IS4IT

Der digitalen Souveränität verpflichtet.

IS4IT GMBH

WHITEPAPER

Das Bau-vor-Betrieb-Prinzip für KI in Unternehmen

Der digitalen Souveränität verpflichtet.

Dokumenteninformationen

Dokument:	*Whitepaper*
Titel:	*Das Bau-vor-Betrieb-Prinzip für KI in Unternehmen*
Kunde:	*IS4IT GmbH*
Autor:	Florian Oelmaier
Status:	**öffentlich**
Version/Stand:	Version 1.0 vom 23.05.2026
Umfang:	35 Seiten
Letzte Änderung:	*24.05.2026*

Historie

Version	Datum	Autor	Änderungen
0.1	19.5.2026	Florian Oelmaier	Erste Version
1.0	23.5.2026	Florian Oelmaier	Freigabe

Verteiler

Name	Firma	Abteilung / Funktion
	public	

Die Informationen in diesem Dokument sind für die im Verteiler benannten Personen bestimmt. Das Dokument darf ohne schriftliche Genehmigung nicht an andere Personengruppen als die oben genannten kopiert, elektronisch weitergeleitet oder auf irgendeine andere Art weiterverteilt werden. Falls Sie dieses Dokument fälschlicherweise erhalten haben, kontaktieren Sie bitte umgehend IS4IT GmbH, Grünwalder Weg 28b, 82041 Oberhaching bei München.

1 Management Summary

KI-Transformation ist kein Technologieprojekt, sondern ein Befähigungsprozess. Das größte Risiko ist nicht der einzelne Fehlversuch oder die KI selbst — es ist die zu langsame Organisation. Und doch braucht KI Kontrolle. Die Grundidee um beides umzusetzen lautet: Governance beginnt nicht am Anfang jeder Idee, sondern dort, wo aus einem Experiment produktive Wirkung wird.

KI-Wirkstufen-Modell

Ein Stufenmodell unterstützt diese Idee und hilft, schnell ins Handeln zu kommen, ohne blind zu werden. Das Modell ordnet KI Einsatz in vier Stufen, geordnet nach dem Handlungsraum der KI ein:

KI baut: KI hilft beim Erstellen von Code, Skripten, Workflows, Vorlagen.
KI sieht: KI verarbeitet geschützte oder sensible Daten
KI wirkt: KI-Output beeinflusst Entscheidungen
KI handelt: KI führt eigenständig Aktionen aus

Das Bau-vor-Betrieb-Prinzip

KI muss nicht selbst im laufenden Betrieb sein, um große Effizienzgewinne zu ermöglichen. Häufig ist der bessere Einstieg, KI als Bauwerkzeug zu nutzen — für Skripte, Workflows, Schnittstellen und Vorlagen, die anschließend stabil, deterministisch und ohne KI im Tagesgeschäft laufen. Hoher Nutzen, niedriges operatives KI-Risiko, geringe Anbieterabhängigkeit. Die Grenze ist hart: die fertige Automatisierung darf im Betrieb keine KI-Aufrufe enthalten, sonst ist sie in einer anderen Stufe im Modell.

„KI baut" ist die risikoärmste KI-Wirkstufe mit dem größten Effizienzhebel.
Wer mit „KI handelt" beginnt, riskiert viel und lernt wenig. Wer mit „KI baut" beginnt, lernt viel und riskiert wenig.

Empowerment statt digitalem Taylorismus

Während „KI sieht", „KI wirkt" und „KI handelt" eine zentrale Steuerung bzgl. Sicherheits-, Architektur- und Risiko-Governance benötigt, eröffnet das risikoärmere „KI baut" die Möglichkeit einer dezentralen Steuerung von unten (Grass-Roots, Citizen Development).

Für die Mitarbeiter heißt das: aus „wegrationalisiert werden" wird „mitbauen können".

Für die Unternehmen bringt das Lerngeschwindigkeit. Eine Organisation, die mit KI schneller lernt, wird langfristig produktiver, anpassungsfähiger und wettbewerbsfähiger.

„KI sieht", „KI wirkt" und „KI handelt" sind Unternehmensarchitektur.
„KI baut" ist Grass-Roots.
Wer beide Modi vermischt, bekommt entweder Stillstand durch Übergovernance oder Schatten-IT in Hochrisiko-Stufen.

© 2026 IS4IT GmbH

2 Inhaltsverzeichnis

© 2026 IS4IT GmbH

© 2026 IS4IT GmbH

3 Die größte Gefahr: zu wenig ausprobieren

KI-Transformation beginnt nicht mit autonomen Agenten. Sie beginnt mit Menschen, die ihre eigene Arbeit besser machen können.

Die größte Gefahr für etablierte Unternehmen besteht nicht darin, dass Mitarbeitende mit KI zu viel ausprobieren. Die größere Gefahr besteht darin, dass sie zu wenig ausprobieren — weil jede Idee erst durch Strategieprogramme, Freigabegremien, Tooldiskussionen und Governance-Schleifen muss. Oder weil Sie sich in der vorherrschenden Unternehmenskultur einfach nicht trauen.

Während große Organisationen noch darüber diskutieren, welche KI-Anwendungsfälle erlaubt sind, bauen kleine Teams und schnelle Startups bereits täglich neue Automatisierungen, Prototypen, Auswertungen, Schnittstellen und Arbeitsabläufe. In der KI-Ökonomie wird nicht nur Technologie zum Wettbewerbsvorteil, sondern vor allem **Lerngeschwindigkeit**.

Deshalb brauchen Unternehmen keinen zentralen KI-Stau, sondern eine dezentrale Befähigungsbewegung: Fachexperten müssen in die Lage versetzt werden, mit KI ihre eigene Arbeit zu verbessern. Nicht irgendwann. Nicht erst nach dem perfekten Zielbild. Sondern jetzt — in sicheren Räumen, mit klaren Leitplanken und mit Gateways dort, wo aus Experimenten produktive Wirkung wird.

Die Leitfrage lautet daher nicht zuerst:

„Wie kontrollieren wir KI?“

Die bessere Frage lautet:

„Wie ermöglichen wir möglichst vielen Menschen, mit KI verantwortungsvoll ins Handeln zu kommen?“

KI-Transformation ist damit kein reines Technologieprojekt. Sie ist ein Company-Change-Prozess hin zu einer Organisation, in der Menschen regelmäßig mit KI lernen, bauen, verbessern und skalieren.

3.1 KI-Transformation ist ein Befähigungsprozess

Eine KI-getriebene Organisation erkennt man nicht daran, dass sie einige große KI-Projekte im Portfolio hat. Man erkennt sie daran, dass viele Teams regelmäßig kleine Verbesserungen bauen, testen, teilen und weiterentwickeln.

Der eigentliche Fortschritt entsteht, wenn Menschen mit tiefem Prozesswissen selbst handlungsfähig werden: Controller, Sachbearbeiterinnen, Vertriebsmitarbeiter, HR-Teams, Operations, Einkauf, IT-Administratoren und viele andere. Sie kennen die Reibung im Alltag. Sie wissen, welche Listen jeden Monat manuell zusammengeführt werden, welche Daten geprüft werden müssen, welche Ausnahmen regelmäßig auftreten und welche kleinen Medienbrüche jeden Tag Zeit kosten.

© 2026 IS4IT GmbH

Genau diese Menschen dürfen nicht länger nur Anforderungsgeber für zentrale IT-Projekte sein. Sie müssen zu aktiven Erbauern werden.

Der Controller weiß, welche Excel-Auswertung jeden Monat manuell zusammenkopiert wird. Eine Sachbearbeiterin kennt die Ausnahmen im Freigabeprozess. Ein Vertriebsmitarbeiter weiß, welche Informationen vor einem Kundentermin aus CRM, E-Mail und ERP zusammengesucht werden müssen. Eine HR-Mitarbeiterin kennt die wiederkehrenden Prüfungen im Onboarding. Ein IT-Administrator kennt die Systemabfragen, Logfile-Prüfungen und Benutzerverwaltungsaufgaben, die eigentlich längst automatisiert sein sollten.

Dieses Wissen ist der Rohstoff der KI-Transformation.

Bisher musste dieses Wissen oft mühsam in Softwareprojekte übersetzt werden: Anforderungen, Prozessdiagramme, Tickets, Backlogs, Spezifikationen, Priorisierungen. Jeder Übergabeschritt kostete Zeit. Jeder Übergabeschritt erzeugte Missverständnisse.

KI verändert diese Arbeitsteilung.

Mit KI kann der Fachexperte selbst erste Lösungen entwerfen: ein Skript, einen Workflow, eine Auswertung, einen Importhelfer, einen Dokumentenabgleich, eine Testdatenroutine oder einen Prototyp für eine Schnittstelle. Die KI übernimmt einen Teil der technischen Übersetzungsarbeit. Der Mensch liefert Kontext, Erfahrung, Urteilskraft und fachliche Prüfung.

Das Ziel ist nicht:

Jeder baut irgendetwas.

Das Ziel ist:

Viele Menschen bauen schnell — aber in sicheren Räumen und mit klaren Gateways vor produktiver Wirkung.

Diese Bewegung gibt es nicht zum Nulltarif. Sie braucht freigegebene Werkzeuge, einfache Entwicklungsumgebungen, Vorlagen, Schulungen, Coaches und Communities. Genau hier liegt der eigentliche Unterschied zwischen agilen Startups und starren Altorganisationen: Startups investieren reflexhaft in Befähigung, weil sie ohne sie nicht handlungsfähig wären. Altorganisationen behandeln Befähigung oft als optionalen Bildungsetat, der bei der nächsten Budgetrunde gekürzt werden kann. Wer mit KI ernst macht, muss diese Investition als strategische Voraussetzung verstehen — nicht als nachgelagerten Trainingsposten. Ob sie wirkt, lässt sich später an den richtigen KPIs ablesen (siehe Abschnitt zur Lerngeschwindigkeit).

3.2 Größtes Risiko: Nicht KI — die langsame Organisation

In vielen Unternehmen wird KI vor allem als Risiko diskutiert: Datenschutzrisiko, Sicherheitsrisiko, Haftungsrisiko, Qualitätsrisiko, Reputationsrisiko. Diese Risiken sind real und müssen ernst genommen werden.

