Guiding Leaders Through the Storm: Der AI-Orchestrator Leader 2026–2030

Executive Summary

Diese Analyse (Stand: 2026-02-12, Zeitzone Europa/Wien) argumentiert, dass die zentrale Führungsrolle der Jahre 2026–2030 weniger „KI-Expert*in“ im engen Sinn ist, sondern ein AI-Orchestrator Leader: eine Führungskraft, die KI-Fähigkeiten, Daten, Sicherheit, Regulierung, Talent und Partner-Ökosysteme so koordiniert, dass Entscheidungs- und Ausführungszyklen schneller werden – ohne Compliance-, Sicherheits- und Vertrauensschäden zu verursachen. Der entscheidende Punkt ist Orchestrierung: KI wird nicht „eingeführt“, sondern dauerhaft als Produktionssystem* mit Governance, Monitoring und Krisenfähigkeit betrieben. [1]

Der regulatorische und geopolitische Kontext 2026–2030 ist „sturm-typisch“: Das World Economic Forum[2] beschreibt 2026 als ein Umfeld, in dem **Unsicherheit** prägend ist; zudem werden **geoökonomische Konfrontation** und **staatlich getriebene Konflikte** als besonders krisenauslösende Risiken im kurzfristigen Horizont hervorgehoben. [3] Diese Makrolage übersetzt sich operativ in: fragmentierte Lieferketten, Sanktionen/Exportkontrollen, Datenlokalität, Cyber- und Desinformationsdruck sowie höhere Energie- und Kapitalkosten.

Parallel verschärfen sich **Pflichten und Reifeanforderungen** durch EU-Rechtsakte, die bis 2026/2027 in die volle Wirkung laufen: Der EU-AI-Act gilt ab **2. August 2026**, einzelne Kapitel früher (u. a. ab **2. Februar 2025** für grundlegende Bestimmungen inkl. KI-Kompetenz/„AI literacy“, ab **2. August 2025** u. a. für Teile der Governance-/GPAI-Regeln). [4] Für digitale Resilienz im Finanzsektor gilt Europäische Union[5] DORA[6] seit **17. Januar 2025**. [7] Die NIS2[8]-Richtlinie verlangt nationale Umsetzung bis **17. Oktober 2024** (Anwendung ab 18. Oktober 2024); in Deutschland[9] wurde ein Umsetzungsgesetz im Bundesgesetzblatt[10] am 6. Dezember 2025 verkündet (BGBl. I). [11] Der Data Act gilt ab **12. September 2025** (mit gestaffelten Pflichten u. a. 2026/2027). [12] Der Cyber Resilience Act greift gestaffelt ab **11. Juni 2026** (Kapitel IV), ab **11. September 2026** (Art. 14), und voll ab **11. Dezember 2027**. [13] Für den Gesundheitsdatenraum (EHDS) beginnt die Anwendung ab **26. März 2027** (weitere Teile später, z. B. 2029/2031). [14]

Technologisch werden 2026–2030 **Energie- und Rechenkapazität** zu einem strategischen Engpass. Die International Energy Agency[15] schätzt für 2024 den Stromverbrauch von Rechenzentren auf rund **415 TWh** (≈1,5% der globalen Stromnachfrage) und projiziert im Basisszenario bis 2030 eine **Verdopplung** auf **~945 TWh**; KI-getriebene „accelerated servers“ tragen wesentlich zum Zuwachs bei. [16]

Für die fünf betrachteten Domänen ergeben sich robuste Leitplanken, die unabhängig vom Szenario tragen:

1. **Business:** KI-Wert entsteht dort, wo Prozesse Ende-zu-Ende neu geschnitten werden (Decision Intelligence + Automatisierung), nicht durch Tool-Piloten im Silo. [17]
2. **Geopolitik:** Der Engpass ist weniger Technik als **Vertrauen, Datenqualität, Resilienz** und die Fähigkeit, KI gegen missbräuchliche Nutzung (Cyber, FIMI/Desinformation) zu „härten". [18]
3. **Leben:** „Persönliche KI" wird nur dann ein Stabilitätsfaktor, wenn Datenschutz, Manipulationsrisiken und Kompetenzaufbau (AI literacy) adressiert sind. [19]
4. **Wealth:** Digitale operative Resilienz (DORA), Modellrisikomanagement und Transparenz sind 2026–2030 nicht optional; KI-Nutzen ohne robuste Kontrollen erhöht Tail-Risiken. [20]
5. **Industriegase:** Die größte Hebelwirkung liegt in Energie-/Anlagenoptimierung, Predictive Maintenance, Demand-/Network-Optimierung und Wasserstoff-Ökosystemen; die Unsicherheit im Wasserstoffhochlauf bleibt hoch (Projektverschiebungen, Kostenlücke). [21]

Begriff und Kernkompetenzen des AI-Orchestrator Leader

Der Begriff **AI-Orchestrator Leader** wird hier als **Führungsfunktion** (nicht zwingend als einzelne Stelle) definiert: Sie verantwortet die **End-to-End-Koordination** von (a) Strategie & Portfolio, (b) Daten- und Modell-Betrieb, (c) Governance/Compliance, (d) Cyber-Resilienz sowie (e) Change- und Krisenfähigkeit – über interne Einheiten und externe Partner hinweg.

Diese Definition ist kompatibel mit etablierten Governance-Rahmenwerken: - Der NIST[22]-Ansatz (AI RMF 1.0) beschreibt vier Kernfunktionen **GOVERN, MAP, MEASURE, MANAGE** als operatives „Betriebssystem" für KI-Risiken und Vertrauenswürdigkeit. [23]
- ISO[24] ISO/IEC 42001 spezifiziert ein AI-Management-System (AIMS) als strukturierte Management-System-Logik (u. a. PDCA), um verantwortliche Entwicklung und Nutzung zu steuern. [25]
- Der EU-AI-Act verlangt u. a. organisatorische Maßnahmen zur **KI-Kompetenz (AI literacy)** und – für Hochrisiko-KI – dokumentierte Risiko-, Daten- und Überwachungsprozesse. [26]

Kernkompetenzen als „Orchestrations-Stack"

Strategie- und Portfoliokompetenz - Werthebel identifizieren (Kosten, Qualität, Geschwindigkeit, Risikoabsenkung, neue Produkte). - KI-Portfolio als Multi-Horizon-Roadmap steuern (H1 Effizienz, H2 Entscheidungssysteme, H3 neue Geschäftsmodelle).

