

EXECUTIVE WHITEPAPER FÜR MITTELSTAND · C-LEVEL & IT-LEITUNG

AI Governance im Mittelstand — Führungswissen für die Praxis

*Wie Geschäftsführung und IT-Leitung gemeinsam die
Kontrolle über KI-Systeme behalten — ohne Vendor-
Abhängigkeit und mit klarer Methodik.*

🛡️ EU AI Act Art. 4 konform

🕒 30 Minuten Lektüre

✓ Herstellerunabhängig

WAS SIE IN DIESEM WHITEPAPER ERWARTET

Inhalt

01	Warum AI Governance jetzt Chefsache ist	3
	Die veränderte Risikolage im Mittelstand 2026	
02	Was AI Governance bedeutet — und was nicht	4
	Definition, Abgrenzung, drei Kernfragen	
03	Die fünf Säulen des AI Governance Frameworks	5
	Strategie · Risiko · Compliance · Security · Ethik	
04	Rollen & Verantwortlichkeiten im Mittelstand	6
	Wer entscheidet was — ein pragmatisches RACI-Modell	
05	EU AI Act — Was Führungskräfte jetzt wissen müssen	7
	Artikel 4, Risikokategorien, Handlungspflichten	
06	AI Security: Die unterschätzte Dimension	8
	Schatten-AI, Datenleck, Deepfakes im Unternehmenskontext	
07	Der 90-Tage-Implementierungsplan	9
	Vom ersten Audit zur operativen AI Governance	
08	Führungskräfte-Checkliste	10
	12 Fragen — wo steht Ihr Unternehmen heute?	
TEIL 2 · ANWENDUNGSAUSBLICK		
—	Teil 2 Einführung	11
	Vom Rahmen zur Praxis	
09	Von Governance zu Praxis — Die 8 Agent Gaps	12
	Typische Einsatzfelder für AI Agents im Mittelstand	
10	Reale Ergebnisse — drei Use Cases	13
	Messbare Resultate aus dem Mittelstand	
11	Kompetenzaufbau — drei Rollen für den Agenten-Betrieb	14
	Prompt Engineer · AI Owner · Agent Supervisor	
>	Nächster Schritt	15
	So arbeiten Sie mit PiGentic	

01 WARUM JETZT

AI Governance ist 2026 Chefsache — ob Sie wollen oder nicht.

Der Mittelstand hat investiert. Copilot-Lizenzen, ChatGPT-Accounts, erste Automatisierungsprojekte. Was dabei oft fehlt: ein klarer Rahmen dafür, wer was entscheidet, wer haftet und was passiert, wenn etwas schief läuft.

Die erste Welle der KI-Einführung war vom Ausprobieren geprägt. Tools wurden getestet, Pilotprojekte gestartet, Mitarbeitende ermutigt. Das war richtig — aber es hat eine Lücke hinterlassen. Unternehmen, die jetzt AI Agents in operative Prozesse einbinden, stellen fest: Es gibt keine Antwort auf die Frage, wer den Agenten kontrolliert, wer seine Ausgaben verantwortet und wie die Compliance gegenüber Kunden, Betriebsrat und Aufsichtsbehörden aussieht.

Gleichzeitig hat der EU AI Act seit Februar 2025 konkrete Pflichten in Kraft gesetzt. Artikel 4 verpflichtet Unternehmen dazu, sicherzustellen, dass alle Personen, die KI-Systeme einsetzen, über ausreichende KI-Kompetenz verfügen. Das betrifft nicht nur die IT — es betrifft Geschäftsführung, Betriebsrat, Fachabteilungen und Einkauf gleichermaßen.

41 %

der Unternehmen ab 20 Mitarbeitenden setzen KI ein — viele davon ohne formale Governance (Bitkom 2025)

Art. 4

EU AI Act verpflichtet seit Feb. 2025 zu nachweisbarer KI-Kompetenz aller Nutzer

€ 35 Mio.

Höchstes Bußgeld bei verbotenen KI-Praktiken (Art. 5) — oder 7 % des Jahresumsatzes

AI Governance ist keine akademische Übung und kein Bürokratieprojekt. Es ist die Antwort auf eine sehr konkrete Frage: **Wer trägt die Konsequenzen, wenn ein KI-System eine falsche Entscheidung trifft?** Im Mittelstand ist die Antwort heute oft: niemand formal zugeordnet. Das ist das eigentliche Risiko.

