INNOQ TECHNOLOGY DAY / BERLIN / 01.12.2021

MLOPs und Model Governance

In ML-Software

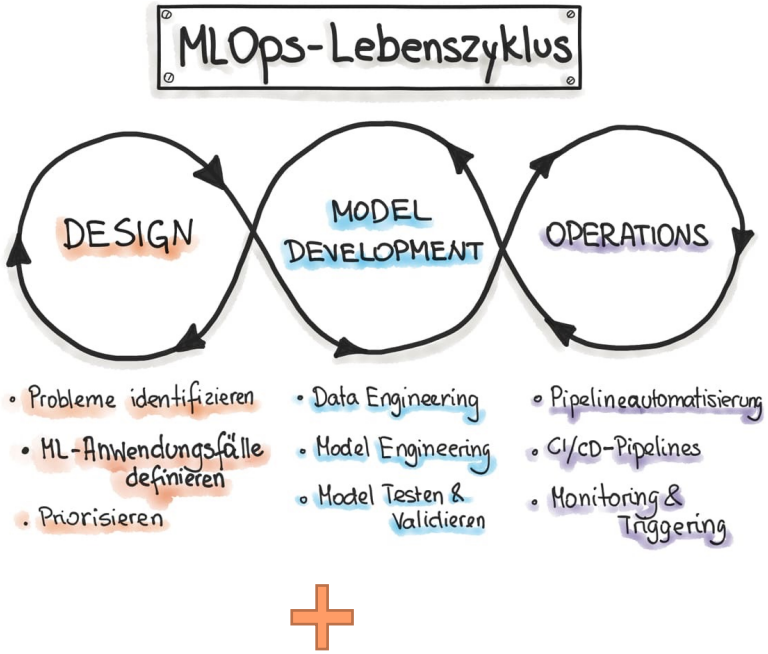
INNOQ

ISABEL BÄR
@isabel_baer

Time-to-Market reduzieren
Lösung: MLOps

Gesetzliche Auflagen und Risiken
Lösung: Model Governance

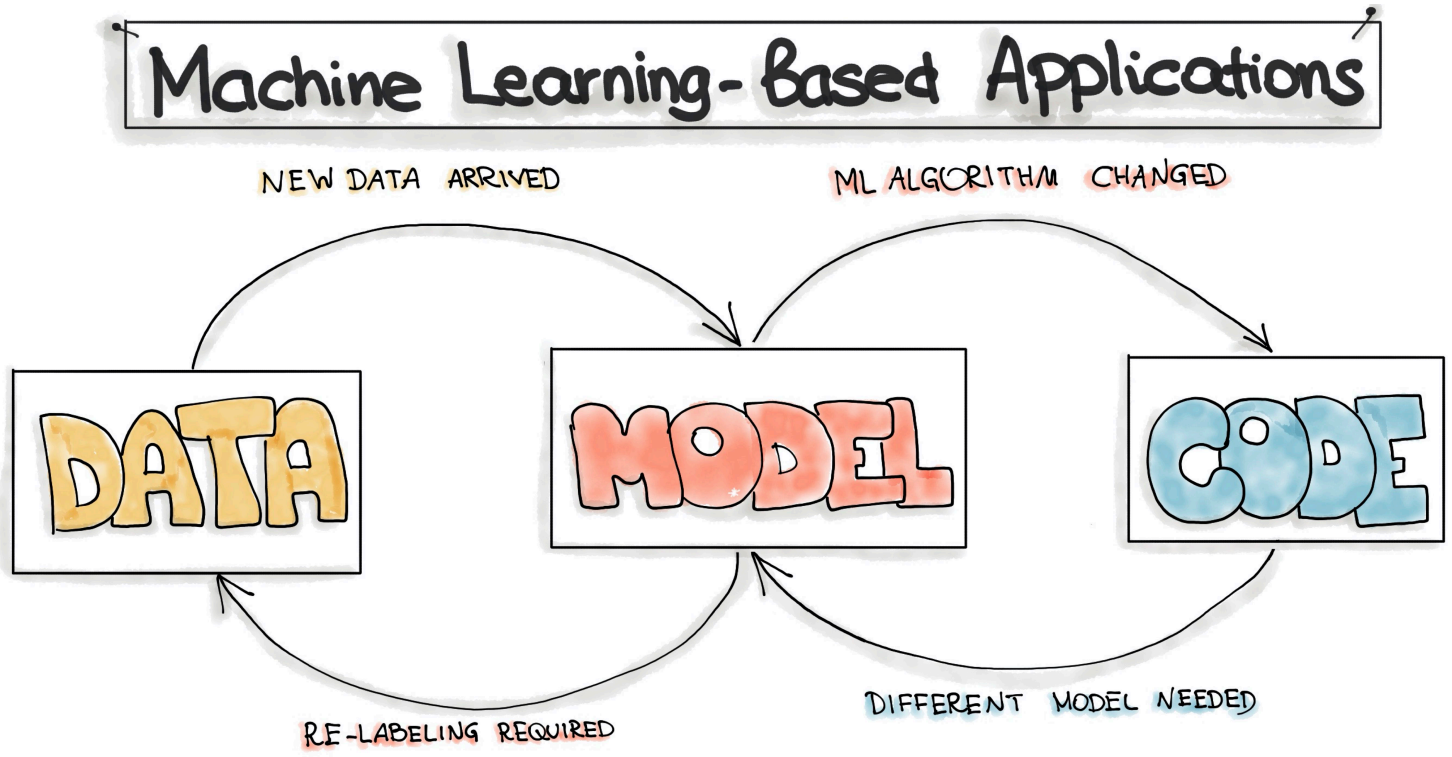
MLOps und Model Governance zusammenbringen



Model Governance ist kein abstraktes, sondern **technisch lösbares Problem**

Time-to-Market reduzieren: MLOps

ML-Software als Herausforderung

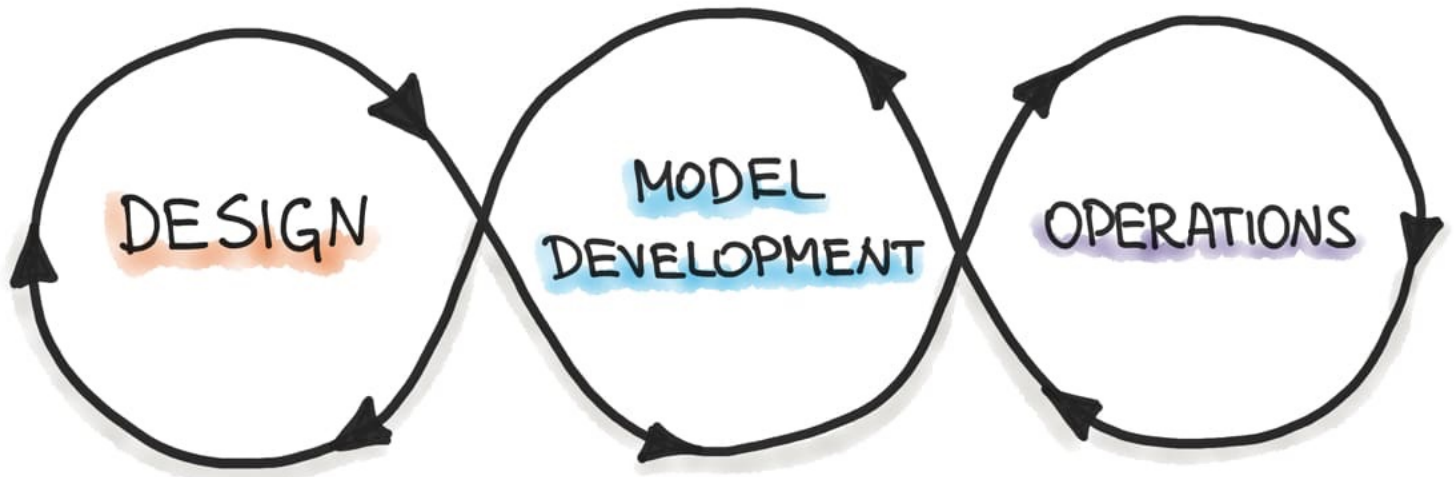


https://ml-ops.org

Changing-Anything-Changes-Everything:

Model Decay

MLOps-Lebenszyklus

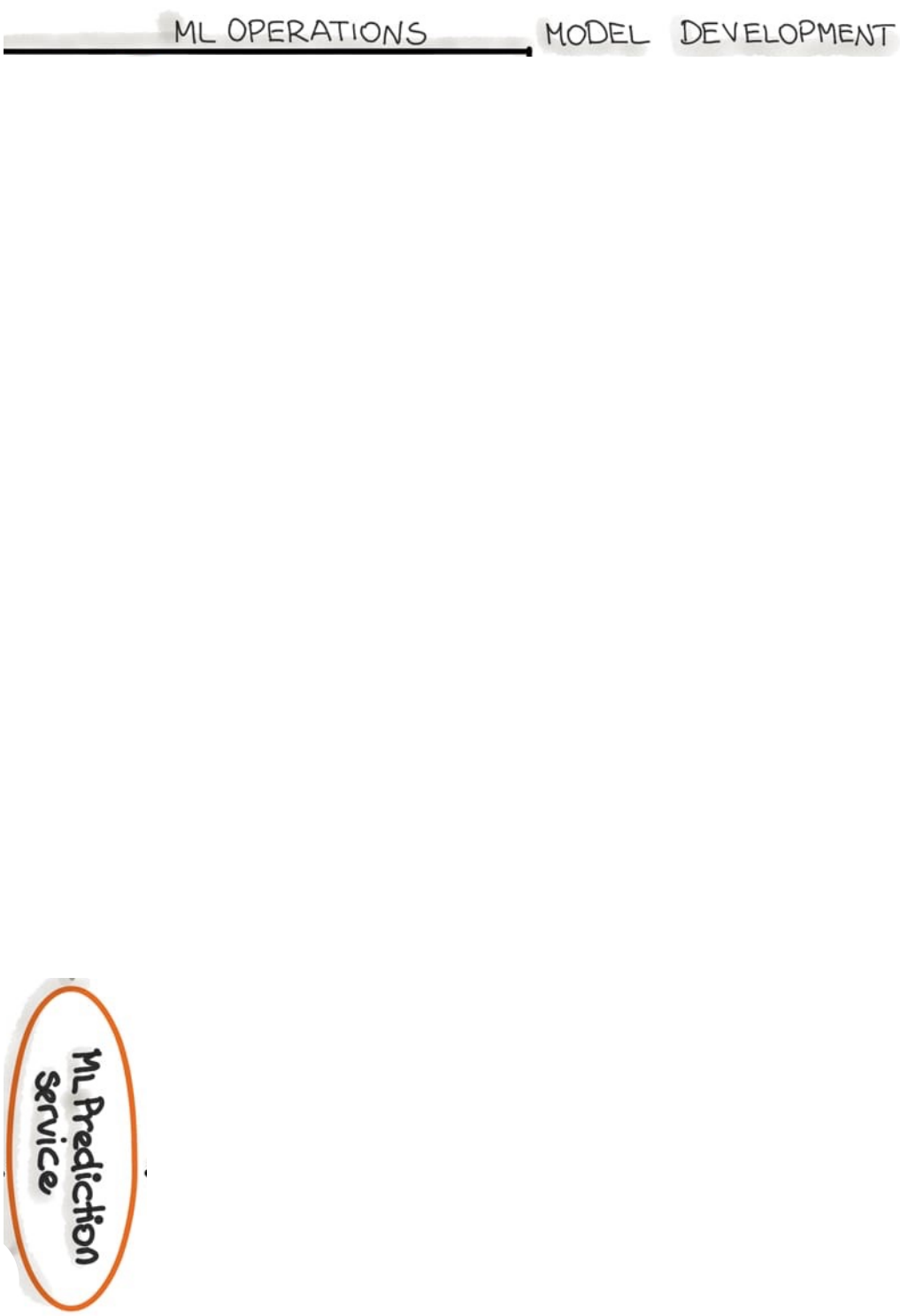


- Probleme identifizieren
- ML-Anwendungsfälle definieren
- Priorisieren

- Data Engineering
- Model Engineering
- Model Testen & Validieren

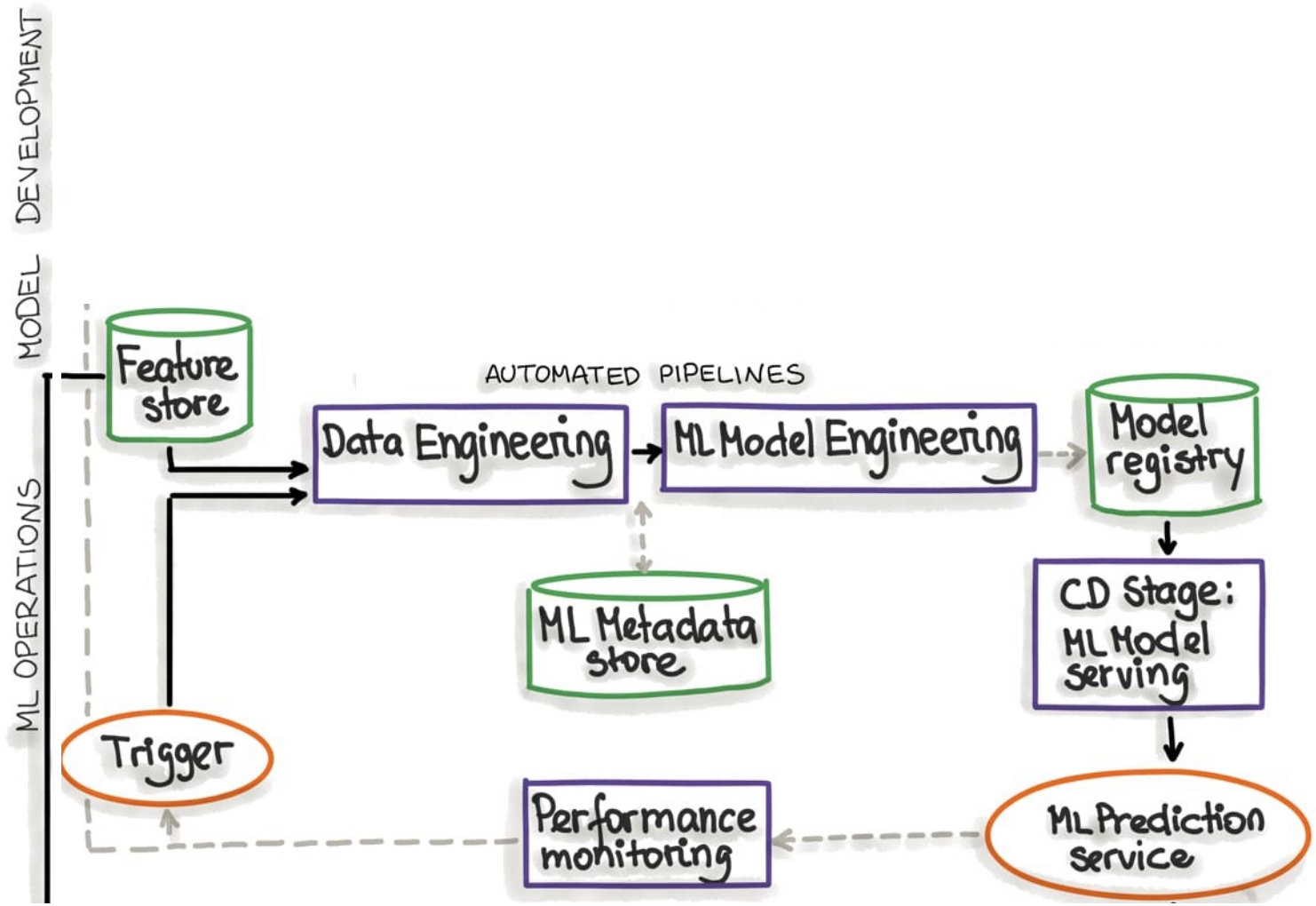
- Pipelineautomatisierung
- CI/CD-Pipelines
- Monitoring & Triggering