Aber es gibt ein weiteres Risiko, das oft unterschätzt wird:

© 2026 IS4IT GmbH

das Risiko, zu langsam zu lernen.

Eine Organisation, die jede KI-Idee wie ein klassisches IT-Projekt behandelt, verliert Geschwindigkeit. Sie produziert Abstimmungen, bevor sie Erfahrungen produziert. Sie baut Gremien, bevor sie Prototypen baut. Sie verlangt Sicherheit, bevor überhaupt verstanden wurde, wo Nutzen entsteht.

Das ist in einer Phase technologischer Umbrüche gefährlich.

Denn während etablierte Unternehmen noch an Zielbildern, Richtlinien und Toolfreigaben arbeiten, bauen andere bereits. Sie testen, verwerfen, verbessern, automatisieren und lernen.

Deshalb muss KI-Governance unternehmerisch gedacht werden. Sie darf nicht nur Risiken reduzieren. Sie muss auch Geschwindigkeit ermöglichen.

Das richtige Modell vermeidet nicht jedes Risiko. Es unterscheidet zwischen Risiken, die niemals akzeptabel sind, und Risiken, die zum Lernen dazugehören.

Nicht akzeptabel sind etwa:

- Schutzdaten in ungeprüften KI-Diensten
- geheime Produktivautomatisierung
- unkontrollierte Schreibrechte
- automatische Außenwirkung ohne Freigabe
- fehlende Verantwortlichkeit
- ungeprüfter Zugriff auf kritische Systeme
- verdeckte Verarbeitung personenbezogener oder vertraulicher Daten

Akzeptabel — ja notwendig — sind dagegen:

- Experimente im sicheren Raum
- verworfene Prototypen
- unperfekte erste Versionen
- doppelte Lernschleifen in verschiedenen Teams
- kleine Fehler ohne produktive Wirkung
- Automatisierungen, die nach wenigen Wochen ersetzt werden
- Ausprobieren, Lernen und Teilen

Wer jedes Experiment verhindern will, verhindert am Ende die Transformation.

Die zentrale Regel lautet deshalb:

Nicht jedes Experiment braucht eine Freigabe. Aber jede produktive Wirkung braucht Verantwortung.

© 2026 IS4IT GmbH

4 Das KI Wirkstufen-Modell: Vier Handlungsräume

Das folgende Modell ist kein Genehmigungskatalog. Es ist ein Enablement-Modell.

Es soll Unternehmen helfen, schnell ins Handeln zu kommen, ohne blind zu werden. Die Grundidee lautet: Solange KI ohne Schutzdaten, ohne produktive Systeme und ohne Außenwirkung zum Bauen, Lernen und Experimentieren genutzt wird, sollte der Einstieg so leicht wie möglich sein.

Erst wenn Datenzugriff, Entscheidungswirkung oder Handlungsspielraum zunehmen, steigen auch Prüf-, Schutz- und Kontrollbedarf.

Governance beginnt damit nicht am Anfang jeder Idee, sondern dort, wo aus einem Experiment produktive Wirkung wird.

Daraus ergeben sich vier Handlungsräume:

Handlungsraum	Leitfrage	Grundregel
KI baut	Was können wir mit KI schneller erstellen?	Im Sandkasten gilt Tempo.
KI sieht	Welche Daten verarbeitet die KI?	Bei Schutzdaten gilt Sicherheit.
KI wirkt	Welche Entscheidungen beeinflusst der Output?	Bei Wirkung gilt Verantwortung.
KI handelt	Welche Aktionen kann die KI auslösen?	Bei Autonomie gilt Kontrolle.

Oder als Merksatz:

Bauen braucht Freiheit. Sehen braucht Schutz. Wirken braucht Verantwortung. Handeln braucht Kontrolle.

4.1 Stufe 1 - KI baut: Der sichere Erlaubnisraum

In dieser Stufe unterstützt KI beim Erstellen von Inhalten, Konzepten, Code, Tests, Dokumentation, technischen Entwürfen oder Prototypen. Sie wird jedoch nicht im laufenden Betrieb eingesetzt und erhält keine personenbezogenen Daten, keine Kundendaten und keine Geschäftsgeheimnisse.

Typische Beispiele sind:

- Generierung von Code
- Erstellung von Testfällen
- Entwurf von Präsentationen
- Arbeit mit Dummy-Daten
- technische Skizzen oder Konzepte
- Dokumentationsentwürfe

© 2026 IS4IT GmbH

- Prototypen für Skripte, Workflows oder Auswertungen
- Beispielcode für Schnittstellen oder Datenkonvertierungen

Diese Stufe ist der zentrale Erlaubnisraum für die KI-Transformation.

Hier sollte die Grundhaltung nicht lauten:

„Darf ich das?“

Sondern:

„Mach einen sicheren Prototyp und zeig, was Du gelernt hast.“

Wer ohne personenbezogene Daten, ohne Kundendaten, ohne Geschäftsgeheimnisse und ohne produktive Systemzugriffe arbeitet, sollte nicht auf ein zentrales KI-Projekt warten müssen. Fachexperten sollen ausprobieren dürfen: ein Skript für eine wiederkehrende Auswertung, ein Workflow für einen manuellen Abgleich, ein Prototyp für einen Importhelfer, eine Testdatenroutine, eine Dokumentationsvorlage oder eine kleine Automatisierung für den eigenen Arbeitsbereich.

In dieser Stufe ist Geschwindigkeit wichtiger als Perfektion. Nicht jeder Prototyp muss bleiben. Nicht jede Idee muss skalieren. Aber jede Iteration erhöht das Verständnis dafür, was mit KI möglich ist und wo echte Reibung im Unternehmen liegt.

Trotzdem ist „KI baut“ kein rechtsfreier Raum. Es gelten klare Mindestregeln:

- keine Schutzdaten in ungeprüfte KI-Dienste
- keine Zugangsdaten, Secrets oder internen Schlüssel in Prompts
- keine ungeprüfte Übernahme von Code in produktive Systeme
- Nutzung freigegebener Werkzeuge
- Arbeit mit anonymisierten, synthetischen oder Dummy-Daten
- Prüfung von KI-generiertem Code auf Sicherheit, Qualität und **Lizenzkonformität** — KI-Modelle können Code-Fragmente erzeugen, die fremden Lizenzen unterliegen. Die KI selbst hilft beim Prüfen: Sie erzeugt SBOMs, klassifiziert verwendete Bibliotheken und schlägt lizenzkonforme Alternativen vor, wenn man sie darum bittet. Zugleich entschärft die strikte Inhouse-Nutzung viele Open-Source-Lizenzfragen praktisch von selbst: Pflichten wie die GPL-Distributionsregeln oder die AGPL-Offenlegungspflicht greifen erst bei Weitergabe an Dritte oder bei Service-over-Network gegenüber externen Nutzern — bei rein interner Verwendung bleiben sie weitgehend folgenlos. Was die KI nicht ersetzt, ist die einmalige organisationsweite Festlegung, welche Lizenzen in welchem Einsatzkontext (intern, kundenseitig, als Produkt) zulässig sind.
- fachliche und technische Prüfung vor produktiver Nutzung

Die Regel lautet:

Freiheit im sicheren Raum — Gateways vor produktiver Wirkung.

Merksatz: KI wird im laufenden Betrieb nicht verwendet. Im sicheren Raum darf schnell gelernt und gebaut werden.

© 2026 IS4IT GmbH

4.2 Stufe 2 - KI sieht: Daten brauchen Schutz

In dieser Stufe verarbeitet KI geschützte oder sensible Informationen, bleibt aber ein passives Werkzeug. Sie fasst zusammen, übersetzt, extrahiert Informationen oder erstellt Entwürfe. Sie entscheidet nicht, speichert nicht dauerhaft und handelt nicht selbstständig.

Typische Beispiele sind:

- Zusammenfassung von Verträgen
- Erstellung von Auswertungen
- Umformulierung interner E-Mails
- Extraktion von Daten aus Dokumenten
- Erstellung von Antwortentwürfen
- Klassifizierung eingehender Dokumente
- Analyse von Supportfällen oder Kundenanfragen

Hier verändert sich die Risikolage deutlich. Sobald KI echte Unternehmensdaten, personenbezogene Daten, Kundendaten oder vertrauliche Informationen verarbeitet, reicht der Experimentiermodus nicht mehr aus.

Jetzt müssen insbesondere geklärt sein:

- Welche Daten werden verarbeitet?
- Welcher KI-Dienst ist freigegeben?
- Wo werden Daten gespeichert — insbesondere innerhalb oder außerhalb der EU?
- Werden Daten zum Training verwendet?
- Gibt es Auftragsverarbeitung oder vergleichbare Vereinbarungen?
- Welche **Unterauftragnehmer** (Sub-Processor) setzt der KI-Anbieter ein, und in welchen Ländern sitzen sie?
- Wer darf die Daten sehen?
- Wie werden Eingaben und Ausgaben gelöscht oder protokolliert?
- Welche Ergebnisse müssen menschlich geprüft werden?

Wichtig ist: Die KI darf in dieser Stufe sehen, aber nicht selbstständig bewirken. Eine automatische Außenwirkung ohne menschliche Freigabe sollte ausgeschlossen sein.

Entscheidend ist nicht nur, was die KI technisch tut, sondern wofür ihr Output anschließend verwendet wird. Eine Vertragszusammenfassung kann ein harmloses Hilfsmittel sein. Wird sie aber zur Grundlage einer rechtlichen Entscheidung, bewegt sich der Fall bereits in Richtung „KI wirkt“.

Merksatz: KI darf sehen, aber nichts selbst bewirken.

4.3 Stufe 3 - KI wirkt: Output bekommt Gewicht

In dieser Stufe handelt KI zwar noch nicht eigenständig, aber ihr Ergebnis hat relevante Auswirkungen. Der Output beeinflusst Entscheidungen, Bewertungen, Prioritäten, Kommunikation oder Geschäftsprozesse.

© 2026 IS4IT GmbH

Typische Beispiele sind:

- Bewerberranking
- Bonitätsscores
- Risikobewertungen
- Fraud-Scoring
- Priorisierung von Kunden
- medizinische, rechtliche oder finanzielle Empfehlungen
- automatische Einstufung von Beschwerden
- Entscheidungsvorbereitung für Freigaben oder Eskalationen

Hier reicht es nicht mehr, nur Datenschutz und Toolfreigabe zu prüfen. Jetzt geht es um Verantwortung.

