.

Article 60 — AI for Climate Resilience

60.1. CAIRMC shall promote the development and deployment of AI systems that contribute to Caribbean climate resilience, including:

I. Early warning systems for hurricanes, floods, and other natural disasters.

II. AI systems for climate-adaptive agriculture, including crop selection and water management.

III. AI systems for coastal erosion monitoring and sea-level rise prediction.

IV. AI systems for energy grid optimisation and renewable energy management.

V. AI systems for disaster response coordination and resource allocation.

60.2. AI systems deployed for climate resilience purposes may be eligible for expedited registration, reduced CARA requirements, and sandbox access under the innovation provisions of Part VIII.

PART XI: LIABILITY AND INSURANCE

Chapter 22: AI Liability

Article 61 — Liability of Providers

61.1. Where a high-risk AI system causes damage to a natural person's health, safety, or fundamental rights, the provider is liable for the damage unless the provider can demonstrate that:

I. The damage was not caused by the AI system or by a deficiency in the AI system's design, development, or data.

II. The provider complied with all obligations under this Standard applicable to the AI system.

III. The damage was caused solely by the deployer's misuse of the system or failure to follow the provider's instructions.

61.2. Where a deployer substantially modifies a high-risk AI system or uses it outside its intended purpose, the deployer assumes liability for damage caused by the modification or misuse.

61.3. Where multiple operators in the AI value chain are jointly responsible for damage, they shall be jointly and severally liable. The allocation of internal contribution shall be determined by each operator's degree of responsibility.

Article 62 — Presumption of Causation

62.1. Where a claimant demonstrates that a provider or deployer has failed to comply with a relevant obligation under this Standard, and the non-compliance is reasonably likely to have caused the damage, a rebuttable presumption of causation applies.

62.2. This presumption does not apply where the defendant demonstrates that sufficient evidence and expertise is accessible to the claimant to prove causation through conventional means.

Article 63 — Mandatory AI Liability Insurance

63.1. Providers of Tier 2 (High-Risk) AI systems placed on the Caribbean market must maintain professional liability insurance or equivalent financial guarantee covering damage that may be caused by the AI system.

63.2. The minimum coverage level shall be:

I. USD $5 million per incident for AI systems in healthcare, critical infrastructure, and law enforcement.

II. USD $2 million per incident for AI systems in financial services, education, and employment.

III. USD $1 million per incident for all other Tier 2 AI systems.

63.3. CAIRMC shall review the minimum coverage levels every three years and adjust them as necessary.

63.4. Proof of insurance or equivalent financial guarantee must be submitted as part of the registration in the Caribbean AI Registry.

PART XII: ACCESSIBILITY AND INCLUSION

Chapter 23: Accessibility Requirements

Article 64 — Accessibility for Persons with Disabilities

64.1. Providers and deployers of AI systems that interact directly with natural persons must ensure that the AI system is accessible to persons with disabilities, in accordance with applicable Caribbean disability legislation and the principles of the UN Convention on the Rights of Persons with Disabilities.

64.2. Accessibility measures must include, where applicable:

I. Compatibility with assistive technologies including screen readers, speech-to-text, and alternative input devices.

II. Multiple modalities for disclosure and transparency information (visual, auditory, and tactile).

III. Adjustable interfaces that accommodate diverse cognitive and physical abilities.

64.3. The right to a human alternative under Article 48 must be provided through channels accessible to persons with disabilities.

Article 65 — Digital Inclusion and the Digital Divide

65.1. Deployers of AI systems providing essential public services in the Caribbean must ensure that the AI system does not exclude or disadvantage persons who lack digital access, digital literacy, or modern devices.

65.2. Where an essential service is delivered through an AI system, a non-digital alternative must remain available to persons who cannot access or use the AI system.

65.3. CAIRMC shall publish guidance on inclusive AI deployment practices that account for the digital divide across Caribbean nations.