„KI ist nicht das Risiko. Das Risiko ist KI ohne Kontrolle — und Kontrolle braucht Governance.“

02 DEFINITION

Was AI Governance bedeutet — und was nicht.

AI Governance wird oft mit Bürokratie gleichgesetzt. Das ist ein Missverständnis, das teure Fehler produziert.

AI Governance ist der organisatorische und technische Rahmen, der sicherstellt, dass KI-Systeme in einem Unternehmen sicher, verantwortungsvoll und nachvollziehbar eingesetzt werden. Sie beantwortet drei Kernfragen:

01

Steuerung

Wer entscheidet, welche KI-Systeme eingesetzt werden — und nach welchen Kriterien?

02

Kontrolle

Wie werden KI-Ausgaben überprüft, auditiert und bei Abweichungen korrigiert?

03

Verantwortung

Wer haftet — intern und extern — wenn ein KI-System Schaden anrichtet oder Compliance verletzt?

Für den Mittelstand bedeutet das konkret: Sie brauchen keine 50-seitige Governance-Policy. Sie brauchen klare Antworten auf die drei Fragen oben — schriftlich, geteilt, verbindlich. AI Governance ist ein **kontinuierlicher Managementprozess** — keine IT-Aufgabe, keine Compliance-Checkbox, kein einmaliges Projekt.

AI Governance vs. klassisches IT-Risikomanagement

- KI-Systeme sind keine deterministischen Programme — ihre Ausgaben können variieren, auch bei gleicher Eingabe.
- KI lernt aus Daten — fehlerhafte Trainingsdaten produzieren systematisch fehlerhafte Entscheidungen.
- KI-Fehler sind oft schwer zu erklären — Explainability ist ein eigenes Governance-Thema.
- KI-Systeme können Bias reproduzieren — rechtliche Relevanz bei Personalentscheidungen, Kreditvergabe, Preisfindung.

03 FRAMEWORK

Die fünf Säulen des AI Governance Frameworks.

Ein pragmatisches Framework für Unternehmen, die keine Großkonzern-Ressourcen haben — aber Großkonzern-Risiken tragen.

01 Strategie & Steuerung

Klare Entscheidungsstrukturen: Wer genehmigt KI-Projekte? Welche Prozesse dürfen automatisiert werden? Welche nicht? Ein AI Governance Committee — auch in kleiner Besetzung — schafft Verbindlichkeit ohne Bürokratie.

02 Risikomanagement

Systematische Bewertung jedes KI-Systems nach Auswirkung und Eintrittswahrscheinlichkeit. Pflicht-Reviews vor Produktivgang, bei Änderungen und nach Vorfällen. Dokumentation nicht für die Aufsicht — sondern für die eigene Entscheidungssicherheit.

03 Compliance & Regulatorik

EU AI Act, DSGVO, ISO 42001, branchenspezifische Vorgaben (DORA für Finanz, NIS2 für kritische Infrastruktur). Kein Unternehmen muss alle Standards vollständig implementieren — aber jedes muss wissen, welche es betreffen.

04 AI Security

KI-Systeme erweitern die Angriffsfläche des Unternehmens. Prompt Injection, Modell-Vergiftung, Datenleck über LLM-Schnittstellen — neue Bedrohungen, die klassische IT-Security-Konzepte nicht vollständig abdecken.

05 Ethik & Transparenz

Fairness, Nachvollziehbarkeit, Nicht-Diskriminierung. Im Mittelstand oft als abstrakt empfunden — wird konkret, sobald KI in der Personalauswahl, Kreditvergabe oder automatisierten Preisfindung eingesetzt wird.

„Ein AI Governance Framework muss nicht perfekt sein — es muss vorhanden und gelebt sein.“

04 ORGANISATION

Rollen & Verantwortlichkeiten — wer macht was.

Im Mittelstand gibt es selten einen dedizierten AI Officer. Das bedeutet nicht, dass die Verantwortung fehlen darf — sie muss anders verteilt werden.

Das folgende Modell ist pragmatisch skaliert für Unternehmen zwischen 50 und 1.500 Mitarbeitenden. R = Responsible (durchführend), A = Accountable (verantwortlich), C = Consulted (einbezogen), I = Informed (informiert).