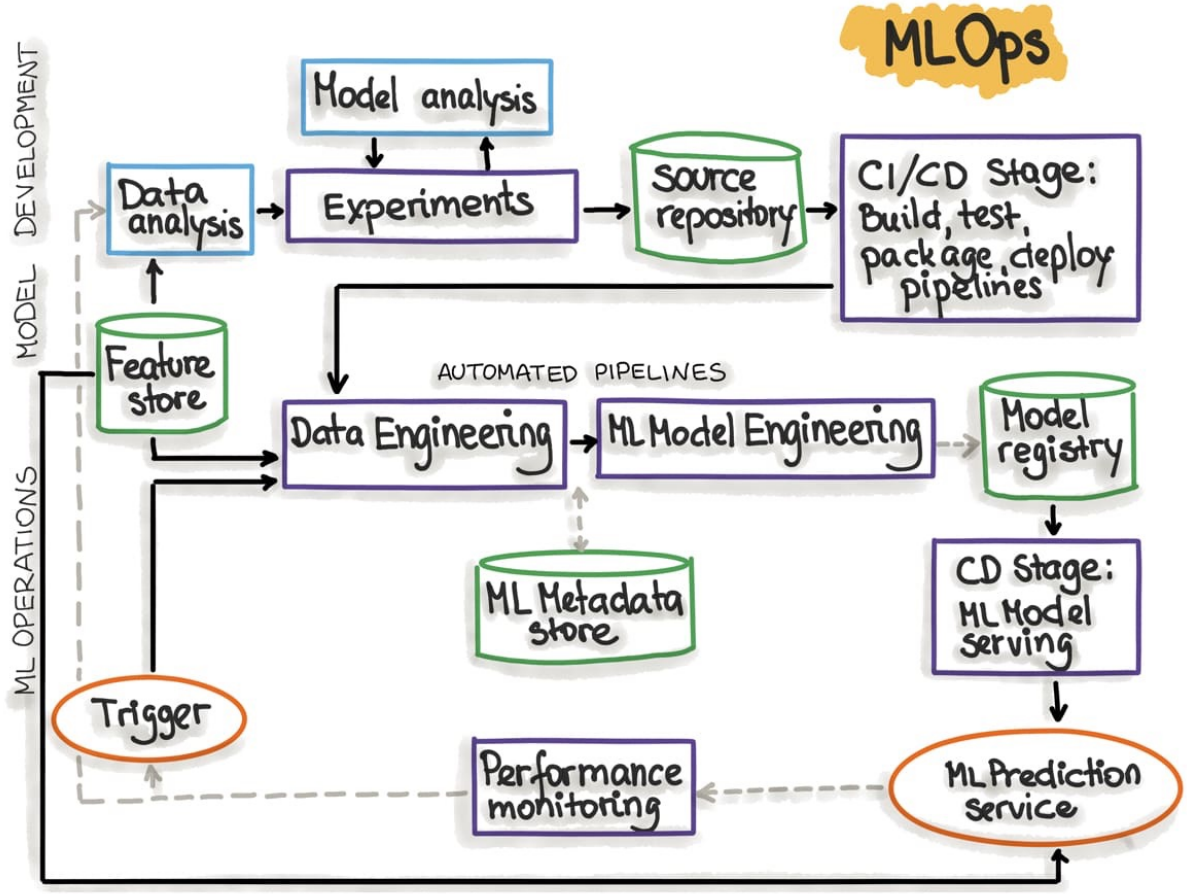
https://ml-ops.org


ML OPERATIONS
MODEL DEVELOPMENT
ML Prediction Service

ML OPERATIONS
MODEL DEVELOPMENT
Data Shifts
Continuous Evaluation
Performance monitoring
ML Prediction service

ML OPERATIONS
MODEL DEVELOPMENT
Trigger
Performance monitoring
ML Prediction service


MODEL DEVELOPMENT
ML OPERATIONS
Feature store
AUTOMATED PIPELINES
Data Engineering
ML Model Engineering
Model registry
ML Metadata store
CD Stage: ML Model serving
Trigger
Performance monitoring
ML Prediction service



https://www.innoq.com/de/articles/2020/10/mlops-operations-fuer-machine-learning/

Development und Operations werden mit MLOPs..

- kombiniert
- automatisiert
- überwacht

MLOPs

Pipeline-Automatisierung

Gesetzliche Auflagen und Risiken
Lösung: Model Governance

Was ist Model Governance...?

Prozesse, durch die ein Unternehmen...

- Richtlinien umsetzt
- Zugriffe auf ML-Modelle kontrolliert
- Interaktionen mit den ML-Modellen und deren Ergebnisse verfolgt
- festhält, auf welcher Grundlage ein Modell erzeugt wurde

https://algorithmia.com/blog/model-governance

Model Governance als Herausforderung für...

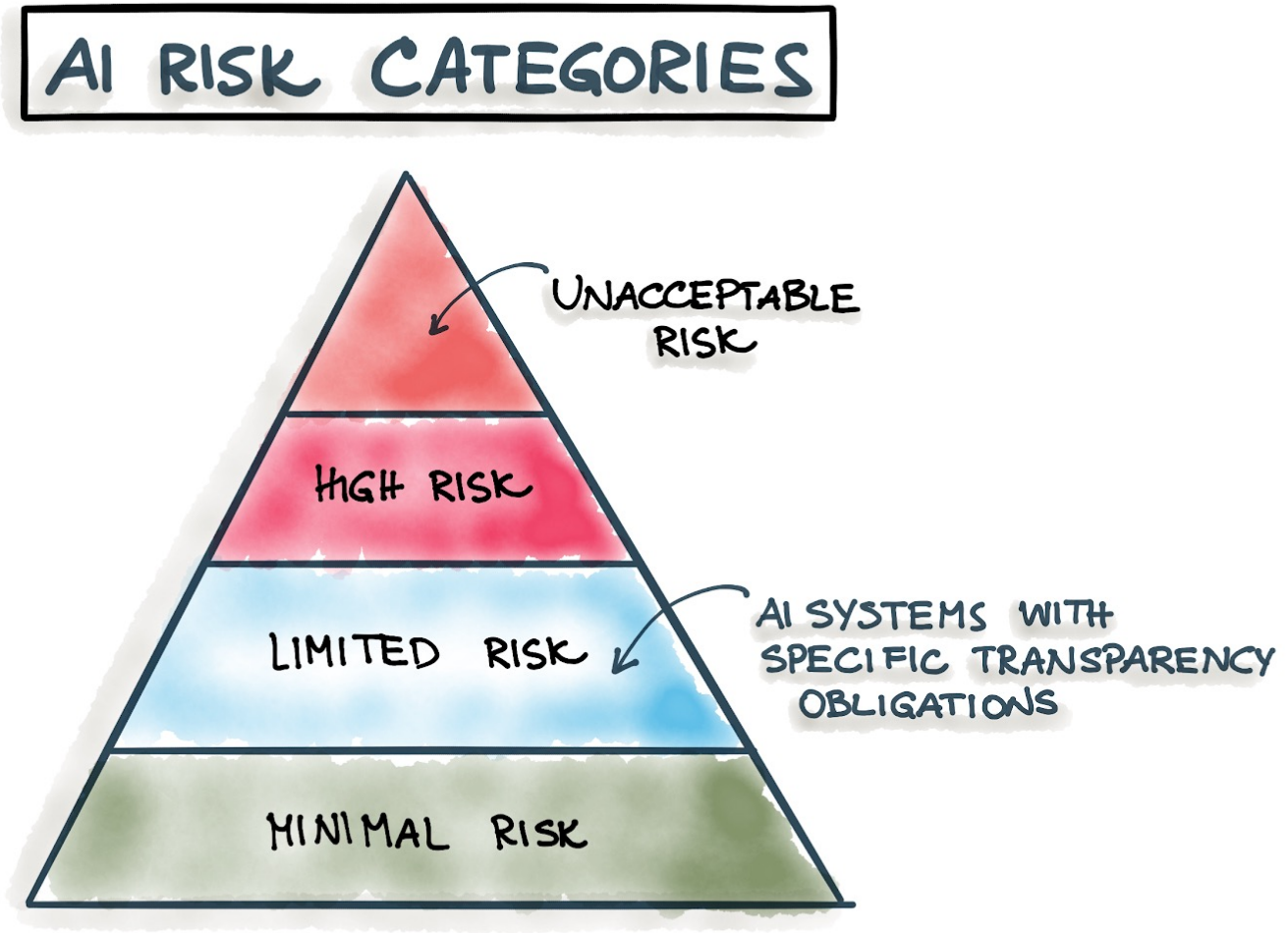
56 % der Unternehmen

https://info.algorithmia.com/hubfs/2020/Reports/2021-Trends-in-ML/Algorithmia_2021_enterprise_ML_trends.pdf?hsLang=en-us

26,2 % der deutschen Unternehmen

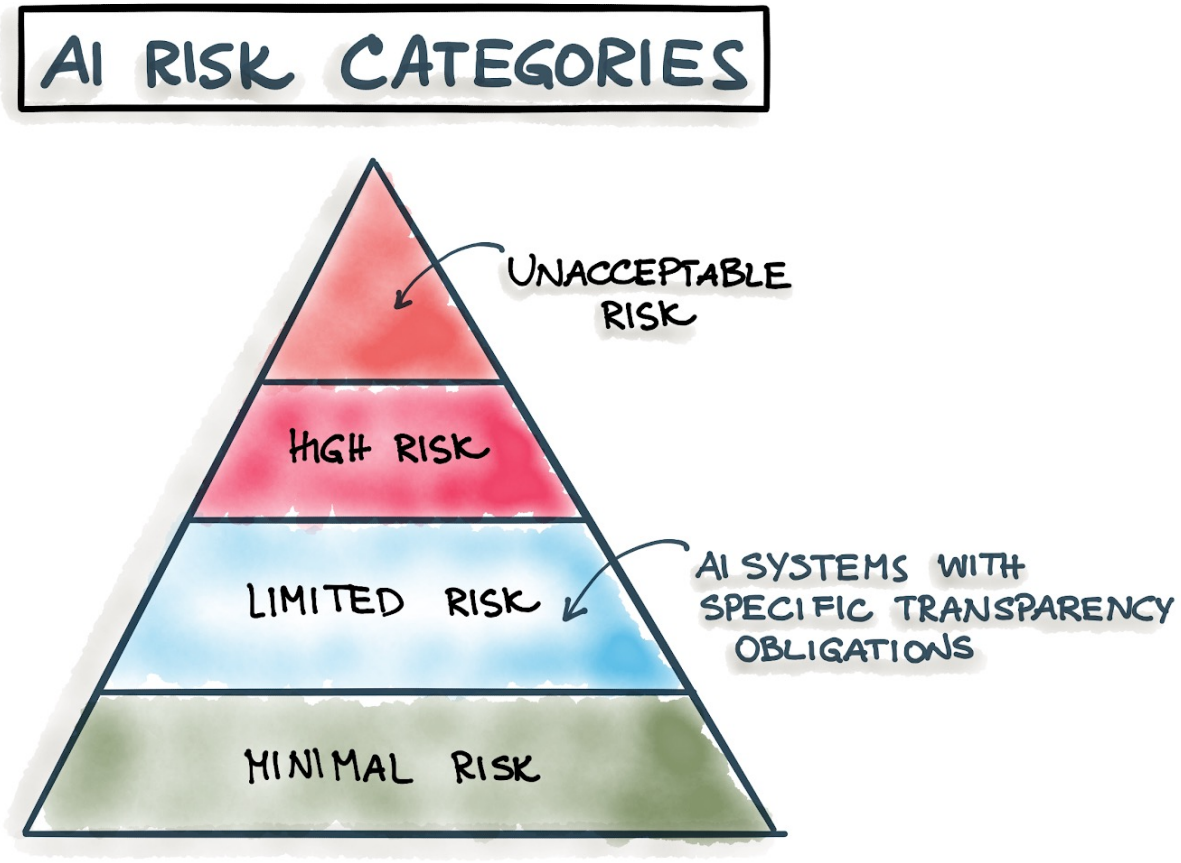
https://www.lufthansa-industry-solutions.com/de-de/studien/idg-studie-machine-learning-2021

