

EXECUTIVE SUMMARY

The 0-to-1 Guardrails System

Das Operating System für AI-Produktlaunches in
regulierten Umgebungen

Für wen ist das?

Product Leader, die AI-Produkte bauen in:

- Health Tech
- Industrial IoT
- Public Sector
- Insurance

Du brauchst dieses Framework, wenn:

- Dein Produkt AI/ML-Features enthält
- Du unter regulatorischen Constraints arbeitest (MDR, EU AI Act, BaFin)
- Du Produkte shipped hast – aber noch nicht mit AI in regulierten Märkten

Das Problem

Die meisten Produkt-Frameworks nutzen 3 Stages:

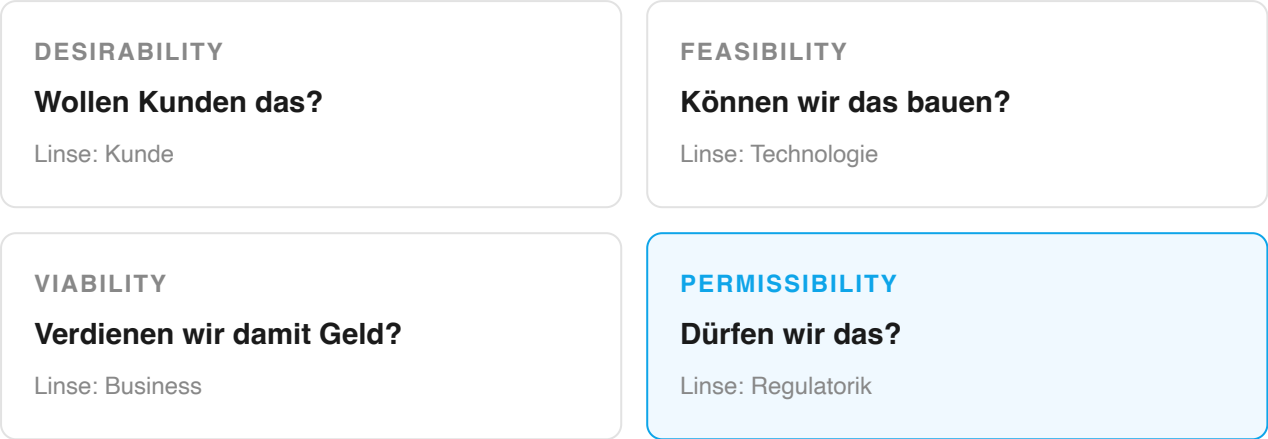
VISION → MVP → LAUNCH

In regulierten Umgebungen scheitert das, weil:

1. **"Launch" versteckt kritische Arbeit.** Die Zulassung ist kein Teil von Launch – sie ist ein eigener Stage, der 6–18 Monate dauert.
2. **AI stirbt in Discovery.** Nicht am Modell, nicht am Code – sondern an 4 Fragen, die nie gestellt wurden.
3. **Guardrails sind generisch.** "Safety" und "Compliance" bedeuten nichts Konkretes.

Die fehlende Dimension: **Permissibility**

Die meisten Frameworks validieren drei Dimensionen:



Du kannst ein Produkt bauen, das Kunden wollen, das technisch funktioniert, das starke Unit Economics hat – und trotzdem blockiert werden, weil der Regulator Nein sagt.

"Dürfen wir das?" ist eine **Discovery-Frage**. Nicht eine **Launch-Überraschung**.

Die Lösung: 4 Stages, 3 Instrumente



Die 3 Instrumente

INSTRUMENT	FRAGE	WO	FUNKTION
4 Bremsen	Bauen wir das überhaupt?	Discovery	Kill-Kriterien (Go/No-Go)
AI Evals	Funktioniert es in unserer Domäne?	Build	Validierung (Testen, Messen, Beweisen)
Guardrails	Bleiben wir innerhalb der Grenzen?	Build → Approval → Launch	Leitplanken pro Stage

Discovery

Bauen wir das? Dürfen wir das?

Instrumente: 4 Bremsen + Regulatory Pathway

Die 4 Bremsen

Jede AI-Idee klingt brillant – bis jemand anfängt, die Architektur zu zeichnen. Dann wird es still. Diese 4 Fragen entscheiden, ob dein Projekt überlebt:

BREMSE	FRAGE	KILL-LOGIK
Ground Truth	Haben wir echte Daten, gegen die wir messen können?	Keine Daten → nicht bauen
Capability Fit	Kann AI das heute – nicht in 2 Jahren?	Wunschdenken → nicht bauen
Regret Risk	Was passiert, wenn die AI falsch liegt?	Konsequenz unklar → nicht bauen
HITL Design	Wer übersteuert? Wer retrainet?	Unbeantwortbar → nicht bauen

◆ Gate: Alle 4 Bremsen bestanden + Regulatory Pathway klar → weiter zu Build.

Eine Bremse nicht bestanden → Projekt stirbt. Besser jetzt als nach 6 Monaten.

Warum das nicht optional ist

Benchmark (einfache Summarization)

0,7%

Legal AI mit RAG (Stanford, 2025)

17–33%

Klinik (Mount Sinai, 2025)

50%

DeepSeek klinisch

80%

Die Benchmark-Zahl ist nicht deine Realität. In deiner Domäne liegt die Fehlerrate 10–100x höher.

Build

Funktioniert es in unserer Domäne?

