IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/47ISM/2026/4730726/
Vol. 2026 (7), Article ID 4730726

A Framework For Evaluating Potential Return On Investment In Artificial Intelligence Based On Implementation Risks*

Matej HAVLAS ORCID 0009-0009-5686-0695 and Veronika NOVORTNA ORCID 0000-0001-9360-3035

Brno University of Technology, FBM, Brno, Czechia

Correspondence should be addressed to: Matej HAVLAS, xhavla06@vutbr.cz

*Presented at the 47th IBIMA International Conference, 29-30 June 2026, Madrid, Spain

Abstract.

Artificial intelligence (AI) is increasingly integrated into organisational practice, yet a substantial share of implementation projects fail to achieve their intended outcomes. Gartner's 2024 forecast indicates that up to 30% of AI initiatives may be cancelled due to unclear value creation, poor data quality, and underestimated costs. Despite the proliferation of maturity models, risk frameworks, and ROI calculators, these tools are typically applied in isolation, leaving organisations without a coherent structure that links technological readiness with financial outcomes. This paper presents a conceptual decision-support framework for evaluating the potential return on investment (ROI) of AI initiatives, integrating three interdependent analytical dimensions: organisational maturity, solution complexity, and data–process health. The framework consolidates previously fragmented approaches and translates AI-related risks into financial indicators, enabling more structured investment planning. The contribution lies not only in integrating existing frameworks but also in positioning organisational readiness as a precondition for meaningful ROI assessment. Future research will focus on empirical validation across industrial and service-sector enterprises.

Keywords: artificial intelligence, return on investment, implementation risk, organisational maturity, decision-support framework

JEL Classification: M15, O33, G31

Paper Type: Conceptual / Theoretical Framework Proposal

Introduction

Artificial intelligence (AI) has emerged as a defining technological force within the broader context of Industry 5.0, a paradigm that emphasises the sustainable, human-centric integration of advanced digital systems into organisational and industrial practice (Xu et al., 2021; Breque et al., 2021). Unlike its predecessor, Industry 4.0, which prioritised automation and connectivity, Industry 5.0 foregrounds the collaboration between human capabilities and intelligent systems as a driver of resilient and value-oriented transformation (European Commission, 2021). Within this context, AI adoption has accelerated significantly, driven by competitive pressure, operational efficiency imperatives, and the promise of data-driven decision-making.

Despite this momentum, a persistent gap exists between AI investment and measurable organisational outcomes. Industry evidence indicates that up to 30% of AI projects are cancelled before completion, with unclear value propositions, poor data quality, and underestimated implementation costs cited as the primary causes (Gartner,

Cite this Article as: Matej HAVLAS and Veronika NOVORTNA Vol. 2026 (7) " A Framework for Evaluating Potential Return On Investment In Artificial Intelligence Based On Implementation Risks " Communications of International Proceedings, Vol. 2026 (7), Article ID 4730726, https://doi.org/10.5171/2026.4730726

2024). These failures reflect not merely technical shortcomings but a fundamental misalignment between strategic intent and organisational readiness.

Existing frameworks address aspects of this challenge individually. Maturity models such as the MITRE AI Maturity Model assess organisational capability; risk frameworks such as NIST's AI Risk Management Framework address compliance and safety; ROI tools provided by vendors focus on financial projections. However, these approaches remain fragmented: they do not establish a unified analytical structure that links readiness, risk, and return within a single evaluative mechanism.

This paper addresses that gap by proposing an integrated decision-support framework for evaluating the potential ROI of AI initiatives. The framework consolidates three analytical dimensions. Organisational maturity, solution complexity, and data–process health. These are conjuncted into a coherent structure that connects technological and organisational risk factors with financial outcomes. In doing so, it offers enterprises a practical basis for structured AI investment planning and prioritisation.

The remainder of the paper is organised as follows. Section 2 presents a thematic synthesis of the relevant literature, identifying the research gap the framework addresses. Section 3 describes the methodology underpinning the review. Section 4 presents the framework and its constituent dimensions. Section 5 positions the framework in relation to existing approaches and discusses its implications. Section 6 concludes with directions for future research.