Wenn KI-Ergebnisse Entscheidungen beeinflussen, müssen Zweck, Kontext und Grenzen klar sein. Es braucht menschliche Kontrolle, Nachvollziehbarkeit, Plausibilitätsprüfungen, Protokollierung und gegebenenfalls rechtliche Bewertung.

Hinzu kommen **Informations- und Transparenzpflichten gegenüber Betroffenen**: In vielen Fällen müssen Bewerber, Kunden, Mitarbeitende oder andere Betroffene darüber informiert werden, dass KI an einer Entscheidung beteiligt war — und welche Rechte sie auf Auskunft, Erklärung oder menschliche Überprüfung haben. Diese Pflichten ergeben sich aus DSGVO, EU AI Act und je nach Kontext aus Arbeits- oder Antidiskriminierungsrecht.

Besonders wichtig ist: Menschliche Kontrolle darf keine Scheinprüfung sein.

Es reicht nicht, dass ein Mensch am Ende formal auf „Freigeben“ klickt. Die prüfende Person muss das KI-Ergebnis verstehen, hinterfragen, korrigieren und ablehnen können. Sonst wird menschliche Kontrolle zur Fassade.

Innerhalb dieser Stufe variiert das Risiko stark. Eine interne Priorisierung von Tickets ist anders zu bewerten als eine Bewertung von Personen, eine Kreditentscheidung oder eine medizinische Empfehlung.

Merksatz: KI entscheidet nicht unbedingt — aber ihr Output zählt.

4.4 Stufe 4 - KI handelt: Autonomie braucht Kontrolle

In der höchsten Stufe führt KI selbst Aktionen aus. Sie nutzt Tools, ruft Systeme auf, schreibt Daten, sendet Nachrichten, startet Workflows oder arbeitet Aufgaben eigenständig ab.

Typische Beispiele sind:

- Einträge im CRM erstellen oder ändern
- E-Mails versenden
- Termine buchen
- APIs aufrufen
- Dateien verändern
- Tickets anlegen oder schließen

© 2026 IS4IT GmbH

- Code deployen
- Datenbanken lesen oder beschreiben
- Workflows auslösen
- Bestellungen vorbereiten oder ausführen

Hier ist besondere Vorsicht erforderlich. Denn handelnde KI-Systeme verbinden natürliche Sprache mit Systemzugriffen. Sie können nicht nur falsche Antworten geben, sondern reale Aktionen auslösen.

Bei agentischen Systemen reicht klassische Zugriffskontrolle allein nicht aus. Da solche Systeme Anweisungen aus natürlicher Sprache verarbeiten, können **manipulierte Inhalte in E-Mails, Dokumenten, Webseiten oder Tickets** zu unbeabsichtigten Aktionen führen — auch ohne Zutun des eigentlichen Nutzers. Das ist der Kern der sogenannten **indirekten Prompt-Injection**: Die KI liest scheinbar harmlose Daten und führt darin versteckte Anweisungen aus. Damit entsteht eine völlig neue Klasse von Angriffsvektoren, die klassische Sicherheitsmodelle nicht abbilden.

Deshalb müssen mindestens vier Risikoarten ausdrücklich berücksichtigt werden:

- **Prompt-Injection** (direkt und indirekt) — die KI wird über manipulierte Eingaben gesteuert
- **Tool-Missbrauch** — freigegebene Tools werden in unerwarteter Reihenfolge oder Kombination eingesetzt
- **Datenabfluss** — sensible Inhalte gelangen über Tool-Aufrufe oder Antworten nach außen
- **Ungewollte Kettenaktionen** — eine Aktion löst weitere Aktionen aus, ohne dass das beabsichtigt war

Daraus ergibt sich der nötige technische und organisatorische Rahmen:

- strikt begrenzte Berechtigungen nach dem Least-Privilege-Prinzip
- Trennung von Lese-, Schreib-, Versand- und Löschrechten
- freigegebene Tools und Datenquellen
- keine pauschalen Admin- oder Vollzugriffe
- Logging aller Tool-Aufrufe
- Monitoring und Alarmierung
- Sandbox-Tests vor Produktiveinsatz
- Limits, Freigaben und Rollback-Möglichkeiten
- Not-Aus-Mechanismen
- Schutz gegen direkte und indirekte Prompt-Injection
- Prüfung auf Datenabfluss und ungewollte Kettenaktionen

Die zentrale Regel lautet:

Eine KI darf nicht alles tun, was sie technisch auslösen könnte, sondern nur das, was fachlich und organisatorisch ausdrücklich erlaubt ist.

Merksatz: KI handelt eigenständig. Deshalb braucht sie harte Grenzen.

© 2026 IS4IT GmbH

4.5 Einordnung in den rechtlichen und normativen Rahmen

Das Modell der vier Handlungsräume ist ein **operatives Priorisierungs- und Befähigungsmodell**. Es ersetzt keine bestehenden rechtlichen oder normativen Rahmenwerke, sondern übersetzt deren risikoorientierte Grundlogik in eine einfache Sprache für den Alltag in Unternehmen.

Die wichtigsten Bezugsrahmen sind:

- **EU AI Act** — risikobasierte Regulierung von KI-Systemen mit besonderen Pflichten für Hochrisiko-Anwendungen, Transparenzpflichten und Anforderungen an menschliche Aufsicht.
- **DSGVO** — Rechtsgrundlagen der Verarbeitung, Zweckbindung, Datenminimierung, Betroffenenrechte, Auftragsverarbeitung, Drittlandtransfers, automatisierte Einzelentscheidungen.
- **NIST AI Risk Management Framework (AI RMF)** — strukturierter Ansatz zur Identifikation, Bewertung und Steuerung von KI-Risiken über den gesamten Lebenszyklus.
- **ISO/IEC 42001** — Managementsystem-Norm für verantwortungsvollen KI-Einsatz, vergleichbar in der Logik mit ISO 9001 oder ISO 27001.

Hinzu kommen je nach Branche und Einsatzfeld weitere Anforderungen: Arbeitsrecht und Mitbestimmung, Antidiskriminierungsrecht, IT-Sicherheits- und Branchenregulierung (etwa NIS2, DORA, MaRisk, MDR), Urheber- und Lizenzrecht, vertragliche Geheimhaltungspflichten sowie interne Konzern- und Compliance-Vorgaben.

Die vier Handlungsräume korrespondieren mit unterschiedlichen rechtlichen Schwerpunkten:

Handlungsraum	Rechtliche und normative Schwerpunkte
KI baut	Vertraulichkeit, Urheber- und Lizenzrecht, Code- und Lieferkettensicherheit, Anbieterbedingungen — solange keine Schutzdaten verarbeitet werden.
KI sieht	DSGVO (Rechtsgrundlage, Zweckbindung, Auftragsverarbeitung, Speicherort, Löschung, Drittlandtransfer, Trainingsnutzung), Geheimhaltungs-, Kunden- und sonstige Vertragsverpflichtungen.
KI wirkt	EU AI Act (insbesondere Hochrisiko-Einstufung), Transparenz- und Dokumentationspflichten, menschliche Aufsicht, Antidiskriminierungs- und Arbeitsrecht, Informationspflichten gegenüber Betroffenen.
KI handelt	Zusätzlich: Berechtigungs- und Protokollierungspflichten, IT-Sicherheits- und Branchenregulierung, Haftungs- und Vertretungsregeln, technische und organisatorische Grenzen für autonome Aktionen.

Wichtig ist: Die vier Handlungsräume sind ein **Werkzeug für die operative Priorisierung**, kein Ersatz für die rechtliche Einzelfallprüfung. Datenschutz, Sicherheit, Recht und Compliance müssen frühzeitig eingebunden werden — insbesondere dort, wo aus einem Prototyp eine produktive Anwendung wird.

© 2026 IS4IT GmbH

Umgekehrt gilt aber auch: Rechtliche und normative Rahmenwerke ersetzen nicht die Befähigung. Eine Organisation kann ISO 42001 zertifiziert sein und trotzdem keine wirksame KI-Praxis haben. Erst das Zusammenspiel aus klarem Rahmen und realer Handlungsfähigkeit macht eine KI-getriebene Organisation aus.

Merksatz: Externe Rahmenwerke geben die Pflichten vor. Das Stufenmodell mit den vier Handlungsräumen macht sie im Alltag handhabbar.

© 2026 IS4IT GmbH

5 Das Bau-vor-Betrieb-Prinzip

Der wichtigste Unterschied wird in vielen KI-Diskussionen übersehen: KI muss nicht zwingend selbst Teil des laufenden Betriebs sein, um große Effizienzgewinne zu ermöglichen.

Die intuitive Annahme lautet häufig: Der größte Effizienzgewinn entsteht dort, wo KI selbstständig handelt. Doch das ist nicht immer richtig. **Nicht jede durch KI ermöglichte Automatisierung muss eine KI-Automatisierung sein.**

Der Unterschied ist entscheidend. In einem Fall wird KI selbst Teil des laufenden Geschäftsprozesses. Sie verarbeitet Daten, beeinflusst Entscheidungen oder löst Aktionen aus. Damit steigen die Anforderungen an Datenschutz, Sicherheit, Kontrolle, Nachvollziehbarkeit und Haftung. Im anderen Fall wird KI als Bauwerkzeug genutzt. Sie hilft, Skripte, Workflows, Schnittstellen, Auswertungen, Vorlagen, Tests oder Softwarebausteine schneller zu erstellen. Das Ergebnis läuft anschließend als klassische Automatisierung — mit deutlich geringerem operativem KI-Risiko.

Häufig ist deshalb der bessere Einstieg, KI zunächst als Bauwerkzeug zu nutzen — für Skripte, Workflows, Auswertungen, Vorlagen, Schnittstellen, Tests, Dokumentation oder klassische Automatisierungen, die anschließend stabil, überprüfbar und ohne KI im Tagesgeschäft laufen.

Kurz gesagt:

Erst KI nutzen, um bessere Automatisierung zu bauen. Erst danach prüfen, wo KI selbst sehen, wirken oder handeln sollte.

