HANISCH

KI-STRATEGIE & SICHERHEITSQUALITÄT

JHGS-i3 METHODOLOGY

Praxisleitfaden

# KI-Chancen nutzen. Regulatorik beherrschen. Zukunft gestalten.

Systemische KI-Compliance & Infrastruktur-Härtung für den Mittelstand

Copyright © 2026 Hanisch KI-Strategie und Sicherheitsqualität™. Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung der Urheberin darf dieses Dokument weder ganz noch teilweise vervielfältigt oder weitergegeben werden.

INHALTSVERZEICHNIS


| | |
|---|---|
| EXECUTIVE SUMMARY (Management Summary)<br>IN 3 SCHRITTEN ZU IHREM DIGITALEN VORSPRUNG | 03 |
| | |
| 01. EINLEITUNG & PROBLEMSTELLUNG: DAS COMPLIANCE-PARADOXON IM MITTELSTAND | 04 |
| | |
| 02. HINTERGRUND / URSACHEN: DIE REALEN RISIKEN FÜR INHABERGEFÜHRTE BETRIEBE | 06 |
| | |
| 03. LÖSUNGSANSATZ / METHODIK: DAS INTEROPERABLE i3-FRAMEWORK ALS SOUVERÄNES SCHUTZSCHILD FÜR DEN MITTELSTAND | 08 |
| | |
| 04. EVIDENZ & BEST PRACTICES: DER INDUSTRIELLE DMAIC-ZYKLUS IN DER KMU-PRAXIS | 10 |
| | |
| 05. 5. FAZIT & AUSBLICK: DER WEG ZUR SOUVERÄNEN KI-STRUKTUR | 12 |
| | |




Copyright © 2026 Hanisch KI-Strategie und Sicherheitsqualität™. Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung der Urheberin darf dieses Dokument weder ganz noch teilweise vervielfältigt oder weitergegeben werden.

## EXECUTIVE SUMMARY (Management Summary)
## IN 3 SCHRITTEN ZU IHREM DIGITALEN VORSPRUNG

Mittelständische Unternehmen stehen heute vor einer anspruchsvollen, aber auch zukunftsweisenden Aufgabe: Auf der einen Seite bietet der strategische Einsatz von Künstlicher Intelligenz eine **fundamentale Chance**, Prozesse nachhaltig zu optimieren, Kosten zu senken und die eigene Belegschaft spürbar von Routineaufgaben zu entlasten. KI ist längst kein reines Werkzeug mehr, sondern der entscheidende Wettbewerbsvorteil. Richtig integriert, fängt sie den wachsenden Fachkräftemangel effektiv ab, verkürzt Reaktionszeiten in der Kundenkommunikation drastisch und liefert datenbasierte Entscheidungsvorlagen in Echtzeit. Sie ermöglicht es KMUs, die eigene Wertschöpfung zu skalieren, ohne gleichzeitig die operativen Fixkosten linear in die Höhe zu treiben – genau das, was die Wirtschaft jetzt fordert und braucht.

Auf der anderen Seite gilt es, den Blick für die technologische Sicherheit und die rechtlichen Spielregeln zu schärfen. Neue europäische Rahmenbedingungen wie der EU AI Act, die NIS-2-Richtlinie und der Cyber Resilience Act fordern von der Führungsebene klare, zukunftssichere Entscheidungen. Dabei sind zentrale Vorgaben – wie die gesetzliche Pflicht zur KI-Kompetenz der Mitarbeiter nach Artikel 4 des EU AI Acts – bereits seit **Februar 2025** voll aktiv, während im **August 2026** die nächsten umfassenden Governance-Pflichten bindend werden.

Die oberste Priorität für Unternehmer liegt daher auf dem konsequenten Schutz des eigenen, über Jahrzehnte aufgebauten Know-hows. Wer moderne KI-Anwendungen im Betrieb implementiert, möchte zu jedem Zeitpunkt die absolute Kontrolle über sensible Firmendaten, Quellcodes und Kundeninformationen behalten.