Theoretical Background

The literature relevant to AI investment evaluation can be organised around three thematic streams, each corresponding to one dimension of the proposed framework: organisational readiness for AI adoption, assessment of AI solution complexity, and data and process quality as enablers of AI performance. While each stream is internally developed, the absence of a framework integrating all three into a unified ROI evaluation structure constitutes the principal research gap this paper addresses.

Organisational Readiness and Maturity

Organisational readiness for AI has received considerable scholarly attention. Pumplun et al. (2019) and Jöhnk et al. (2021) identify infrastructure, human capital, and governance as foundational prerequisites for successful AI adoption, arguing that technical deployment without organisational preparation consistently produces suboptimal outcomes. The MITRE AI Maturity Model (2022) formalises progression through five levels, from Initial to Optimised and links maturity advancement to reduced implementation risk and improved ROI predictability. Strategic alignment, cybersecurity resilience, and asset readiness emerge across multiple frameworks as the core components of organisational maturity (Ahmed et al., 2022; Jabbar et al., 2024). What remains underexplored is how these maturity dimensions translate directly into financial risk adjustments within a ROI calculation.

Solution Complexity and Use-Case Evaluation

The complexity of an AI use case is a significant determinant of implementation risk and investment return. Microsoft's Business Envisioning Framework (2024) provides a structured methodology for evaluating use cases along dimensions of business alignment, technical feasibility, and user impact. CognitivePath (2024) extends this by emphasising measurable business outcomes and mission alignment as scoring criteria. Barredo Arrieta et al. (2020) and Gunning et al. (2021) highlight that algorithmic complexity increases computational costs, reduces interpretability, and demands more intensive governance. Kontogiannis and Vouros (2023) further demonstrate that higher solution complexity correlates with longer development cycles and greater uncertainty in return timelines. These findings collectively support the treatment of solution complexity as a risk multiplier in ROI evaluation, though existing frameworks do not formalise this relationship.

Data and Process Quality as ROI Enablers

AI system performance is fundamentally constrained by the quality and governance of underlying data assets. Bernasconi et al. (2023) establish the FAIR Principles: Findability, Accessibility, Interoperability, and Reusability, as the reference standard for evaluating data governance maturity. Folorunso et al. (2022) demonstrate through empirical application that FAIR-compliant data pipelines substantially improve model accuracy and reduce post-deployment remediation costs. The Data Management Body of Knowledge (DMBOK) framework emphasises standardisation and automation of ETL processes as conditions for reliable AI operation (Jati et al., 2022). Monte Carlo (2025) and DBT Labs (2024) extend this into contemporary data observability practice, linking continuous monitoring of data pipelines to sustained AI performance and reduced model degradation. Despite this evidence, ROI evaluation frameworks rarely incorporate data and process health as a systematic input variable.

Research Gap

The literature review reveals that organisational maturity, solution complexity, and data–process health are each well-theorised in isolation. What is absent is a unified framework that integrates these three dimensions into a coherent mechanism for risk-adjusted ROI evaluation. Existing ROI tools tend to focus on financial projections without adjusting for implementation risk; maturity models assess readiness without connecting their outputs to financial outcomes. This paper proposes a framework designed to bridge these gaps.

Methodology

The framework presented in this paper was developed through a systematic literature review conducted in accordance with the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) reporting guideline (Page et al., 2021). PRISMA was applied as a transparency and reporting standard, not as a research method per se; the underlying method is a systematic review of peer-reviewed and grey literature.

