



AIMLIA PRIMER

Artificial Intelligence / Machine Learning Impact Assessment A Practical Guide for Legal, Compliance, and Product Teams

CREATED BY JOSHUA HEIMAN
EDITED AND REVISED BY CHIARA WIRZ

What is an AIMLIA?

An **Artificial Intelligence / Machine Learning Impact Assessment (AIMLIA)** is a structured, periodically iterative process for **identifying, evaluating, and mitigating the risks of AI/ML systems** before and during deployment.

It combines legal, operational, and ethical considerations into a single workflow that can be integrated into your existing risk assessments, Product, Governance, and other Compliance processes.

Why Conduct an AIMLIA?

- **Legal Compliance:** Meet obligations under privacy, consumer protection, sectoral, and emerging AI-specific laws, regulations, and industry standards (e.g., CPRA, GDPR, EU AI Act, NIST AI Risk Management Framework).
 - **Risk Management:** Identify potential harms, liabilities, and operational disruptions early.
 - **Ethical Accountability:** Ensure AI systems are fair, transparent, and aligned with organizational values.
 - **Business Enablement:** Foster informed risk tolerance decisions and reduce the risk of costly rework, product delays, and reputational damage.
-

The AIMLIA Process

Each step can be scaled for the size and risk profile of the AI/ML use case.
The process is **iterative** — repeat as the system evolves.

1. Assess – Define Scope and Context

Goal: Clearly understand what the AI/ML system will do, where it will operate and data will be hosted, and who it affects.

Checklist:

- Describe the AI/ML system, intended use cases and functionality.
 - Identify stakeholders: internal teams, external users, vendors, regulators.
 - Map jurisdictions and relevant legal regimes.
 - Consider potential for scope creep (new uses not originally intended).
-

2. Identify – Spot Legal, Ethical, and Operational Risks

Goal: List all foreseeable risks from multiple angles.

Checklist (non-exclusive list):

- Data risks: sensitive categories, data provenance, training datasets, cross-border transfers.
 - Model risks: Risk-based compliance requirements, bias, explainability, robustness, adversarial vulnerability.
 - Regulatory risks: applicable laws and regulations, licensing, sectoral rules.
 - Ethical risks: impacts on vulnerable populations, potential misuse.
-

3. Map – Document Data and Decision Flows

Goal: Understand exactly how information moves and decisions are made.

Checklist:

- Data sources, collection methods, storage locations, and retention.
- Data transformations: anonymization, aggregation, enrichment.
- Decision points: when and how the model influences outcomes.

- Roles and responsibilities: controller, processor, vendor, partner.
- Cross-border data transfers and lawful bases.

4. Limit – Apply Safeguards and Controls

Goal: Minimize risks through technical, contractual, and procedural controls.

Checklist:

- Data minimization and purpose limitation.
- Access controls and encryption.
- Contractual restrictions with vendors and partners.
- Guardrails on model use (e.g., human-in-the-loop for high-stakes decisions).
- Policy enforcement: geo-blocking, consent verification, output filtering.

5. Integrate – Embed into Governance and Operations

Goal: Make AI/ML risk management a repeatable part of business processes.

Checklist:

- Incorporate AIMLIA into software development life cycles and procurement workflows.
- Partner with business functions to make informed risk tolerance decisions and measure performance.
- Define escalation protocols for high-risk or non-compliant uses or outputs.
- Assign cross-functional ownership (Legal, Privacy, Product, Security).
- Establish and periodically update AI/ML policies, governance frameworks, company-wide trainings to ensure robust compliance.
- Include AIMLIA outcomes and performance metrics in compliance reports and board updates.

6. Audit – Monitor, Test, and Document Continuously

Goal: Ensure ongoing compliance, performance, and readiness for regulator or client review.

Checklist:

- Bias and fairness testing at defined intervals.
 - Model performance monitoring and drift detection.
 - Documentation: records of processing, model cards, decision logs.
 - Incident response procedures for identified harms or breaches.
 - Periodic review and re-assessment of AIMLIA.
-

Tips for Successful AIMLIA Adoption

- **Start Early:** Begin the AIMLIA process at the concept stage, not post-deployment.
 - **Involve the Right People:** Legal, Privacy, Compliance, Product, Engineering, Security, and Ethics teams should all contribute.
 - **Right-Size the Effort:** Match the depth of the AIMLIA to the risk level of the AI use case.
 - **Document Everything:** Written records and data logs are your best defense in regulatory and litigation contexts.
 - **Review Regularly:** Laws, risks, and technology change quickly — keep the AIMLIA living and current – keep an inventory for all AI/ML systems and their AIMLIAs.
-

Resources & References

- **NIST AI Risk Management Framework** (2023) – U.S. federal guidance on AI risk governance.
- **OECD AI Principles** – International best practices for trustworthy AI.
- **EU AI Act** (pending) – Risk-based obligations for AI providers and users.
- **ISO/IEC 23894** – AI risk management standard.
- **CPRA** (California Privacy Rights Act) – Sensitive data protections and high-risk processing assessments
- **GDPR** – Special category data, DPIA requirements, cross-border data transfer rules..

Introducing AIMLIA

(Artificial Intelligence / Machine Learning
Impact Assessment)



Navigating the impact
of AI with precision and vision.