Der größte Hebel liegt nicht immer dort, wo KI am „intelligentesten“ wirkt. Entscheidend ist, mit hoher Geschwindigkeit zu lernen, produktive Entlastung zu schaffen und Risiken dort zu kontrollieren, wo reale Wirkung entsteht.

Eine Automatisierung, die ohne KI im laufenden Betrieb arbeitet, ist in der Regel:

- **stabiler** — keine wechselnde Modellqualität, keine versionsbedingten Antwortänderungen
- **deterministisch** — gleiche Eingabe erzeugt gleiche Ausgabe, damit testbar und vorhersagbar
- **besser prüfbar** — Code, Logik und Datenflüsse sind nachvollziehbar und auditierbar
- **günstiger im Betrieb** — keine laufenden Inferenzkosten, keine Token-Abrechnung
- **compliance-freundlicher** — geringere Datenschutz-, Transparenz- und Dokumentationslast
- **wartbarer** — klassische Software-Engineering-Praktiken greifen, ohne KI-spezifische Eigenheiten
- **unabhängiger** — keine Abhängigkeit von einem KI-Anbieter, dessen Modell, Preise, AGB oder Verfügbarkeit sich jederzeit ändern können

Ein mit KI-Unterstützung gebautes Skript, ein Workflow oder eine Schnittstelle kann anschließend als klassische Automatisierung laufen. Der Nutzen bleibt bestehen, während

© 2026 IS4IT GmbH

das laufende KI-Risiko gering bleibt — und die strategische Anbieterabhängigkeit im Tagesgeschäft sinkt.

Daraus folgt eine harte begriffliche Grenze: **Enthält die fertige Automatisierung im laufenden Betrieb weiterhin KI-Aufrufe, fällt sie nicht mehr unter „KI baut“.** Sie wechselt — je nach Funktion — in „KI sieht“, „KI wirkt“ oder „KI handelt“, mit allen entsprechenden Pflichten. „KI baut“ beschreibt ausschließlich Automatisierungen, deren Produktivbetrieb ohne Modell-Inferenz auskommt. Diese Trennung muss in der Praxis konsequent eingefordert werden, sonst verliert das gesamte Modell seine Risiko-Entlastung.

Das ist der Kern des Bau-vor-Betrieb-Prinzips:

KI hilft beim Bauen. Die Automatisierung läuft kontrolliert im Betrieb.

Die bessere Leitfrage lautet daher nicht nur:

„Welchen Prozess können wir mit KI automatisieren?“

Sondern:

„Welche stabile Automatisierung können unsere Fachexperten mit Hilfe von KI schneller bauen?“

5.1 Steuerung: Grass-Roots und Unternehmensarchitektur

Mit dem Wechsel zwischen den Handlungsräumen wechselt das Risiko. Dadurch ist es möglich, auch das **Steuerungsmodell** zu wechseln. Das ist eine zentrale, oft übersehene Konsequenz des Modells:

Handlungsraum	Steuerungsmodus	Treiber
KI baut	dezentral, Grass-Roots, Citizen Development	Fachbereiche mit Plattformunterstützung der IT
KI sieht	zentral gesteuert über Plattform-Governance	IT, Datenschutz, Informationssicherheit
KI wirkt	zentral geplant über Unternehmensarchitektur	Architektur, Compliance, Fachverantwortung, Recht
KI handelt	zentral kontrolliert über Sicherheits- und Risiko-Governance	Security, Architektur, Risikomanagement, Vorstand

In der Stufe **„KI baut“** ist Grass-Roots richtig und gewollt. Hier dürfen viele Menschen gleichzeitig ausprobieren, weil weder Schutzdaten noch produktive Wirkung im Spiel sind. Geschwindigkeit und Lernen schlagen Planung.

Sobald KI aber sieht, wirkt oder handelt, kippt die Logik. Jetzt geht es um Datenarchitektur, Identity- und Berechtigungskonzepte, Datenflüsse über Systemgrenzen hinweg, regulatorische Pflichten, Haftung und unternehmensweite Auswirkungen. Diese Themen lassen sich **nicht aus der Fläche heraus** lösen. Sie brauchen zentrale Programme, architektonische Leitentscheidungen und klare Verantwortlichkeiten auf Unternehmensebene.

© 2026 IS4IT GmbH

Anders gesagt:

„KI baut“ ist Grass-Roots. „KI sieht“, „KI wirkt“ und „KI handelt“ sind Unternehmensarchitektur.

Wer diese Trennung verwischt, bekommt entweder Stillstand (weil zentrale Gremien jede kleine Bau-Idee blockieren) oder unkontrollierte Schatten-IT in Hochrisiko-Stufen (weil Fachbereiche eigenmächtig KI auf Schutzdaten loslassen). Beides ist gefährlich.

5.2 KI baut: Fachexperten werden zu Erbauern

Die wichtigste Veränderung durch KI liegt nicht darin, dass Software schneller geschrieben wird. Sie liegt darin, dass mehr Menschen überhaupt an der Entstehung von Automatisierung beteiligt werden können — **innerhalb des sicheren Bau-Raums**.

Das ist ein kultureller Bruch.

Bisher waren Fachexperten meist Anforderungsgeber. Sie beschrieben ihr Problem, warteten auf Priorisierung, erklärten Sonderfälle, prüften Zwischenergebnisse und hofften, dass ihre Realität richtig verstanden wurde.

Mit KI können sie einen Teil dieser Übersetzungsarbeit selbst übernehmen.

Das Citizen-Developer-Modell[1] ist deshalb kein Notbehelf und keine Schatten-IT mit freundlicherem Namen. Es ist ein gezieltes Befähigungsmodell für Wissensarbeiter.

Fachexperten sollen nicht darauf warten müssen, dass jede kleine Automatisierung als zentrales Projekt eingeplant wird. Sie sollen selbst erste „fachnahe Micro-Automatisierungen“ bauen, testen und verbessern dürfen — solange sie innerhalb klarer Leitplanken bleiben.

Die Rolle der IT in „KI baut“ verschiebt sich dadurch: weg vom Nadelöhr für jede kleine Lösung, hin zum Plattformanbieter, Coach und Qualitätsgaranten. Zusammen mit der zentralen Rolle für „KI sieht, wirkt & handelt“ ergibt das eine Doppelrolle: **Plattform für die Vielen. Architekt für das Ganze.**

Das Modell verbindet vier Stärken:

- **Fachbereiche** kennen den Prozess, die Ausnahmen, die Datenqualität und den tatsächlichen Arbeitsaufwand.
- **KI** hilft bei der technischen Umsetzung: Code, Skripte, Workflows, Tests, Dokumentation, Schnittstellenlogik und Fehlersuche.
- **IT** stellt sichere Plattformen, Standards, Repositories, Vorlagen und Betriebsregeln bereit.
- **Governance** definiert Gateways, ab denen Prüfung, Freigabe und Verantwortung verbindlich werden.

[1] Die konkreten Spielregeln, das Gateway und die Pflichten für die Plattform-IT im „Citizen Developer Modell“: siehe Anhang

© 2026 IS4IT GmbH

Nicht jede Form von Citizen Development braucht dieselbe Freigabe. Entscheidend ist der Freiheitsgrad.

5.3 Kein digitaler Taylorismus

KI darf nicht zu einem digitalen Taylorismus werden, bei dem Arbeit immer feiner zerlegt, überwacht, standardisiert und von oben optimiert wird.

Der bessere Ausgangspunkt ist die Wissensarbeit.

Menschen in Fachbereichen sind nicht nur Ausführende von Prozessen. Sie sind Träger von Erfahrungswissen, Kontext, Urteilskraft und Verantwortung. Sie wissen, warum ein Prozess in der Praxis anders läuft als im Handbuch. Sie kennen die Ausnahmen, Abkürzungen, Qualitätsprobleme und stillen Workarounds.

KI-gestütztes Bauen sollte dieses Wissen nicht ersetzen, sondern wirksam machen.

Das Ziel ist nicht, Menschen aus dem Prozess herauszuoptimieren. Das Ziel ist, Menschen von wiederkehrender Reibung zu entlasten, damit sie mehr Zeit für das haben, was nicht automatisiert werden kann: Kontext verstehen, Entscheidungen verantworten, Beziehungen gestalten, Kundenprobleme lösen, Neues entwickeln.

In diesem Sinne passt KI-gestütztes Bauen eher zu Peter Druckers Verständnis von Wissensarbeit als zu einem industriellen Kontrollmodell. Führung bedeutet dann nicht, jede Handlung vorzugeben, sondern Rahmenbedingungen zu schaffen, in denen Menschen eigenverantwortlich bessere Lösungen entwickeln können.

An dieser Stelle trifft sich das Bau-vor-Betrieb-Prinzip mit einer menschlichen Führungskultur: Vertrauen statt Misstrauen, Befähigung statt Anweisung, Selbstverantwortung statt Gehorsam, Lernen statt reiner Kontrolle.[2]

Eine KI-getriebene Organisation ist deshalb nicht die Organisation, in der KI möglichst viel kontrolliert.

Es ist die Organisation, in der Menschen mit KI ihre eigene Arbeit kontinuierlich verbessern können.

5.4 Ausweg statt Verstärker des Automatisierungsdrucks

Man könnte einwenden, die Anforderung zu „Erbauern“ zu werden baue sozialen Druck auf die Mitarbeiter auf.

Der eigentliche soziale Druck im KI-Zeitalter entsteht aber nicht durch dieses Modell. Er entsteht durch die berechtigte Sorge, dass KI Wissensarbeit automatisiert, ohne dass die Wissensarbeitenden daran beteiligt sind. Wer auf zentrale KI-Programme wartet, wartet im schlimmsten Fall auf seine eigene Wegrationalisierung.

[2] Vergleiche Manifest für menschliche Führung - Marcus Raitner

© 2026 IS4IT GmbH

Das Bau-vor-Betrieb-Prinzip ist deshalb kein Verstärker dieses Drucks, sondern ein Ausweg aus ihm.

Wer mit KI baut, gestaltet die eigene Arbeitsumgebung aktiv mit, statt darauf zu warten, von einer Automatisierung getroffen zu werden, die andere für ihn entschieden haben. Aus „wegrationalisiert werden“ wird „mitbauen können“. Mitarbeitende beziehen erstmals eine konstruktive Position gegenüber der Automatisierung ihrer eigenen Arbeit — nicht als Anforderungsgeber im Ticketsystem, sondern als Erbauer im sicheren Raum.

