LEXIFY INSIGHTS

YOUR TRUSTED LEGAL NEWSLETTER

ISO/IEC 42005:2025: AI IMPACT ASSESSMENT

Technology & Digital Assets | 12/2025

Introduction

The increasing regulatory, ethical, and operational scrutiny on artificial intelligence ("**AI**") systems necessitates structured governance mechanisms. ISO standards introduced are grounded in the plan, do, check, and act ("**PDCA**") cycle, mirroring quality assurance traditions. This article explores how organisations can systematically embed AI Impact Assessments ("**AI-IAs**") within this cycle, aligning with **ISO 42005 Clause 5**. We examine timing triggers, scope considerations, documentation practices, and decision-making models, arguing for the centrality of impact assessments as both legal compliance tools and organisational governance mechanisms.

Do we need an AI-IA?

The first and most frequent question from both technologists and managers is deceptively simple: "*Do we need to conduct an AI Impact Assessment?*" The answer, however, depends on the regulatory, operational, and ethical profile of the system in question.

Under current European regulatory framework, impact assessments are mandatory for deployers of high-risk AI systems, however strongly recommended in all other cases. Additionally, from a data protection perspective under both Swiss and European law, a Data Protection Impact Assessment ("**DPIA**") is required.

Importantly, many organisations choose to conduct AI-IAs voluntarily, even if not mandated, to fulfil internal governance expectations or to comply with procurement conditions (e.g., under the MCC-AI High-Risk clauses).

Thus, the requirement is both legal and strategic, particularly in environments where organisational trust and compliance maturity are central.

Timing considerations

Organisations should design their AI-IA workflows to accommodate both time-based and event-based triggers:

- time-based triggers include fixed review intervals, such as quarterly or annually, or upon reaching specific developmental milestones (e.g., post-training, post-deployment); and
- event-based triggers arise from substantial modifications (even incidents in testing phase) to the system's purpose, architecture, data input, or target population, or from external developments such as incidents, user complaints, or changes in the regulatory environment.

Thresholds and legal boundaries

During the planning phase, organisations must articulate the purpose, scope, and methodology of the impact assessment. This includes identifying applicable legal frameworks (e.g., AI Act, GDPR, and/or sectoral laws), setting risk thresholds, and defining acceptable metrics for harm, fairness, and performance.

Conducting the Assessment(s)

The implementation phase entails conducting the assessment itself. This includes mapping foreseeable impacts of the system in different operational contexts. Typically, the AI-IA will include:

- scenario planning (normal use, edge cases, and misuse);
- stakeholder analysis (especially where rights may be infringed);
- technical testing (e.g., robustness and bias detection); and
- organisational analysis (e.g., management and Chief Artificial Intelligence Officer).

The AI Act increasingly favours modular assessments, distinguishing between fundamental rights, safety, data protection, and sector-specific norms. This encourages the use of composite frameworks integrating DPIAs, human rights impact assessments (HRIAs), and other AI-IA. Multiple AI-IAs shall be conducted depending on the sectoral requirements.

Completion of the Assessment(s)

Once the assessment is completed, organisations must evaluate whether the results support deployment, indicate the need for mitigation, or justify halting development. This includes:

- a formal analysis of residual risks;
- identification of mitigation measures (technical, procedural, communicative); and
- an approval process involving senior management or ethics boards.

All findings must be documented, version-controlled, and stored in a manner suitable for external audits or post-market monitoring (especially in financial realm).

In the final stage, organisations must formally approve the assessment results, implement mitigation, and plan review mechanisms. Crucially, organisations must avoid "*infinite impact assessments*" processes that lack formal closure and decision. Instead, results must be archived with clear evidence of endorsement and subsequent action.

The results of AI-IAs must also be available upon request to national supervisory authorities.

Conclusion

AI Impact Assessments are rapidly becoming not only a regulatory necessity but a central component of responsible innovation. By embedding AI-IAs within the ISO 42005 PDCA cycle, organisations can move from compliance to governance from reacting to AI risks to anticipating and managing them proactively. Clause 5 of ISO 42005 provides a very broad vision of what should be implemented.

Lexify as Your Consultant

Lexify continuously monitors regulatory developments and assists European and international companies within this sector. For further information or support, our legal team is at your disposal.

Contact

Connect with us

Thank you for taking the time to read our article. We hope you find it informative and engaging. If you have any questions, feedback, or would like to explore our services further, we're here to assist you.

Contact Information

For inquiries about our legal assistance, please contact:

Emanuele Gambula
+41 76 232 66 83
emanuele.gambula@lexify.io

Alberto Borri
+41 77 461 38 47
alberto.borri@lexify.io

Follow Us

Stay updated and connected with us on social media for the latest news, insights, and updates:

- **LinkedIn**: Lexify
- **X:** Lexify
- **YouTube:** Lexify

Explore More

Visit our website, register to our Newsletter at https://www.lexify.io/ and never miss a legal insight!