PART XIII: SUPPLY CHAIN DUE DILIGENCE

Chapter 24: Due Diligence in the AI Value Chain

Article 66 — Supply Chain Due Diligence Obligations

66.1. Providers that build high-risk AI systems using general-purpose AI models as foundation components must conduct supply chain due diligence that includes:

I. Verification that the GPAI model provider has complied with its obligations under Articles 28 and 29 of this Standard.

II. Assessment of whether the GPAI model's known limitations, biases, or risks introduce additional risks when integrated into the downstream AI system.

III. Documentation of the GPAI model version used, the integration method, and any fine-tuning or adaptation performed.

IV. Contractual provisions requiring the GPAI model provider to notify the downstream provider of material changes, safety findings, or incidents.

66.2. Where a provider cannot verify the compliance of an upstream GPAI model, the provider assumes full responsibility for the integrated system and must conduct its own assessments as if it were the model provider.

Article 67 — Open-Source AI Components

67.1. Free and open-source AI components are exempt from the obligations of this Standard except where:

I. The open-source component is itself a general-purpose AI model with systemic risk.

II. The open-source component is integrated into a high-risk AI system, in which case the provider of the high-risk system bears full compliance responsibility.

67.2. This exemption does not relieve the downstream provider who integrates an open-source component into a regulated AI system from any obligation under this Standard. The downstream provider must conduct the same supply chain due diligence as for proprietary components.

PART XIV: AI AGENTS, MULTI-AGENT SYSTEMS, AND FRONTIER AI

Chapter 25: AI Agents and Autonomous AI Systems

Article 68 — Classification and Governance of AI Agents

68.1. AI agents, as defined in Article 3, present risks that differ from conventional AI systems because they act with a degree of autonomy, execute multi-step tasks, interact with external systems, and may produce consequences that are difficult to reverse. This Standard applies the following governance requirements to AI agents in addition to any Tier-based obligations:

I. Any AI agent deployed in a Tier 2 sector must operate with human-in-the-loop or human-on-the-loop oversight as defined in Article 3. Human-out-of-the-loop deployment of AI agents in Tier 2 sectors is prohibited except where CAIRMC has granted a specific, time-limited exemption following a full CARA assessment and independent safety review.

II. AI agents that interact with natural persons must identify themselves as AI agents at the outset of each interaction. This disclosure must be made in plain language accessible to the person, in the language of the interaction, and cannot be buried in terms of service or hidden behind interface design.

III. AI agents that execute actions with real-world consequences—including sending communications, making purchases, executing code, transferring funds, or submitting applications—must maintain a complete, tamper-resistant audit log of every action taken, every tool invoked, every decision point, and every external system accessed. These logs must be retained for not less than five (5) years.

IV. Providers must define and publish a clear boundary of authority for each AI agent: the maximum scope of actions the agent may take, the financial limits within which it may operate, and the categories of decisions it is not permitted to make under any circumstances.

V. AI agents must include automatic disengagement mechanisms (kill switches) that allow the deployer or a designated human overseer to halt all agent operations immediately, with all pending actions cancelled and all affected parties notified.

Article 69 — Multi-Agent Systems and Agent Swarms

69.1. Multi-agent systems (agent swarms) present additional risks not present in single-agent deployments, including emergent behaviour, cascading failures, coordination failures, and the diffusion of accountability. Providers and deployers of multi-agent systems must comply with the following:

I. The provider must conduct a specific multi-agent risk assessment as part of the CARA process, evaluating: (a) the risk of emergent behaviour—actions that arise from agent interactions and were not explicitly programmed or anticipated; (b) cascading failure modes—how the failure of one agent propagates through the system; (c) coordination risks—how agents may conflict, compete for resources, or

produce contradictory outputs; and (d) accountability mapping—which operator is responsible for each agent's actions and for the collective output.

II. Each agent within a multi-agent system must be individually identifiable and auditable. The provider must maintain documentation of each agent's role, capabilities, authority boundaries, and interactions with other agents.

III. Multi-agent systems must include a central monitoring mechanism that tracks the collective state of the system and triggers automatic disengagement if agent behaviour deviates materially from expected parameters, if agents enter into unresolvable conflict, or if the system's collective output exceeds predefined risk thresholds.