Dieser Praxisleitfaden zeigt auf, wie Cybersicherheit und KI-Management nicht als bürokratische Hürde zu betrachten sind, sondern als aktiver, strategischer Standortvorteil genutzt werden können. Es gibt technologisch souveräne Alternativen in der Praxis: Durch den gezielten Einsatz von datenschutzkonformen, europäischen Open-Source-Modellen und unabhängigen, selbstgehosteten Automatisierungs-Plattformen verbleiben alle Datenströme physisch und rechtlich genau dort, wo sie hingehören – auf den eigenen Serverstrukturen, vollständig in der Hand des Inhabers.

**Das Beste für die Ressourcen:** Dieser Leitfaden beschreibt einen Weg, der sich ohne monatelange Blockade der Kernmannschaft begleitend im Hintergrund umsetzen lässt. Indem operative Geschäftsprozesse methodisch analysiert, wertschöpfende Use Cases gemeinsam mit den Mitarbeitern identifiziert und die organisatorischen Schutzkonzepte der Infrastruktur gezielt auf cyber-technische Risiken ausgerichtet werden, entsteht eine sichere, vollkommen regelkonforme Basis, die von Dauer ist – und das Unternehmen jederzeit optimal auf zukünftige externe Audits vorbereitet.



Copyright © 2026 Hanisch KI-Strategie und Sicherheitsqualität™. Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung der Urheberin darf dieses Dokument weder ganz noch teilweise vervielfältigt oder weitergegeben werden.

## 1. EINLEITUNG & PROBLEMSTELLUNG:
## DAS COMPLIANCE-PARADOXON IM MITTELSTAND

Die wirtschaftliche Landschaft steht vor einer wegweisenden Transformation. Der gezielte Einsatz von Künstlicher Intelligenz (KI) ist für kleine und mittelständische Unternehmen (KMU) eine **fundamentale Chance**, um sich einen dauerhaften digitalen Vorsprung zu sichern, administrative Prozesse drastisch zu vereinfachen und dem wachsenden Fachkräftemangel proaktiv zu begegnen. Ob es um automatisierte Abläufe in der Verwaltung, intelligente Assistenzsysteme oder die effiziente Aufbereitung von Daten geht – KI entlastet die Kernmannschaft spürbar von zeitraubenden Routineaufgaben und schafft den nötigen Freiraum für echte Wertschöpfung.

In der alltäglichen Praxis vieler etablierter, oft inhabergeführter Betriebe herrscht beim Thema Künstliche Intelligenz jedoch eine völlig verständliche Skepsis. Da die Technologie in den Medien oft hochgradig abstrakt oder rein theoretisch dargestellt wird, bleibt der reale Nutzen für das eigene Gewerbe häufig unsichtbar. Es entsteht in vielen Führungsetagen das Gefühl, technologisch nicht mehr Schritt halten zu können oder dass KI schlichtweg unvereinbar mit der eigenen, über Jahrzehnte erfolgreich aufgebauten Betriebswelt ist.

Dabei liegen die echten Hebel moderner Anwendungen keineswegs im Ersetzen von bewährtem Handwerk oder etablierten Produktionsprozessen, sondern in der konsequenten Befreiung vom täglichen administrativen Ballast:

- **Effizienz im Büroalltag:** Das Verfassen von zähen Kunden-E-Mails, das Formulieren von Angeboten oder das Zusammenfassen komplexer Lieferantenbestimmungen lässt sich auf einfache, sprachliche Anweisung fehlerfrei beschleunigen. Der zeitfressende Dokumentenaufwand nach Feierabend schrumpft für den Inhaber auf ein absolutes Minimum.
- **Sicherung von Betriebswissen:** Wertvolle Erfahrungswerte, alte Projektberichte und interne Richtlinien werden über einfache Fragen sofort für das gesamte Team abrufbar – ganz ohne das zeitaufwendige Suchen in analogen Ordnerstrukturen oder verstreuten Netzlaufwerken.