EU-Rechtsrahmen für KI



https://germany.representation.ec.europa.eu/news/fur-vertrauenswurdige-kunstliche-intelligenz-eu-kommission-legt-weltweit-ersten-rechtsrahmen-vor-2021-04-21_de

Hochrisiko-Systeme



- Sicherheitskomponenten von Fahrzeugen (Straße, Schiene, Wasser, Luft)
- Beurteilung bei Bewerbungsverfahren, Beförderungen, Kündigungen
- Bestimmung der Kreditwürdigkeit
- Bestimmung des Zugangs zu öffentlichen Leistungen

Hohe Datenqualität

Dokumentation und Protokollierung

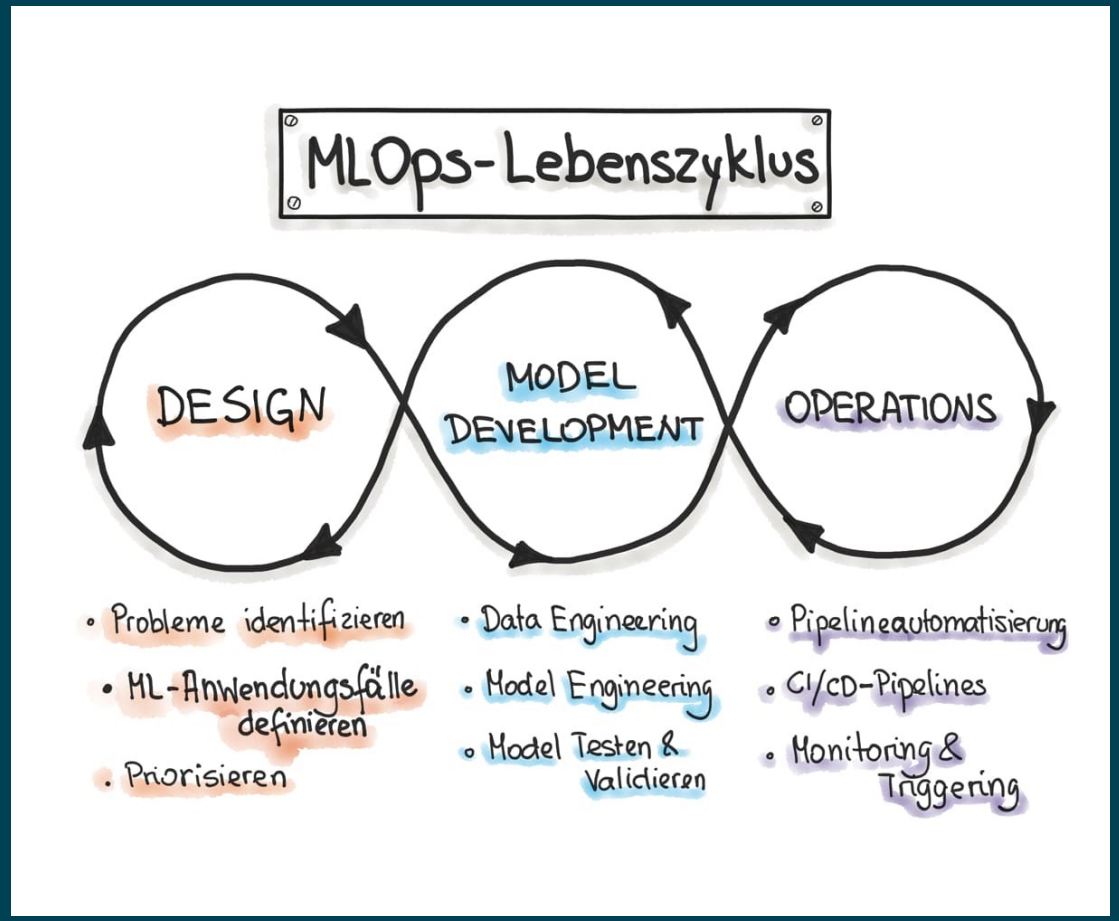
Risikobewertung und -minderung

Diskriminierungsfreiheit

Nachvollziehbarkeit und Transparenz

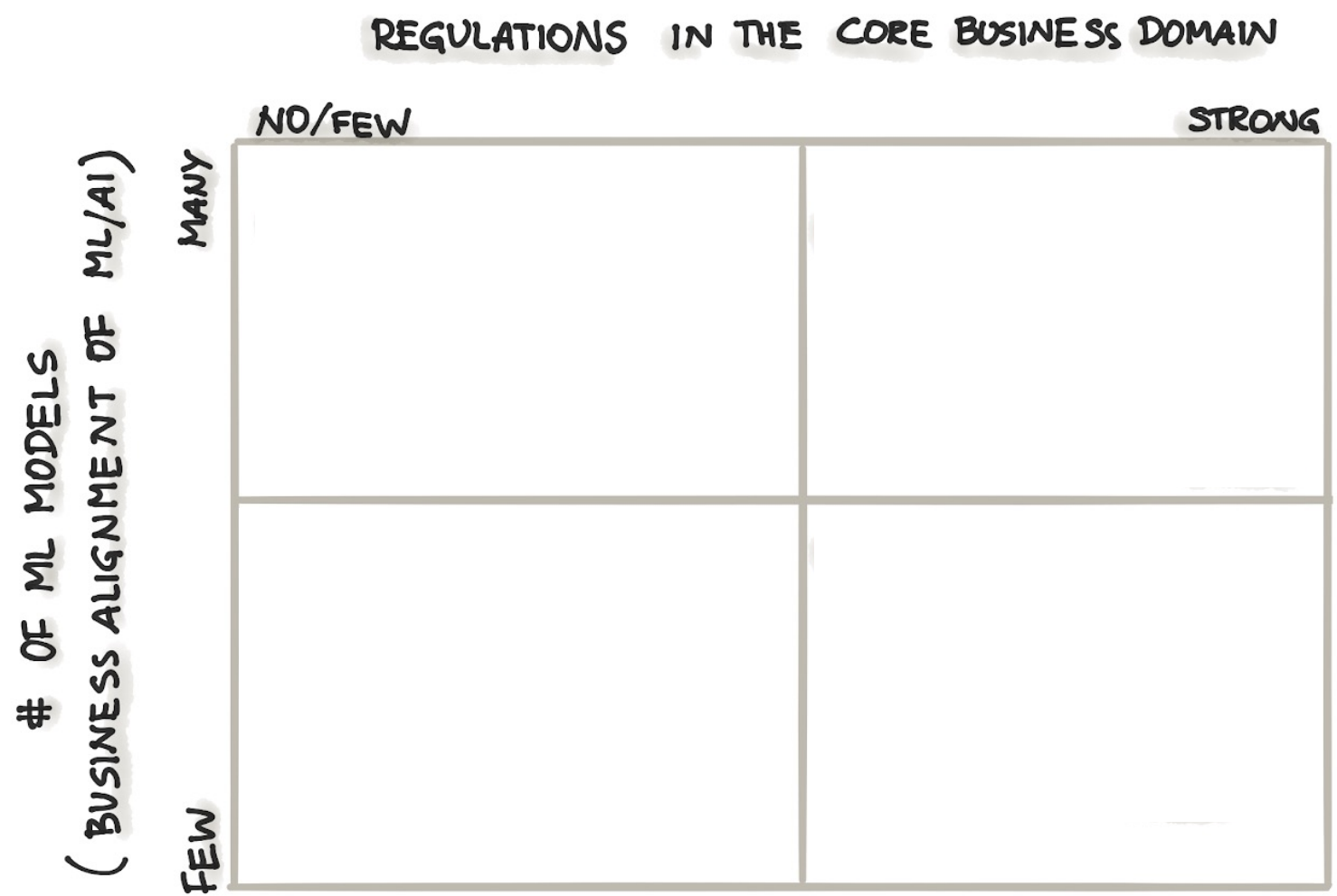
Robustheit Sicherheit Genauigkeit

Konformitätsprüfung (CE-Kennzeichnung)