Daten- und KI-Systemkompetenz - Verständnis für Daten-/Modell-Lebenszyklus (Training, Evaluation, Deployment, Monitoring). - Architekturentscheidungen (Cloud/Edge, Lakehouse, Vektor-Suche/RAG, MLOps, Sicherheit) treffen und delegierbar machen. [27]

Governance- und Regulierungsfähigkeit - AI Act (Risk-Tiering, Hochrisiko-Pflichten), DORA/NIS2 (Resilienz), Data Act (Datenzugang/Portabilität), Cyber Resilience Act (Produkt-Security) in Policies und Kontrollen übersetzen. [28]

Cyber- und Missbrauchsresilienz - Schutz gegen Prompt-Injection, Datenexfiltration, Model/Training-Poisoning, Supply-Chain-Angriffe, Deepfake-Kampagnen, KI-basierte Betrugs-/Phishing-Skalierung. [29]

Führung, Change, Krisenfähigkeit - AI literacy-Programme, Rollenumbau, Betriebsrats-/Stakeholder-Einbindung, und etablierte Krisenkommunikation (siehe Template-Abschnitt). [30]

Rollenbild in einem Satz

Der AI-Orchestrator Leader macht aus KI-Initiativen ein **messbar gesteuertes, regulatorisch robustes, energie- und cyberresilientes Produktionssystem**, das in Business, Geopolitik, Leben, Wealth und Industriegasen unterschiedliche Ziele verfolgt – aber nach derselben Orchestrationslogik betrieben wird. [1]

Strategische Frameworks und Technologie-Stack für AI-Orchestration

Ein Referenz-Framework: OODA-Plus für KI-Zeitalter

Für 2026–2030 ist der wichtigste strategische Shift: **Entscheidungen werden zum Produkt**. AI-Orchestration zielt darauf, den Zyklus *Observe* → *Orient* → *Decide* → *Act* (OODA) zu industrialisieren:

1. **Observe:** Daten & Signale (IoT, Märkte, Lieferketten, OSINT, Kunden, Anlagen).
2. **Orient:** Modelle + Wissensgraph/RAG + Szenarien.
3. **Decide:** Entscheidungslogik (Policy, Constraints, Human-in-the-Loop).
4. **Act:** Automatisierte Workflows (IT/OT, ERP, Trading-Ops, Kommunikation).
5. **Learn:** Monitoring, Incident-Learning, Drift-Kontrolle, Audit-Trail.

Der AI-Orchestrator Leader verantwortet dabei explizit die **GOVERN-Funktion** im Sinn des NIST AI RMF: Governance muss dauerhaft gelten, nicht nur „vor Go-Live“. [23]

Vergleich zentraler Governance- und Steuerungsrahmenwerke

Rahmenwerk	Primärziel	Stärken für 2026–2030	Typische Artefakte, die der AI-Orchestrator braucht
NIST AI RMF 1.0 (GOVERN/MAP/MEASURE/MANAGE)	Praktisches KI-Risikomanagement	Funktionsorientiert, organisations- und use-case-agnosti	AI Risk Register, Mess-/Monitoring-Katalog,

Rahmenwerk	Primärziel	Stärken für 2026–2030	Typische Artefakte, die der AI-Orchestrator braucht
		sch; stark für Operationalisierung	Control-Mapping, Playbooks [23]
ISO/IEC 42001 (AIMS)	Management-System für verantwortliche KI	Audit-/zertifizierungsnah; PDCA-Logik; Governance „als System“	Policy-Set, Rollen/RACI, Audit-Plan, Continual-Improvement-Loop [25]
EU-AI-Act	Rechtspflichten + Durchsetzung	Risk-Tiering; Hochrisiko-Pflichten (Risk Mgmt, Daten-Governance, Human Oversight, Cybersecurity)	Konformitäts-/Technische Doku, Logging, Post-Market Monitoring, AI-Literacy-Programm [31]
BSI-C5 (Cloud) als Sicherheitsanker	Mindestanforderungen für Cloud-Security + Nachweise	Praktisch für Beschaffung/Betrieb, prüfbar, „audit once – certify many“	C5-Berichte, Kontroll-Auswertung, korrespondierende Kontrollen beim Kunden [32]

Technologie-Stack 2026–2030 als „Minimum Viable AI-Factory“

Die Architektur muss gleichzeitig **skalierbar** und **auditierbar** sein (AI Act, DORA, NIS2, CRA). Die folgenden Bausteine sind in der Praxis (Domänen-übergreifend) das Minimum:

Daten-Schicht - Data Ingestion (Batch/Streaming), Datenqualitäts-Gates, Data Lineage. - Datenklassifizierung (personenbezogen/sensitiv/OT-kritisch), Data-Loss-Prevention. - „Data Contracts“ (v. a. relevant im Kontext Data Act-Portabilität und Lieferanten-/Geräte-Daten). [12]

Modell- und Applikationsschicht - Modellregistry, Feature Store (für klassische ML), Prompt/Policy Registry (für GenAI/Agenten). - RAG-Komponenten: Vektor-Index, Dokumentenpipeline, Zitierfähigkeit/Source-Tracing. - Evaluations-Harness: Robustheit, Bias-Checks, Adversarial Testing (besonders für General-Purpose/Frontier-Modelle und „systemic risk“-Diskussionen im AI Act). [33]

MLOps/LLMOps - CI/CD für Modelle, Canary Releases, Rollback, Drift-Detektion, Monitoring. - Logging/Retention passend zu Hochrisiko-Pflichten (mindestens mehrmonatige Logs; AI Act adressiert Logging und die Nutzbarkeit für Aufsicht/Anwender). [34]