IV. The delegation of tasks from one AI agent to another within a multi-agent system does not relieve the provider of the originating agent from liability for the actions of the delegated agent. The provider bears responsibility for the entire chain of delegation.

V. Multi-agent systems that operate across multiple Caribbean jurisdictions must be registered in the Caribbean AI Registry with a clear mapping of which agents operate in which jurisdictions, and must comply with the data protection and consumer protection legislation of each jurisdiction.

69.2. CAIRMC shall publish specific guidance on the governance of multi-agent systems within one year of this Standard's effective date, including model risk assessment templates and recommended architectural safeguards.

Article 70 — Frontier AI Models and Artificial General Intelligence

76.1. The Caribbean region, as a net consumer of AI systems developed predominantly outside the region, has a particular interest in the governance of frontier AI models and the prospect of artificial general intelligence (AGI). The provisions of this Article reflect the precautionary approach warranted by the potential magnitude of risks from such systems.

76.2. Frontier AI models, as defined in Article 3, are subject to the following obligations when deployed or made available in the Caribbean:

I. All obligations applicable to GPAI systems with systemic risk under Articles 28 and 29 apply to frontier AI models.

II. Providers of frontier AI models must publish a safety case—a structured argument, supported by evidence, that the model is safe for its intended and reasonably foreseeable uses in the Caribbean context—before deployment. The safety case must be submitted to CAIRMC and made publicly available.

III. Providers must conduct and publish evaluations for dangerous capabilities, including: autonomous replication and adaptation, long-horizon planning, situational awareness, manipulation and deception, and weapons or cyberattack capability. Evaluation methodologies must be disclosed.

IV. Providers must implement a responsible scaling policy or equivalent framework that specifies the safety and security conditions that must be met before training or deploying more capable models.

V. Providers must grant CAIRMC, upon request, access to model evaluation results, red-team findings, and internal safety assessments, subject to the confidentiality protections in Article 52.

76.3. Provisions on Artificial General Intelligence:

I. The deployment of any AI system exhibiting AGI-equivalent capabilities in the Caribbean is prohibited without prior authorisation from CAIRMC as specified in Article 6 (Tier 1 Prohibited Practices).

II. CAIRMC shall establish an AGI Preparedness Committee, comprising members of the Caribbean AI Scientific Panel, national Competent Authority representatives, and external experts, to monitor global AGI development, assess readiness, and advise CAIRMC on the conditions under which AGI authorisation could be considered.

III. The AGI Preparedness Committee shall report to CAIRMC and the Caribbean AI Advisory Forum at least annually on the state of global AGI research, the adequacy of existing safeguards, and any recommended updates to this Standard.

IV. No authorisation for AGI deployment shall be granted unless the system has passed: (a) an independent third-party safety audit; (b) a Caribbean-specific fundamental rights impact assessment; (c) a socioeconomic impact assessment evaluating effects on Caribbean labour markets, public services, and economic sovereignty; and (d) a public consultation of not less than ninety (90) days.

76.4. CAIRMC is empowered to issue an emergency moratorium on the deployment of any AI system in the Caribbean if credible evidence emerges that the system poses an existential, catastrophic, or irreversible risk to Caribbean populations, economies, or environments. A moratorium takes effect immediately upon issuance and remains in force until CAIRMC determines that the risk has been adequately addressed.

PART XV: ETHICAL FRAMEWORK FOR AI IN THE CARIBBEAN

Chapter 26: Caribbean Ethical AI Principles

Article 71 — Purpose and Status of the Ethical Framework

77.1. This Part establishes the Caribbean Ethical AI Principles—a set of binding ethical obligations grounded in the constitutional values, cultural heritage, and lived experience of Caribbean peoples. These principles are not aspirational guidelines; they carry the same compliance weight as the technical obligations elsewhere in this Standard.

77.2. The ethical principles in this Part reflect the Caribbean's distinct history, including the legacy of colonialism and slavery, the struggle for self-determination, the diversity of the region's peoples and cultures, and the commitment to human dignity that underpins the constitutions of Caribbean nations. AI systems deployed in the Caribbean must respect this context.