Parallel zu diesen wirtschaftlichen Entlastungsmöglichkeiten entfaltet sich jedoch ein neuer rechtlicher Rahmen in Europa, der von der Führungsebene klare Weitsicht verlangt. Der **EU AI Act** hat die Einführung von KI-Tools schlagartig aus der reinen Testphase in den Fokus der geschäftskritischen Verantwortung gerückt. Viele Inhaber und Geschäftsführer stehen nun vor der großen Herausforderung, diese komplexen Vorgaben ohne eigene Compliance-Abteilung fehlerfrei im laufenden Betrieb umzusetzen.



Copyright © 2026 Hanisch KI-Strategie und Sicherheitsqualität™. Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung der Urheberin darf dieses Dokument weder ganz noch teilweise vervielfältigt oder weitergegeben werden.

**Die gesetzlichen Fristen sind bereits voll im Gang und dulden keinen Aufschub mehr:**

- **Die Pflicht zur KI-Kompetenz (Artikel 4 EU AI Act):** Bereits seit **Februar 2025** schreibt der Gesetzgeber zwingend vor, dass Unternehmen konkrete Maßnahmen ergreifen müssen, um die KI-Kompetenz ihrer Mitarbeiter und Führungskräfte sicherzustellen. Wer Systeme im Betrieb bereitstellt oder nutzt, muss gewährleisten, dass das Personal über das notwendige Wissen zur sicheren Anwendung und prozessualen Risikobewertung verfügt.
- **Bereits aktive Verbote:** Seit **August 2025** sind bestimmte, als inakzeptabel eingestufte KI-Praktiken zum Schutz der Grundrechte strengstens untersagt und strafbewehrt.
- **Der Stichtag im August 2026:** In diesem Spätsommer greift die nächste, entscheidende Stufe des Gesetzes. Die strengen Governance- und Transparenzpflichten für eine Vielzahl von KI-Anwendungen werden bindend. Wer ab diesem Zeitpunkt keine dokumentierten Prozesse vorweisen kann, riskiert nicht nur empfindliche rechtliche Konsequenzen, sondern auch den plötzlichen Ausschluss aus der digitalen Lieferkette. Größere Partner und Konzerne sind im Rahmen von **NIS-2** und dem **Cyber Resilience Act (CRA)** künftig gesetzlich dazu verpflichtet, die IT-Sicherheit und Compliance ihrer Zulieferer zunehmend strenger zu prüfen.

Aus dieser Gemengelage entsteht das **Compliance-Paradoxon des Mittelstands**: Geschäftsführer wollen und sollten die immensen Effizienzgewinne zur bürokratischen Entlastung nutzen, sorgen sich jedoch vor rechtlichen Fallstricken und organisatorischen Fehlern. Die Angst vor dem Unbekannten führt oft zu einer lähmenden Blockadehaltung, während im Hintergrund durch die unkontrollierte Nutzung freier Online-Tools längst eine ungeschützte und hochriskante „Schatten-KI“ im Betrieb Einzug hält.



Copyright © 2026 Hanisch KI-Strategie und Sicherheitsqualität™. Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung der Urheberin darf dieses Dokument weder ganz noch teilweise vervielfältigt oder weitergegeben werden.

## 2. HINTERGRUND / URSACHEN:
## DIE REALEN RISIKEN FÜR INHABERGEFÜHRTE BETRIEBE

Für eine sichere, regelkonforme KI-Struktur müssen die realen Ursachen der aktuellen Unsicherheiten im Mittelstand analysiert werden. Viele Betriebe stehen an einer Weggabelung: Sie spüren den Veränderungsdruck, sehen aber oft noch nicht, was sich durch Technologie in ihren Abläufen optimieren lässt – und welche verdeckten Risiken entstehen.Die unsichtbare Hürde: „Was soll KI überhaupt in meinem Betrieb?“

In der täglichen Praxis herrscht oft eine verständliche Skepsis: Da die Technologie meist abstrakt dargestellt wird, bleibt der reale Nutzen unsichtbar. Es entsteht das Gefühl, technologisch nicht mehr Schritt halten zu können oder dass KI schlichtweg unvereinbar mit der eigenen, etablierten Betriebswelt ist.