Sicherheits- und Compliance-Schicht - Zero Trust, Secrets Management, Härtung gegen Prompt-Injection/Tool-Abuse. - Lieferkettensicherheit (Model/Package-SBOM), besonders relevant unter Cyber Resilience Act-Pflichten ab 2026/2027-Stichtagen. [13]
- Cloud-Beschaffung und Nachweisführung über C5-Testate/Reports (in der Bundesverwaltung als präferierter Nachweisweg hervorgehoben). [32]

Compute-/Energy-Schicht - Compute-Portfolio: Cloud-GPU, On-Prem-HPC, Edge-Inference. - Energie-/Kapazitäts-Controlling: KI-Workloads konkurrieren 2026–2030 stärker mit Energie-/Netzengpässen; IEA erwartet starkes Wachstum der Rechenzentrumsnachfrage bis 2030. [16]
- Für große Organisationen: Rechenzentrums-Energie-Reportingpflichten in der EU (Energieeffizienz-Regime) werden als Transparenzhebel wichtiger. [35]

Szenarioanalyse 2026–2030 nach Domäne

Methodik und Annahmen

Die Szenarien basieren auf fünf gemeinsamen Treibern: 1) KI-Fähigkeitskurve (GenAI/Agenten, Edge-Inference), 2) Regulierung & Haftung, 3) Energie/Compute-Engpässe, 4) geopolitische Fragmentierung, 5) Cyber- und Informationsintegrität. [36]

Wahrscheinlichkeiten: Da keine domänenspezifischen Wahrscheinlichkeiten vorgegeben sind, werden **keine objektiven Wahrscheinlichkeiten behauptet**. Im Folgenden werden – explizit als **Planungs-Priors (nicht spezifiziert durch Auftraggeber, nicht aus Primärquelle ableitbar)** – Gewichte angegeben, um Portfolio-Entscheidungen robust zu machen.

Domänen-Szenarien in Kurzform

Domäne	Best Case (Planungs-Prior)	Baseline (Planungs-Prior)	Worst Case (Planungs-Prior)
Business	25%	55%	20%
Geopolitik	15%	50%	35%
Persönliches Leben	20%	60%	20%
Wealth	20%	55%	25%
Industriegase	20%	55%	25%

Diese Priors dienen als Startwerte für interne Planung und sollten quartalsweise mit Frühindikatoren (siehe KPI-Abschnitt) aktualisiert werden.

Zeitachse mit regulatorischen und systemischen Inflektionspunkten

```
gantt
    dateFormat  YYYY-MM-DD
```

```
    title 2026–2030: Regulierung & systemische Inflektionspunkte
    section EU KI- und Datenregime
    AI Act gilt (Hauptanwendung)           :milestone, 2026-08-02, 1d
    AI Act: Produkt-/Sicherheitskomponenten (Art. 6(1)) :milestone, 2027-08-0
2, 1d
    Data Act gilt                          :done, 2025-09-12, 1d
    EHDS gilt (Hauptanwendung)             :milestone, 2027-03-26, 1d
    CRA: Kapitel IV (notified bodies etc.) :milestone, 2026-06-11, 1d
    CRA: Art. 14 (Vulnerability Handling)  :milestone, 2026-09-11, 1d
    CRA gilt voll                          :milestone, 2027-12-11, 1d
    section Resilienz
    DORA gilt                              :done, 2025-01-17, 1d
    NIS2 nationale Anwendung (EU-weit)     :done, 2024-10-18, 1d
    section Klima/Handel
    CBAM Compliance-Phase                  :milestone, 2026-01-01, 1d
```

Belegstellen: AI Act-Stichtage. [37] Data Act-Stichtage. [12] EHDS-Stichtage. [14] CRA-Stichtage. [13] DORA-Stichtag. [7] NIS2-Stichtage. [38] CBAM-Übergang 2026. [39]

Business 2026–2030

Baseline-These: Unternehmen industrialisieren KI in Kernprozessen, aber unter engeren Compliance-/Security-Auflagen; Wettbewerbsvorteile entstehen über *Prozess-Re-Design* + *Datenqualität* + *Betriebssicherheit*. Die OECD zeigt, dass GenAI bereits 2024 in KMU-Kontexten untersucht wird (Survey mit >5.000 KMU, u. a. in Deutschland und Österreich) – der Skill-/Adoptionsdruck ist also real und breit. [40]

Best Case (25%)
2026–2027: Agentische Assistenten werden in „kontrollierten Korridoren“ produktiv (z. B. Customer Service, Sales Ops, Procurement), Qualität stabilisiert sich durch Evaluations-/Monitoring-Pipelines. 2028: AI Act-Review-Dynamik führt zu klareren Standards; Unternehmen, die früh auf ISO/IEC-kompatible AIMS-Strukturen setzen, reduzieren Audit-Kosten. 2029–2030: KI wird zur „Entscheidungsinfrastruktur“, vergleichbar ERP-Einführung, und skaliert über Partnerdatenräume (Data Act-fähig). [41]

Baseline (55%)
2026: Fokus auf Compliance-Readiness (AI Act-Geltung ab Aug 2026). 2027: mehr harte Arbeit in Daten-Lineage, Logging, Human Oversight-Design (Hochrisiko-Use-Cases) statt „glänzender Demos“. 2028–2030: ROI entsteht selektiv, vor allem dort, wo Datenqualität hoch ist und Prozesse standardisiert sind. [42]

Worst Case (20%)
Mehrere Branchen erleben „KI-Rückschläge“ durch Sicherheitsvorfälle, IP-/Datenlecks, fehlerhafte Entscheidungen, die (unter AI Act) zu Marktaufsicht/Haftungsdruck führen. Investitionen werden defensiver; KI wird auf nicht-kritische Bereiche begrenzt. [43]

Schlüssel-Inflektionspunkte - 2026-08-02: AI Act gilt – Governance-/Dokumentationspflichten werden operativ entscheidend. [37]

- 2027-12-11: CRA voll – Software-/Produktsecurity drückt stärker in „AI-in-Product“-Strategien. [13]

Geopolitik 2026–2030

Hier wird Geopolitik als Handlungsfeld für Staaten, Unternehmen und kritische Infrastrukturen verstanden: Sanktions-/Exportkontroll-Compliance, Desinformation, Cyber, Lieferketten-Resilienz, „energy & compute“ als strategische Ressourcen.