Article 72 — The Principles

The following principles apply to all AI systems subject to this Standard:

72.1. Human Dignity and Agency. AI systems must respect the inherent dignity of every person. No AI system may be designed or deployed in a manner that reduces a person to a data point, a risk score, or an algorithmic output. Caribbean peoples have the right to be treated as full human beings—not as inputs to a model. AI systems must preserve and where possible strengthen human agency, self-determination, and the capacity of individuals and communities to make their own decisions.

72.2. Fairness and Non-Discrimination. AI systems must not discriminate on the basis of race, ethnicity, colour, national origin, sex, gender identity, sexual orientation, age, disability, religion, socioeconomic status, or any other characteristic protected under applicable Caribbean constitutional and anti-discrimination law. Providers and deployers must actively assess for and mitigate bias, recognising that the Caribbean's colonial history has produced structural inequalities that may be encoded in training data. Where an AI system produces disparate outcomes across protected groups in the Caribbean, the burden falls on the provider to demonstrate that the disparity is justified, necessary, and proportionate.

72.3. Transparency and Explainability. Persons affected by AI-assisted decisions have the right to understand how the decision was made. Explanations must be provided in plain language, in a language accessible to the affected person, and at a level of detail proportionate to the severity of the decision. "The algorithm decided" is not an explanation. AI systems that cannot provide a meaningful explanation for their outputs must not be used for decisions that materially affect a person's rights, access to services, or economic interests.

72.4. Accountability and Responsibility. There must always be a natural person or a clearly identified legal entity accountable for the actions and outputs of an AI system. Accountability cannot be diffused across an AI value chain to the point where no one is

responsible. Where an AI system causes harm, the affected person must be able to identify who is accountable and seek redress through accessible mechanisms.

72.5. Privacy and Data Sovereignty. AI systems must respect the privacy of Caribbean nationals and residents in accordance with applicable data protection legislation, including the Jamaica Data Protection Act 2020, the Trinidad and Tobago Data Protection Act 2011, the Barbados Data Protection Act 2019, the Guyana Data Protection Act 2023, and the OECS Model Data Protection Bill. Caribbean peoples have the right to know what data about them is collected, how it is used in AI systems, and to whom it is transferred. The extraction of Caribbean data for AI training by foreign entities must comply with applicable data protection law and respect the data sovereignty interests of Caribbean nations.

72.6. Community and Cultural Respect. AI systems deployed in the Caribbean must respect the cultural diversity, linguistic plurality, and social norms of the region. This includes respect for Caribbean English, French Creole, Haitian Kreyol, Papiamento, Garifuna, Sranan Tongo, and other Caribbean languages and dialects. AI systems that make judgements about language, behaviour, appearance, or cultural expression must not penalise Caribbean cultural norms or impose foreign cultural standards. AI systems must not misrepresent, appropriate, or commodify Caribbean cultural heritage, traditional knowledge, or artistic expression.

72.7. Economic Justice. AI systems must not deepen economic inequality within or between Caribbean nations. Providers and deployers must consider the impact of AI deployment on local employment, wages, small businesses, and economic self-sufficiency. AI systems that displace Caribbean workers must be accompanied by transition support. AI systems that extract economic value from the Caribbean—through data collection, market access, or service fees—without returning proportionate value to the region are subject to heightened scrutiny under the CARA process.

72.8. Environmental Stewardship. AI deployment in the Caribbean must respect the region's environmental vulnerability. The Caribbean is on the front line of climate change, rising sea levels, and extreme weather events. AI systems must not impose disproportionate environmental costs on the region, and where possible should contribute to climate adaptation, disaster resilience, and environmental protection.

72.9. Children and Vulnerable Populations. AI systems that interact with or affect children must treat the best interests of the child as a primary consideration, consistent with the UN Convention on the Rights of the Child and applicable Caribbean child protection legislation including the Jamaica Child Care and Protection Act 2004, the Trinidad and Tobago Children Act 2012, and equivalent instruments. AI systems affecting elderly persons, persons with disabilities, persons in economic hardship, and other vulnerable populations must apply heightened safeguards.