Das verändert nicht jede Rolle und schützt nicht vor jedem Wandel. Aber es ist der entscheidende Unterschied zwischen Automatisierung, die mit den Menschen geschieht, und Automatisierung, die über sie hinwegläuft.

5.5 Nicht nur Effizienz, sondern Lerngeschwindigkeit messen

Natürlich soll KI messbare Effizienzgewinne bringen. Manuelle Arbeit soll sinken. Fehler sollen reduziert werden. Durchlaufzeiten sollen kürzer werden. Medienbrüche sollen verschwinden.

Aber wer KI-Transformation nur nach eingesparten Stunden bewertet, greift zu kurz.

Der größere Hebel liegt darin, die Verbesserungsfähigkeit der Organisation zu erhöhen.

Sinnvolle Kennzahlen sind daher nicht nur:

- eingesparte Bearbeitungszeit
- reduzierte Fehlerquote
- geringere Nacharbeit
- kürzere Durchlaufzeit
- geringere externe Entwicklungskosten

Sondern auch:

- Wie viele Fachexperten bauen aktiv mit KI?
- Wie schnell wird aus einer Idee ein Prototyp?
- Wie viele Prototypen schaffen es in einen Pilot?
- Wie viele manuelle Workarounds wurden ersetzt?
- Wie viele Automatisierungen werden von anderen Teams wiederverwendet?
- Wie lange dauert ein Produktiv-Gateway?
- Wie viele produktive Automatisierungen haben klare Owner?
- Wie viele Experimente wurden bewusst beendet, weil sie keinen Nutzen brachten?

Die wichtigste Kennzahl ist nicht nur Effizienz.

Die wichtigste Kennzahl ist:

Lerngeschwindigkeit.

Eine Organisation, die mit KI schneller lernt, wird langfristig produktiver, anpassungsfähiger und wettbewerbsfähiger.

© 2026 IS4IT GmbH

5.6 Unternehmerisches Risiko gehört dazu

Ein Unternehmen kann KI nicht risikofrei einführen. Der Versuch, jedes Risiko vorab auszuschließen, erzeugt ein anderes Risiko: Stillstand.

KI-Transformation braucht deshalb eine bewusste Risikohaltung.

Nicht jedes Risiko ist gleich. Manche Risiken sind nicht verhandelbar: Datenschutzverstöße, unkontrollierte Produktivzugriffe, fehlende Verantwortlichkeit, verdeckte Außenwirkung oder unsichere Verarbeitung vertraulicher Informationen.

Andere Risiken gehören zum Lernen: Prototypen, die verworfen werden. Experimente, die keinen Nutzen bringen. Automatisierungen, die nach drei Wochen ersetzt werden. Doppelte Versuche in verschiedenen Teams. Kleine Fehler in nicht-produktiven Umgebungen.

Diese Risiken sind kein Zeichen schlechter Steuerung. Sie sind der Preis organisationaler Lernfähigkeit.

Entscheidend ist daher nicht, Risiko zu vermeiden.

Entscheidend ist, Risiko dort zuzulassen, wo der Schaden begrenzt ist — und es dort streng zu kontrollieren, wo reale Wirkung entsteht.

Oder kurz:

Viel Freiheit im sicheren Raum von „KI baut“. Aber klare Verantwortung vor produktiver Wirkung.

5.6.1 Make-or-Buy neu gedacht

Aus dem Bau-vor-Betrieb-Prinzip ergibt sich auch eine neue Make-or-Buy-Strategie.

Für standardisierte, auditierbare und regulierte Grundfunktionen sollte man weiterhin kaufen. Ein Unternehmen sollte beispielsweise nicht sein eigenes Buchhaltungssystem bauen, wenn am Markt ERP-Systeme verfügbar sind, die Rollen- und Rechtemodelle, Prüfpfade, Standardschnittstellen und regulatorische Anforderungen bereits mitbringen.

Kernsysteme müssen stabil, prüfbar und langfristig wartbar sein.

Außen herum entsteht jedoch ein neuer Raum für **Make**: firmenspezifische Automatisierung, die genau zu den eigenen Prozessen passt.

Die neue Make-or-Buy-Frage lautet daher nicht:

„Bauen wir jetzt alles selbst?“

Sondern:

„Welche Teile müssen stabil gekauft werden — und welche Lücken können unsere eigenen Fachexperten schneller und für unsere Zwecke passgenauer schließen als jeder externe Anbieter?“

© 2026 IS4IT GmbH

Dort, wo heute Excel-Listen manuell gepflegt, Dateien kopiert, Daten umformatiert, Reports zusammengebaut, Importe vorbereitet, Statusinformationen abgeglichen oder Systemgrenzen per Hand überbrückt werden, können Fachexperten mit KI-Unterstützung selbst kleine Automatisierungen bauen.

Die Strategie lautet also:

Standardisierte Kernsysteme kaufen — und die firmenspezifische Automatisierung darum herum durch Fachexperten mit KI-Unterstützung bauen lassen.

© 2026 IS4IT GmbH

6 Die richtige Reihenfolge für Effizienzgewinne

Wer KI-Projekte mit dem Ziel priorisiert, manuelle Arbeitsstunden zu reduzieren, sollte nicht mit maximaler Autonomie beginnen. Die bessere Reihenfolge lautet: zuerst stabile Automatisierung mit Hilfe von KI bauen, dann KI kontrolliert auf Daten anwenden, anschließend entscheidungsrelevante Nutzung prüfen und erst zuletzt handelnde Agenten einsetzen.

Wer KI-Projekte aber ausschließlich nach eingesparten Arbeitsstunden priorisiert, übersieht den eigentlichen Hebel. KI verändert nicht nur einzelne Prozesse. KI verändert, wer Prozesse verbessern kann. Deshalb beginnt die richtige Reihenfolge nicht mit maximaler Autonomie, sondern mit maximaler Befähigung.

Die im Folgenden genannten Prozentwerte sind Erwartungswerte des Autors, keine empirisch belegten Benchmarks. Sie sollen den Text greifbar machen und eine Diskussionsgrundlage liefern — vergleichbar mit den Daumenwerten, die im klassischen Projektmanagement seit Jahrzehnten verwendet werden, bevor sie irgendwann durch Studien gestützt wurden. Das tatsächliche Potenzial hängt stark von Prozessreife, Datenqualität, Standardisierungsgrad und regulatorischem Umfeld ab.

6.1 Erst: KI baut

Automatisiere alles, was regelhaft, wiederkehrend und prüfbar ist. Lass dir diese Automatisierungen mit Unterstützung von KI bauen — aber nutze KI nicht im laufenden Betrieb.

Als Orientierungswert: In vielen typischen Verwaltungs-, IT- oder Backoffice-Prozessen lassen sich hier Einsparungen an manueller Arbeit im Bereich von 25 bis 35 Prozent erzielen.

Im Vergleich zu klassischen Automatisierungsprojekten lassen sich Prototypen heute oft schneller erstellen, fachlich enger iterieren und besser auf konkrete Prozesse zuschneiden — ohne sofort auf schlecht passende Standardtools ausweichen zu müssen.

6.1.1 1. Fachexperten befähigen

Menschen mit Prozesswissen bekommen Zugang zu freigegebenen KI-Werkzeugen, einfachen Entwicklungsumgebungen, Vorlagen, Schulungen und Communities.

Sie lernen, wie man sichere Prototypen baut, mit Dummy-Daten arbeitet, Prompts dokumentiert, Code prüft und Risiken erkennt.

6.1.2 2. Im sicheren Raum bauen

Teams erstellen Prototypen, Skripte, Workflows, Auswertungen und Automatisierungen ohne Schutzdaten und ohne produktive Wirkung.

Die Grundhaltung lautet:

Nicht warten. Ausprobieren. Lernen. Teilen.

© 2026 IS4IT GmbH

6.1.3 3. Wirkung sichtbar machen

Gute Prototypen werden gezeigt, getestet, gemessen und mit anderen Teams geteilt.

So entsteht ein interner Marktplatz für Ideen, Vorlagen und wiederverwendbare Bausteine.

6.1.4 4. Über Gateways produktiv setzen

Sobald echte Daten, produktive Systeme, Entscheidungen oder Außenwirkung betroffen sind, erfolgt eine risikogerechte Prüfung.

Nicht als Blockade, sondern als Qualitätsschleuse.

6.1.5 5. Skalieren, was trägt

Wiederverwendbare Lösungen werden standardisiert, dokumentiert und in den Betrieb überführt.

Was lokal nützlich war, kann teamübergreifend, bereichsübergreifend oder unternehmensweit nutzbar werden.

So entsteht eine Organisation, die nicht auf zentrale KI-Programme wartet, sondern kontinuierlich aus der Fläche heraus lernt.

6.2 2. Dann: KI sieht

Im nächsten Schritt wird KI für verbleibende unstrukturierte Lese-, Analyse- und Schreibarbeit eingesetzt. Dazu gehören Zusammenfassungen, Extraktionen, Entwürfe oder Klassifizierungen.

In geeigneten verbleibenden Lese-, Analyse- und Schreibprozessen sind oft weitere **10 bis 20 Prozent** Effizienzgewinn möglich.

6.3 3. Danach: KI wirkt

Anschließend kann KI zur Vorbewertung, Priorisierung und Entscheidungsvorbereitung eingesetzt werden. Das erhöht die Geschwindigkeit und Qualität von Prozessen, benötigt aber klare Prüfung, Kontrolle und Dokumentation.

In geeigneten Prozessen kann dies zusätzliche **5 bis 10 Prozent** Einsparung bringen.

6.4 4. Zuletzt: KI handelt

Erst am Ende sollten KI-Agenten eigenständig handeln — und auch dann nur in eng begrenzten, kontrollierten und gut überwachten Szenarien.

In klar begrenzten Szenarien können auch hier Effizienzgewinne im Bereich von weiteren **5 bis 10 Prozent** möglich sein, allerdings bei deutlich höheren Anforderungen an Sicherheit, Kontrolle und Governance.

© 2026 IS4IT GmbH

7 Fazit

Der erfolgreiche Einsatz von KI beginnt nicht mit maximaler Autonomie von agentischen KI-Systemen. Er beginnt mit maximaler Befähigung.