Das Problem liegt darin, dass KI fälschlicherweise oft mit Science-Fiction verwechselt wird. Dabei geht es in der Realität eines KMUs um viel greifbarere, alltägliche Sorgen, die jeder Betriebsinhaber kennt: Den lästigen Papierkram nach Feierabend. Wer den bürokratischen Aufwand im Hintergrund einmal sauber organisieren lässt, gewinnt genau die Freiheit zurück, sich wieder auf das zu konzentrieren, was man über Jahrzehnte gelernt und aufgebaut hat.

**Das Souveränitäts-Problem: Wo landen die Betriebsgeheimnisse?**

Die gängigsten, leicht zugänglichen KI-Anwendungen im Internet basieren fast ausnahmslos auf Systemen, deren Server im außereuropäischen Ausland stehen. Für ein mittelständisches Unternehmen entsteht hier ein unbemerktes und kritisches Einfallstor:

- **Abfluss von Firmen-Know-how (IP-Drain):** Werden interne Kalkulationen, sensible Kundenkorrespondenzen, vertrauliche Verträge oder gar Quellcodes und Rezepturen unüberlegt in standardmäßige Online-Masken eingegeben, verlassen diese Daten den Schutzraum des Unternehmens. Sie werden von den Betreibern oft dauerhaft gespeichert und zum Training der globalen Modelle verwendet.
- **Der fundamentale DSGVO-Konflikt:** Sobald personenbezogene Daten von Kunden, Lieferanten oder Mitarbeitern das europäische Datenschutzrecht verlassen, steht der Betrieb unbeabsichtigt im Compliance-Verstoß.

Die Lösung für den Mittelstand liegt daher nicht im Verzicht auf moderne Tools, sondern im Erhalt der **technologischen Souveränität**. Die Prozesse müssen von vornherein so konzipiert sein, dass die Datenhoheit physisch und rechtlich klar in der Hand des Inhabers verbleibt.

**Die verdeckte Gefahr: Schatten-IT und die unkontrollierte Schatten-KI**

- Während die Führungsebene noch über Budgets diskutiert, hat die operative Realität die Planung längst überholt. Mitarbeiter im Mittelstand sind pragmatisch: Bei



Copyright © 2026 Hanisch KI-Strategie und Sicherheitsqualität™. Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung der Urheberin darf dieses Dokument weder ganz noch teilweise vervielfältigt oder weitergegeben werden.

zeitaufwendigen Aufgaben suchen sie nach schnellen Lösungen. Daraus entsteht eine der am meisten unterschätzten Sicherheitslücken:
**Die Schatten-KI.**

- **Der blinde Fleck der Geschäftsführung:** Aus Frust über umständliche interne Prozesse oder mangelnde Werkzeuge weichen Mitarbeiter eigenmächtig auf frei zugängliche, öffentliche Online-KI-Tools aus. Da diese Dienste meist ohne Anmeldung oder über private Accounts genutzt werden können, tauchen sie in keinem IT-Protokoll des Unternehmens auf.
- **Systemischer Abfluss durch Belegschafts-Pragmatismus:** Ohne böse Absicht, sondern rein um „schnell die Arbeit zu erledigen", werden sensible interne Daten in diese Systeme kopiert – wie vertrauliche Kundenlisten zur Formatierung oder interne Kalkulationen zur Überprüfung.
- **Das Kontroll-Vakuum:** Da diese Daten auf Servern in Drittstaaten landen, verliert das Unternehmen die faktische Hoheit über sein geistiges Eigentum, während die Geschäftsführung im Ernstfall die organisatorische Haftung trägt.