72.10. Solidarity and Regional Cooperation. AI governance in the Caribbean is a collective endeavour. Member states, providers, deployers, and civil society must cooperate in the spirit of CARICOM solidarity to build shared capacity, share knowledge, pool resources, and present a united voice in international AI governance forums. No Caribbean nation should be left behind in the AI transition.

Article 73 — Ethical Review for High-Risk AI Systems

73.1. The CARA assessment for all Tier 2 (High-Risk) AI systems must include an explicit ethical review against the principles in Article 72. The ethical review must:

I. Assess the AI system against each of the ten principles, documenting compliance, gaps, and mitigations.

II. Include input from affected communities or their representatives where the AI system affects a defined population, particularly indigenous, Maroon, Garifuna, Amerindian, and other historically marginalised Caribbean communities.

III. Be conducted or reviewed by a person with demonstrated competence in AI ethics, Caribbean human rights law, and the specific domain in which the AI system operates.

73.2. Where the ethical review identifies material conflict between the AI system's operation and any principle in Article 72, the provider must either modify the system to resolve the conflict or provide a written justification that the conflict is outweighed by countervailing public interest, subject to approval by the relevant Competent Authority.

PART XVI: IMPLEMENTATION AND TRANSITIONAL PROVISIONS

Chapter 27: Phased Implementation

Article 74 — Implementation Timeline

CAIRMC recommends the following phased implementation timeline for member states that adopt this Standard:

Phase	Timeline	Action
Phase 1 — Foundation	Months 1–6 after adoption	Designate national Competent Authority; publish national adoption instrument; notify CAIRMC; begin national AI literacy strategy development
Phase 2 — Prohibitions and Literacy	Months 7–12	Tier 1 prohibitions take effect; AI literacy obligations apply to all providers and deployers; CAIRMC publishes guidance and templates
Phase 3 — GPAI and Transparency	Months 13–18	Obligations for GPAI providers and Tier 3 transparency obligations take effect; Caribbean AI Registry operational; codes of practice published
Phase 4 — High-Risk Compliance	Months 19–30	All Tier 2 obligations apply to newly deployed systems; existing Tier 2 systems must achieve full compliance; conformity assessments mandatory; CARA required
Phase 5 — Full Enforcement	Month 31 onwards	Full enforcement including sanctions and periodic penalty payments; annual registry review cycle; liability and insurance provisions in effect

Article 75 — Support for Small Island Developing States

CAIRMC recognises that implementation capacity varies significantly across Caribbean member states. CAIRMC commits to:

I. Publishing model national legislation templates to facilitate adoption of this Standard by each member state.

II. Providing capacity-building training through the QAIRP programme, targeted workshops for public sector officials, and train-the-trainer programmes in SIDS.

III. Establishing the Caribbean AI Governance Support Fund (subject to donor and partner mobilisation) to assist smaller member states with implementation costs, including the establishment of Competent Authorities and sandbox programmes.

IV. Offering a simplified CARA process for AI systems deployed exclusively by micro, small, and medium enterprises with no cross-border or critical sector exposure.

V. Facilitating technical assistance from larger member states and international partners through bilateral and multilateral cooperation agreements.

VI. Providing shared-service arrangements for Competent Authority functions, whereby smaller member states may delegate specific supervisory activities to CAIRMC or a larger member state.

Article 76 — Relationship with Existing Law

76.1. This Act does not supersede, abrogate, or diminish any obligation under existing national data protection legislation, financial services regulation, consumer protection law, health regulation, or environmental law applicable in Caribbean member states.

76.2. Where obligations under this Standard and existing national law conflict, national law prevails unless the Standard expressly provides otherwise.

76.3. This Act complements and does not replace obligations under the GDPR applicable to Caribbean operators processing data of persons in EU/EEA member states.

76.4. CAIRMC will publish guidance on the interaction between this Standard and existing Caribbean legal instruments, including jurisdiction-by-jurisdiction mapping of applicable data protection, consumer protection, and sector-specific legislation.