Unternehmen werden nicht dadurch KI-getrieben, dass sie einige große KI-Projekte starten oder möglichst schnell autonome Agenten einführen. Sie werden KI-getrieben, wenn viele Menschen im Unternehmen lernen, mit KI ihre eigene Arbeit zu verbessern.

Der wichtigste Hebel liegt deshalb oft in der Stufe **„KI baut“**: Fachexperten nutzen KI, um Skripte, Workflows, Auswertungen, Schnittstellen, Tests, Vorlagen oder kleine Automatisierungen zu erstellen. Diese Lösungen können anschließend als klassische, prüfbare und kontrollierbare Automatisierung laufen — ohne dass KI im laufenden Betrieb selbst entscheiden oder handeln muss.

Dafür braucht es keine Kultur des Wartens, sondern eine Kultur des Machens: sichere Experimentierräume, freigegebene Werkzeuge, einfache Vorlagen, Communities, sichtbare Prototypen und schnelle Gateways vor produktiver Wirkung.

Das Ziel ist nicht, jedes Risiko zu vermeiden. Das Ziel ist, unternehmerisch mit Risiko umzugehen: viel Freiheit dort, wo der mögliche Schaden gering ist; klare Kontrolle dort, wo reale Wirkung entsteht.

Die pragmatische Reihenfolge lautet daher:

erst befähigen, dann bauen, dann über Gateways produktiv setzen, dann skalieren.

So entsteht keine unkontrollierte Schatten-IT. Es entsteht eine lernende, schnelle und verantwortliche Organisation — eine Organisation, in der KI nicht Menschen ersetzt, sondern Menschen befähigt, bessere Arbeitssysteme zu bauen.

Und zugleich gilt die zweite, ebenso wichtige Regel: Diese Befähigungsbewegung lebt im sicheren Bau-Raum. Sobald KI sieht, wirkt oder handelt, übernimmt nicht mehr die Fläche, sondern die Unternehmensarchitektur:

„KI baut“ ist Grass-Roots. „KI sieht“, „KI wirkt“ und „KI handelt“ sind Unternehmensarchitektur.

Nur wer beide Modi sauber trennt, vermeidet die zwei großen Fehler — Stillstand durch Übergovernance und Schatten-IT in Hochrisiko-Stufen.

Oder als abschließender Merksatz:

Governance darf nicht vor dem Lernen stehen. Sie muss dort greifen, wo Lernen produktive Wirkung bekommt.

Die operative Umsetzung — Citizen-Developer-Regeln, Gateway, Inventar, Identitäten, IT-Doppelrolle und Make-or-Buy — ist im Anhang ausgeführt.

© 2026 IS4IT GmbH

8 Anhang: Detailregeln für die Umsetzung

Citizen Developer und Doppelrolle der IT. Fachexperten werden vom Anforderungsgeber zum Erbauer. Die IT ist Plattform für die vielen Builder im Bau-Raum — und zugleich Architekt und Steuerer für alle Stufen mit produktiver Wirkung. Jede produktive Citizen-Lösung steht in einem unternehmensweiten Inventar mit benanntem Autor und harter Nachfolgeregelung: Geht der Autor, wird übernommen oder abgeschaltet. **Keine produktive Lösung ohne Owner.**

Governance an der richtigen Stelle. Nicht vor dem Prototyp, sondern vor dem produktiven Einsatz. Das Gateway ist Qualitätsschleuse und kontrollierte Übergabe vom Builder an die zentrale Steuerung — und selbst der erste KI-Anwendungsfall im eigenen Haus: KI bereitet die Freigabe vor, Menschen entscheiden Ausnahmen. Externe Rahmenwerke (EU AI Act, DSGVO, NIST AI RMF, ISO/IEC 42001) geben die Pflichten vor; das Modell macht sie im Alltag handhabbar. **Governance darf nicht vor dem Lernen stehen. Sie muss dort greifen, wo Lernen produktive Wirkung bekommt.**

Identitäten und Geheimnisse. Jede produktive Citizen-Lösung erhält eine eigene technische Identität mit minimalen Rechten; Zugangsdaten ausschließlich über einen zentralen Secrets-Tresor. Viele kleine Identitäten begrenzen den Schadensradius eines Vorfalls drastisch — anders als ein einzelner Agent mit Vollmacht.

8.1 Regeln für Citizen Developer

Die wichtigste Rolle im Bau-vor-Betrieb-Prinzip ist der Mitarbeiter als eigenverantwortlicher Erbauer: der Citizen Developer. Er braucht Freiheit. Aber diese Freiheit braucht auch Regeln.

8.1.1 Regel 1: Jeder darf prototypisieren

Ohne Schutzdaten, ohne produktive Systeme, ohne Außenwirkung.

Ziel ist Lernen, Ausprobieren und Sichtbarmachen von Potenzial. Dafür braucht es keine Projektanträge und keine langen Freigaben, sondern klare Spielregeln und einfache Werkzeuge.

Es gibt nur eine Einschränkung: Sobald KI geschützte Daten verarbeitet, Entscheidungen beeinflusst oder Aktionen ausgelöst werden — also in den Handlungsräumen „KI sieht“, „KI wirkt“ und „KI handelt“ — greift kein Grass-Roots-Modell mehr, sondern zentrale Planung über Unternehmensarchitektur, Datenschutz, Informationssicherheit, Compliance und Fachverantwortung. Citizen Developer dürfen den Erlaubnisraum von „KI baut“ nicht eigenmächtig verlassen. Solange sie aber mit KI deterministische Systeme bauen, die kein KI im Betrieb benutzen, ist das Risiko beherrschbar.

8.1.2 Regel 2: Befähigte AI Builder dürfen pilotieren

Mit freigegebenen Tools, begrenztem Nutzerkreis, dokumentiertem Zweck und klarer fachlicher Verantwortung.

© 2026 IS4IT GmbH

Diese Personen können aus Fachbereichen kommen und werden gezielt geschult: nicht zu professionellen Softwareentwicklern, sondern zu verantwortungsvollen Erbauern kleiner Automatisierungen.

8.1.3 Regel 3: Produktive Automatisierung braucht ein Gateway

Sobald reale Daten, produktive Systeme, Außenwirkung, Schreibrechte oder kritische Prozesse betroffen sind, greift ein risikogerechtes Produktiv-Gateway.

So entsteht kein Genehmigungsapparat für jede Idee, sondern ein skalierbares Modell:

maximale Freiheit am Anfang, zunehmende Verbindlichkeit bei zunehmender Wirkung.

8.2 Eine neue Aufgabe für die Governance

Das Produktiv-Gate darf nicht zum Vorab-Genehmigungsprozess für jede Idee werden. Dann würde es genau die Geschwindigkeit zerstören, die KI ermöglichen soll.

Das Gate gehört an die richtige Stelle:

nicht vor den Prototyp, sondern vor den produktiven Einsatz.

Fachexperten sollen im sicheren Raum schnell ausprobieren dürfen. Erst wenn eine Automatisierung echte Daten verarbeitet, produktive Systeme nutzt, Entscheidungen beeinflusst, Nachrichten versendet oder dauerhaft betrieben werden soll, wird sie geprüft.

Damit wird Governance vom Bremsklotz zur Qualitätsschleuse.

Das Gateway hat dabei noch eine zweite, oft unterschätzte Funktion: Es ist der **strukturelle Übergang vom Grass-Roots-Modus in den zentral gesteuerten Modus**. Solange eine Idee im Handlungsraum „KI baut“ lebt, gelten die dezentralen Spielregeln. In dem Moment, in dem sie Schutzdaten berührt, Entscheidungen beeinflusst oder Aktionen auslöst, wechselt sie in „KI sieht“, „KI wirkt“ oder „KI handelt“ — und damit in die Welt von Unternehmensarchitektur, zentralen Sicherheits- und Datenschutzprogrammen, Identity- und Berechtigungskonzepten sowie formaler Verantwortung.

Genau dieser Übergabepunkt ist das Gateway. Es ist nicht nur eine Qualitätsprüfung, sondern die kontrollierte Übergabe vom dezentralen Builder an die zentrale Steuerung.

Ein praktikables Gateway-Modell kann so aussehen:

Phase	Was erlaubt ist	Was nötig ist
Experiment	Ausprobieren mit Dummy-Daten, lokale Prototypen, KI-gestützte Entwürfe	keine Vorabfreigabe, aber klare Spielregeln
Team-Pilot	begrenzte Nutzung im Team, begrenzte Daten, fachliche Prüfung	Registrierung, Owner, kurzer Check
Produktive Nutzung	wiederkehrender Einsatz mit echten Daten oder Prozesswirkung	Produktiv-Gateway mit Tests, Dokumentation und Freigabe

© 2026 IS4IT GmbH

Phase	Was erlaubt ist	Was nötig ist
Kritische Nutzung	Schreibrechte, externe Wirkung, kritische Prozesse	formaler Review durch IT, Security, Datenschutz, Compliance oder Management

Die Gateways müssen leichtgewichtig genug sein, damit Menschen sie nutzen — und klar genug, damit niemand produktive Risiken versteckt.

Ein Gateway, das Wochen dauert, erzeugt Ausweichbewegungen. Ein Gateway, das schnell, verständlich und hilfreich ist, macht dezentrale Innovation sichtbar.

Schlechte Governance erzeugt Schatten-IT.

Gute Governance macht Schatten-IT unnötig.

8.2.1 Vom KI-gebauten Prototyp in den Betrieb

Ein zentraler Punkt bleibt wichtig: Nur weil eine Automatisierung mit KI-Unterstützung gebaut wurde, ist sie noch nicht automatisch für den produktiven Einsatz geeignet.

Die Stufe „KI baut“ beschreibt zunächst nur, dass KI nicht selbst im laufenden Betrieb eingesetzt wird. Das reduziert das operative KI-Risiko. Es sagt aber noch nichts darüber aus, welches Risiko die gebaute Automatisierung später im Betrieb hat.

Ein mit KI-Unterstützung erstelltes Skript kann harmlos sein, wenn es lokal eine Testdatei formatiert. Dasselbe Skript kann kritisch werden, wenn es produktive Kundendaten verarbeitet, Daten in ein CRM schreibt, Reports für Managemententscheidungen erzeugt, Dateien automatisch löscht oder externe Nachrichten versendet.