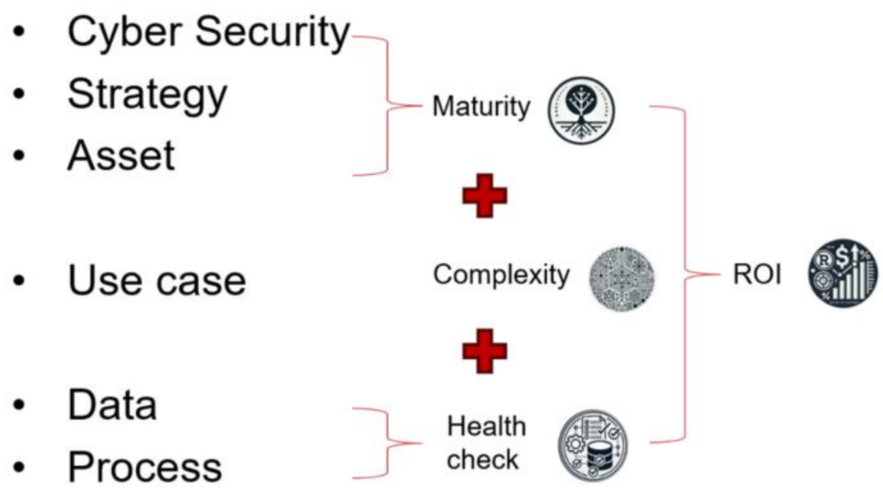
The review was conducted across two academic databases: Scopus and Web of Science, supplemented by targeted searches in institutional repositories and recognised industry sources. The primary search terms included: artificial intelligence implementation, AI maturity model, AI return on investment, AI risk management, data governance AI, and organisational readiness AI. Searches were restricted to publications from 2019 to 2025 to ensure relevance to the current AI deployment landscape.

Inclusion criteria required that studies address at least one of the three framework dimensions (organisational maturity, solution complexity, or data–process health) in the context of enterprise AI adoption, and that they be published in peer-reviewed journals, conference proceedings, or by recognised institutional bodies. Studies focused exclusively on narrow technical AI topics without organisational or financial dimensions were excluded, as were non-English publications.

A total of 947 records were identified through database searches and supplementary sources. Following removal of duplicates and screening of titles and abstracts, 74 studies met the inclusion criteria and were analysed in full. Perplexity AI was used as a supplementary monitoring tool to identify emerging grey literature and industry frameworks; all AI-assisted outputs were verified against primary sources before inclusion. The synthesis proceeded through thematic clustering of findings across the three framework dimensions, identifying convergent evidence and areas where integration across dimensions was lacking.

The Proposed Framework

The proposed framework integrates three interdependent analytical dimensions—organisational maturity, solution complexity, and data–process health—into a risk-adjusted ROI evaluation structure. Together, these dimensions determine both the probability of implementation success and the expected magnitude of financial return. Figure 1 presents the framework schematically.



Source: Havlas & Novotná, 2025

Organisational Maturity

Organisational maturity captures the overall readiness of an enterprise to adopt, integrate, and sustain AI initiatives. The framework evaluates maturity across three components: strategic alignment, cybersecurity resilience, and asset readiness.

Strategic alignment assesses the degree to which AI initiatives are embedded within long-term planning and governance structures. Enterprises with mature strategic alignment demonstrate executive sponsorship, clear value-realisation mechanisms, and integration of AI into performance measurement frameworks. The MITRE AI Maturity Model and Microsoft's AI Readiness Approach provide reference standards for this evaluation (MITRE, 2022; Microsoft, 2024).

Cybersecurity resilience evaluates the organisation's capacity to protect AI systems against threats including data breaches, adversarial inputs, and model integrity attacks. Key indicators include the robustness of threat-detection mechanisms, incident-response capabilities, and adherence to AI-specific security standards such as Google's Secure AI Framework (SAIF) and the AI-Integrated Cybersecurity Risk Management model developed by Jabbar et al. (2024).

Asset readiness captures the adequacy of technical infrastructure, data architecture, and workforce competencies required to operationalise and sustain AI systems. Reference frameworks including the DNV AI Maturity Assessment and IBM's AI readiness guidelines emphasise the need to align infrastructure, human expertise, and governance with strategic objectives (Jöhnk et al., 2021).

Enterprises can be classified across five maturity levels: Initial, Developing, Defined, Managed, and Optimised, with each level associated with a different risk profile and ROI probability range. Lower maturity levels imply a higher risk adjustment factor, reducing the projected ROI accordingly.