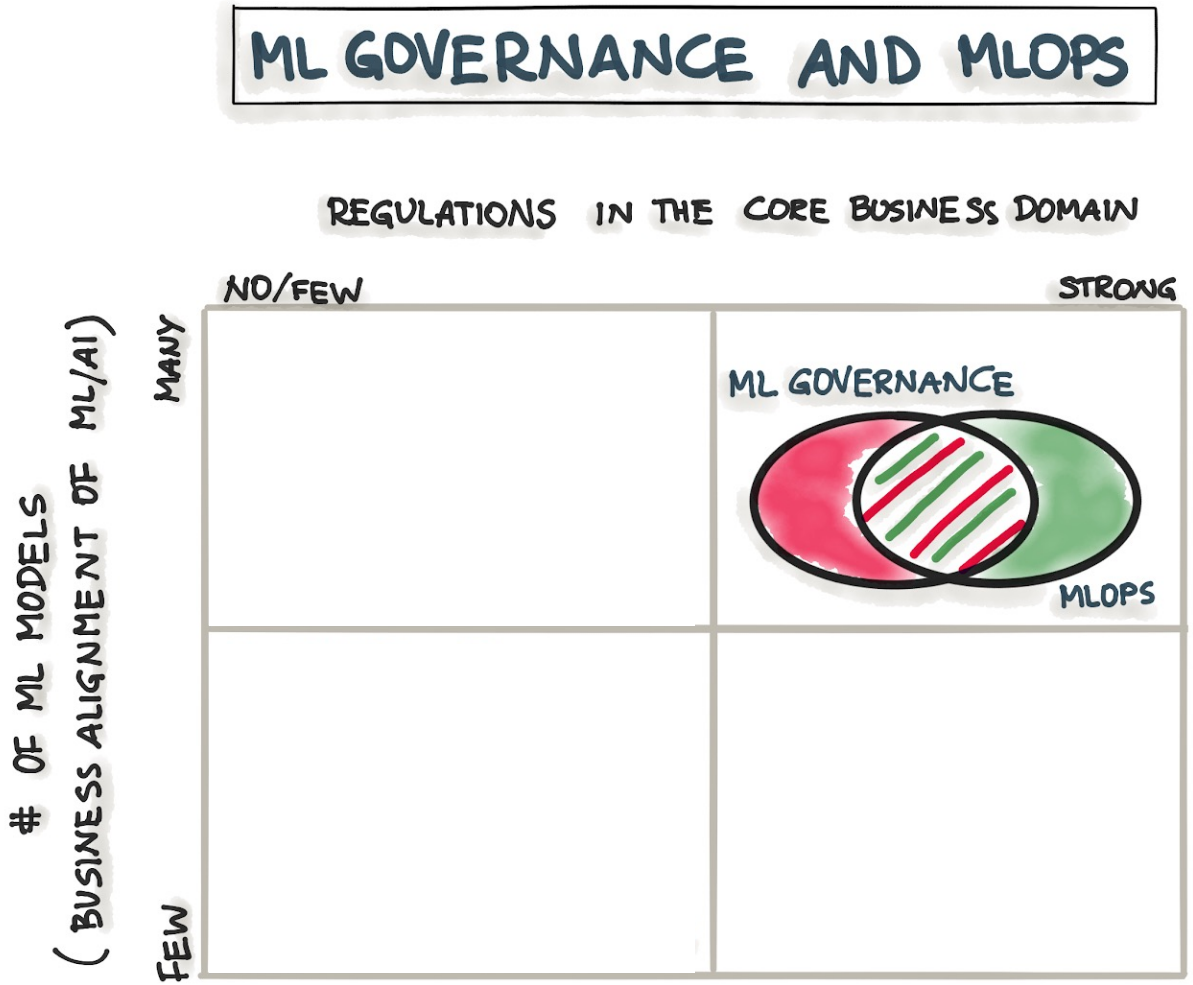
+ **Model Governance**

ML GOVERNANCE AND MLOPS



@visenger

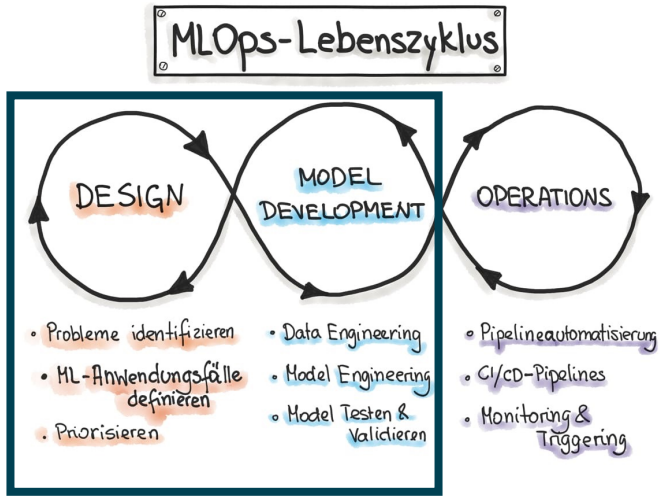
Starke Regulierung & Starkes BA



Hochrisiko
-Systeme

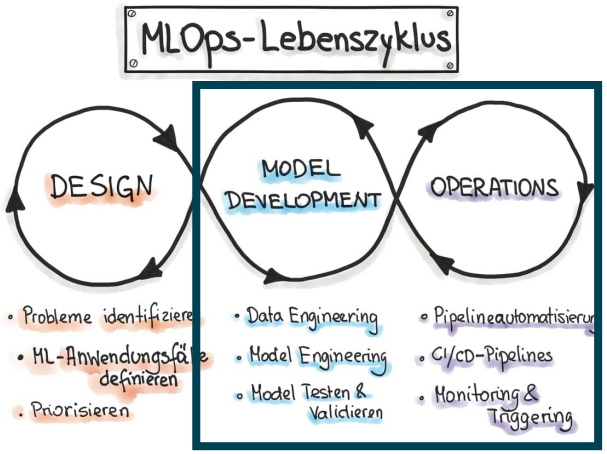
Unternehmerisches
Risiko

Regulierte
Branchen
(Gesundheits-
und
Bankensektor)



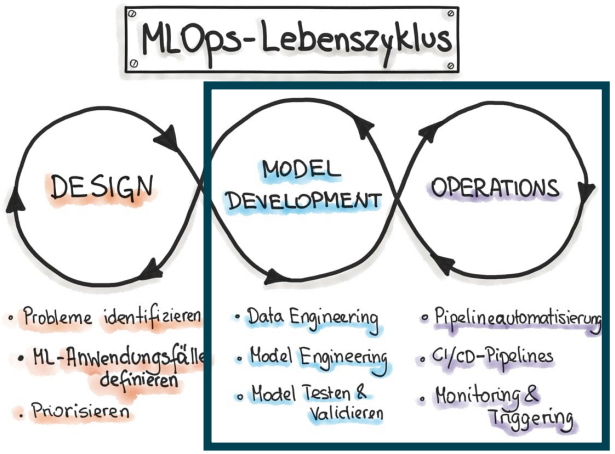
MLOps Lebenszyklus	Komponente	Aufgaben und Artefakte
• Design & Model Development	• **Reproduzierbarkeit**	• Modell Metadaten Management • Modelldokumentation
	• **Prüfbarkeit**	• Validierung (Performance, Eignung, Reproduzierbarkeit)
	• **Erklärbarkeit**	• Erklärungen des Modellverhaltens

https://www.oreilly.com/library/view/the-framework-for/9781098100483/ch01.html



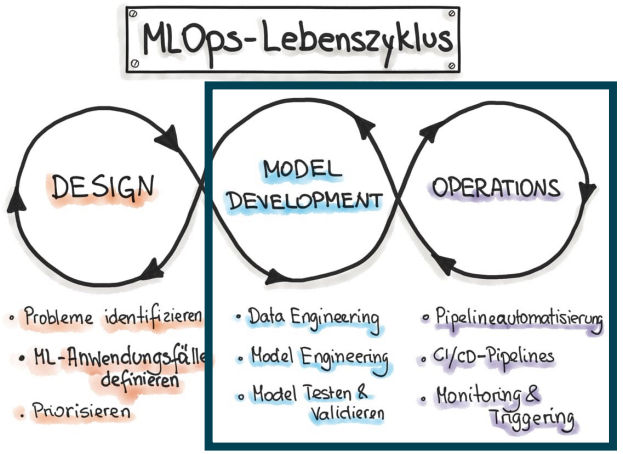
MLOps Lebenszyklus	Komponente	Aufgaben und Artefakte
• Model Development & Operations	• **Monitoring, Sichtbarkeit, Kontrolle**	• Visuelle Informationsaufbereitung (Logging, Metriken, Audits) • Versionierung von Modell und Daten • Usage Reports • Verwaltung von Endpunkten
	• **Monitoring und Alarmierung**	• Plattform- und Infrastrukturintegration mit Dashboard und Monitoring Tools