Instrumente: AI Evals + Guardrails (Technical, Data)

AI Evals

Hier werden die Bremsen aus Discovery mit echten Daten validiert:

EVAL	WAS WIRD GETESTET
Domain-spezifische Hallucination Tests	Fehlerrate auf DEINEN Daten, nicht auf Benchmarks
Bias Testing	Disparate Impact auf geschützte Merkmale (Art. 10 EU AI Act)
Performance Benchmarks	Gegen echte Produktionsdaten, nicht synthetische
Regression Tests	Nach jedem Model-Update: Wird es besser oder schlechter?

Guardrails in Build

DIMENSION	PRÜFFRAGE
Technical	Architektur skaliert? Performance reicht?
Data	Datenqualität reicht für Zulassung? Bias dokumentiert?

- ◆ Gate: AI Evals bestanden, Datenqualität verifiziert, Dokumentation gestartet → weiter zu Approval.

Approval

Hier ist der Beweis, dass wir dürfen.

Instrument: Conformity Assessment

"Dürfen wir?" wurde in Discovery geklärt. Approval beweist es dem Regulator.

FOCUS	OUTPUT
Conformity Assessment	Regulatorische Freigabe
Dokumentation	Technical File komplett (Annex IV)
Zertifizierung	CE-Marking / BfArM-Listung

Regulatory Checkpoints

CHECKPOINT	FRAGE
Klassifizierung	MDR Rule 11: SaMD Class I / IIa / IIb / III?
EU AI Act	High-Risk per Annex III? → Dual Conformity
Dokumentation	Annex IV Technical File + EN 62304?
Bias & Fairness	Art. 10 Disparate Impact bestanden?
Explainability	Art. 50 Transparenz-Anforderungen erfüllt?

◆ Gate: Approval erteilt, Post-Market-Plan steht → weiter zu Launch.

Launch

Läuft es sicher?

Instrument: Operational Guardrails (Monitoring)

FOCUS	OUTPUT
Go-to-Market	Activation-Targets erreicht
Post-Market Monitoring	Surveillance-System aktiv (Art. 72)
Incident Response	Prozess getestet, Meldewege klar
Model Drift Detection	Performance-Degradation erkannt

◆ Gate: Activation on track, Monitoring live, Incidents handled.

Stage Readiness Check

Bevor du zum nächsten Stage weitergehst – eine Frage pro Stage:

STAGE READINESS CHECK

Discovery → Build

4 Bremsen bestanden? Reg. Pathway klar?

☐ JA / NEIN

Build → Approval

AI Evals bestanden? Datenqualität verifiziert?

☐ JA / NEIN

Approval → Launch

Conformity Assessment bestanden?

☐ JA / NEIN

Launch → Scale

Monitoring aktiv? Incident Response getestet?

☐ JA / NEIN

JA → Weiter zum nächsten Stage

NEIN → Pause & Fix

Was dieses Framework verhindert

PROBLEM	OHNE FRAMEWORK	MIT FRAMEWORK
Falsches Produkt gebaut	Entdeckt bei Approval	Getötet in Discovery
Timeline unterschätzt	6+ Monate Verzögerung	Realistisch von Anfang an
Budget-Überraschungen	Regulatory-Kosten ungeplant	Kosten in Discovery geschätzt
AI Act verpasst	Blockiert bei Launch	In Discovery klassifiziert
Schlechte Datenqualität	Conformity gescheitert	AI Evals in Build
Kein Post-Market-Plan	Panik nach Launch	Monitoring steht vor Launch

Key Deadlines

REGULIERUNG	DEADLINE	KONSEQUENZ
EU AI Act (High-Risk)	Aug 2026	bis €35M / 7% Umsatz
MDR + AI Act (Dual Conformity)	Aug 2027	Marktzugang blockiert
DiGA (neue Zertifizierungen)	seit 2025	Keine Listung ohne BSI/ISO

In regulierten Umgebungen ist die Frage nicht:

"Wie schnell können wir shippen?"

Die Frage ist:

"Wie shippen wir, ohne 6 Monate auf einen Use Case zu verbrennen, der in Discovery hätte sterben müssen?"

Das 0-to-1 Guardrails System ist die Antwort.

Du hast das System verstanden. Aber:

- Du weißt nicht, ob dein Produkt unter High-Risk fällt?
- Dein Team hat keine Regulatory-Erfahrung?
- Ihr seid schon im Build – ohne Discovery gemacht zu haben?

Was ich mache:

Diagnostic	Ich prüfe, wo euer Produkt im Framework steht – welche Bremsen nicht gezogen wurden, welche Evals fehlen, welcher Regulatory Pathway gilt.
Advisory	Ich begleite euer Team durch die Stages – von der Klassifizierung bis zum Approval-Plan.

Kein Staffing. Kein Outsourcing. Euer Produkt, eure Entscheidungen – mit jemandem, der die Execution-Lücke kennt.

Olcay Chasan

Product Leader für 0-to-1 Builds in regulierten Umgebungen. AI-Produkte in Health Tech, Industrial IoT und Insurance shipped – mit MDR, EU AI Act und BaFin-Anforderungen.

chasan.de [LinkedIn](#)

Dieses Dokument dient der allgemeinen Information. Es stellt keine rechtliche, regulatorische oder Compliance-Beratung dar. Regulatorische Anforderungen ändern sich. Konsultieren Sie qualifizierte Fachleute vor Compliance-Entscheidungen.

© 2026 Olcay Chasan. Alle Rechte vorbehalten.