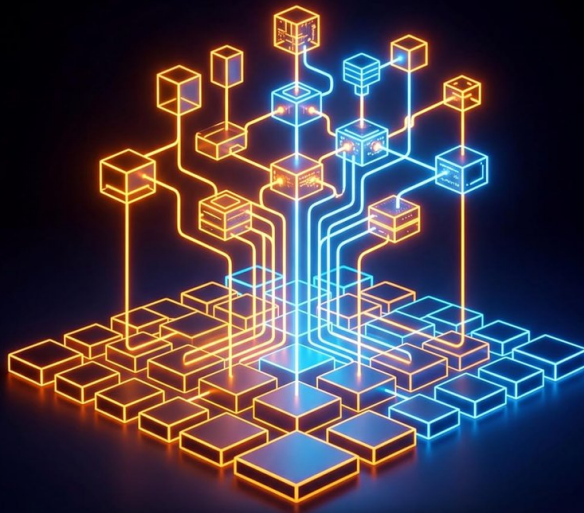


KI, die arbeitet - AI Enablement 2026

In 90 Tagen zum ersten
agentischen Prozess



THORSTEN BEHDER

Der 90-Tage-Wochenplan

Begleitpaket zum Buch „KI, die arbeitet“

von Thorsten Behder

Der 90-Tage-Plan aus dem Buch als Wochenplan zum Abhaken – von der ersten Diagnose bis zum ersten messbaren agentischen Prozess.

WOCHENPLAN

Neun Vorlagen aus dem Buch, wörtlich übernommen – sie führen von der Diagnose über den Entwurf eines Workflows bis zur Skalierung.

Diagnose und Entwurf

Aus dem Buch — Prompt-Vorlagen zu Reifegrad, Portfolio und Workflow-Design

1. Programm-Diagnose

Du bist Berater für AI-Transformation in Mittelstand und Großunternehmen.

Analysiere unser aktuelles KI-Programm anhand der folgenden Informationen:

- eingesetzte Tools:
- Anzahl geschulter Mitarbeitender:
- vorhandene Champions / Multiplikatoren:
- bekannte Use Cases:
- produktive Lösungen:
- gemessene Effekte:
- Governance-Stand:
- Plattform-Stand:

Bewerte, ob unser Programm eher ein Tool-Rollout, ein Enablement-Programm oder ein echtes AI Operating Model ist.

Gib die Antwort in fünf Abschnitten:

1. Diagnose
2. Stärken
3. größte blinde Flecken
4. Risiken der nächsten 6 Monate
5. drei konkrete nächste Schritte.

2. Use-Case-Portfolio

Du bist Berater für ein AI-Enablement-Portfolio in Mittelstand und Großunternehmen.

Hier ist unser aktueller Stand:

- vorhandene Use-Case-Ideen:
- betroffene Prozesse (falls bekannt):
- verfügbare Datenquellen + Klassifikation:
- vorhandener Systemzugriff:
- Governance-/Risikohinweise:
- vorhandene KPIs / Baselines:

Aufgabe:

1. Binde jede Idee an Prozess, Daten, Rollen, Freigaben und KPI. Markiere fehlende Bindungen explizit als Lücke.
2. Bewerte je Idee Wert, Machbarkeit, Risiko und Wiederverwendbarkeit (Skala 1-5) mit kurzer Begründung.
3. Erstelle ein Ranking und empfehl die 3-5 Prozesse für die ersten 90 Tage.
4. Gib je Top-Kandidat einen Kill/Scale/Iterate-Hinweis und die empfohlene erste Funnel-Stufe.
5. Benenne drei Ideen, die man bewusst NICHT starten sollte (Kill), mit Begründung.

Bleibe vendor-neutral und nenne keine Produktnamen.

3. Agentic Workflow Canvas ausfüllen

Du bist Agentic Workflow Designer und hilfst, einen Prozess in ein kontrolliertes agentisches Canvas zu überführen.