https://www.oreilly.com/library/view/the-framework-for/9781098100483/ch01.html



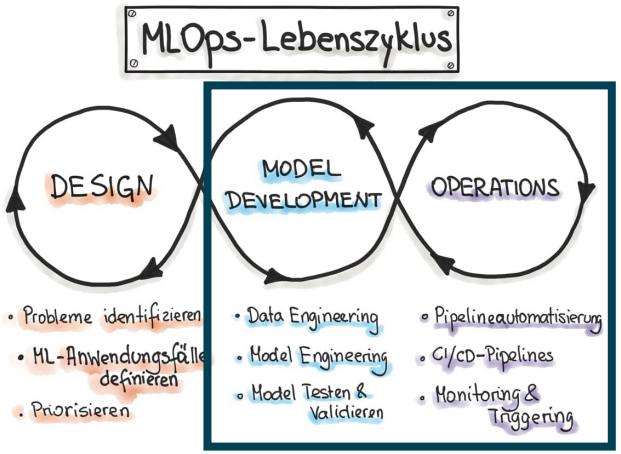
MLOps Lebenszyklus	Komponente	Aufgaben und Artefakte
• Model Development & Operations	• **Sicherheit**	• Daten-, Informations- und Infrastruktursicherheit • Einhaltung von IT-Standards • Authentifizierung • Management von Modellendpunkten und API • Management von Schlüsseln • Systemprüfung

https://www.oreilly.com/library/view/the-framework-for/9781098100483/ch01.html



MLOps Lebenszyklus	Komponente	Aufgaben und Artefakte
• Model Development & Operations	• **Modell-Katalog**	• Registrierung, Speicherung, Versionierung • Anbindung an Speicherort der Modelle • Anbindung an die Quellcodeverwaltung der Modelle und zugehörigen Data-Pipelines (GitHub, GitLab) • Metriken zur Modellnutzung

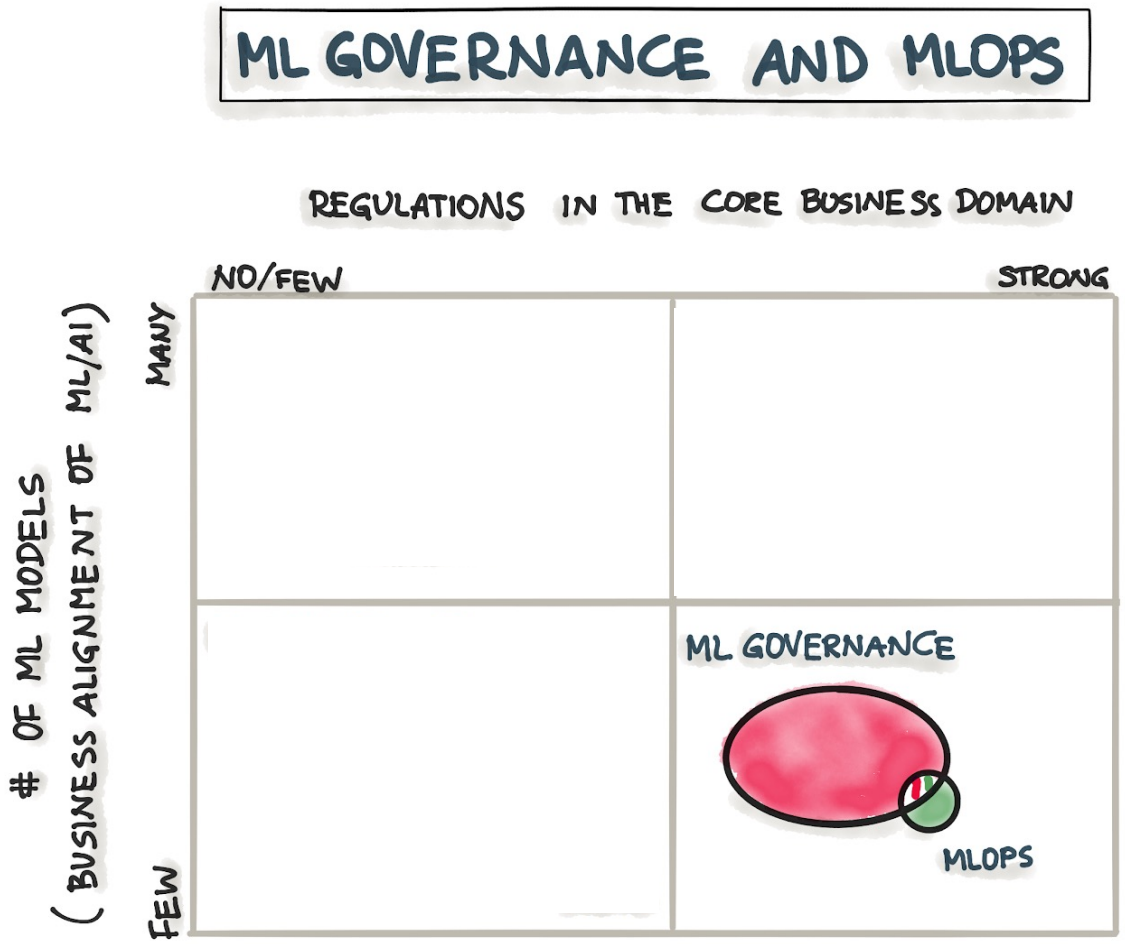
https://www.oreilly.com/library/view/the-framework-for/9781098100483/ch01.html



MLOps Lebenszyklus	Komponente	Aufgaben und Artefakte
• Model Development & Operations	• **Konformität**	• Protokollierung, Metriken, Audits • Sicherheitsüberprüfung • Konformitätsprüfung und Konformitätsbescheinigung (CE-Kennzeichnung)

