Brochure

ISO/IEC 42001:2023 Gap-Analysis
Your way to responsible and secure AI usage

Are you aware of the risks associated with using Artificial Intelligence (AI) in your organization? Our gap analysis based on the international standard ISO/IEC 42001:2023 shows where your organization currently stands in terms of AI management – and what concrete steps are needed for optimization.

Identify gaps in your AI Management System

With the increasing use of innovative Artificial Intelligence (AI), conscious, responsible, and transparent application is more important than ever. Already leveraging the benefits of AI? Then your organization should operate an AI Management System to ensure secure and transparent implementation and documentation of AI practices.

Your benefits at a glance

- **Clear baseline assessment**
  Receive a well-founded analysis of how your organization currently aligns with the requirements of the ISO/IEC 42001 standard.
- **Identify risks – seize opportunities**
  Gaps in your AI Management System are identified, evaluated, and prioritized.
- **Confidence in action**
  You receive concrete, actionable recommendations – technical, organizational, and personnel-related – including quick wins for rapid improvement.
- **Regulatory advantage**
  Be optimally prepared for future regulatory requirements in the field of AI governance.
- **Management-Friendly presentation**
  All findings are compiled in a concise report and presented in a final workshop.
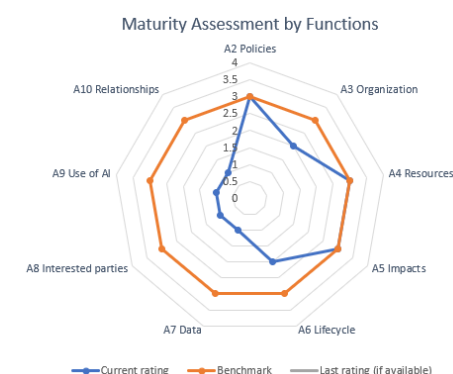

Fig. Example of a maturity assessment

Scope of analysis – what we assess

Our experts analyze your existing AI management practices based on the key components of the ISO/IEC 42001 standard:

- **Governance & Organization**
  Internal responsibilities, policies, and accountabilities
- **Resources & Data Management**
  Handling of training data, data quality, and data security
- **AI System Development & Lifecycle**
  Development, integration, use, maintenance, and decommissioning
- **Risk & Impact Management**
  Assessment of ethical, legal, and societal impacts
- **Transparency & Communication**
  Information for stakeholders, internal and external traceability
- **Third-Party Collaboration**
  Oversight and responsibility in externally sourced AI systems

Where appropriate, we extend our assessment by integrating additional frameworks, such as the 'Responsible AI in a Dynamic Regulatory Environment' by the Cloud Security Alliance (CSA) – especially in cases of in-house AI development or the use of Microsoft Copilot.

Our approach – efficient. transparent. tailored.

1. **Kick-Off & Scoping**
   Definition of goals, scope, interviewees, and available documentation
2. **Current state analysis**
   Review of documents & structured interviews to determine AI maturity
3. **Evaluation & Reporting**
   Identification of deviations from ISO standard, risk classification, and action plan
4. **Final Workshop**
   Presentation and discussion of results, finalization of the report

Optional: Microsoft Copilot Readiness Check
Additional review of data flows and protection measures related to Copilot and sensitive information.

Ready to take responsibility for AI?
Request your ISO/IEC 42001:2023 Gap Analysis now and take your AI maturity to the next level.