Solution Complexity

Solution complexity refers to the level of intricacy associated with a specific AI use case, encompassing technical sophistication, scope of business requirements, and operational integration demands. Higher complexity entails greater uncertainty, longer implementation timelines, and increased resource demands, all of which influence the risk profile and expected return of an AI initiative.

The framework evaluates two sub-dimensions: technical complexity and risk profile. Technical complexity assesses algorithmic sophistication, data requirements, model interpretability, and integration needs. Highly complex systems such as large language models or multi-modal predictive pipelines present substantially higher computational costs and governance burdens than rule-based or supervised learning applications (Barredo Arrieta et al., 2020; Gunning et al., 2021). Risk profile examines exposure to cybersecurity threats, regulatory compliance requirements, and operational disruption, complementing the organisational maturity dimension by focusing on project-level rather than enterprise-level risk.

Structured methodologies such as Microsoft's Business Envisioning Framework (Microsoft, 2024) and CognitivePath's AI Use Case Scoring Approach (CognitivePath, 2024) provide systematic bases for assessing use cases. Within the proposed framework, solution complexity functions as a risk multiplier: high-complexity projects with low organisational maturity receive substantially discounted projected ROI estimates.

Data–Process Health

The performance and long-term viability of AI systems depend fundamentally on the quality, reliability, and governance of underlying data assets and operational processes. The data–process health dimension provides a diagnostic assessment of how well these foundations support accurate, scalable, and trustworthy AI operation.

Data quality and governance constitute the first sub-dimension. Reliable AI requires data that is accurate, complete, consistent, and timely-properties formalised in the FAIR Principles (Bernasconi et al., 2023). Effective governance encompasses data sourcing policies, cleaning procedures, version control, and lineage tracking throughout the AI lifecycle.

Process maturity and reliability assess the robustness of data pipelines supporting AI systems, including ETL processes, monitoring mechanisms, and anomaly detection capabilities. The DMBOK framework provides reference standards for standardisation and automation of these processes (Jati et al., 2022). Organisations with immature data pipelines face significantly elevated risks of model degradation, accuracy loss, and costly post-deployment remediation.

Risk and compliance address the regulatory and ethical dimensions of data use within AI systems, evaluating adherence to privacy, security, and fairness standards as defined by frameworks including NIST (2023) and Coherent Solutions (2025). Failure to meet compliance requirements introduces both financial penalties and reputational risks that directly affect projected ROI.

Risk-Adjusted ROI Calculation

The ROI calculation dimension integrates outputs from the three preceding dimensions into a composite risk-adjusted return estimate. Unlike conventional ROI assessment, which focuses on direct cost–benefit ratios, the proposed approach applies a risk coefficient derived from the combined assessment of maturity, complexity, and data health to adjust projected financial returns.

Financial indicators considered include cost savings through automation and error reduction, revenue growth enabled by AI-driven product or service enhancements, productivity gains across operational functions, and avoided costs from improved decision quality. Implementation costs including infrastructure, integration, maintenance, and training are evaluated against both short- and long-term return horizons (Sellamuthu et al., 2023).

Beyond financial performance, the framework incorporates intangible value dimensions including enhanced decision-making capability, improved customer experience, and accelerated innovation cycles. These non-financial outcomes are treated as strategic multipliers that strengthen the long-term financial case for AI investment (Molin et al., 2024).

The risk coefficient adjusts projected returns downward in proportion to identified weaknesses across the three dimensions. An organisation with low maturity, high solution complexity, and poor data governance would receive a substantially discounted ROI projection, signalling the need for preparatory investment before committing to the full AI initiative. This mechanism supports scenario planning and portfolio prioritisation, enabling decision-makers to compare AI initiatives on a consistent, risk-adjusted basis.

Discussion

Positioning Relative to Existing Frameworks

The proposed framework occupies a distinctive position relative to established approaches. Taken individually, the MITRE AI Maturity Model assesses organisational capability but does not generate financial outputs. NIST's AI Risk Management Framework addresses compliance and safety without connecting risk levels to return projections. Microsoft's Business Envisioning Framework evaluates use-case feasibility but does not account for the organisational maturity context in which a use case will be deployed. Vendor-provided ROI calculators generate financial projections without systematic risk adjustment derived from readiness or complexity assessment.