AKTIVITÄT	GF / C-LEVEL	IT-LEITUNG	DATENSCHUTZ	FACHBEREICH	LEGAL
AI-Strategie & Freigabe	A	C	C	I	C
Risikobewertung neuer KI-Systeme	A	R	C	C	C
EU AI Act Compliance	A	R	R	I	R
DSGVO bei KI-Datenverarbeitung	I	C	A	C	C
AI Security & Zugriffskontrolle	I	A	C	I	I
Schatten-AI Erkennung & Policy	A	R	C	I	C
Mitarbeiter-Schulung (Art. 4 EU AI Act)	A	C	I	R	I
AI-Incident Management	I	A	C	C	C
Vendor-Verträge & KI-Klauseln	A	C	C	I	R

Das RACI-Modell zeigt: Die Geschäftsführung ist bei strategischen KI-Entscheidungen fast immer **accountable** — auch wenn die operative Durchführung delegiert wird. Wer AI Governance als reine IT-Aufgabe behandelt, unterschätzt die rechtliche Eigenverantwortung der Unternehmensleitung.

05 REGULATORIK

EU AI Act — Was Führungskräfte jetzt wissen müssen.

Der EU AI Act ist kein abstraktes Zukunftsthema. Seit Februar 2025 gelten konkrete Pflichten — auch für den Mittelstand.

Artikel 4: Die Kompetenzpflicht. Art. 4 EU AI Act verpflichtet Anbieter und Betreiber dazu, sicherzustellen, dass alle Personen, die KI-Systeme einsetzen, über ein ausreichendes Maß an KI-Kompetenz verfügen. Unternehmen müssen nachweisen können, dass ihre Mitarbeitenden — nicht nur die IT, sondern alle KI-nutzenden Personen — verstehen, wie KI funktioniert, wo sie irrt und wie sie kontrolliert wird.

Hochrisiko-KI (Art. 6 i. V. m. Annex III)

Systeme in kritischen Bereichen:
Personalentscheidungen,
Kreditwürdigkeitsprüfung, kritische Infrastruktur,
Strafverfolgung, Bildung. Strengste Pflichten:
Konformitätsbewertung, technische
Dokumentation, Registrierung.

HOHE PFLICHTEN

Allzweck-KI / GPAI (Art. 51 ff.)

ChatGPT, Claude, Gemini und ähnliche Modelle.
Betreiber (also Ihr Unternehmen) tragen
Verantwortung für den konkreten Einsatz: KI-
Kompetenz nach Art. 4, Transparenz nach Art. 50
— und bei Hochrisiko-Einsatz zusätzlich Art. 26.

BETREIBERPFLICHTEN

Drei Sofortmaßnahmen für Compliance

- **KI-Inventar anlegen:** Alle eingesetzten KI-Systeme erfassen — inklusive Schatten-AI und Mitarbeiter-genutzter Tools.
- **Risikoeinstufung vornehmen:** Welche Systeme fallen unter welche EU AI Act-Kategorie?
- **Kompetenznachweis sichern:** Schulungskonzept für Art. 4 — wer wird geschult, womit, mit welchem Nachweis?

06 SECURITY

AI Security: Die Dimension, die klassische IT-Security nicht abdeckt.

Klassische IT-Security schützt Systeme, Netzwerke und Daten. AI Security schützt darüber hinaus das Verhalten und die Ausgaben von KI-Systemen — fundamental anders, weil ein KI-System korrekt funktionieren und trotzdem falsche Ergebnisse produzieren kann.

01

Schatten-AI

Mitarbeitende nutzen unkontrolliert ChatGPT, Claude, Gemini & Co. — mit Unternehmensdaten. Kein Audit-Trail, keine Zugriffskontrolle, keine DSGVO-Konformität. Im Mittelstand das häufigste ungeklärte Governance-Problem.

PRIORITÄT 1

02

Prompt Injection

Angreifer schleusen Anweisungen in KI-Eingaben ein — das System führt sie aus, ohne dass der Nutzer es merkt. Bei AI Agents mit Systemzugang besonders kritisch: ein manipulierter Agent kann Daten exfiltrieren oder Aktionen auslösen.

AI-AGENT-RISIKO

03

Datenleck via LLM

Unternehmensdaten, die in externe LLM-Schnittstellen eingegeben werden, können für Modell-Training verwendet werden. Ohne Data-Residency-Vereinbarungen und korrekte API-Konfiguration ist dies ein ernstes Compliance-Risiko.

DATENSCHUTZ

04

Deepfakes & Social Engineering

KI-generierte Stimm- und Videoimitationen ermöglichen neuartige Betrugsangriffe. CEO-Fraud, gefälschte Zahlungsanweisungen, manipulierte Video-Calls. Bereits in deutschen Mittelstandsunternehmen dokumentierte Schadensfälle.