**Organisatorische Schutzlücken erkennen (Die Governance-Perspektive)**

Ein häufiger Irrglaube in kleineren Betrieben ist, dass der bestehende IT-Dienstleister oder eine einfache Firewall das Thema KI-Sicherheit automatisch miterledigen. Klassische IT-Sicherheit schützt die Leitungen und sperrt unbefugte Zugriffswerkzeuge. KI-Sicherheit nach modernen Standards setzt jedoch auf einer ganz anderen Ebene an – der **organisatorischen Governance**:

- **Fehlende Richtlinien zur KI-Kompetenz:** Ohne klare, einfache Schulungen und Vorgaben gemäß Artikel 4 des AI Acts wissen Mitarbeiter schlichtweg nicht, welche Daten sie in eine KI eingegeben dürfen und wie die Systeme sicher bedient werden. Ein reines Verbot führt in der Praxis nur dazu, dass die Schatten-KI noch tiefer in den verdeckten Bereich rutscht.
- **Das Risiko der Schnittstellen:** Wenn Systeme automatisiert Daten austauschen, müssen die logischen und organisatorischen Übergänge so konzipiert sein, dass das Risiko für einen unkontrollierten Datenabfluss nach außen minimiert wird.

Ein strukturiertes Framework schließt diese Lücken im Hintergrund. Es sorgt dafür, dass die Belegschaft agil mit der Technologie arbeitet, während die Geschäftsführung die Gewissheit hat, dass gesetzliche Fristen eingehalten werden und sensible Daten im eigenen Haus verbleiben.



Copyright © 2026 Hanisch KI-Strategie und Sicherheitsqualität™. Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung der Urheberin darf dieses Dokument weder ganz noch teilweise vervielfältigt oder weitergegeben werden.

## 3. LÖSUNGSANSATZ / METHODIK:
## DAS INTEROPERABLE i3-FRAMEWORK ALS SOUVERÄNES SCHUTZSCHILD FÜR DEN MITTELSTAND

Für kleine und mittlere Unternehmen ist es operativ nicht leistbar, isolierte Einzellösungen für jedes neue Gesetz aufzubauen. Die Antwort für eine ressourcenschonende und regelkonforme Umsetzung ist das i3-Framework. Es verzahnt gesetzliche Leitplanken, Informationssicherheit und reale Wertschöpfung über drei strategische Säulen miteinander:

***Säule 1 (Intelligence): Strategische KI-Governance & Use-Case-Validierung***

Die erste Säule bildet das prozessuale und regulatorische Fundament. KI-Management im Mittelstand darf nicht bedeuten, fertige Software blind in bestehende Strukturen zu werfen. Der Ansatz setzt direkt an der vorhandenen Prozesslandschaft des KMUs an:

- **Praxisorientierte Use-Case-Identifikation:** Gemeinsam mit der Geschäftsführung und im direkten Dialog mit der Belegschaft wird ermittelt, wo zeitintensive Routinen liegen, welche administrativen Engpässe die Mitarbeiter blockieren und an welchen Stellen der Einsatz von KI einen klaren wirtschaftlichen Nutzen verspricht.
- **Strukturierte Anforderungsanalyse:** Es wird definiert, was das System im Kontext des Unternehmens leisten muss, um eine echte Entlastung im Alltag zu ermöglichen.
- **Regulatorische Einordnung: Regulatorische Einordnung:** Jede geplante Anwendung wird frühzeitig nach den Kriterien des EU AI Acts klassifiziert. Durch diese strategische Governance werden Haftungsrisiken für die Unternehmensführung proaktiv minimiert. Die Konzeption orientiert sich dabei an internationalen Best Practices und Standards (wie der ISO/IEC 42001 für KI-Managementsysteme), um das Unternehmen optimal auf zukünftige Audits vorzubereiten.
- ***Säule 2 (Integrity): Validierte IT- & KI-Sicherheitsqualität (Infrastruktur-Härtung)***