The proposed framework integrates the most operationally significant elements of each approach into a unified evaluative structure. Organisational maturity assessment draws on MITRE and Microsoft readiness models; solution complexity evaluation builds on Microsoft's Business Envisioning methodology; data–process health incorporates FAIR Principles and DMBOK standards; and the risk-adjusted ROI calculation mechanism addresses the gap left by conventional cost–benefit tools. This integration does not replace any individual framework but provides a connective structure that enables their joint application.

Implications for Practice

For practitioners, the framework offers a structured basis for three types of decision. First, it supports go/no-go decisions on individual AI initiatives by making risk exposure explicit before financial commitments are made. Second, it supports portfolio prioritisation by enabling consistent, risk-adjusted comparison across multiple AI projects competing for resources. Third, it identifies preparatory investments—in maturity development, data infrastructure, or process standardisation—that are prerequisites for achieving projected returns.

The finding that organisational readiness functions as a precondition rather than a background variable has direct managerial implications. Enterprises that proceed with high-complexity AI deployments before achieving sufficient maturity are, in effect, accepting a substantially lower probability of realising projected returns. The framework makes this trade-off quantifiable and therefore actionable.

Limitations

The framework is conceptual in its current form and has not yet been empirically validated. The risk coefficient mechanism and the weighting of sub-dimensions require calibration against real implementation data across diverse organisational and sectoral contexts. Additionally, the framework addresses enterprise AI adoption in industrialised contexts and may require adaptation for public-sector organisations, SMEs, or developing-economy settings where institutional conditions differ substantially. The reliance on self-assessment for maturity and data health scoring introduces subjectivity that empirical validation would help address.

Conclusion

This paper has presented a conceptual framework for evaluating the potential return on investment in AI initiatives, integrating three analytical dimensions: organisational maturity, solution complexity, and data–process health, into a risk-adjusted ROI calculation structure. The framework addresses a persistent gap in the AI investment literature: the absence of a unified mechanism that connects readiness and risk assessment with financial outcome evaluation.

The principal theoretical contribution lies in establishing organisational readiness as a precondition for meaningful ROI assessment, and in providing a structured mechanism through which maturity, complexity, and data quality jointly determine a risk coefficient applied to projected returns. This approach enables enterprises to move beyond optimistic, risk-naive financial projections toward evidence-based investment planning.

Future research should pursue empirical validation of the framework across multiple industries and organisational sizes. Quantitative calibration of the risk coefficient would substantially strengthen the framework's practical applicability. Sector-specific adaptations, particularly for public administration and healthcare, represent a further avenue for development as AI governance requirements in these domains continue to evolve.

Additional Information

Acknowledgements and Financial Disclosure: This paper was supported by grant FP-S-22-7977 of the Internal Grant Agency at Brno University of Technology.

References

Ahmed, I., Jeon, G., & Piccialli, F. (2022). From Artificial Intelligence to Explainable Artificial Intelligence in Industry 4.0: A Survey on What, How, and Where. IEEE Transactions on Industrial Informatics, 18(8), 5031–5042. https://doi.org/10.1109/TII.2022.3146552

Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Bernasconi, A., Simon, A. G., Guizzardi, G., Santos, L. O. B. da S., & Storey, V. C. (2023). Ontological Representation of FAIR Principles: A Blueprint for FAIRer Data Sources. In Lecture Notes in Computer Science (pp. 261–277). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-34560-9_16

Breque, M., De Nul, L., & Petridis, A. (2021). Industry 5.0: Towards a Sustainable, Human-Centric and Resilient European Industry. European Commission, Directorate-General for Research and Innovation.