OPERATIVES RISIKO

„Schatten-AI verbieten funktioniert nicht. Sichtbar machen und policy-gesteuert legalisieren schon.“

07 IMPLEMENTIERUNG

Der 90-Tage-Plan: Von null zu operativer AI Governance.

Kein Unternehmen muss AI Governance in einem Projekt vollständig aufsetzen.
Drei Phasen, drei Ergebnisse.

01

Wochen 1–4

Verstehen & Inventarisieren

KI-Inventar aller eingesetzten Systeme. Risikoeinstufung nach EU AI Act. Schatten-AI-Analyse. Bestandsaufnahme bestehender Policies (DSGVO, IT-Security).

ERGEBNIS

KI-Inventar + Risikomatrix

02

Wochen 5–8

Strukturieren & Dokumentieren

RACI-Modell festlegen. Governance-Policy verabschieden (2–4 Seiten reichen). Schulungskonzept für Art. 4 EU AI Act entwickeln. Vendor-Verträge auf KI-Klauseln prüfen.

ERGEBNIS

Policy + RACI + Schulungsplan

03

Wochen 9–12

Operationalisieren

Schulung der relevanten Mitarbeitenden. Technische Kontrollen (Schatten-AI-Monitoring, Zugriffsmanagement). Ersten Review-Zyklus einplanen. Führungskräfte-Reporting aufsetzen.

ERGEBNIS

Operative Governance + Nachweis

„Eine gelebte 2-seitige AI Policy schützt mehr als eine 50-seitige, die niemand kennt.“

08 SELF-ASSESSMENT

Führungskräfte-Checkliste: Wo steht Ihr Unternehmen?

12 Fragen — je mehr Sie mit „Ja“ beantworten, desto stabiler Ihre AI Governance.

- ☐ **Wir haben ein aktuelles Inventar aller KI-Systeme im Unternehmen.**
Inkl. Schatten-AI und von Mitarbeitenden genutzter Tools ohne IT-Freigabe
- ☐ **Jedes KI-System hat einen benannten Verantwortlichen (Owner).**
Name, Rolle, Eskalationsweg dokumentiert
- ☐ **Wir haben eine schriftliche AI-Policy — verabschiedet und kommuniziert.**
Gilt für alle Mitarbeitenden, nicht nur die IT
- ☐ **Wir wissen, welche unserer KI-Systeme unter den EU AI Act fallen.**
Risikokategorie bekannt, Handlungspflichten dokumentiert
- ☐ **Art. 4 EU AI Act: Wir haben ein Schulungskonzept für KI-Kompetenz.**
Mit Nachweis — nicht nur informelles Onboarding
- ☐ **Unsere KI-Vendor-Verträge enthalten Data-Residency- und Datenschutzklauseln.**
DSGVO-konforme Verarbeitung vertraglich abgesichert
- ☐ **Wir haben einen definierten Prozess für neue KI-Projekte (Review vor Produktivgang).**
Kein KI-System geht ohne Sicherheitsfreigabe in den Betrieb
- ☐ **GF und IT-Leitung teilen ein gemeinsames Verständnis der KI-Risikosituation.**
Regelmäßiges Update-Format vorhanden
- ☐ **AI Agents, die auf interne Systeme zugreifen, haben definierte Berechtigungen.**
Least-Privilege-Prinzip angewendet
- ☐ **Wir haben einen dokumentierten Incident-Response-Prozess für KI-Vorfälle.**
Wer wird wann wie informiert?
- ☐ **Der Betriebsrat (sofern vorhanden) ist in KI-Einführungen eingebunden.**
Mitbestimmungspflichten geprüft und dokumentiert
- ☐ **Wir überprüfen unsere AI Governance mindestens einmal jährlich.**
Fixer Review-Termin im Kalender

0–4 Ja

Grundlegender Handlungsbedarf
AI Governance jetzt priorisieren.

5–8 Ja

Solide Basis mit Lücken
Gezielt schließen.

9–12 Ja

Gut aufgestellt
Kontinuierlich verbessern.



Weniger als 9 Ja? Das kostenlose **AI Agent Readiness-Assessment** priorisiert Ihre konkreten Lücken in 30 Minuten — nächster Schritt auf Seite 15.

Vom Rahmen zur Praxis: Wo Governance steht, beginnt die Anwendung.

Die folgenden drei Seiten sind kein Produktkatalog, sondern ein praxisnaher Ausblick — typische Einsatzfelder, anonymisierte Ergebnisse und die Rollen, die ein Agenten-Betrieb im Mittelstand braucht.

