AI Governance, MLOps

mit omega-ml

Januar 2025

Wie omega-ml bei KI Governance unterstützt

KI Governance muss laufend mit starken Engineering-Prozessen und -Tools umgesetzt werden; keine einmalige “organisatorische Übung”

① Werkzeug zur operativen Umsetzung von KI Governance

MLOps “aus einem Guss” ✅
Die KI- und MLOps Technologie-Landschaft ist kompliziert. omega-ml liefert alle vor-integrierten Bausteine für Entwicklung, Betrieb, Überwachung

KI Lebenszyklus von A bis Z ✅
Transparente und nachvollziehbare Datenbeschaffung aus jeglichen technisch erreichbaren Quellen, Modell-Entwicklung von Anfang an “sauber” getrackt und dokumentiert, geordnete Trennung von Entwicklung und Betrieb, integriertes Logging & Monitoring der Modell-Nutzung

Für alle KI Use Cases ✅
Dank einheitlicher, flexibler Architektur bildet omega-ml die zentrale Plattform für alle KI Use Cases. Auf operativer Ebene lassen sich die KI Use Cases effizient entwickeln, testen und betrieben. Auf taktischer Ebene stehen die wesentlichen Informationen im Modell-Inventar und der integrierten Dokumentation zur Verfügung.

② Nachvollziehbarkeit für alle Daten- und KI-Modelle

Automatisches Inventar ✅
- Erfassung der Daten-, Modelle, Schnittstellen für KI-Services
- Metadaten über Modelle erfassen u.a. Daten-Lineage, Versionen, Typus
- Quelle/Referenz für zentralisiertes IT Inventar

Einfaches Audit-Logging ✅
- Automatisches Log von Trainings- und Evaluationsprozessen (technische Logs)
- Metriken-Tracking in Entwicklung-, Test und Produktion

Integriertes Drift-Monitoring ✅
- automatisches Monitoring aufgrund von laufenden Logs
- Erweiterbare Metriken und Alert-Regeln

Integration in moderne IT Entwicklungsprozesse ✅
- Einfache Nutzung in bestehenden Entwicklungsumgebungen
- DevOps und CICD

③ Reduzierte Komplexität für alle KI Anwendungen

Einheitliche Architektur ✅
alle KI Anwendungen folgen demselben Bau-Muster

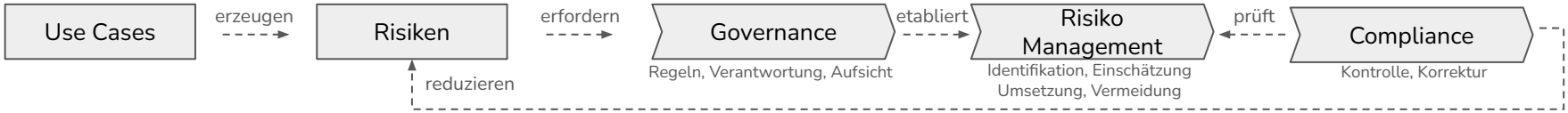
Eindeutige Zuständigkeiten ✅
Plattformbetrieb v.v. Daten- und Modell-Verantwortung ist jederzeit klar (kein “über den Zaun werfen”)

Integration in IT Operations & Security, ohne Vendor-Lock-in ✅
Open Source im Kern, ermöglicht Einsatz bestehender Data Science und KI Technologien, keine Abhängigkeiten (z.B. freie Wahl der Cloud oder on-premise)

Skalierbar und flexibel ✅
Beliebige Art und Anzahl der KI Anwendungen, Modelle, Datenquellen, Performance- Anforderungen

KI Governance nach FINMA 08/24

KI Governance ist Erweiterung der Führungs-, Kontrollstrukturen & -Prozesse



Use Case Relevanz für KI Governance
- Regulierung/Recht
- Finanzielle Auswirkung
- Rechtliche Risiken
- Reputationsrisiken
- Operative Bedeutung
- Betroffene Kunden
- Negative Auswirkungen

Risiko-Wahrscheinlichkeit
- Komplexität der KI ✅
- Daten (Quelle, Qualität, PID, ...) ✅
- Entwicklungs/Qualitäts-Prozesse ✅
- Autonomie & Prozess-Einbindung ✅
- Maintenance-Zyklus ✅
- Vernetzung von KI ✅
- Stabilität, Abhängigkeit ✅

Operationelle Risiken
- Gefahr für Verluste
- aufgrund von Versagen von Menschen, Verfahren, Systemen

Modell-Risiken ✅
- mangelnde Robustheit
- Korrektheit
- Bias, Erklärbarkeit

IT & Cyber-Risiken
- Cyberangriff
- Datenverluste, -leak
- Zugriffsschutz ✅
- Schutz kritischer Daten ✅

Rechts-/Reputation
- Zuordnung Verantwortung
- u.a. durch Abhängigkeiten

Zentrales Inventar ✅
- Risikoklassifizierung
- Massnahmen
- Zuständigkeiten

Vorgaben
- Nutzungsregeln/-grenzen
- Prozesse für Entwicklung, Implementierung, Ueberwachung ✅
- Modell-Tests ✅
- Systemkontrollen ✅
- Dokumentations-Standard
- Schulung, Qualifikation