Baseline-These: Der geopolitische Wettbewerb verschiebt sich in Richtung **Geoökonomie + Technologie-/Daten-Souveränität**. Der Global Risks Report 2026 betont „Age of competition“ und nennt geoökonomische Konfrontation als zentrales kurzfristiges Krisenrisiko; Desinformation und Cyber-Insecurity zählen ebenfalls zu den Top-Risiken im Zwei-Jahres-Ausblick. [3]

Best Case (15%)
„Competitive cooperation“: Mindeststandards für KI-Sicherheit (z. B. Hiroshima Code of Conduct) stabilisieren Basisschutz; internationale Normen reduzieren ungebremste Eskalation. [44]

Baseline (50%)
Sicherheits- und Verteidigungsakteure nutzen KI zunehmend, aber mit Fokus auf Responsible Use. NATO[45] betont 2024 in der revidierten KI-Strategie u. a. die Prinzipien verantwortlicher Nutzung (Lawfulness, Accountability, Explainability/Traceability etc.) und adressiert als Umfeldfaktoren u. a. Datenverfügbarkeit sowie Energiebedarf „compute intensive AI“. [46] Unternehmen übersetzen dies in „Resilience by Design“: Red-Teaming, Supply-Chain-Security, Kommunikations-Playbooks.

Worst Case (35%)
Zunahme von Konflikten, Sanktionen und Cyber-Ereignissen führt zu stärkerer Fragmentierung (Datenlokalität, Cloud-Souveränität, Exportkontrollen für Chips/Modelle). KI wird als Multiplikator für Desinformation und Betrug genutzt; ENISA beschreibt 2025 u. a. „AI as lure“ und die Proliferation betrügerischer Websites, die KI-Tools imitieren, um Malware zu verteilen. [47]

Schlüssel-Inflektionspunkte - 2026–2028: Vertrauens- und Informationsintegrität (Deepfakes/Desinfo) wird makroökonomisch und sicherheitspolitisch ein Hauptthema (WEF-Technologie-Risikoranking). [3]
- 2026–2030: „Energy & AI“: IEA sieht Rechenzentren als wachsenden Treiber der Stromnachfrage in fortgeschrittenen Volkswirtschaften; Energiepolitik wird KI-Politik. [48]

Persönliches Leben 2026–2030

„Life“ wird hier als individuelle Lebensführung verstanden: Gesundheit, Bildung, Produktivität, Familie, digitale Identität und mentale Resilienz.

Best Case (20%)
Persönliche KI-Assistenten werden zu „Co-Piloten“ für Lernen, Planung und

Gesundheitsnavigation, ohne systemische Privatsphäre-/Manipulationsschäden. Voraussetzung ist AI literacy und transparente Nutzung. Der AI Act definiert AI literacy als Pflichtaufgabe für Anbieter und Betreiber (Maßnahmen zur Sicherstellung eines ausreichenden KI-Kompetenzniveaus). [30]

Baseline (60%)
Nutzen entsteht, aber heterogen: Menschen mit höherer digitaler Kompetenz profitieren überproportional; neue „Hygienestandards" entstehen (Datenminimierung, lokale Verarbeitung, klare Tool-Grenzen).

Worst Case (20%)
Manipulative KI-Praktiken (u. a. durch Desinformation, betrügerische KI-Tools, psychologisch optimierte Nudges) verstärken Stress, Polarisierung und Fehlentscheidungen. Der AI Act verbietet bestimmte manipulative oder täuschende Techniken sowie weitere Praktiken (z. B. Social Scoring) – dennoch bleibt die Durchsetzung und die „Grauzone" massenhaft. [43]

Inflektionspunkte - 2027-03-26: EHDS-Anwendung startet – Gesundheitsdatennutzung bekommt EU-weit klarere Regeln/Interoperabilität, aber mit Transition und Implementing Acts. [14]

Wealth Management 2026–2030

Wealth umfasst private und institutionelle Vermögensverwaltung, Banking-/Brokerage-Operations, Risiko- und Compliance-Systeme.

Baseline-These: KI wird in Finance weiter ausgerollt (z. B. Fraud, Scoring, Compliance), aber die „License to operate" ist digitale Resilienz. Die European Central Bank[49] (Bankenaufsicht) beschreibt 2025, dass Banken KI u. a. für Kredit-Scoring und Betrugserkennung nutzen. [50] Gleichzeitig gilt DORA seit 2025 und setzt robuste ICT-Risikomanagement-Pflichten. [7]

Best Case (20%)
KI verbessert Risiko-Früherkennung (Fraud/AML, Markt-/Liquiditätsstress) und senkt operative Fehler; menschliche Entscheidungsrollen werden klarer (Human-in-the-Loop).

Baseline (55%)
Schrittweise Prozessautomation; starke Investitionen in Vendor-/Third-Party-Risk (DORA-Register, Outsourcing governance).

Worst Case (25%)
„Model-Risk meets Market-Risk": Fehlkalibrierte Modelle + gleichgerichtete KI-Strategien erhöhen prozyklische Effekte (z. B. Herding, Flash-Move-Risiken). Zudem nehmen KI-getriebene Betrugswellen zu.

Inflektionspunkte - 2026–2027: CRA-Pflichten treffen FinTech-/Software-Lieferketten; Audits und SBOM-Pflichten erhöhen TCO. [13]

Industriegase 2026–2030

Industriegase (u. a. Sauerstoff, Stickstoff, Argon, Wasserstoff, Spezialgase) sind kapital- und energieintensiv, stark OT-getrieben, und systemrelevant für Stahl, Chemie, Medizin, Halbleiter, Wasser/Abwasser.