Die zweite Säule dient dem Schutz des über Jahre aufgebauten Know-hows und des geistigen Eigentums nach außen. Da KMUs oft als geschätzte Zulieferer in globalen Lieferketten agieren, ist der Nachweis von Datenintegrität ein harter Wettbewerbsfaktor. Hierbei müssen zwei Ebenen der Informationssicherheit lückenlos ineinandergreifen:

**Ebene A: Die klassische Cybersecurity-Basis (Infrastruktur-Schutz)**

Die Einführung neuer digitaler Anwendungen erfordert eine strukturierte Begleitung auf Ebene der Informationssicherheit. Die bestehende IT-Infrastruktur muss systematisch analysiert werden, um sicherzustellen, dass durch die neuen Datenflüsse keine Schwachstellen im Unternehmensnetzwerk entstehen. Die Definition klarer, organisatorischer



Copyright © 2026 Hanisch KI-Strategie und Sicherheitsqualität™. Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung der Urheberin darf dieses Dokument weder ganz noch teilweise vervielfältigt oder weitergegeben werden.

Sicherheitsvorgaben zielt darauf ab, traditionelle Einfallstore zu minimieren und die allgemeine Cyber-Resilienz zu stärken.

**Ebene B: Die neuen KI-spezifischen Risikofaktoren (Der blinde Fleck)**

Im Gegensatz zu klassischer Software verarbeiten KI-Modelle natürliche Sprache und interagieren dynamisch mit Daten. Hieraus entstehen neuartige Risiken, die von herkömmlichen Sicherheitsmechanismen (wie einfachen Firewalls) nicht erfasst werden:

- **Sicherheitsrisiko „Schatten-KI“:** Nutzen Mitarbeiter unkontrolliert freie Online-Tools für den Arbeitsalltag, werden oft sensible Unternehmensdaten, interne Kalkulationen oder Kundendaten unwissentlich an Server im Ausland übertragen.
- **Schnittstellen als Datenbrücke:** Wenn KI-Systeme über Programmierschnittstellen (APIs) an interne Datenbanken angebunden werden, können schlecht konfigurierte Berechtigungen dazu führen, dass tiefergehende Systembereiche unfreiwillig offengelegt werden.
- **Systemische Manipulation:** Ohne klare Schutzvorgaben an den semantischen Schnittstellen besteht das Risiko, dass Systeme durch gezielte, fehlerhafte Eingaben manipuliert werden, um geschützte Datenstrukturen auszulesen.

*Der Schutz vor Datenexfiltration und eine vorausschauende Schnittstellen-Governance im Rahmen des Cyber Resilience Acts (CRA) unterstützen die Härtung des gesamten Betriebssystems und sichern die Schnittstellen zu Kunden und Partnern nachweisbar ab.*

***Säule 3 (Infrastructure): Technologische Souveränität & Autarke Prozesse***

Diese Säule realisiert die digitale Unabhängigkeit des KMUs bei voller Interoperabilität im Markt.

- **Der souveräne Eigenbetrieb (Self-Hosting):** Datenschutzkonforme, europäische Open-Source-Modelle werden lokal oder in privaten, DSGVO-konformen Clouds betrieben, um die Abhängigkeit von Drittstaaten-Anbietern zu vermeiden.
- **Unabhängige Prozess-Automatisierung:** Die Verknüpfung der internen Systeme erfolgt über selbstgehostete, unabhängige Automatisierungs-Plattformen. Alle Datenströme fließen physisch kontrollierbar und verbleiben klar im eigenen Haus, während die Anbindungsfähigkeit an bestehende ERP- oder CRM-Systeme erhalten bleibt.
- **Organisatorisches Sicherheits-Alignment:** Die technische Struktur wird konzeptionell in ein robustes Informationssicherheits-Managementsystem eingebettet, das sich an bewährten Standards (wie der ISO/IEC 27001) orientiert. Damit erfüllt das KMU gleichzeitig wesentliche Kriterien zur Absicherung digitaler Lieferketten nach NIS-2.



Copyright © 2026 Hanisch KI-Strategie und Sicherheitsqualität™. Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung der Urheberin darf dieses Dokument weder ganz noch teilweise vervielfältigt oder weitergegeben werden.