https://www.oreilly.com/library/view/the-framework-for/9781098100483/ch01.html

Starke Regulierung & Wenig BA

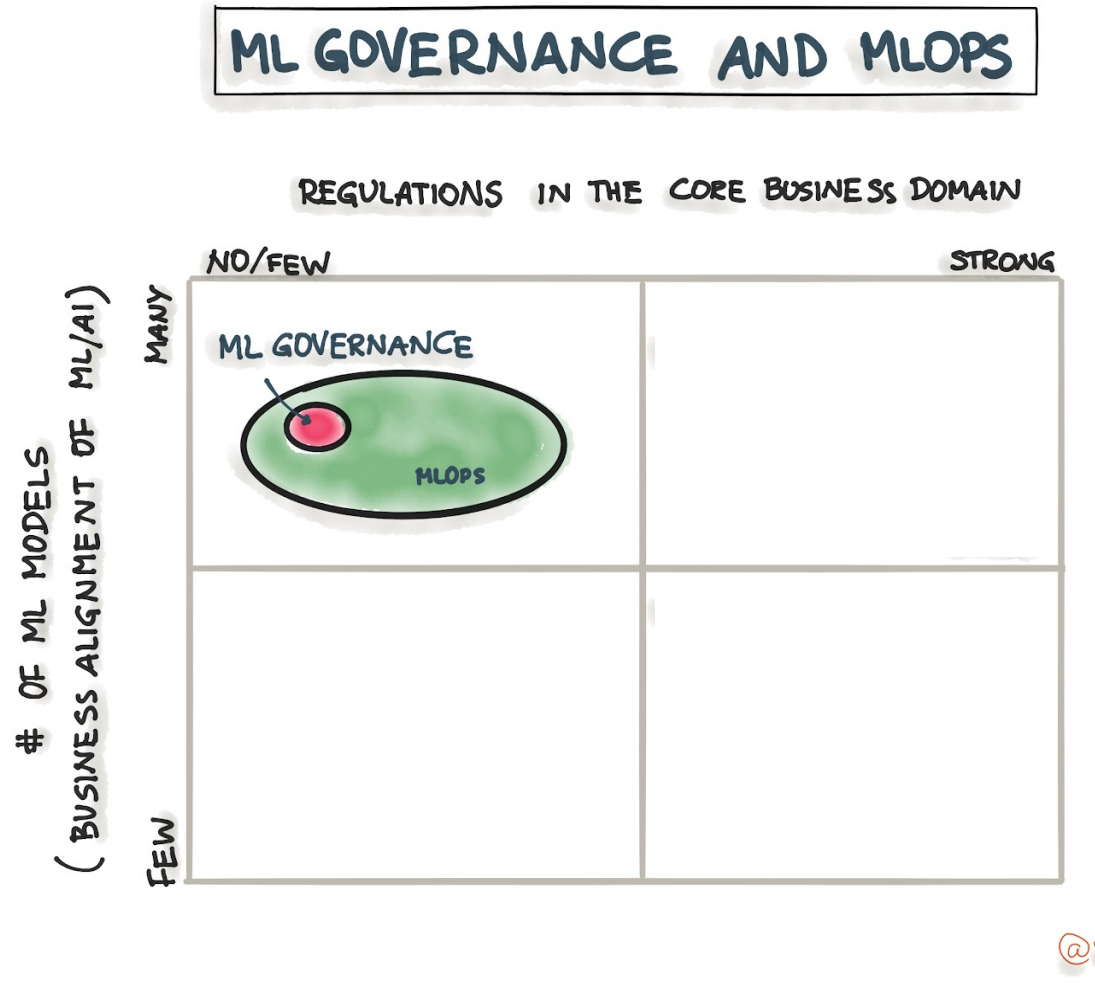


Hochrisiko -Systeme

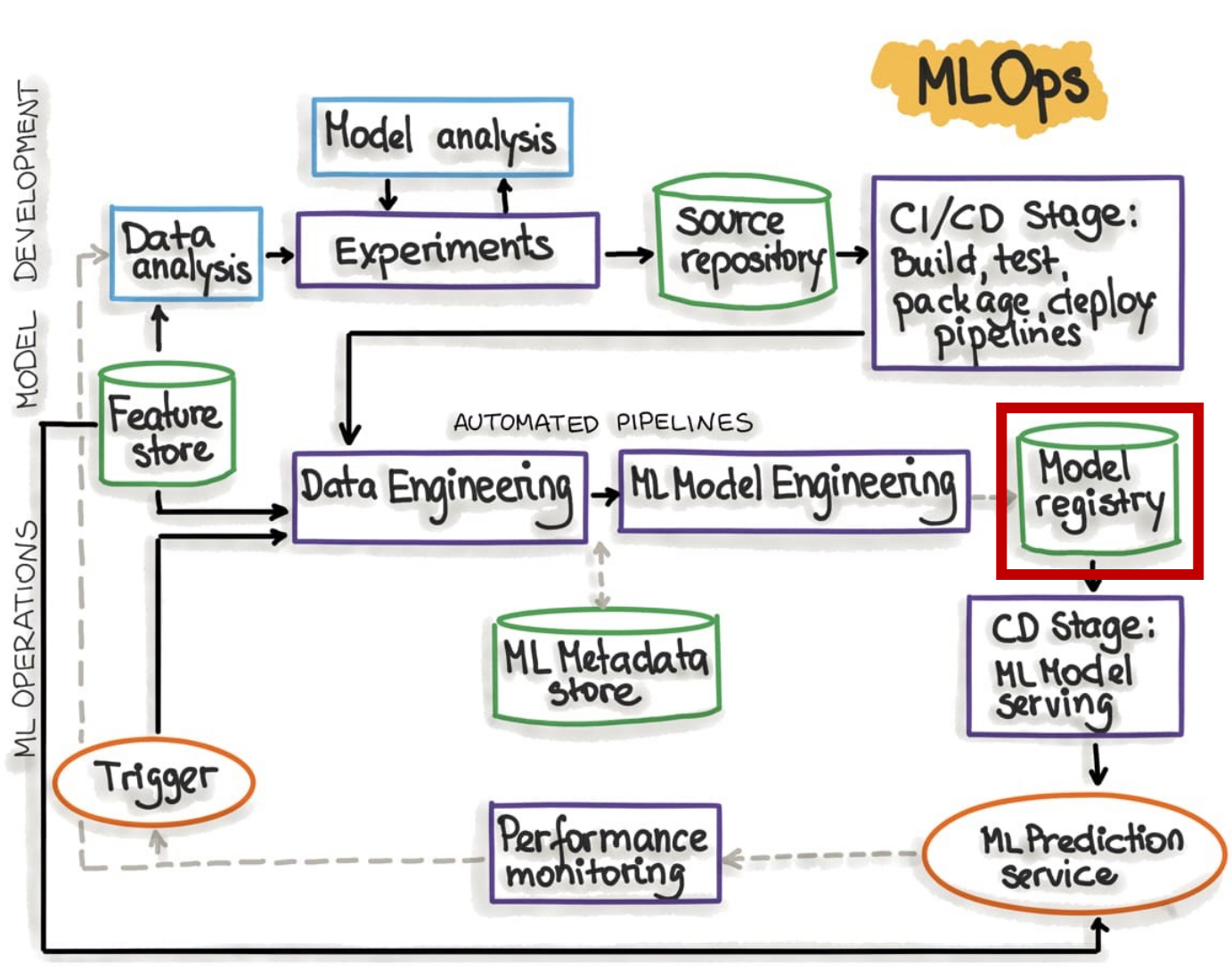
Regulierte Branchen (Gesundheits- und Bankensektor)