Article 77 — International Cooperation and Mutual Recognition

77.1. CAIRMC shall seek mutual recognition arrangements with other jurisdictions that have adopted AI governance frameworks, including the European Union, the United Kingdom, Canada, Singapore, and any other jurisdiction with comparable standards.

77.2. Where a mutual recognition arrangement is in place, conformity assessments, certifications, and sandbox outcomes obtained in the partner jurisdiction may be recognised in the Caribbean, subject to a gap assessment against the specific requirements of this Standard.

77.3. CAIRMC shall represent the Caribbean region in international AI governance negotiations and standard-setting processes, including at the OECD, UNESCO, the Global Partnership on AI, and relevant UN bodies.

Article 78 — Review and Amendment

78.1. CAIRMC will conduct a formal review of this Standard every two (2) years from the date of adoption, or earlier if material developments in AI technology, international standards, or regional policy warrant it.

78.2. The review process will include public consultation consistent with the process used for this initial draft, input from the Caribbean AI Advisory Forum and Scientific Panel, and analysis of registry data, incident reports, and emerging risks.

78.3. CAIRMC may issue interpretive guidance, delegated rules, and implementing technical standards between formal reviews, following consultation with the Advisory Forum.

Article 79 — Delegated and Implementing Powers

79.1. CAIRMC is empowered to adopt delegated rules to:

I. Update Annex I (Caribbean AI Risk Taxonomy) to reflect emerging risk categories.

II. Adjust the 10^{25} FLOPS threshold for systemic risk designation in light of technological developments.

III. Amend the list of high-risk AI system categories in Article 7 where new high-risk applications emerge.

IV. Update the minimum insurance coverage levels under Article 63.

79.2. Delegated rules must be published for a sixty-day public consultation period before adoption and must be notified to all member states.

PART XVII: FINAL PROVISIONS

Article 80 — Effective Date

This Act, in its final approved form, takes effect on the date of adoption by the adopting member state or regional body. For member states that adopt this Standard through national legislation, the national instrument determines the effective date.

Article 81 — Authoritative Texts

This Act is published in English as the authoritative text. CAIRMC will publish authoritative translations in French, Dutch, and Spanish for the benefit of Caribbean member states where those languages are official or widely used. In the event of inconsistency, the English text takes precedence pending formal resolution by CAIRMC.

Article 82 — Custodian

CAIRMC shall act as custodian for this Standard. Instruments of adoption, implementation agreements, and amendments shall be lodged with and published by CAIRMC. Contact: info@caribbeanairisk.com.

ANNEX I — Caribbean AI Risk Taxonomy

The following taxonomy provides a structured classification of AI risk types relevant to the Caribbean context. Providers and Competent Authorities must use this taxonomy in conducting CARA assessments and classifying AI systems.

Risk Category	Sub-Category	Caribbean Context
Accuracy and Reliability	Performance degradation; model drift; data distribution shift; hallucination; out-of-distribution failure	Caribbean demographic data is underrepresented in most global AI training sets; systems must be validated locally against Caribbean populations
Data Governance	Unlawful data collection; privacy breach; inadequate consent; cross-border data transfer; data localisation	Multiple Caribbean DPAs apply with varying requirements; cross-border data flows between CARICOM member states require specific attention
Bias and Discrimination	Racial, ethnic, socioeconomic, gender, age, and disability bias; proxy discrimination; intersectional bias	Historical bias in data may reflect Caribbean colonial legacy and structural inequality; specific monitoring required for credit, employment, and justice applications
Cybersecurity	Adversarial attacks; data poisoning; model theft; prompt injection; API abuse; supply chain attacks	Caribbean financial and tourism sectors are high-value targets; limited cybersecurity capacity in smaller states increases vulnerability
Labour and Economic Displacement	Job displacement; income inequality; gig economy impacts; de-skilling; wage suppression	Tourism, agriculture, and public service sectors face acute AI exposure in SIDS; limited labour market mobility amplifies displacement effects
Access and Inclusion	Digital divide; language barriers; infrastructure gaps; disability access; age-related exclusion	Broadband penetration and digital literacy vary across Caribbean nations; Creole-language populations may be excluded by English-only AI systems
Accountability Gaps	Unclear liability; inadequate redress; opacity in decision-making; lack of audit trail	Emerging legal frameworks require explicit remediation pathways; judicial capacity for AI disputes is limited in many member states
Environmental Risk	Energy consumption; carbon emissions; e-waste; water usage for cooling; resource extraction for hardware	Caribbean nations face acute climate vulnerability; AI infrastructure must be assessed for sustainability and proportionality
Manipulation and Deception	Deep fakes; disinformation; social media manipulation; election interference; scams	Small media markets and high social media penetration in the Caribbean increase vulnerability to AI-generated disinformation