Deshalb gilt:

KI-gebaut heißt nicht automatisch produktiv freigegeben.

Vor der produktiven Nutzung muss geprüft werden, was die Automatisierung im Betrieb tatsächlich tut:

- Welche Daten verarbeitet sie?
- Greift sie auf personenbezogene Daten, Kundendaten, Finanzdaten oder Geschäftsgeheimnisse zu?
- Liest sie nur Daten oder schreibt, verändert, versendet oder löscht sie auch Daten?
- Greift sie auf produktive Systeme, Datenbanken, APIs oder Cloud-Dienste zu?
- Hat sie externe Wirkung gegenüber Kunden, Bewerbern, Lieferanten oder Behörden?
- Kann ein Fehler finanzielle, rechtliche, operative oder reputative Schäden verursachen?
- Gibt es Tests, Logging, Fehlerbehandlung und Dokumentation?
- Wer ist fachlich verantwortlich?
- Wer ist technisch verantwortlich?
- Wie kann die Automatisierung gestoppt, zurückgerollt oder abgeschaltet werden?

© 2026 IS4IT GmbH

Das Produktiv-Gateway bewertet also nicht nur die KI-Nutzung im Bauprozess, sondern vor allem die spätere Wirkung der gebauten Automatisierung.

Eine einfache Einteilung hilft:

Betriebswirkung der Automatisierung	Beispiel	Erforderliche Kontrolle
Nur lokale Hilfstätigkeit	Datei umbenennen, CSV formatieren, Testdaten erzeugen	fachliche Prüfung
Verarbeitung interner Daten	Report erstellen, Listen abgleichen	Zugriffskontrolle, Tests, Dokumentation
Verarbeitung geschützter Daten	HR-, Kunden-, Vertrags- oder Finanzdaten auswerten	Datenschutzprüfung, Berechtigungskonzept, Logging
Schreibzugriff auf Systeme	CRM aktualisieren, Tickets schließen, Stammdaten ändern	technische Freigabe, Rollback, Protokollierung
Externe Wirkung	E-Mails versenden, Kunden informieren, Dokumente erzeugen	Vier-Augen-Prinzip, Freigabe vor Versand
Kritische Prozesse	Finance, HR, Produktion, Recht, Medizin, Sicherheit	formaler Change- und Freigabeprozess

Für einfache Micro-Automatisierungen kann das Gateway leichtgewichtig sein. Für kritische Automatisierungen braucht es einen formalen Freigabeprozess.

Entscheidend ist, dass es überhaupt ein Gateway gibt — aber an der richtigen Stelle.

8.2.2 Das Gateway ist selbst ein KI-Anwendungsfall

Ein langsames Gateway zerstört die Geschwindigkeit, die das Modell ermöglichen soll. Wenn Fachbereiche im Bau-Raum in Tagen arbeiten und das Gateway dann Wochen dauert, kippt das gesamte Modell. Deshalb muss das Gateway selbst auf Tempo getrimmt sein.

Das gelingt nur, wenn KI nicht nur beim Bauen hilft, sondern auch im Gateway konsequent eingesetzt wird. Das Gateway ist damit der **erste konkrete Anwendungsfall der Handlungsräume „KI sieht“ und „KI wirkt“** im eigenen Unternehmen: KI sieht den Code, die Datenflüsse, die Berechtigungen, die Dokumentation und die Tests; KI wirkt auf die Freigabe-Empfehlung.

Im Standardfall bereitet die KI die Gateway-Entscheidung nach klar definierten Regeln vollständig vor. Sie:

- analysiert Code, Skripte, Workflows und Konfiguration
- klassifiziert Datenflüsse, Schutzbedarf und Drittsystemzugriffe
- prüft Berechtigungen, Logging, Fehlerbehandlung und Rollback-Pfade
- bewertet Tests, Dokumentation und benannte Verantwortlichkeiten

© 2026 IS4IT GmbH

- erzeugt SBOM und prüft Lizenzlage
- prüft, ob ein gültiger Inventar-Eintrag mit benanntem Citizen-Autor und Nachfolgeregelung vorliegt
- formuliert ein begründetes Freigabe-Votum

Nur in fraglichen, neuartigen oder grenzwertigen Fällen entscheidet ein menschliches Gremium. So bleibt Geschwindigkeit auch im Gateway erhalten — und Gremien werden mit Ausnahmen, nicht mit Routinearbeit befasst. Die Freigabe selbst wird im Inventar registriert; ohne Inventar-Eintrag gibt es keine produktive Freigabe.

Damit greift das Bau-vor-Betrieb-Prinzip auch für das Gateway selbst: Es ist eine zentrale, kontrolliert eingesetzte KI-Anwendung mit klaren Regeln, klarer Datenbasis und klarer Verantwortung — keine dezentrale Bastelei. Die fachliche, technische und rechtliche Verantwortung bleibt menschlich. Aber die Routine, die heute Gremien lähmt, übernimmt die KI.

Wichtig ist dabei: Auch wenn das Gateway formal in „KI sieht“ / „KI wirkt“ gehört, ist es der **risikoärmste denkbare Anwendungsfall dieser Klasse**. Verarbeitet werden nur unternehmensinterne Artefakte (Code, Doku, Konfiguration, Metadaten — keine Kundendaten und keine personenbezogenen Echtdaten). Der Zweck ist eng definiert. Die Plattform ist ohnehin freigegeben. Der EU AI Act stuft Code-Prüfung nicht als Hochrisiko-Anwendung ein. Und die finale Entscheidung in fraglichen Fällen bleibt menschlich. DSGVO-, AI-Act- und vertragliche Fragen lassen sich für diesen Anwendungsfall einmal sauber klären und greifen dann pauschal für alle Gateway-Prüfungen. Das macht das Gateway zu einem besonders gut beherrschbaren Erstanwendungsfall — und zugleich zu einem Beleg dafür, dass das Modell auch für sich selbst gilt.

Die Grundregel lautet:

KI bereitet die Freigabe vor — Menschen entscheiden Ausnahmen.

Oder kürzer:

KI-gebaut heißt nicht automatisch produktiv freigegeben. KI-geprüft heißt nicht automatisch sicher. Erst die risikogerechte Freigabe macht aus einem Prototyp eine betriebsfähige Automatisierung — aber sie muss schnell sein.

8.2.3 Identitäten und Geheimnisse für Citizen-Lösungen

Sobald eine Citizen-Lösung produktiv läuft, braucht sie technischen Zugriff auf Daten und Systeme — und damit Zugangsdaten, API-Schlüssel oder Tokens. Dieser Punkt entscheidet in der Praxis darüber, ob das Modell sicher skaliert oder zur Schatten-IT mit Vollzugriff verkommt.

Die Grundregeln lauten:

- Jede produktive Citizen-Lösung erhält eine **eigene technische Identität** mit minimalen Rechten — niemals die persönlichen Zugangsdaten des Autors, niemals geteilte Sammel-Accounts.

© 2026 IS4IT GmbH

- Berechtigungen folgen strikt dem **Least-Privilege-Prinzip**: nur die Felder, Datensätze, Endpunkte und Aktionen, die fachlich tatsächlich gebraucht werden.
- Zugangsdaten, API-Schlüssel und Tokens werden ausschließlich über einen **zentralen Secrets-Tresor** verwaltet und zur Laufzeit injiziert.
- **Hartkodierte Secrets im Code sind ein hartes Ausschlusskriterium im Gateway** — keine Ausnahme, keine Übergangsfristen.
- Identitäten und Berechtigungen sind an das Inventar gekoppelt: Wird eine Lösung stillgelegt oder wechselt der Owner, werden die zugehörigen Rechte automatisch geprüft und gegebenenfalls entzogen.

Diese Disziplin ist nicht nur Hygiene, sondern ein zentrales **Sicherheitsargument für das Modell**: Viele kleine, eng begrenzte Identitäten begrenzen den Schadensradius eines einzelnen Vorfalls drastisch. Bei einem klassischen Agenten-Setup mit weitreichenden Rechten kann ein einziger erfolgreicher Prompt-Injection-Angriff oder ein einziges kompromittiertes Token unternehmensweit Wirkung entfalten. Fünfhundert Micro-Automatisierungen mit jeweils minimalen Rechten sind in der Summe deutlich beherrschbarer als ein einziger Agent mit Generalvollmacht.

Anders gesagt: Granularität ist hier ein Sicherheitsmerkmal, kein Verwaltungsaufwand.

8.3 Neuartige Strukturen in der Unternehmensarchitektur

8.3.1 Fachnahe Micro-Automatisierung statt Schatten-IT

Viele der interessantesten KI-gestützten Automatisierungen sind keine großen Softwareprodukte. Es sind kleine, konkrete Lösungen für wiederkehrende Aufgaben: ein Importhelfer, ein Prüfskript, ein Report, ein Datenabgleich, eine Konvertierung, eine vorbereitete Schnittstelle oder ein Workflow für einen eng begrenzten Prozess.

Solche Lösungen sollten nicht als „Wegwerf-Code“ verstanden werden. Besser ist der Begriff:

fachnahe Micro-Automatisierung.

Fachnahe Micro-Automatisierung meint kleine, klar abgegrenzte technische Lösungen, die direkt aus einem konkreten Prozessproblem entstehen. Sie müssen nicht für zehn Jahre gebaut werden. Sie müssen aber sicher, verständlich, prüfbar und abschaltbar sein.

Typische Beispiele sind:

- ein Skript zur Bereinigung monatlicher Excel-Exporte
- ein Prüfbericht für unvollständige Stammdaten
- ein Importhelfer für CSV-Dateien
- ein Abgleich zwischen zwei Listen oder Systemexporten
- eine automatische Erstellung interner Statusberichte
- eine Konvertierung zwischen Datenformaten
- eine vorbereitende Auswertung für Controlling, HR, Einkauf oder Vertrieb
- ein PowerShell- oder Python-Skript für wiederkehrende IT-Administrationsaufgaben

© 2026 IS4IT GmbH

Gerade solche Aufgaben bleiben in Unternehmen oft manuell, weil sie für ein großes IT-Projekt zu klein, für Standardsoftware zu speziell und für den Fachbereich technisch zu aufwendig waren.

KI senkt diese Hürde.