Die EIGA[51] positioniert die Branche als besonders erfahren in Produktion/Transport/Lagerung/Anwendung von Wasserstoff (über 100 Jahre) und als Partner für Europas Klimaziele. [52] Gleichzeitig zeigt die IEA: Wasserstoffnachfrage stieg 2024 auf ~100 Mt; Low-emissions Wasserstoff bleibt <1% der Produktion, Projektpipeline bis 2030 wurde nach unten revidiert (37 Mtpa möglich aus angekündigten Projekten; 4,2 Mtpa aus „operational or reached FID"). [53]

Best Case (20%)
- KI-Optimierung senkt Energieintensität von Luftzerlegungsanlagen (ASU), verbessert Verfügbarkeit durch Predictive Maintenance und Remote Operations.
- Wasserstoff-Hochlauf gelingt selektiv, getragen durch robuste Offtake-Politiken/Quoten; Industriegase-Anbieter werden Integratoren (H2-Supply + CO2-Management + O2 für industrielle Dekarbonisierung). [54]

Baseline (55%)
- Breite Digitalisierung: Sensorik + Digital Twin + „virtuelle Operatoren" unterstützen Betrieb. Beispiel: Nippon Gases[55] nutzt Digital-Twin-Technologie zur präziseren Sauerstoffdosierung in Abwasserbehandlung, um Energieverbrauch und Emissionen zu senken; genannt wird ein digitales „virtuelles Operator"-System (MiruGas). [56]
- Investitionen gehen in modulare On-site-Anlagen: Linde[57] berichtet 2024 von 59 neuen Long-Term-Agreements und 64 zu bauenden/zu betreibenden On-site-Anlagen; Nachfrage getrieben u. a. durch Elektronik (Batterien) und Dekarbonisierung. [58]
- CBAM-Compliance (ab 2026) und ETS-Verschärfung erhöhen Bedarf an Emissions-/Energieoptimierung entlang der Kundenbasis. [59]

Worst Case (25%)
- Energie-/Netzengpässe + hohe Strompreise + Cyber-/OT-Risiken führen zu Produktions- und Lieferstörungen.
- Wasserstoff-Projekte verzögern sich weiter; Investitionscommitment sinkt.

Inflektionspunkte - 2026-01-01: CBAM-Definitivphase (Zertifikate/Reporting) – belastet energie-/CO2-intensive Lieferketten und verstärkt Datennachweis-Pflichten. [39]
- 2026–2030: Energie-/Compute-Konkurrenz – Datenzentren werden größerer Nachfragetreiber; für energieintensive Industrie steigen Systemspannungen. [16]

Governance, Organisation und Talentpfade

Zielbild-Organisation

AI-Orchestration gelingt selten „nebenbei“ in IT. Notwendig ist ein Operating Model, das Business-Ownership, Risiko/Compliance und Engineering zusammenbringt.

```
flowchart TB
    A[Aufsichtsrat/Board] --> B[CEO / Geschäftsführung]
    B --> C[AI-Orchestrator Leader]
    C --> D[AI Governance Council]
    D --> E[Data Governance]
    D --> F[Model Risk & Compliance]
    D --> G[Cybersecurity / OT-Security]
    D --> H[AI Product Portfolio]
    H --> I[Domänen-Squads (Business, Wealth, Industriegase, etc.)]
    I --> J[MLOps/LLMOps Plattformteam]
    G --> K[Incident Response & Crisis Comms]
    F --> K
    E --> J
    J --> I
```

Erläuterung (Rollen & Mandate) - **AI Governance Council:** entscheidet Policy-Set (z. B. zugelassene Modelle, Datenklassen, Human-Oversight-Standards), Priorisierung, Risikoakzeptanz. Orientierung: NIST AI RMF (GOVERN) und ISO/IEC 42001-Logik. [60]
- **Model Risk & Compliance:** AI Act-Klassifizierung (Hochrisiko ja/nein), technische Doku, Logging-/Monitoring-Anforderungen, Lieferanten-Audit-Pfad. [61]
- **Cybersecurity/OT-Security:** besonders kritisch in Industriegasen; CRA-Pflichten ab 2026/2027 verstärken „secure by design“. [62]
- **Plattformteam:** stellt „AI Factory“ bereit (Daten, MLOps, Monitoring, IAM).

Talent- und Skill-Pfad 2026–2030

Der AI-Orchestrator Leader muss Talent als **Pipeline** planen, nicht als Einzelrekrutierung.

Rollenprofile (minimal) - AI Product Owner / AI Portfolio Manager (Wert + Risiko + Adoption) - Data Steward / Data Product Manager (Qualität, Verträge, Lineage; wichtig bei Data Act) [12]
- ML/LLM Engineer + MLOps/Platform Engineer - AI Security Engineer (Prompt-/Agent-Security, Red-Teaming) - Compliance Counsel (AI Act/DORA/NIS2/CRA) - OT-Data Engineer (Industriegase: SCADA/Edge)

Upskilling-Pfad - Baseline: AI literacy für gesamte relevant betroffene Belegschaft (Pflichtaufgabe nach AI Act). [30]
- Advanced: Zertifizierbare Tracks (z. B. ISO/IEC 42001-AIMS-Auditor-Kompetenz, Secure-MLOps).

Risiken, Ethik und Regulierung in EU und Deutschland

EU-AI-Act als „Backbone“ (Status bis 2026)

Anwendungstermine - Geltung ab 2. August 2026; Teile früher (u. a. Kapitel I/II ab 2. Februar 2025; weitere Teile ab 2. August 2025). [37]

AI literacy - Anbieter und Betreiber müssen Maßnahmen ergreifen, um ein ausreichendes KI-Kompetenzniveau für Personal sicherzustellen. [30]

Verbotene Praktiken - Der AI Act enthält explizite Verbote u. a. für manipulative/irreführende Techniken mit erheblichem Schadenpotenzial und weitere Praktiken (z. B. Social Scoring-Logik). [63]

Hochrisiko-KI: zentrale Pflichten - Risiko-Management-System als kontinuierlicher, iterativer Prozess über den Lebenszyklus. [64]
- Daten- und Data-Governance-Anforderungen für Trainingsdaten und Entwicklung. [65]
- Transparenz/Information gegenüber Betreibern (Deployers). [66]
- Human Oversight-Mechanismen. [67]
- Anforderungen an Genauigkeit, Robustheit und Cybersecurity. [68]