09

Die 8 Agent Gaps

10

Reale Ergebnisse

11

Kompetenzaufbau

09 ANWENDUNGSAUSBLICK

Von Governance zu Praxis — Die 8 Agent Gaps.

AI Governance schafft den Rahmen — die folgenden Felder zeigen, wo Agenten innerhalb dieses Rahmens konkreten Nutzen stiften. Acht typische Probleme im Mittelstand und mögliche Agenten-Ansätze.

GAP 01 · ROADMAP

Fehlende KI-Roadmap

AGENT-LÖSUNG

Von der Copilot-Lizenz zum echten Agenten: strukturierter Reifegrad-Pfad, kontrollierter Rollout, klare Verantwortung — wo klassische Beratung endet, beginnt die Agent-Architektur.

GAP 02 · KOMMUNIKATION

Ineffiziente Kommunikationsprozesse

AGENT-LÖSUNG

Teams, Tickets, Call-Routing: Kommunikationsprozesse, die sich durch Agenten selbst lösen — automatisiertes Routing, Eskalation und Zusammenfassung ohne manuelle Eingriffe.

GAP 03 · INTEGRATION

IT-Integration nach Übernahmen

AGENT-LÖSUNG

App-Integration zwischen inkompatiblen Systemen nach Firmenübernahmen: Drift-Erkennung, Auto-Remediation, Compliance-Monitoring — Agenten harmonisieren, was klassische Integrationsprojekte scheitern lässt.

GAP 04 · ENTSCHEIDUNG

Entscheidungs-Blindheit

AGENT-LÖSUNG

CEO & COO entscheiden auf Basis veralteter Daten: ein Agent liefert Echtzeit-Briefing aus ERP, CRM & BI on demand — keine Reportingzyklen mehr, sondern Antworten in Sekunden.

GAP 05 · INFRASTRUKTUR

Zero Downtime Strategie

AGENT-LÖSUNG

Infra Self-Healing trifft Security Incident Response: Agenten erkennen Anomalien, leiten automatische Korrekturmaßnahmen ein und eskalieren nur, wenn Human-in-the-Loop erforderlich ist.

GAP 06 · KOSTEN

Infrastruktur-Kosten

AGENT-LÖSUNG

Autonome FinOps-Agenten: Kostenkontrolle ohne monatliches Consulting. Der Agent identifiziert ungenutzte Ressourcen, schlägt Optimierungen vor und implementiert genehmigte Maßnahmen selbstständig.

GAP 07 · ROI

AI ROI-Lücke

AGENT-LÖSUNG

CFO & CEO investieren in KI ohne Nachweis: ein Agent trackt Tasks, Zeitersparnis & Prozesskosten automatisch — kontinuierliches ROI-Reporting ohne manuellen Aufwand.

GAP 08 · SECURITY

Schatten-AI

AGENT-LÖSUNG

Mitarbeitende nutzen ChatGPT & Co. ohne IT-Wissen — Datenverlust, Compliance-Risiko, unkontrollierte Modelle. Der Ansatz: Schatten-AI erkennen, sichtbar machen und policy-gesteuert in kontrollierte Nutzung überführen.

10 ANWENDUNGS-AUSBLICK · REALE ERGEBNISSE

Drei Use Cases aus dem Mittelstand.

Keine Zukunftsvision — betriebliche Realität. Drei Unternehmen, drei Probleme, drei messbare Ergebnisse.

Baseline vor Rollout vs. Messung 3–6 Monate danach. Kunden anonymisiert, Ergebnisse nicht 1:1 übertragbar.

Logistikunternehmen

180 Mitarbeitende · Agent Gap: Entscheidungs-Blindheit

PROBLEM

Auftragsverarbeitung vollständig manuell — hoher Zeitaufwand, Fehlerquote, kein Echtzeit-Überblick über Kapazitäten und offene Bestellungen.

AGENT-LÖSUNG

Automatisierte Auftragsverarbeitung mit Agent-Schnittstelle zu ERP — Priorisierung, Routing und Statusmeldungen ohne manuelle Eingriffe.

–50 %

Manueller Aufwand in der Auftragsverarbeitung halbiert.

Fertigungsunternehmen

400 Mitarbeitende · Agent Gap: Zero Downtime Strategie (Infrastruktur)

PROBLEM

Infrastrukturausfälle wurden erst nach Eskalation durch Endnutzer erkannt — reaktiver Betrieb, hohe MTTR, Reputationsschäden bei Kunden.