CognitivePath. (2024). Scoring AI Use Cases for Maximum Success. Retrieved from https://cognitivepath.com/ai-use-case-scoring/

Coherent Solutions. (2025). AI-Powered Data Governance: Implementing Best Practices and Frameworks. Retrieved from https://www.coherentsolutions.com/insights/ai-powered-data-governance-implementing-best-practices-and-frameworks

DBT Labs. (2024). Data governance frameworks for AI-driven organisations. Retrieved from https://www.getdbt.com/blog/data-governance-frameworks-ai

European Commission. (2021). Industry 5.0: A Transformative Vision for Europe. Publications Office of the European Union.

Folorunso, S., Ogundepo, E., Basajja, M., Awotunde, J., Kawu, A., Oladipo, F., & Ibrahim, A. (2022). FAIR Machine Learning Model Pipeline Implementation of COVID-19 Data. Data Intelligence, 4(4), 971–990. https://doi.org/10.1162/dint_a_00182

Gartner. (2024). Gartner: 30% of Gen AI Projects to be Abandoned by 2025. Retrieved from https://technologymagazine.com/ai-and-machine-learning/gartner-30-of-gen-ai-projects-to-be-abandoned-by-2025

Gunning, D., Vorm, E., Wang, J. Y., & Turek, M. (2021). DARPA's Explainable AI (XAI) Program: A Retrospective. Applied AI Letters, 2(4). https://doi.org/10.1002/ail2.61

Jabbar, H., Al-Janabi, S., & Syms, F. (2024). AI-Integrated Cyber Security Risk Management Framework for IT Projects. In 2024 International Jordanian Cybersecurity Conference (IJCC) (pp. 76–81). IEEE. https://doi.org/10.1109/IJCC64742.2024.10847294

Jati, P. H. P., Lin, Y., Nodehi, S., Cahyono, D. B., & van Reisen, M. (2022). FAIR Versus Open Data: A Comparison of Objectives and Principles. Data Intelligence, 4(4), 867–881. https://doi.org/10.1162/dint_a_00176

Jöhnk, J., Weißert, M., & Wyrtki, K. (2021). Ready or Not, AI Comes—An Interview Study of Organizational AI Readiness Factors. Business & Information Systems Engineering, 63, 5–20. https://doi.org/10.1007/s12599-020-00676-7

Kontogiannis, A., & Vouros, G. A. (2023). Inherently Interpretable Deep Reinforcement Learning Through Online Mimicking. In Explainable and Transparent AI and Multi-Agent Systems (pp. 160–179). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-40878-6_10

Microsoft. (2024). Evaluate and Prioritize an AI Use Case with Business Envisioning. Retrieved from https://learn.microsoft.com/en-us/microsoft-cloud/dev/copilot/isv/business-envisioning

MITRE. (2022). MITRE AI Maturity Model. Retrieved from https://aimaturitymodel.mitre.org/

Molin, A., Rudmark, D., Koutsikouri, D., & Nylén, D. (2024). Examining Value Creation in Public Sector AI Implementation. In Lecture Notes in Computer Science (pp. 317–333). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-70274-7_20

Monte Carlo. (2025). Data Quality Governance That Actually Works. Retrieved from https://www.montecarlodata.com/blog-data-quality-governance/

NIST. (2023). AI Risk Management Framework. National Institute of Standards and Technology. Retrieved from https://www.nist.gov/itl/ai-risk-management-framework

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Pumplun, L., Tauchert, C., & Heidt, M. (2019). A New Organisational Chassis for Artificial Intelligence—Exploring Organisational Readiness Factors. In Proceedings of the 27th European Conference on Information Systems (ECIS). AIS Electronic Library.

Sellamuthu, S., Vaddadi, S. A., Venkata, S., Petwal, H., Hosur, R., Mandala, V., Dhanapal, R., & Singh, J. (2023). AI-based recommendation model for effective decision to maximise ROI. Soft Computing. https://doi.org/10.1007/s00500-023-08731-7

Xu, X., Lu, Y., Vogel-Heuser, B., & Wang, L. (2021). Industry 4.0 and Industry 5.0—Inception, conception and perception. Journal of Manufacturing Systems, 61, 530–535. https://doi.org/10.1016/j.jmsy.2021.10.006