DORA, NIS2, CRA, Data Act, EHDS als „zweite Klammer“

- **DORA (Finanzsektor)**: Anwendung seit 17. Januar 2025; beinhaltet u. a. ICT-Risikomanagement und Drittparteienrisiken. [7]
- **NIS2**: Umsetzung in den Mitgliedstaaten bis 17. Oktober 2024; Anwendung ab 18. Oktober 2024. [38] In Deutschland: Umsetzungsgesetz im Bundesgesetzblatt verkündet (6. Dezember 2025). [69]
- **Cyber Resilience Act**: gestaffelt ab 2026/2027, voll ab 11. Dezember 2027 – erhöht den Druck auf Produkt-Security, Vulnerability Handling, technische Doku. [13]
- **Data Act**: gilt ab 12. September 2025; weitere Staffelungen 2026/2027 – relevant für vernetzte Produkte, Datenportabilität, Cloud-Switching. [12]
- **EHDS**: Anwendung ab 26. März 2027 (weitere Teile später) – wirkt auf Gesundheits-Use-Cases und Datenzugang/Secondary Use. [14]

Risikokategorien, die 2026–2030 typischerweise eskalieren

Cyber- und Betrugsrisiken - ENISA dokumentiert 2025 u. a. den Trend gefälschter KI-Tool-Webseiten als Malware-Vektor („AI as lure“). [70]

Energie- und Infrastrukturabhängigkeit - IEA: Rechenzentren als wachsender Treiber; Strom- und Netzplanung wird für KI-Skalierung zum Faktor. [16]

Informationsintegrität/Desinformation - WEF: Desinformation und Cyber-Insecurity als Top-Risiken im 2-Jahres-Horizont; adverse AI outcomes steigen im 10-Jahres-Horizont stark. [3]

Implementierungsleitfaden: KPIs, Budgets, Playbooks, Kommunikation

KPI-Set und Monitoring-Dashboards

Die KPI-Logik folgt drei Ebenen: 1) **Wert (Outcome KPIs)**, 2) **Betrieb (Reliability/Cost KPIs)**, 3) **Risiko/Compliance (Guardrail KPIs)** – kompatibel zur NIST-Logik MAP/MEASURE/MANAGE. [23]

Domäne	Outcome-KPIs	Betriebs-KPIs	Risiko/Compliance-KPIs
Business	Durchlaufzeit Kernprozess; Qualitätsquote; Umsatz/Conversion-Lift	Modell-/Agent-Uptime; Kosten pro 1.000 Entscheidungen; Datenqualitäts-Score	AI Act-Klassifizierungsabdeckung; Audit-Findings; Incident-Rate
Geopolitik (Unternehmen/Institution)	Time-to-Insight; Supply-Chain-Resilience Index	Data-Freshness; False-Positive-Rate in Alerts	Desinfo-Detektionsquote; Cyber-MTTD/MTTR; Red-Team-Findings
Persönliches Leben	Zeitgewinn/Woche; Gesundheits-Adhärenz; Lernfortschritt	Assistenz-Nutzungsrate; lokale/verschlüsselte Verarbeitung-Quote	Datenschutz-Vorfälle; Manipulations-/Scam-Exposure
Wealth	Fraud-Loss-Rate; Risk-Adjusted Return (Kontextabh.); Operational Error Rate	Ausführungs-Latenz; System-Uptime	DORA-Kontrollabdeckung; Modellvalidierungs-Status; Vendor-Risk-Heatmap
Industriegase	kWh pro t Produkt; Anlagenverfügbarkeit; CO2e-Intensität	Predictive-Maintenance-Trefferquote; OT-Telemetry-Coverage	OT-Security-Events; Safety Near-Miss Rate; CRA-/AI-Act-Doku-Status

Hinweis: exakte KPI-Definitionen sind organisationsspezifisch und daher nicht spezifiziert; die Tabelle gibt ein domänenadäquates Mindestset.

Budget- und ROI-Leitplanken 2026–2030

Da keine Unternehmensgröße, Umsatzbasis oder Capex/Opex-Struktur spezifiziert ist, werden **Bandbreiten als Richtwerte** formuliert (nicht als externe Benchmark behauptet). Sie sollten gegen Energie-/Compute-Kosten und regulatorische Aufwände kalibriert werden (IEA: wachsende Stromnachfrage; AI Act/CRA: steigender Nachweisaufwand). [71]

Investitionsblock	Typischer Anteil am KI-Programm-Budget	ROI-Treiber	Sensitivitäten (2026–2030)
Datenplattform & Qualität	25–40%	bessere Modelle, weniger Fehlerkosten	Data Act-Portabilität/Contracts; EHDS-Interoperabilität (Health) [72]
MLOps/LLMOps & Monitoring	15–25%	schnellere Releases, weniger Incidents	AI Act Logging/Monitoring; Auditkosten [34]
Security/Compliance (inkl. Red-Team)	15–30%	Avoided Losses, Vermeidung von Stillstand/Strafen	NIS2/DORA/CRA-Pflichten; Threat Landscape [73]
Use-Case-Delivery (Squads)	20–35%	direkte Werthebel je Domäne	Talentverfügbarkeit; Prozessreife
Change & AI literacy	5–15%	Adoption, Fehlerreduktion	AI Act-AI-Literacy-Pflicht [30]

ROI-Annahmen (explizit als Annahmen) - Baseline: ROI entsteht primär über **Fehler-/Ausfallvermeidung** (Security/OT), **Energie-Optimierung** (Industriegase) und **Kosten pro Entscheidung** (Business/Wealth).
- Best-Case-Hebel: neue Produkte/Services, neue Datenmonetarisierung (Data Act-fähige Angebote). [12]

```
pie title Beispielhafte Budgetverteilung (Baseline)
    "Datenplattform & Qualität" : 35
    "MLOps/LLMOps & Monitoring" : 20
    "Security/Compliance" : 25
    "Use-Case-Delivery" : 15
    "Change & AI literacy" : 5
```

Taktische Playbooks für Führungskräfte

Kurzfristig (0–6 Monate) - AI-Portfolio-Triage: „Stop/Start/Scale“ anhand Risiko-Tiering (AI Act) und Business-Wert. [37]
- Minimal-Governance live: Model/Prompt Registry, Logging, Incident-Playbook, Red-Team-Cadence. [74]
- AI literacy-Programm starten (Pflichtpfad nach AI Act). [30]

