Osmond
RISK MATTERS

AI Risk Management & Governance

Consultingangebot

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

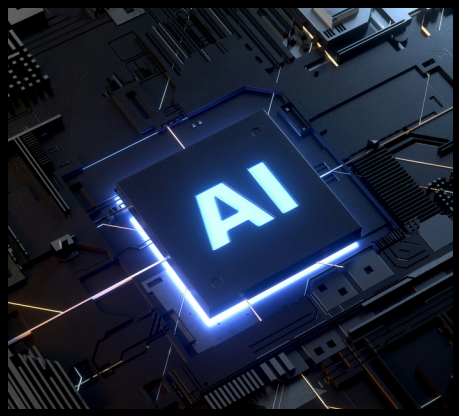
29/08/2025

Überlick und Nutzen

Agentische AI-Systeme bringen neue Anforderungen an Sicherheit, Datenschutz und Regulierung mit sich. Unternehmen müssen klären, wie diese Systeme sicher, kontrollierbar und rechtskonform betrieben werden können. Die Nachfrage nach Services zur Absicherung, Überwachung und Vermeidung von Datenlecks wächst stark. Gefragt sind auditierbare Lösungen – idealerweise eingebettet in ein AI Management System, die Standards wie den NIST AI RMF, ISO/IEC 42001, EU AI Act erfüllen.

Zielsetzung

Für Unternehmen mit komplexen Strukturen, regulatorischen Anforderungen und strategischem AI-Einsatz bieten wir ein umfassendes, strukturiertes Risikomanagement nach dem NIST AI RMF kompatibel mit ISO/IEC 42001.



Leistungsstruktur

MAP - AI verstehen & Risiken identifizieren

- Erfassung und Klassifikation aller AI-Systeme
- Analyse von Geschäftsprozessen, Stakeholdern und potenziellen Auswirkungen
- Aufbau und Pflege eines AI Risk Registers
- Einordnung in Risikoklassen analog dem EU AI Act (z. B. Hochrisiko-AI)

MEASURE - Risiken bewerten & quantifizieren

- Durchführung von Risikoanalysen (technisch, organisatorisch, ethisch)
- Entwicklung von Key Risk Indicators (KRIs)
- Unterstützung bei Impact Assessments

MANAGE - Risiken steuern & mindern

- Ableitung und Umsetzung von Schutzmassnahmen
- Etablierung eines KI-Incident-Managements
- Integration in bestehende ISMS/GRC-Systeme
- Unterstützung bei Anwendungs-/Modellvalidierung und Monitoring

GOVERN - Governance & kontinuierliche Verbesserung

- Aufbau einer KI-Governance-Struktur
- Erstellung und Pflege von Richtlinien und Leitlinien
- Schulung und Sensibilisierung von Mitarbeitenden
- Regelmässige Audits, Reviews und Management-Reporting

Projektvorgehen zur Umsetzung

Quelle: NIST AI RMF

1. Gap-Analyse & Reifegradbewertung
2. Aufbau eines AI Risk Management Frameworks
3. Durchführung von Risiko- und Impact-Assessments
4. Entwicklung von Richtlinien & ethischen Leitlinien
5. Integration & Umsetzung in bestehende Systeme
6. Schulung & Awareness
7. Monitoring, Reporting & kontinuierliche Verbesserung

Lieferobjekte

1. AI RMF Roadmap
2. Risikoanalyse und Klassifikation
3. AI RMF-konforme Risiko-Metriken
4. Governance-Dokumente
5. Test- und Validierungsberichte gemäss Kundeanforderungen
6. Schulungs- und Awareness-Materialien
7. Mapping-Dokumente (u.a. EU AI Act, ISO 42001)

Mehrwert

- AI Anwendungen sind sicher und entsprechen dem Datenschutz
- Vertrauen schaffen bei Kunden, Partnern und Investoren
- Geeignet für komplexe Organisationen mit mehreren KI-Anwendungen
- Klare Projektstruktur mit messbaren Ergebnissen
- Skalierbare Governance für zukünftiges Wachstum