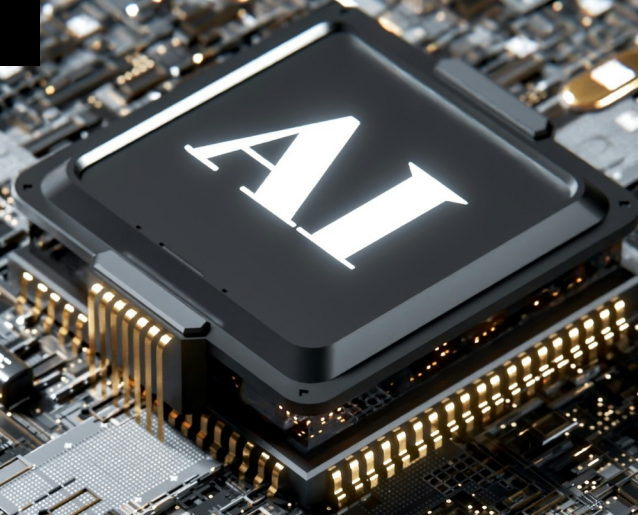




Osmond
RISK MATTERS



Governance und Risikomanagement beim Einsatz von Künstlicher Intelligenz (AI)

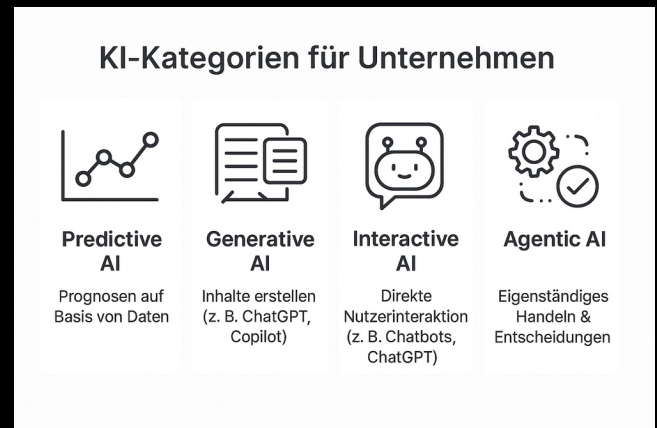
Fact Sheet

Osmond GmbH
+41 56 511 22 90
Rummelmatt 6, CH-5610 Wohlen
info@osmond.ch
www.osmond.ch

20/09/2025

Überblick und Nutzen

Es ist von entscheidender Bedeutung, dass Unternehmen, die AI einsetzen, die Auswirkungen dieses Einsatzes auf das Risikoprofil aktiv berücksichtigen und Governance-, Risikomanagement- und Kontrollsysteme entsprechend anpassen. Dies sollte durch ein AI Management System erfolgen, das Transparenz schafft, Verantwortlichkeiten klärt und die Einhaltung regulatorischer sowie ethischer Standards sicherstellt.



AI-Systeme bergen mehrere Risiken

- **Risiken des Modells:** Probleme wie mangelnde Robustheit, Korrektheit, Verzerrungen, Halluzination und Erklärbarkeit
- **IT-, Cyber- und Datenschutzrisiken:** Schwachstellen in der IT-Sicherheit und Cybersicherheit
- **Abhängigkeit von externen Anbietern:** Hardware-Lösungen, Modelle oder Cloud-Dienste
- **Marktkonzentration:** Abhängigkeit von einigen wenigen Anbietern
- **Autonomes Handeln:** Schwierigkeiten bei der Zuweisung von Verantwortlichkeiten aufgrund von dezentralen Zuständigkeiten
- **Potentielle Rechtsfragen:** Komplexität, die zu rechtlichen Herausforderungen führen können
- **Rufschädigung:** Risiken, die den Ruf des Unternehmens beeinträchtigen

Relevante AI Rahmenwerke und Gesetze

- **NIST AI RMF** <https://www.nist.gov/itl/ai-risk-management-framework>
- **ISO 42001** <https://de.isms.online/iso-42001/everything-you-need-to-know-about-iso-42001/>
- **SANS AI Security** <https://www.sans.org/mlp/critical-ai-security-guidelines/>
- **EU AI Act*** <https://artificialintelligenceact.eu/de/>

*Markortprinzip: Der EU AI Act gilt auch ausserhalb der EU, wenn die AI-Produkte oder -Dienstleistungen von Unternehmen auf dem EU-Markt verfügbar sind oder EU-Bürger betreffen.

Rahmenwerk Schwerpunkte

Governance

- **AI Framework:** Robuste und pragmatische AI Strategie, AI Politik, AI Leitlinien
- **Zentrales Inventar:** Führen eines zentral verwaltetes Inventar mit Risikoklassifizierungen und Massnahmen
- **Klare Verantwortlichkeiten:** Definition der Rollen für die Anschaffung / Entwicklung, Implementierung, Überwachung und Nutzung von AI
- **Testen:** Festlegung von Anforderungen für die Bewertung der Datenqualität und das Testen von AI-Anwendungen und AI-Modellen
- **Standards:** Festlegung umfassender Dokumentationsrichtlinien
- **Ausbildung:** Massnahmen für eine gründliche Ausbildung aller Beteiligten
- **Outsourcing:** Sicherstellen, dass Drittanbieter über die notwendigen Fähigkeiten und Erfahrungen verfügen. Führen von Tests, Kontrollen, Vertragsklauseln (Haftung) und Verantwortlichkeiten



Quelle: NIST AI Framework

Schritte der Anwendung

1. **AI framework aufsetzen:** AI Framework auf den AI Einsatz anpassen
2. **Bewertung der derzeitigen Praktiken:** Bewertung und Gap Analyse
3. **Risikobewertung:** Identifizierung von Risiken und Entwicklung von Strategien zur Risikominderung
4. **Schliessung der Gaps:** Definition und Einführung von Governance und Kontrollen
5. **Awareness:** Schulung und Förderung eines verantwortungsvollen Umgangs mit AI
6. **Überwachen und verbessern:** Entwickeln von Messgrössen, Review und Assessments

Bankenspezifische Informationen

- FINMA Aufsichtsmitteilung 08/24
<https://www.finma.ch/de/dokumentation/finma-aufsichtsmitteilungen/>
- Bankiervereinigung - Generative AI in Banking - A Comprehensive Overview
<https://www.swissbanking.ch/de/services/downloads>

Osmond unterstützt Unternehmen bei der AI Governance nach Standards und regulatorischen Vorgaben – mit Fokus auf Risikomanagement, IT Security, Datenschutz und Compliance