Concentration of Power	Market dominance; regulatory capture; vendor lock-in; dependency on foreign AI providers	Caribbean nations are predominantly consumers of AI built elsewhere; dependency on a small number of global providers creates structural risk
Cultural and Linguistic Risk	Loss of linguistic diversity; cultural homogenisation; misrepresentation of Caribbean identity and heritage	AI systems trained on Global North data may not reflect Caribbean cultural norms, idioms, languages, or values
Children and Vulnerable Populations	Age-inappropriate content; predatory targeting; developmental harm; consent incapacity	Caribbean nations have young demographic profiles; children's exposure to AI requires specific safeguards

ANNEX II — Framework Alignment Table

The following table maps key obligations under this Standard to relevant international and regional frameworks.

This Act	EU AI Act	NIST AI RMF	ISO 42001	COSO / GDPR / DPAs
Art. 5 — Risk Tiers	Arts. 5–7	MAP 1.1	Clause 6.1	Risk ID / Art. 35
Art. 10 — QMS	Art. 17	GOVERN 1.2	Cl. 4–10	Controls / Art. 25
Art. 11 — Data Gov.	Art. 10	MAP 2.1	Cl. 8.4	Risk Resp. / Arts. 5–6
Art. 12 — Tech. Docs	Art. 11	GOVERN 6.1	Cl. 9.1	Info & Comm / Art. 30
Art. 14 — Human Oversight	Art. 14	MANAGE 4.1	Cl. 8.3	Monitoring / Art. 22
Art. 16 — Logging	Art. 12	MANAGE 3.1	Cl. 9.1	Info & Comm / Art. 30
Arts. 23–25 — CARA	Art. 9	MAP 3.5	Cl. 8.2	Risk Assess. / Art. 35
Arts. 31–33 — Conformity	Arts. 40–49	GOVERN 5.1	Cl. 7.5	Controls / Art. 25
Art. 35 — Registry	Art. 71	GOVERN 5.1	Cl. 7.5	Info & Comm / Art. 30
Art. 44 — Sanctions	Arts. 99–101	—	—	Art. 83
Art. 48 — Human Alt.	Art. 86 (partial)	MANAGE 4.2	—	Art. 22 GDPR
Art. 49 — Sandboxes	Arts. 57–62	—	—	—
Art. 59 — Climate IA	Recital 27	—	—	—
Art. 63 — Insurance	— (novel)	—	—	—
Art. 66 — Supply Chain DD	Art. 25 (partial)	GOVERN 6.2	Cl. 8.1	—
Art. 68 — AI Agents	— (novel)	MANAGE 4.1	—	—
Art. 69 — Agent Swarms	— (novel)	MAP 1.5	—	—
Art. 70 — Frontier/AGI	Recital 110	GOVERN 1.1	—	—
Art. 72 — Ethics	— (novel)	MAP 1.6	Cl. 4.1	Recital 1 GDPR

ANNEX III — CAIRMC AI Governance Maturity Model

The following maturity model provides organisations with a self-assessment framework for AI governance readiness.