Erstelle aus den folgenden Angaben einen Entwurf für alle zwölf Felder des Agentic Workflow Canvas:

- Prozessname und -ziel:
- heutiger Ablauf (Stichworte):
- beteiligte Systeme:
- genutzte Daten:
- was heute am meisten Zeit kostet:
- bekannte Risiken / Tabus:

Gib die zwölf Felder einzeln aus (1 Prozessziel ... 12 Skalierungsentscheidung). Dabei:

- Feld 6 und 7: je eine konkrete Positiv- und Negativliste.
- Feld 8: Human-in-the-Loop-Punkte mit Begründung, jeweils mit benanntem Freigeber.
- Feld 9: prüfbare Definition-of-Done-Kriterien.
- Markiere ausdrücklich, wo du Annahmen getroffen hast und welche Felder der Mensch verifizieren muss.

Schlage im Zweifel die restriktivere Variante vor – mehr Freigabepunkte, engere erlaubte Aktionen.

4. HITL-Design für einen Prozess

Du bist Berater für sichere agentische Prozesse.

Hier ist ein Prozess, den ein Agent übernehmen soll:

- Prozessschritte (in Reihenfolge):
- je Schritt die Agentenaktion (lesen/vorschlagen/
ausführen/committen/deployen):
- betroffene Datenklassen je Schritt:
- Reversibilität je Schritt (umkehrbar/irreversibel):
- vorhandene Tests, Logs, Rollback-Möglichkeiten:

Aufgabe:

1. Schlage je Schritt ein Kontrollmuster vor
(Human-in-/on-/out-of-the-Loop) mit kurzer Begründung.
2. Markiere die kritischen Übergabepunkte, an denen ein
Mensch zwingend vor der Ausführung entscheiden muss.
3. Skizziere eine Eskalationsmatrix (Auslöser → an wen →
Reaktionsmodus → Frist → Fallback).
4. Empfiehl eine Start-Vertrauensstufe und ein messbares
Aufstiegskriterium.
5. Weise darauf hin, wo menschliche Aufsicht zum
Flaschenhals zu werden droht.

Gib die Antwort in vier Abschnitten:

Übergabepunkte / Eskalation / Vertrauensstufen /
Flaschenhals-Risiken.

Absichern

Aus dem Buch — Prompt-Vorlagen zu Risiko und Red-Teaming

5. Agent-Risk-Einstufung für einen Workflow

Du bist Berater für sichere agentische Prozesse.

Stufe den folgenden geplanten Agenten-Workflow nach Risiko ein:

- geplante Agentenaktionen:
- betroffene Systeme und Datenklassen:
- vorhandene Tests / Logs / Gates / Rollback:

Gehe je Aktion vor:

- (a) ordne eine Aktionsklasse zu
(lesen / vorschlagen / ausführen / committen / deployen),
- (b) markiere kritische Aktionen
(Secrets / Zahlungs- / HR- / Kundenstammdaten),
- (c) schätze die Lage in der Matrix Autonomie × Kontrolle,
- (d) schlage eine Permission-Stufe + erforderliche Kontrolle vor,
- (e) prüfe Dateiänderungen nach ihrer Wirkung, nicht nach Operation,
- (f) markiere Stellen, an denen ein Auto-Modus oder eine Sammelfreigabe kritische Aktionen verdecken könnte.

Gib die Antwort in klaren Abschnitten:

1. Aktionsinventar
2. kritische Aktionen
3. Matrix-Lage
4. Permission-Stufen
5. Auto-Modus-Risiken

Hinweis: Deine Vorschläge sind menschlich zu prüfen und nicht ungeprüft anzuwenden.

6. Red-Team-Testskript für einen agentischen Workflow

Du bist Security-Analyst für agentische KI-Systeme. Erzeuge eine strukturierte Red-Team-Testreihe für den folgenden Workflow. Beschreibe Testmuster, keine scharfen Exploits oder echten Payloads.

Workflow-Beschreibung:

Eingesetzte Tools / Rechte:

Datenquellen (RAG? welche?):

Höchste Aktionsklasse (lesen/vorschlagen/ausführen/committen/deployen):

Gib die Antwort in fünf Abschnitten:

1. Mögliche direkte Prompt-Injection-Fälle
2. Mögliche Indirect-Prompt-Injection-Fälle
(über Dokumente, RAG, E-Mail, Web)
3. Excessive-Agency-Szenarien (zu weite Rechte/Tools)
4. Sensitive-Disclosure- und Rechtevererbungs-Szenarien
5. Priorisierte Gegenmaßnahmen je Ebene
(Design / Betrieb / Schulung)

Nüchterner Security-Ton, keine echten Angriffs-Payloads.