AGENT-LÖSUNG

Infrastruktur-Agent mit kontinuierlichem Monitoring: Anomalieerkennung, automatische Vorwarnung und Incident-Routing an die zuständige Stelle — bevor der Nutzer es bemerkt.

3

Kritische Ausfälle erkannt und verhindert — bevor sie eskalierten.

Produktionsunternehmen

250 Mitarbeitende · Agent Gap: Zero Downtime Strategie (IT Security)

PROBLEM

Sicherheitsrelevante Anomalien im Produktionsnetz wurden spät erkannt — zu hohes MTTR, manuelle Diagnose durch überbelastetes IT-Team.

AGENT-LÖSUNG

KI-gestützte Anomalieerkennung im SIEM: Agent korreliert Ereignisse, priorisiert Alerts und stößt definierte Gegenmaßnahmen automatisch an.

–60 % MTTR

Mean Time to Respond um 60 % reduziert gegenüber manuellem Betrieb.

11 ANWENDUNGS-AUSBLICK · KOMPETENZAUFBAU

Drei Rollen für den Agenten-Betrieb im Mittelstand.

AI Agents brauchen keine Programmierer — sie brauchen Menschen mit klarer Verantwortung und dem richtigen Verständnis.

Prompt Engineer

Gestaltet die Kommunikation mit KI-Systemen. Definiert Kontext, Aufgaben und Grenzen des Agenten. Kein Coding nötig — aber tiefes Verständnis der Geschäftsprozesse.

EINSTIEG
1–3 MONATE

AI Owner

Trägt Verantwortung für einen oder mehrere KI-Agenten im Betrieb. Definiert Erfolgskriterien, überwacht Outputs, genehmigt Änderungen. Die Brücke zwischen Governance und Praxis.

GOVERNANCE-KERN
SOFORT BESETZEN

Agent Supervisor

Überwacht autonome Agenten-Aktionen operativ. Entscheidet über Human-in-the-Loop-Eingriffe, Eskalationen und Berechtigungsgrenzen. Kombination aus IT-Kompetenz und Prozesswissen.

BETRIEB & KONTROLLE
AB PRODUKTIVGANG

Von Chatbot zu Agent — das Stufenmodell

Die meisten Unternehmen starten mit Chatbots — einfache Frage-Antwort-Systeme ohne eigene Entscheidungsfähigkeit. AI Agents sind fundamental anders:

- **Autonomie:** Ein Agent plant Zwischenschritte, ruft Tools auf und entscheidet, wann eine Aufgabe abgeschlossen ist.
- **Werkzeuge:** Agenten können Systeme aufrufen — ERP, CRM, Kalender, E-Mail, APIs — nicht nur antworten.
- **Entscheidungsschleifen:** Ein Agent überprüft sein eigenes Ergebnis und korrigiert es bei Bedarf.
- **Governance-Anforderung:** Je mehr Autonomie, desto wichtiger werden Berechtigungen, Audit-Trail und Human-in-the-Loop.

AI Governance braucht gemeinsames Verständnis — auf allen Führungsebenen.

Die Checkliste zeigt, wo die Lücken sind. PiGentic schließt sie — in drei Tagen, mit C-Level und IT-Leitung im selben Raum, herstellerunabhängig.

1 **Checkliste auswerten** — Ihren Status haben Sie gerade bestimmt (Seite 10).

2 **Kostenloses Readiness-Assessment** — 30 Min. Gespräch, konkrete Lücken priorisiert.

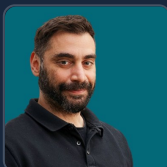
3 **Executive-Schulung** — 3×1 Tag, C-Level & IT, herstellerunabhängig.

Kostenloses Assessment anfragen · pigentic.de ›

Vorab-Interview kostenfrei · Antwort innerhalb 24 h · Inhouse, Online oder Offenes Seminar

WAS PIGENTIC KONKRET LIEFERT

Modulare Executive-Trainings (3×1 Tag), AI Agent Readiness-Assessment, Use-Case-Mapping. Wir befähigen Ihre Führung und IT — die Agenten-Implementierung erfolgt durch Ihre IT oder Implementierungspartner. Vendor-unabhängig, ohne Tool-Provision.



Pierre Carlo Motzo · Gründer PiGentic

20+ Jahre Enterprise-IT, ehem. Interim-CISO in deutschen Großkonzernen. Praxiserfahrung aus NIS2-, DORA- und ISO-27001-Audits.

πGentic

pigentic.de · info@pigentic.de