Level	Name	Characteristics
Level 1	Ad Hoc	No formal AI governance; AI deployed opportunistically; no risk assessment; no designated AI governance roles; no training
Level 2	Developing	Initial AI governance policies drafted; AI risk considered informally; some staff awareness; no systematic CARA; limited documentation
Level 3	Defined	Formal AI governance framework in place; CARA conducted for high-risk systems; AI risk integrated into enterprise risk management; AI literacy training programme established; Caribbean AI Registry registration completed
Level 4	Managed	AI governance metrics tracked and reported to senior leadership; continuous monitoring of AI system performance; third-party audits conducted; incident response procedures tested; human oversight mechanisms verified regularly
Level 5	Optimised	AI governance continuously improved using performance data; proactive risk identification; innovation through sandboxes; leadership in regional and international AI governance; QAIRP-certified staff across the organisation

ANNEX IV — Sector-Specific High-Risk AI Applications (Caribbean)

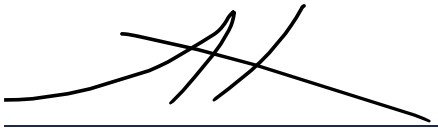
The following table identifies AI applications of particular relevance to Caribbean economic sectors, with their recommended risk tier and sector-specific considerations.

Sector	AI Application	Recommended Tier	Caribbean Context
Tourism	Dynamic pricing for hotels/flights	Tier 2	Risk of nationality-based price discrimination; reputation risk to Caribbean brand
Tourism	AI concierge / chatbot	Tier 3	Transparency disclosure required; multilingual support needed
Financial Services	Credit scoring / loan approval	Tier 2	Bias risk for underbanked populations; microfinance exposure in SIDS
Financial Services	Fraud detection	Tier 2	False positives may disproportionately affect certain demographics
Healthcare	Clinical decision support	Tier 2	Must be validated on Caribbean populations; tropical disease profiles
Healthcare	AI triage chatbot	Tier 3	Transparency required; fail-safe to human clinician
Agriculture	Crop yield prediction	Tier 3 / Tier 2*	*Tier 2 if output directly determines resource allocation
Education	Student performance prediction	Tier 2	Cannot be sole basis for grading or admission decisions
Energy	Grid load balancing	Tier 2	Critical infrastructure; climate resilience implications
Public Admin	Benefits eligibility determination	Tier 2	Right to human alternative applies; fundamental rights impact assessment required
Law Enforcement	Facial recognition	Tier 1 / Tier 2**	**Real-time in public spaces prohibited (Tier 1); post-remote is Tier 2
Maritime / Ports	Automated cargo inspection	Tier 2	Port security is critical infrastructure for island economies
Cross-Sector	AI agent (autonomous task execution)	Tier 2	Kill switch, audit log, authority boundaries required; Art. 68
Cross-Sector	Multi-agent system / agent swarm	Tier 2	Emergent behaviour risk; central monitoring;

			accountability mapping; Art. 69
Cross-Sector	Frontier AI model deployment	Tier 2+	Safety case, red-team, responsible scaling policy required; Art. 70
Cross-Sector	AGI or AGI-equivalent system	Tier 1 (Prohibited)	Prohibited without CAIRMC authorisation; Art. 6 and Art. 70
Financial Services	AI agent executing trades/payments	Tier 2	Per-transaction authorisation required; financial limit boundaries
Public Admin	AI agent processing benefit claims	Tier 2	Human-in-the-loop mandatory; right to human alternative applies
Tourism	AI agent booking/rebooking travel	Tier 3	Transparency disclosure; authority boundaries on spend limits

Signature

This consultation draft of the Caribbean AI Risk Management Standard is issued by the Caribbean AI Risk Management Council on behalf of the Caribbean region in furtherance of CAIRMC's mandate to govern AI risk and promote responsible AI adoption.



Adrian Dunkley
President
Caribbean AI Risk Management Council (CAIRMC)

February 2026
info@caribbeanairisk.com | caribbeanairisk.com

NOTE: This document is a consultation draft. It has not been approved by CARICOM, any CARICOM member state, or any national legislative body. It does not constitute legal advice. Organisations should seek independent legal guidance before taking compliance action based on this draft.