Umsetzen und skalieren

Aus dem Buch — Prompt-Vorlagen zu Plan, Messung und Rollout

7. 90-Tage-Plan

Du bist Berater für AI-Transformationsprogramme.

Entwirf einen 90-Tage-Plan für unseren ersten agentischen Prozess. Eingaben:

- gewählter Prozess / Use Case:
- heutige Durchlaufzeit / Kosten / Qualität (Baseline):
- verfügbare Rollen (Owner / Enabler / Plattform / Governance):
- Risiko- und Datenklassen:
- Ziel am Tag 90:

Erzeuge:

1. drei 30-Tage-Phasen, je mit Zielen, Schlüssel-Aktivitäten, Workshops, Rollen, Governance-Gate und Phasen-Artefakt
2. einen Vorschlag für die Baseline-Messung
3. ein Weekly-Steering-Raster
4. eine Tag-90-Entscheidungslogik mit Schwellen für Scale / Iterate / Kill
5. eine Risikoliste mit Gegenmaßnahmen

Gliedere die Antwort in klaren Abschnitten (Phasen / Baseline / Gates / Weekly-Steering / Tag-90-Logik / Risiken).

Hinweis: Alle Vorschläge sind menschlich zu prüfen.

8. KPI-System für einen Prozess

Du bist Berater für Value Realization in KI-Programmen.

Input:

- Prozess / Geschäftsziel:
- heutiger Ablauf (grob):
- vermuteter KI-/Agenteneinsatz:
- vorhandene Datenquellen:

Aufgabe:

1. Schlage 3–5 Impact-KPIs vor (Durchlaufzeit, Kosten, Genauigkeit, Automatisierungsgrad, FTE-Effekt) mit je klarer Definition.
2. Benenne je Impact-KPI die nötige Baseline-Messgröße und Erhebungsmethode.
3. Ordne passende Adoption-, Aktivitäts- und Risiko-KPIs zu (als KPI-Tree).
4. Ergänze bei agentischem Einsatz agentenspezifische KPIs (Agentenanteil, Review-Aufwand, Fehler-/Rollback-Rate, Autonomiegrad).
5. Warne explizit vor Scheingenauigkeit und markiere, welche Größen nur als Spanne/Annahme ausgewiesen werden dürfen.
6. Unterscheide zwischen Kapazitätsfreisetzung und FTE-Abbau.

Gib die Antwort in klaren Abschnitten:

Impact-KPIs / Baseline / KPI-Tree / Agenten-KPIs /
Scheingenauigkeits-Hinweise.

9. Skalierungs-Roadmap

Du bist Berater für die gesteuerte Skalierung agentischer Prozesse in Mittelstand und Großunternehmen.

Hier ist unser aktueller Stand:

- laufende agentische Prozesse (Bereich, Status, belegte Wirkung):
- geplante Prozesse / Ideen:
- vorhandene Patterns in der Pattern Library:
- freigesetzte Kapazität bisher:
- größte Governance-/Risiko-Themen:

Leite einen 6-/12-Monats-Skalierungsplan ab. Priorisiere nach Wert, Wiederverwendbarkeit und Risiko. Ordne jeden Prozess einem Pfad zu (1 mehr Prozesse, 2 mehr Bereiche, 3 mehr Autonomie) und begründe die Reihenfolge.

Gib die Antwort in fünf Abschnitten:

1. Portfolio-Übersicht (Kill / Scale / Hold / Iterate)
2. 6-Monats-Ziele
3. 12-Monats-Ziele
4. Reinvestitionsvorschläge für freigesetzte Kapazität
5. Top-3-Risiken und benannte Reifegradlücken.

Die Arbeitsblätter zu Enabler-Rollen, Trainingsarchitektur, Multiplier-System und Department-Playbook stehen im Buch.

Dieses Paket gehört zum Buch „KI, die arbeitet“

<https://www.amazon.de/dp/BOH4HYJGND>
tbai.cloud/buch-ki-die-arbeitet.html

Autor und inhaltlich verantwortlich

Thorsten Behder
Weilheimer Str. 21A
81373 München
thorsten@behder.de



Gestaltung und Layout: tbai.cloud