Outsourcing
- Tests, Prüfung
- Vertragsklauseln
- Verantwortlichkeiten
- Haftungsregelung
- Fähigkeiten, Erfahrung

Datenqualität ✅
- korrekt, konsistent, vollständig, repräsentativ, aktuell, integer
- Bias-/nicht repräsentativ (unpassend für Use Case)
- Datenformat spezifisch (unstrukturiert, Bild, Ton)

Abhängigkeiten
- unklare Datenquellen bei eingekauften Systemen
- Gefahr Manipulation

Modell-Tests ✅
- definierte Metriken/Ziele, Schwellenwerte
- Genauigkeit
- Robustheit
- Stabilität, Bias

Monitoring ✅
- Datenqualität
- Daten- & Modell-Drift
- Analyse von Fehlern
- Anomalie-Erkennung

Dokumentation ✅
- Zweck der Anwendung
- Datenauswahl- & Lineage
- Modellauswahl
- Metriken
- Annahmen, Grenzen
- Testung und Kontrolle
- Fallback-Lösungen

Datenauswahl ✅
- Datenquellen
- Datenqualität, insbes. Integrität, Korrektheit, Zweckmässigkeit, Relevanz, Bias, Stabilität

Kontrolle ✅
- Risikoeinstufung mit Begründung & Prüfung
- Robustheit,Zuverlässigkeit
- Nachvollziehbarkeit
- Reproduzierbarkeit
- Unabhängige Prüfung
- Umsetzung Massnahmen

✅ **MLOps** als Prozess, Methodik & Tooling unterstützt die effiziente operative und taktische Umsetzung (abgestuft nach Risikoeinschätzung; z.B. ist Mitigation von Modell-Risiken unterschiedlich stark ausgeprägt in einem internen KI Tool für Kunden-Segmentierung v.s. Self-Service Investment Advisory für Kunden)

Zusammenfassung von https://www.finma.ch/news/2024/12/20241218-mm-finma-am-08-24/

AI Governance ⇔ MLOps “same, same”

What is MLOps?
The Processes, Principles and Guidelines that define and control
Model Development & Testing, Delivery, Operations & Management of Model Risk

Relation to AI Governance
AI Governance defines the organization-level strategy & policies that MLOps needs to adhere to
MLOps is the platform-level for day-to-day operations & tactical implementation of AI
=> Effective AI Governance is enabled by MLOps

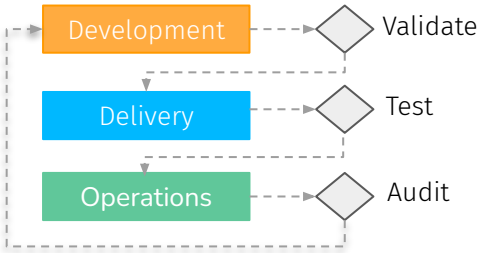
AI Lifecycle Capabilities for AI Governance

mandates capabilities across lifecyle

Development	Delivery	Operations	Risk Management
Reproducibility	Release-Building	Observability	Auditability
Validation	Change Management	Monitoring & Alerting	Conformity Legal, Ethical
Documentation	Catalog / Inventory	Security	Ownership
🤷 Data Scientist	🤷 Data Scientist	🤷 ML Engineer	🤷 Product Owner

Lifecycle Processes for AI Governance

Each phase needs a deliberate check



omega-ml capabilities for AI Governance
- Provided by omega-ml (omega-ml delivers tooling/platform to establish capability)
- Provided in combination with existing processes (omega-ml supports organization-defined capability/processes)
- Processes and tools provided by organization (omega-ml does not currently provide tooling for this)

Vergleich KIVO und FINMA 08/24

Aspekte	Massnahmen und Ergebnisse	Hochrisiko-KI (KIVO)	FINMA 08/2024	Adressierte Risiken	
Organisatorisch	Grundsätze und Regeln	X	X	Auswirkungen auf Gesundheit, Sicherheit, Grundrechte, Bildung, Beschäftigung	Wesentliche Risiken mit Auswirkungen auf finanzielle Stabilität, Kunden bzw. das gesamte Finanzsystem
	AI-Kompetenz / Mitarbeiterschulung	X	X		
	Risikomanagement-System	X	X		
Prozesse, Methoden, Tooling: MLOps	Internes Register, Risikobewertung und -minderung	X	X		
	Datenqualität, Datenschutz	X	X		
	Technische Dokumentation	X	X		
	Überwachung, Protokollierung, menschliche Aufsicht	X	X		
	Cybersicherheit, Robustheit & Genauigkeit, Leitplanken	X	X		
Rechtlich & regulatorisch	Transparenz für Benutzer	X			
	Konformitätsbewertung	X			
	CE-Konformitätserklärung & Kennzeichnung	X			
	Unabhängige Bewertung		X		
	Registrierung, Zusammenarbeit mit Behörden	X	X		
	Datenschutz, andere sektorale Vorschriften	X	X		