Mittelfristig (6–18 Monate) - „AI-Factory“ stabilisieren: MLOps/LLMOps, Drift-Monitoring, auditierbare Doku-Pipelines. [75]
- Drittparteiensteuerung: Cloud-/Vendor-Nachweise über C5-Berichte operationalisieren (inkl. korrespondierende Kontrollen beim Kunden), besonders relevant in regulierten

Bereichen. [32]
- Energie-/Compute-Governance: FinOps + EnergyOps für KI-Workloads (IEA-Projektionen als Strukturrisiko). [16]

Langfristig (18–48 Monate) - Cross-Domain-Orchestrierung: gemeinsame Datenprodukte, Standard-Policies, federated Learning/Edge-Inference dort, wo Daten nicht fließen dürfen (GDPR/EHDS-Kontexte). [76]
- Szenario-basierte Krisenübungen: Deepfake-Crisis, OT-Cyber Incident, Market-Stress + Model-Failure. [77]

Stakeholder-Kommunikation und Krisenmanagement-Vorlagen

Template A: „Message House“ bei KI-Vorfall (extern) - *Was ist passiert?* (faktenbasiert, Zeitstempel, betroffene Systeme)
- *Welche Auswirkungen?* (Kunden/Produktion/Sicherheit)
- *Was tun wir jetzt?* (Containment, Rollback, Monitoring)
- *Was tun wir als Nächstes?* (Post-Mortem, Verbesserungen, unabhängige Prüfung)
- *Was können Betroffene tun?* (Schritte, Kontaktkanäle)

Template B: Executive-Lagebild (intern, 1 Seite) - Situation (T+0/T+4h/T+24h)
- Risiko-Einschätzung (operativ, rechtlich, reputativ)
- Entscheidungen erforderlich (3–5 Punkte)
- Ressourcenbedarf (People/Compute/Partner)
- Nächste Kommunikationsfenster

Template C: Regulatorisches Incident-Protokoll (Finance/CI) - Zuordnung: DORA/NIS2/AI-Act-Relevanz
- Logs/Beweise gesichert?
- Drittparteien betroffen?
- Kundeninformation/Marktkommunikation (Zeitpunkt, Inhalt)
- Lessons learned + Control-Update

Fallstudien, Präzedenzfälle und Primärquellen

Präzedenzfälle 2020–2026 als „Beweise der Richtung“

Cloud-Sicherheitsnachweise (C5) als Orchestrations-Baustein
Ein BSI-Vortrag (2022) beschreibt C5 als umfassende Sammlung von Sicherheitskriterien für Cloud-Dienste, mit standardisierten Prüfberichten, die Vergleichbarkeit schaffen; außerdem wird C5 als präferierte Methode des BSI zur sicheren Cloud-Nutzung hervorgehoben und die Rolle korrespondierender Kontrollen betont. [32]

Industriegase: Digital Twin & „Virtual Operator“ - Nippon Gases (2026) nutzt Digital Twin zur präziseren Sauerstoffdosierung in der Abwasserbehandlung, mit Ziel Energie- und Emissionsreduktion; ein „virtueller Operator“ (MiruGas) sammelt 24/7 Anlageninformationen. [56]

- Wissenschaftliche Evidenz, dass Digital Twin-Modelle in Realanlagen hohe Genauigkeiten erreichen können, z. B. Demonstration digital-twin-basierter Aeration-Control mit >95% Modellgenauigkeit (Wasser/Abwasser-Kontext). [78]

Wasserstoff-Marktunsicherheit (für Industriegase & Energiepolitik) - IEA: 2024 ~100 Mt Nachfrage, Low-emissions <1% Produktion; Pipeline-Revision zu 37 Mtpa (announced) bis 2030; 4,2 Mtpa aus FID/operational bis 2030. [53]

Geopolitik/Verteidigung: Responsible AI - NATO (2024) hebt Responsible-Use-Prinzipien hervor und nennt Energie/Compute als Kontextfaktor für KI-Einsatz. [46]

Extrapolierte Use-Cases 2026–2030 (analytische Ableitung)

Business - „Decision-Ops“: KI erstellt Optionen + Begründung, Mensch genehmigt innerhalb definierter Policy; Logging + Audit-Ready (AI Act-fähig). [79]

Geopolitik (Unternehmen) - Geo-Exposure-Engine: automatisches Mapping von Lieferanten/Materialien auf Sanktions-/Exportkontrollrisiken, kombiniert mit Desinformations-/Cyber-Alerting (WEF-Risikolage). [77]

Life - Personal Health Copilot im EHDS-Rahmen (ab 2027 zunehmend): datensparsame KI-Assistenz, interoperabel, mit klarer Zweckbindung. [14]

Wealth - „Resilience-First AI“: KI-gestützte Betrugserkennung und Prozessautomatisierung unter DORA-Kontrollen; Vendor-Risk-Heatmaps und Testprogramme. [80]

Industriegase - Autonomous Plant Advisor: Digital Twin + Echtzeit-Daten zur Energie-Optimierung, Disturbance-Prediction, Wartungsfenster-Optimierung; ergänzt um CBAM/ETS-Datenanforderungen in Kundenlieferketten. [81]

Empfohlene Primärquellen und autoritative Referenzen

EU-Recht/Offizielle Quellen - EU-AI-Act (Regulation (EU) 2024/1689) inkl. Stichtage, Hochrisiko-Pflichten, AI literacy. [82]
- DORA (Regulation (EU) 2022/2554) – Anwendung ab 17. Januar 2025. [7]
- NIS2 (Directive (EU) 2022/2555) – Transposition/Anwendung. [38]
- Data Act (Regulation (EU) 2023/2854) – Anwendung ab 12. September 2025. [12]
- Cyber Resilience Act (Regulation (EU) 2024/2847) – gestaffelte Anwendung ab 2026/2027. [13]
- EHDS (Regulation (EU) 2025/327) – Anwendung ab 26. März 2027, gestaffelte Teile. [14]
- CBAM-Guidance/Kommissionsseiten (Übergang 2023–2025, Compliance ab 2026). [83]