## 04. EVIDENZ & BEST PRACTICES:
## DER INDUSTRIELLE DMAIC-ZYKLUS IN DER KMU-PRAXIS

Die größte Sorge im Mittelstand gilt dem internen Ressourcenaufwand. KMUs können es sich nicht leisten, Kernmitarbeiter über Monate für IT-Projekte abzustellen. Für eine schlanke Umsetzung wird der gesamte Prozess methodisch entlang des bewährten Lean Six Sigma DMAIC-Zyklus strukturiert.

**1. Define (Definieren)**

Im ersten Schritt werden die klaren operativen Ziele sowie die rechtlichen Rahmenbedingungen für das KMU abgesteckt.

- **Abgrenzung wertschöpfender Use Cases:** Anstatt Technologie blind zu streuen, werden spezifische Prozesse isoliert (z. B. administrative Entlastung im Büroalltag).
- **Aufklärung von „Schatten-KI“:** Es wird transparent erfasst, welche freien Online-Tools die Belegschaft nutzt, um Sicherheitsrisiken und unkontrollierten Datenabfluss zu lokalisieren.
- **Abstimmung der Compliance-Ziele:** Die gesetzlichen Anforderungen – wie die bereits aktive Pflicht zur KI-Kompetenz nach Artikel 4 des EU AI Acts – werden fest als Meilensteine verankert.

**2. Measure (Messen)**

Hier wird der aktuelle Ist-Zustand der betroffenen Prozesse und Datenflüsse sachlich erfasst.

- **Dokumentation der Datenströme:** Welche Informationen fließen in den Prozessen? Wo handelt es sich um reine Maschinendaten, wo um sensibles geschäftliches Know-how (Rezepturen, Kalkulationen) und wo um personenbezogene Daten nach DSGVO?
- **Systemlandschaft analysieren:** Es wird ermittelt, welche bestehenden ERP-, CRM- oder lokalen Serversysteme für eine spätere, unabhängige Verknüpfung in Frage kommen.

**3. Analyze (Analysieren)**

Die Analysephase dient der Identifikation von organisatorischen Schwachstellen und regulatorischen Risiken.

- **Risikoklassifizierung:** Die Anwendungen werden den Stufen des EU AI Acts zugeordnet, um Überregulierung zu vermeiden und nur das rechtlich Notwendige umzusetzen.



Copyright © 2026 Hanisch KI-Strategie und Sicherheitsqualität™. Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung der Urheberin darf dieses Dokument weder ganz noch teilweise vervielfältigt oder weitergegeben werden.

- **Schnittstellen-Bewertung:** Die logischen Datenübergänge werden geprüft, um den unkontrollierten Abfluss von Betriebsgeheimnissen zu stoppen.
- **Prozess-Flaschenhälse:** Es wird ermittelt, an welchen Stellen manuelle Medienbrüche den Betrieb Zeit kosten und durch den Einsatz lokaler, souveräner Automatisierungen beschleunigt werden können.

**4. Improve (Verbessern)**

In dieser Phase erfolgt die tatsächliche Umsetzung der technologisch souveränen und regelkonformen Struktur nach dem $i^3$-Framework.

- **Etablierung der KI-Governance: Etablierung der KI-Governance:** Es werden einfache Richtlinien für die Belegschaft ausgerollt und Schulungen zur Erfüllung der KI-Kompetenzpflicht implementiert. Die Governance-Strukturen orientieren sich dabei systematisch am globalen Standard der ISO/IEC 42001 für KI-Managementsysteme.
- **Konzeption der souveränen Infrastruktur:** Der Übergang von unsicheren Drittstaaten-Systemen hin zu lokal betriebenen, europäischen Open-Source-Modellen und unabhängigen Automatisierungs-Plattformen auf den eigenen Serverstrukturen wird strukturiert. Die Datenhoheit verbleibt damit physisch und rechtlich klar in der Hand des Inhabers.
- **Organisatorisches Sicherheits-Alignment:** Die organisatorischen Leitplanken werden so gesetzt, dass die Prozesse konform zu bewährten Standards (wie der ISO 27001) aufgesetzt sind und die Anforderungen zur Absicherung digitaler Lieferketten nach NIS-2 und CRA berücksichtigen.

