ICML
International Conference
On Machine Learning

DATA
INTELLIGENCE
LAB

Computational
Intelligence and
Operations Lab

Position: AI Governance Needs ISO-like Interoperability Protocols, Not Just Laws

Azmine Toushik Wasi, Mst Rafia Islam, Mahfuz Ahmed Anik, Taki Hasan Rafi, Md Manjurul Ahsan, Dong-Kyu Chae

ICML 2026 · POSITION PAPER TRACK

The Problem

AI regulation is fragmenting across borders

Similar architectures, data, and risk pathways are governed by sharply divergent regulatory philosophies, from **ex ante** control to **voluntary** guidance.

European Union

BINDING · RISK-TIERED

EU AI Act: four risk tiers, conformity assessment, post-market monitoring.

China

REGISTRATION · SECURITY

Algorithm filing, data governance, and security review for public-facing systems.

United States

SECTORAL · VOLUNTARY

No federal statute; lifecycle guidance via the NIST AI Risk Management Framework.

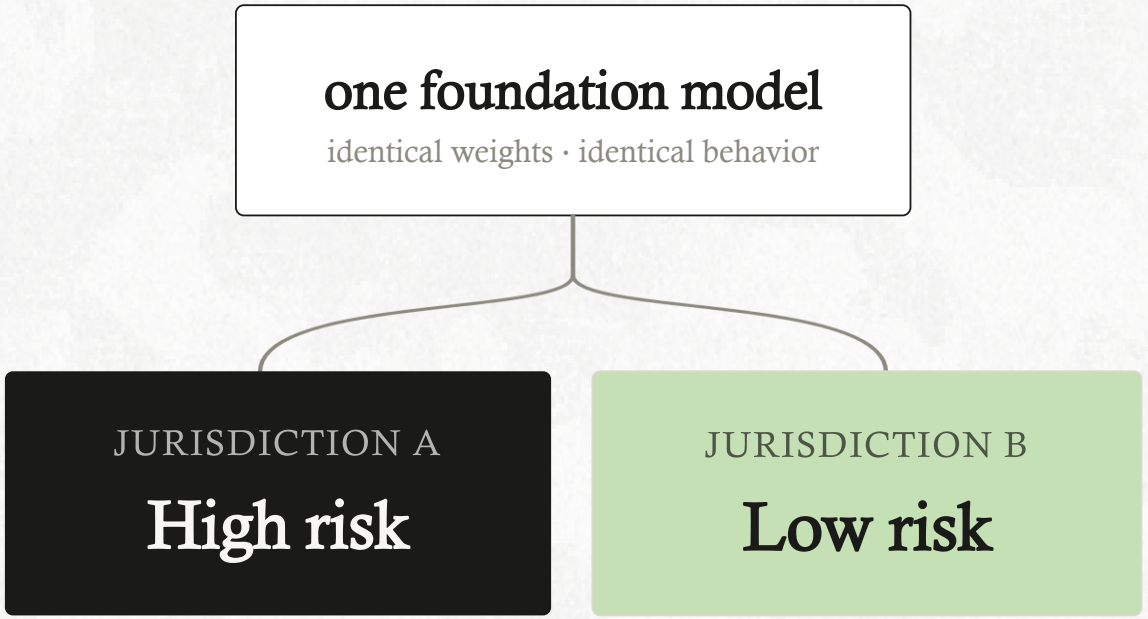
ASEAN

NON-BINDING · REGIONAL

Generative-AI principles emphasizing innovation, without enforceable requirements.

The Standardization Vacuum

The same system can be high-risk and low-risk at once



Without a shared technical language, classification diverges by border, producing **compliance uncertainty**, **duplicated assessments**, and barriers to cross-border deployment.

The result is structural fragmentation that acts as a **non-tariff barrier**, disproportionately burdening SMEs while favoring large incumbents.

Our Position

Laws set the thresholds; standards operationalize them

Laws are indispensable for normative thresholds and enforcement, but insufficient to ensure **consistent operationalization** across heterogeneous systems and jurisdictions.

We argue for a **complementary technical layer** : shared, machine-readable representations of AI risk.

Laws
DEFINE WHAT

What constitutes acceptable AI behavior, normative thresholds and enforcement authority.

↓ demonstrated through ↓

Standards
SPECIFY HOW

How compliance is shown in practice, ISO-like, machine-readable interoperability protocols.

Precedent

GDPR succeeded because standards made it actionable

Ambitious regulation drives global change only when paired with implementation mechanisms. GDPR was operationalized through technical and organizational standards.

THE LAW

GDPR

Harmonized privacy obligations with extraterritorial reach and substantial penalties.

→

IMPLEMENTATION STANDARD

ISO 27001

A unified information-security management system mapping requirements to controls.

+

IMPLEMENTATION PRINCIPLE

Privacy by Design

Privacy embedded proactively across the full data lifecycle, by default.

Caveat: ISO 27001 governs organizational *process*; AI manifests must govern model *outputs,* behavior that is stochastic and emergent.

The Proposal

We propose machine-readable AI risk manifests

An **AI nutrition label** : a modular, versioned manifest, analogous to a software bill of materials, that can be parsed, validated, and compared programmatically.

It carries an interoperable compliance credential across borders, integrating into MLOps pipelines, procurement, and regulatory workflows.

```
{
"manifest_version"
:
"1.2"
,

"system_id"
:
"fm-7b-instruct"
,

"intended_use"
:
"decision-support"
,

// risk class is jurisdiction-tagged
"risk_class"
:
{
"eu_ai_act"
```

Minimum Viable Baseline

Three dimensions, reported in a shared vocabulary

01 — FAIRNESS

Bias

At least one global fairness metric, with demographic groups and mitigation strategy disclosed.

must report · should stratify by group

02 — SUSTAINABILITY

Energy

Training and inference energy with full measurement context — hardware, utilization, methodology.

must disclose hw context

03 — LINEAGE

Data provenance

Verifiable record of data sources and lineage, enabling downstream traceability and audit.

must hash dataset artifacts

These do not harmonize legal thresholds — they let jurisdiction-specific obligations be read through one common interoperability layer.

Answering The Objections

Standards need not stifle innovation or entrench incumbents

OBJECTION 1

Formal standards constrain fast-moving research and slow innovation.

OUR REPLY

This assumes the absence of standards preserves agility. It overlooks the **coordination costs** that fragmented requirements already impose at scale.

OBJECTION 2

Compliance burdens entrench large incumbents and raise barriers for SMEs.

OUR REPLY

Uncoordinated fragmentation **already** costs small actors more. The issue is not whether standards exist, but how they are **designed**.

Modular, versioned, outcome-oriented standards specify **what** must be demonstrated, not **how,** enabling infrastructure, not gatekeeping.

The Way Forward

From siloed compliance to interoperable conformance

01 **Open, modular, extensible protocols** — with low-cost implementation paths, reference implementations, and capacity-building for the Global South and SMEs.

02 **A multi-stakeholder body** (ISO, IEC, IEEE) releasing major schema versions on multi-year cycles, with room for localized modules.

03 **Standards as coordination infrastructure** — embedded in certification, sandboxes, and procurement; complementing law, never replacing it.

DATA INTELLIGENCE LAB

Computational Intelligence and Operations Lab

Thank You!

If you have any questions, please ask!