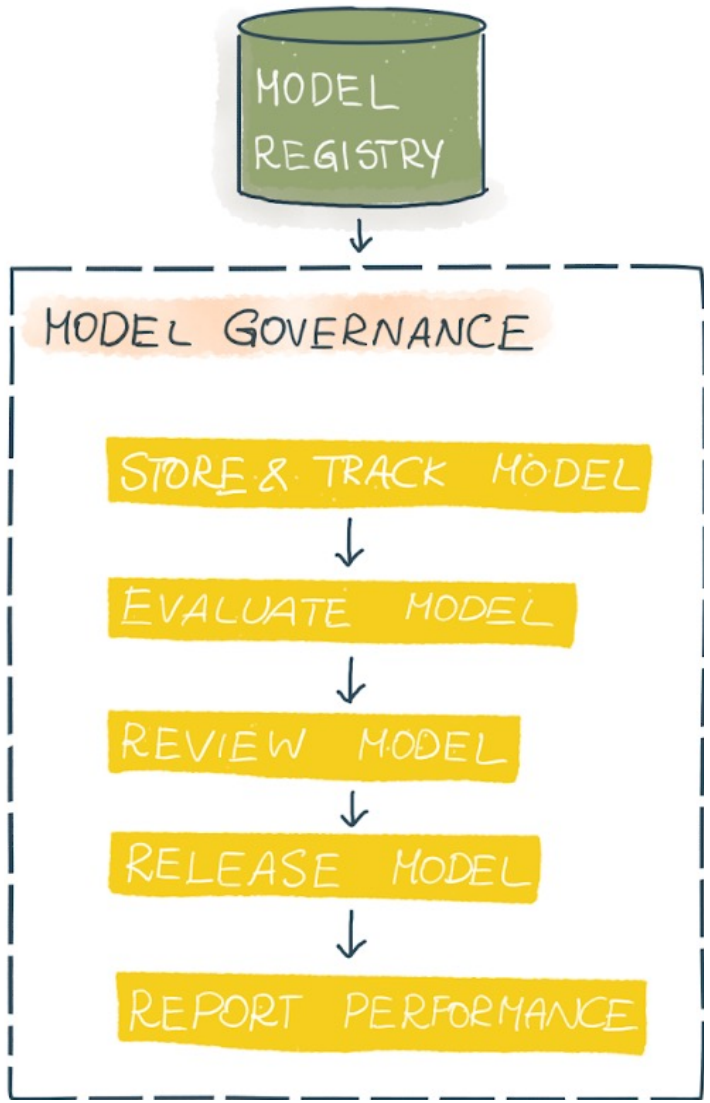
@visenger

Wenig Regulierung & Starkes BA

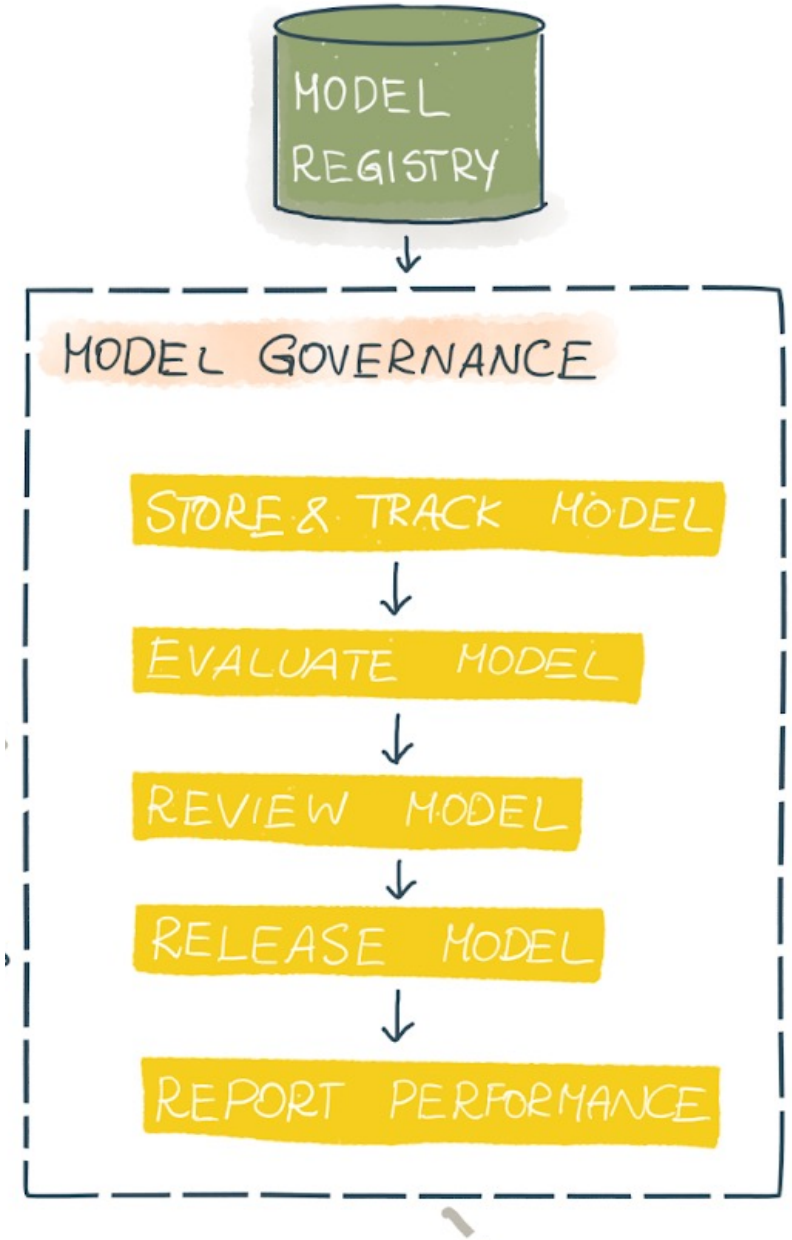


ML-System ist eng an den Unternehmenserfolg gebunden





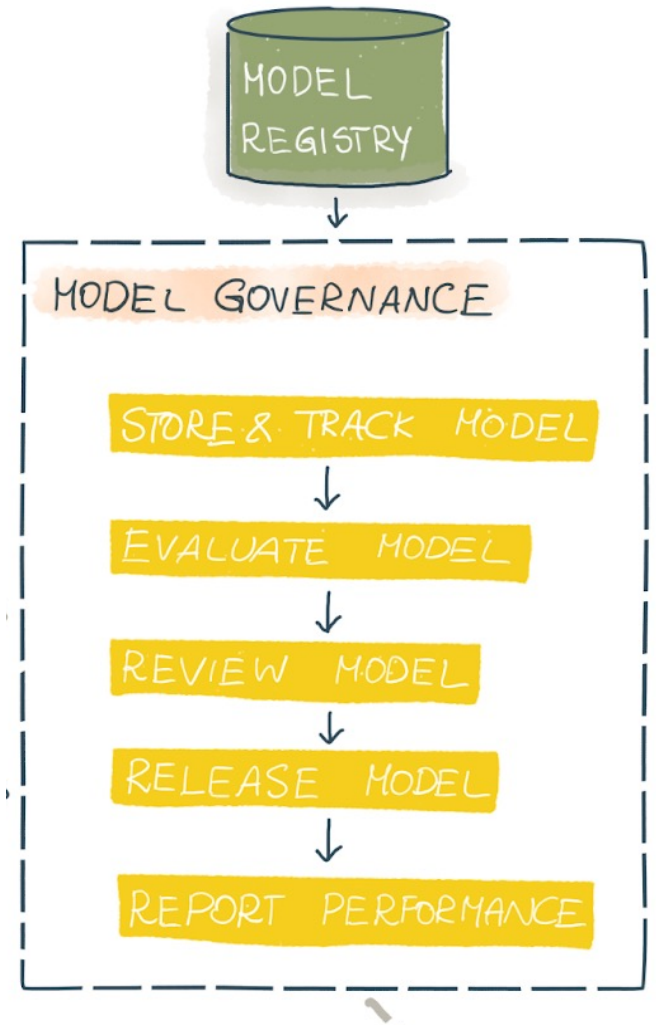
[https://services.google.com/fh/files/misc/practitioners_guide_to_mlops_whitepaper.pdf]



Model Governance

- Speicherung/ Versionierung von Modellen
- Auswertung und Erklärbarkeit
- Prüfung
- Freigabe
- Bericht: Zusammenfassung, Visualisierung und Hervorhebung von Metriken aus dem Monitoring

[https://services.google.com/fh/files/misc/practitioners_guide_to_mlops_whitepaper.pdf]

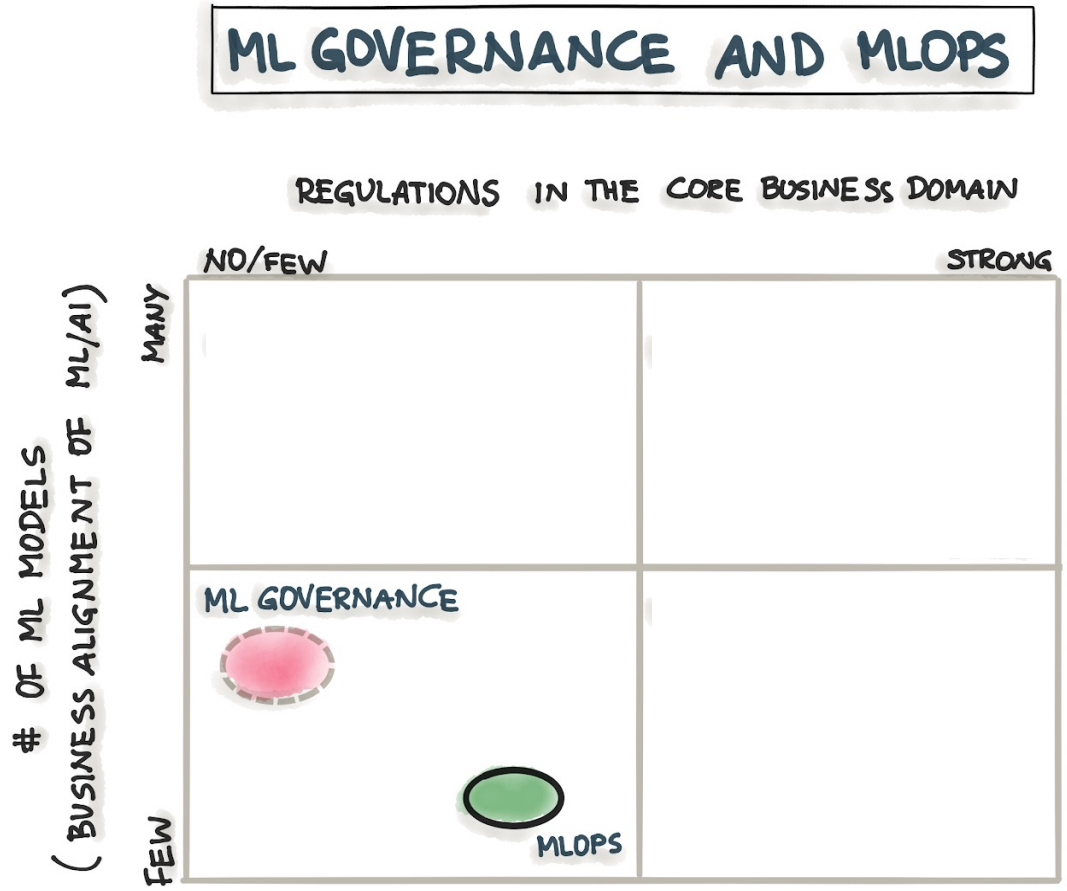


Ziele

- Hohe Datenqualität
- Evaluation der Modelle
- Interpretier- und Erklärbarkeit
- Continuous Evaluation und Reporting der Metriken
- Schaffung von Transparenz und Reproduzierbarkeit

[https://services.google.com/fh/files/misc/practitioners_guide_to_mlops_whitepaper.pdf]

Wenig Regulierung & wenig BA



Unternehmen stehen am Anfang des ML-Einsatzes

Danke! Fragen?

Isabel Bär

isabel.baer@innoq.com

@isabel_baer

INNOQ

www.innoq.com

Quellen

EU-Rechtsrahmen: https://germany.representation.ec.europa.eu/news/fur-vertrauenswurdige-kunstliche-intelligenz-eu-kommission-legt-weltweit-ersten-rechtsrahmen-vor-2021-04-21_de, https://planit.legal/das-ki-gesetz-der-eu-entwurf-und-diskussionsstand/

Model-Governance-Framework: https://www.oreilly.com/library/view/the-framework-for/9781098100483/ch01.html

Model Governance als Teil von MLOps:
[https://services.google.com/fh/files/misc/practitioners_guide_to_mlops_whitepaper.pdf]