Anders als bei klassischen Citizen-Developer-Bewegungen löst KI dabei auch das alte Übernahme- und Wartungsproblem weitgehend. Sie erklärt fremden Code, überführt ihn in andere Sprachen, ergänzt fehlende Tests und erzeugt Dokumentation gezielt so, dass nachfolgende Bearbeiter — Mensch wie KI — direkt anschließen können. Das klassische „VBA-Friedhof"- oder „Excel-Hölle"-Argument verliert dadurch seinen Schrecken. Was bleibt, ist keine technische, sondern eine organisatorische Frage.

8.3.2 Inventar und Nachfolgeregelung für Citizen-Lösungen

Jede Citizen-Lösung hat einen Citizen-Autor — eine namentlich benannte Person aus dem Fachbereich, die sie gebaut hat und fachlich verantwortet. Sobald eine Lösung produktiv geht, reicht das nicht mehr aus. Es braucht ein **unternehmensweites Inventar aller produktiven Citizen-Lösungen** als verbindliches Register.

Pflichtfelder pro Eintrag:

- eindeutiger Name und Kurzbeschreibung
- Citizen-Autor (fachlich verantwortlich)
- technische Ansprechperson (Plattform, IT, ggf. Vertretung)
- Status (Pilot, Produktiv, Stillgelegt)
- verarbeitete Datenarten und Schutzklassen
- angebundene Systeme und Berechtigungen
- Gateway-Freigabe und Datum
- letzter Review
- Abschalt- und Rollback-Prozedur

Das Inventar ist nicht Selbstzweck. Es ist die Voraussetzung für die zweite Pflicht: die **Nachfolgeregelung**.

Wenn der Citizen-Autor das Unternehmen verlässt, die Abteilung wechselt oder die Rolle aufgibt, gibt es im Inventar nur zwei zulässige Ergebnisse:

1. **Ein neuer Citizen-Verantwortlicher wird benannt** — fachlich qualifiziert, ausreichend befähigt und ausdrücklich einverstanden, die Lösung zu übernehmen. Übergabe samt Doku, Prompts, Tests und Zugriffen.
2. **Die Lösung wird abgeschaltet** — Zugriffe entfernt, Daten und Artefakte bereinigt, Stillgelegt-Status gesetzt.

Eine produktive Citizen-Lösung ohne benannten Owner ist nicht akzeptabel. Sie ist per Definition Schatten-IT — selbst wenn sie ursprünglich sauber durchs Gateway gekommen ist.

Damit das im Alltag funktioniert, muss der Inventar-Eintrag Teil des Gateway-Prozesses sein: Keine produktive Freigabe ohne Inventar-Registrierung, keine Personalveränderung beim

© 2026 IS4IT GmbH

Autor ohne automatische Prüfung der zugehörigen Einträge. Idealerweise ist das Inventar an Identity- und HR-Prozesse angebunden, sodass Austritte oder Rollenwechsel automatisch eine Owner-Klärung auslösen.

Damit die Flexibilität nicht zu Risiko wird, hat jede fachnahe Micro-Automatisierung einen klaren Status:

- **Prototyp:** wird ausprobiert, nutzt keine produktiven Schutzdaten und hat keine produktive Wirkung.
- **Pilot:** wird mit begrenzten Daten, begrenztem Nutzerkreis und fachlicher Kontrolle getestet.
- **Produktiv:** ist geprüft, dokumentiert, freigegeben, im Inventar registriert und einem benannten Citizen-Autor zugeordnet.
- **Stillgelegt:** wird nicht mehr genutzt; Zugriffe wurden entfernt, Daten und Artefakte wurden bereinigt, Inventar-Eintrag entsprechend markiert.

So entsteht keine unkontrollierte Schatten-IT, sondern ein kontrollierter Raum für schnelle, fachnahe Automatisierung — mit einer Sichtbarkeit, die in vielen klassischen IT-Landschaften nicht einmal für offizielle Anwendungen vorhanden ist.

8.3.3 Die Kehrseite: Lock-in durch Micro-Automatisierung

Diese Strategie hat eine bewusst akzeptierte Kehrseite: Je mehr fachnahe Automatisierungen rund um ein Kernsystem entstehen, desto tiefer wird die Bindung an dieses System. Hunderte kleine Skripte, Workflows und Schnittstellen hängen an konkreten Feldern, APIs, Datentypen und Prozessen des ERP, CRM oder DMS. Ein Systemwechsel wird damit deutlich teurer und langwieriger.

Dieses Phänomen ist nicht neu. Schon heute zementieren Mitarbeitende, die ein System gelernt haben, Schatten-Reports, gewachsene Schnittstellen und etablierte Arbeitsweisen das Kernsystem oft stärker als die Software selbst. KI verändert daran qualitativ wenig — sie verstärkt den Effekt aber quantitativ, weil viel mehr Automatisierungen entstehen.

Daraus folgen zwei Konsequenzen für die Kernsystem-Auswahl:

- Besonderes Augenmerk auf **langlebige, gut dokumentierte und standardisierte Schnittstellen** — der Lock-in entsteht weniger durch das System selbst als durch die Vielzahl der Automatisierungen rundherum.
- **Strategische Anbieterstabilität** wird wichtiger als das letzte Funktionsfeature. Wer das Kernsystem alle fünf Jahre wechseln muss, verliert den Effizienzhebel des Modells.

Das ist der eigentliche Grassroots-Hebel.

Nicht ein zentrales KI-Team entscheidet allein, welche Prozesse verbessert werden. Die Organisation selbst entwickelt Sensorik für Reibung — und die Fähigkeit, diese Reibung zu reduzieren.

© 2026 IS4IT GmbH

8.4 Die neue Rolle der IT

Damit KI-gestütztes Bauen skaliert, muss sich auch die Rolle der IT verändern. Sie übernimmt dabei eine **Doppelrolle**, die exakt der Trennung der Handlungsräume folgt.

8.4.1 Im Handlungsraum „KI baut“: Plattform für viele Builder

Die IT muss nicht jede kleine Automatisierung selbst entwickeln. Aber sie muss die Umgebung bereitstellen, in der Fachbereiche sicher bauen können.

Dazu gehören:

- freigegebene KI-Werkzeuge
- freigegebene Programmiersprachen und Frameworks
- einfache Entwicklungsumgebungen für Fachbereiche
- Vorlagen für Reports, Datenimporte, Exporte und Schnittstellen
- geprüfte Bibliotheken und Komponenten
- zentrale Code-Repositories
- ein unternehmensweites Inventar produktiver Citizen-Lösungen mit Autor, Status und Abhängigkeiten
- Anbindung des Inventars an HR- und Identity-Prozesse, damit Austritte und Rollenwechsel automatisch eine Owner-Klärung auslösen
- einfache Test- und Freigabeprozesse
- klare Regeln für Daten, Secrets und Zugangsdaten
- Trennung von Test- und Produktivumgebungen
- technische Prüfungen vor Zugriff auf kritische Systeme
- definierte Verantwortlichkeiten für Betrieb, Wartung und Abschaltung
- Communities of Practice für AI Builder
- Sprechstunden, Coaching und Beispiele

In dieser Rolle wird die IT vom Flaschenhals zur Plattform. Sie sorgt dafür, dass dezentrale Geschwindigkeit nicht in Chaos umschlägt.

8.4.2 In „KI sieht, wirkt & handelt“: Architekt und Steuerer

Sobald KI geschützte Daten verarbeitet, Entscheidungen beeinflusst oder Aktionen auslöst, reicht die Plattform-Rolle nicht mehr. Hier wird die IT zum **zentralen Architekten und Steuerer** — gemeinsam mit Datenschutz, Informationssicherheit, Compliance und den fachlich Verantwortlichen.

In dieser Rolle gehört zu ihren Aufgaben:

- KI-Referenzarchitekturen für unternehmensweite Use Cases
- Datenarchitektur, Datenflüsse und Datenklassifizierung
- Identity- und Berechtigungskonzepte für KI-Systeme und Agenten
- Auswahl und Vertragsgestaltung mit KI-Anbietern (inkl. Sub-Processor und Drittlandtransfers)

© 2026 IS4IT GmbH

- Sicherheitsarchitektur gegen Prompt-Injection, Tool-Missbrauch und Datenabfluss
- Monitoring, Logging und Incident Response für KI-Systeme
- Integration mit bestehender Enterprise Architecture und Risikomanagement
- Lifecycle-Management von Modellen, Prompts, Tools und Agenten

Diese Themen lassen sich nicht aus der Fläche heraus lösen. Sie brauchen zentrale Programme, architektonische Leitentscheidungen und klare Verantwortlichkeiten.

8.4.3 Die IT wird damit nicht unwichtiger. Im Gegenteil.

Sie spielt zwei Rollen gleichzeitig — und muss beide gut beherrschen:

Plattform für die Vielen. Architekt für das Ganze.

Das Ziel ist nicht maximale Freiheit. Das Ziel ist kontrollierte Geschwindigkeit.

8.4.4 Eine neue Rolle für Systemhäuser

Für kleinere und mittlere Unternehmen ist diese Doppelrolle aus eigener Kraft nicht immer leistbar. Eine 80-Personen-Organisation kann keine eigene Plattform-Mannschaft aufbauen, die freigegebene Tools kuratiert, Vorlagen pflegt, Coaching anbietet und gleichzeitig Architekturentscheidungen für KI-Datenflüsse trifft.

Genau hier entsteht ein neues Geschäftsmodell für Systemhäuser und IT-Dienstleister, deren klassisches Auftragscoding durch KI ohnehin schrumpft. Wer in der KI-Ökonomie weiter relevant bleiben will, verschiebt seine Wertschöpfung — vom Code-Lieferanten zum Befähigungsanbieter:

- freigegebene KI-Plattformen als Service
- gepflegte Vorlagen-, Bibliotheks- und Komponentenkataloge
- Coaching, Sprechstunden und Communities für AI Builder
- Gateway-Dienste mit KI-gestützter Prüfung
- Architekturberatung für „KI sieht“, „KI wirkt“, „KI handelt“

Damit wird das Modell auch für Organisationen tragfähig, die die Doppelrolle nicht intern abbilden können. Das ist absehbar — und Systemhäuser, die das früh erkennen, gewinnen einen Markt, der ihnen sonst verlorengeht.

© 2026 IS4IT GmbH