Deutschland (offiziell) - Nationale KI-Strategie-Portal der Bundesregierung (Strategierahmen, Förderlogik). [84]
- Bundestitel/Publikation: Nationale Sicherheitsstrategie (Stand 21. Juni 2023) als Referenz für integrierte Sicherheitslogik. [85]
- NIS2-Umsetzungsgesetz im Bundesgesetzblatt (Verkündung 6. Dezember 2025). [69]

Standards & Risk Frameworks - NIST AI RMF 1.0 (GOVERN/MAP/MEASURE/MANAGE). [23]
- ISO/IEC 42001 (AIMS) und ISO-Einordnung. [86]
- ISO/IEC 23894 (AI Risk Management Guidance) und ISO/IEC 22989 (Begriffe/Konzepte) als Normen-Backbone. [87]

Energie/Industrie - IEA „Energy and AI“ und Datacenter-Stromnachfrage (415 TWh 2024; ~945 TWh 2030 Basisszenario). [16]
- IEA Global Hydrogen Review 2025 (Marktstatus, Projektpipeline, Kostenlücke). [53]
- EIGA-Positionierung Wasserstoff & Safety-/Standards-Fokus. [88]
- Linde-Beispiel für modulare On-site-Industrial-Gas-Expansion. [58]

Cyber-Threat Intelligence - ENISA Threat Landscape 2025 (u. a. KI-Missbrauch als Köder). [70]

Makro-Risikolage - Global Risks Report 2026 (Key Findings, Risiko-Rankings). [89]

---

[1] [15] [17] [23] [27] [60] [74] https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

[2] [25] [41] [86] https://www.iso.org/standard/42001

https://www.iso.org/standard/42001

[3] [18] [36] [77] [89] https://www.weforum.org/publications/global-risks-report-2026/digest/

https://www.weforum.org/publications/global-risks-report-2026/digest/

[4] [8] [19] [26] [28] [30] [31] [33] [34] [37] [42] [43] [49] [57] [61] [63] [64] [65] [66] [67] [68] [75] [79] [82] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AL_202401689

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AL_202401689

[5] [11] [38] https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[6] [14] [45] [76] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng

https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng

[7] [20] [73] [80] https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[9] [16] [71] https://www.iea.org/reports/energy-and-ai/energy-demand-from-ai

https://www.iea.org/reports/energy-and-ai/energy-demand-from-ai

[10] [87] https://www.iso.org/standard/77304.html

https://www.iso.org/standard/77304.html

[12] [72] https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

[13] [22] [51] [62] https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[21] [58] https://www.linde-engineering.com/news-and-events/press-releases/2025/record-wins-for-linde%E2%80%99s-small-on-site-solutions-in-2024-driven-by-electronics-and-decarbonization

https://www.linde-engineering.com/news-and-events/press-releases/2025/record-wins-for-linde%E2%80%99s-small-on-site-solutions-in-2024-driven-by-electronics-and-decarbonization

[24] [56] [81] https://www.gasworld.com/story/nippon-gases-applies-digital-twin-to-wastewater-oxygen-control/2172454.article/

https://www.gasworld.com/story/nippon-gases-applies-digital-twin-to-wastewater-oxygen-control/2172454.article/

[29] [47] [55] [70] https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

[32] https://www.isaca.de/images/Publikationen/Prasentationen/ISACA%20Fokus%20Event%20-%20BSI-Vortrag%20-%20Sichere%20Cloudnutzung%20mit%20C5%20-%20221103.pdf

https://www.isaca.de/images/Publikationen/Prasentationen/ISACA%20Fokus%20Event%20-%20BSI-Vortrag%20-%20Sichere%20Cloudnutzung%20mit%20C5%20-%20221103.pdf

[35] https://energy.ec.europa.eu/topics/energy-efficiency/energy-efficiency-targets-directive-and-rules/energy-efficiency-directive/energy-performance-data-centres_en

https://energy.ec.europa.eu/topics/energy-efficiency/energy-efficiency-targets-directive-and-rules/energy-efficiency-directive/energy-performance-data-centres_en

[39] [59] [83] https://eur-lex.europa.eu/EN/legal-content/summary/carbon-border-adjustment-mechanism.html

https://eur-lex.europa.eu/EN/legal-content/summary/carbon-border-adjustment-mechanism.html

[40] https://www.oecd.org/en/publications/generative-ai-and-the-sme-workforce_2d08b99d-en.html

https://www.oecd.org/en/publications/generative-ai-and-the-sme-workforce_2d08b99d-en.html

[44] https://www.mofa.go.jp/files/100573473.pdf

https://www.mofa.go.jp/files/100573473.pdf

[46] https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

[48] https://iea.blob.core.windows.net/assets/34eac603-ecf1-464f-b813-2ecceb8f81c2/EnergyandAI.pdf

https://iea.blob.core.windows.net/assets/34eac603-ecf1-464f-b813-2ecceb8f81c2/EnergyandAI.pdf

[50] https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2025/html/ssm.nl251120_1.en.html

https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2025/html/ssm.nl251120_1.en.html

[52] [88] https://www.eiga.eu/

https://www.eiga.eu/

[53] [54] https://www.iea.org/reports/global-hydrogen-review-2025/executive-summary

https://www.iea.org/reports/global-hydrogen-review-2025/executive-summary

[69] https://www.recht.bund.de/bgbl/1/2025/301/VO.html

https://www.recht.bund.de/bgbl/1/2025/301/VO.html

[78] https://www.sciencedirect.com/science/article/abs/pii/S0011916424009469

https://www.sciencedirect.com/science/article/abs/pii/S0011916424009469

[84] https://www.ki-strategie-deutschland.de/

https://www.ki-strategie-deutschland.de/

[85] https://www.publikationen-bundesregierung.de/pp-de/publikationssuche/nationale-sicherheitsstrategie-2197780

https://www.publikationen-bundesregierung.de/pp-de/publikationssuche/nationale-sicherheitsstrategie-2197780

Josef David – 2026-02-12