**5. Control (Steuern & Überwachen)**

Der letzte Schritt sorgt dafür, dass die neu gewonnenen Effizienz- und Sicherheitsstandards dauerhaft im KMU verankert bleiben.

- **Einführung von Qualitätsmetriken:** Einfache Kontrollmechanismen überwachen fortlaufend die Stabilität der automatisierten Prozesse und die Einhaltung der Datenschutzvorgaben im Alltag.
- **Herstellung der „Audit-Readiness“:** Dokumente, Risikoanalysen und Schulungsnachweise werden so strukturiert abgelegt, dass das Unternehmen optimal auf Compliance-Anfragen von Großkunden vorbereitet ist und die Anforderungen für spätere Zertifizierungen nach ISO/IEC 42001 oder ISO 27001 erfüllt.

*Praxis-Ergebnis:* Durch die konsequente Anwendung des DMAIC-Zyklus wird sichergestellt, dass das KI-Management im Mittelstand kein theoretisches Papiermonster bleibt. Es entsteht eine schlanke, transparente Struktur, die Haftungsrisiken für die Geschäftsführung minimiert und gleichzeitig den administrativen Ballast im Betrieb spürbar senkt.



Copyright © 2026 Hanisch KI-Strategie und Sicherheitsqualität™. Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung der Urheberin darf dieses Dokument weder ganz noch teilweise vervielfältigt oder weitergegeben werden.

## 5. FAZIT & AUSBLICK:
## DER WEG ZUR SOUVERÄNEN KI-STRUKTUR

Die KI-Transformation im Mittelstand ist gelebte Realität. Unternehmen, die jetzt handeln, sichern sich einen messbaren operativen Vorsprung durch die Entlastung von administrativen Routinen und schützen zeitgleich ihr wertvolles Betriebs-Know-how.

Der EU AI Act, die NIS-2-Richtlinie und der Cyber Resilience Act setzen klare gesetzliche Fristen. Pauschale Verbote oder oberflächliche IT-Tools greifen zu kurz – sie forcieren meist nur eine riskante „Schatten-KI". Der Schlüssel zum Erfolg liegt in technologischer Souveränität und klarer Governance: Durch die Kombination aus europäischen Open-Source-Modellen, lokal gehosteten Automatisierungen und dem DMAIC-Prozess bleiben alle Daten unter der physischen Kontrolle des Inhabers. So wird regulatorische Compliance zum echten strategischen Standortvorteil.

### IHRE NÄCHSTEN SCHRITTE: DIE ERSTBEWERTUNG

Jedes Unternehmen bringt eine eigene Prozesslandschaft mit. In einem unverbindlichen Erstgespräch analysieren wir Ihre spezifischen Herausforderungen, identifizieren Potenziale für administrative Entlastungen und skizzieren Ihre regulatorischen Meilensteine.

Sichern Sie Ihren digitalen Vorsprung und treffen Sie proaktiv Vorsorge.

**Digitaler Leser:** Klicken Sie einfach auf den folgenden Link, um direkt zu unserem Online-Kalender auf der Website zu gelangen:

**➔ Hier direkt Ihren Wunschtermin für das 30-minütige Erstgespräch buchen**

**Print-Leser:** Scannen Sie einfach den untenstehenden QR-Code mit Ihrem Smartphone, um direkt mobil auf unserer Kontaktseite Ihren Wunschtermin auszuwählen.



**Impressum gemäß § 5 DDG:** Hanisch KI-Strategie und Sicherheitsqualität | Inhaberin: Julia Hanisch | Altvaterstr. 27, 71032 Böblingen | E-Mail: office@jhqs-i3.de