IPRPD
International Journal of Business & Management Studies
ISSN 2694-1430 (Print), 2694-1449 (Online)
Volume 06; Issue no 12: December, 2025
DOI: 10.56734/ijbms.v6n12a5

AI MANAGEMENT

(Establishing a New Subfield in Management Science Through a Structured Framework)

Jibran Bashir[1]

[1]*Jibran Bashir Leadership Institute (JBLI), Pakistan*

Abstract

Artificial Intelligence (AI) is increasingly central to business and public-sector organizations, offering transformative potential in productivity, decision-making, service delivery, and innovation. Despite this promise, many AI initiatives fail due to strategic misalignment, fragmented governance, and limited integration of technical and organizational factors. This paper introduces AI Management as a novel subfield of management science, presenting a structured framework for the effective adoption, operationalization, and oversight of AI initiatives. The framework integrates ten core functions—AI Leadership, AI Strategy, AI Transformation, AI Operationalization (ModelOps), AI Security, AI Performance & Value Management, Data Governance, AI Governance, AI Culture, and AI Risk Management—across vertical, horizontal, and pillar dimensions. By embedding ethics, regulatory compliance, strategic alignment, and value creation into organizational processes, AI Management provides a systematic approach for scaling AI responsibly, bridging its transformative potential with practical outcomes, and enabling sustainable organizational and societal impact.

Keywords

Artificial Intelligence, AI Management, AI Leadership, AI Strategy, AI Transformation, AI Operationalization, AI Security, AI Performance & Value Management, AI Governance, Data Governance, AI Culture & AI Risk Management

Introduction

Artificial intelligence has become an integral part of the modern workplace, with a transformative potential comparable to that of the steam engine during the Industrial Revolution. (Mayer, Yee, Chui & Roberts: 2025). The integration of Artificial Intelligence (AI) into the workplace is catalyzing a profound transformation across industries, fundamentally altering how organizations function and compete. Within business organization contexts, AI plays a pivotal role in enhancing Organizational Performance (OP)**,** a multidimensional construct that reflects an organization's overall effectiveness in achieving its strategic goals. OP encompasses critical dimensions such as profitability, market share, customer satisfaction, innovation, and operational efficiency. Automation enabled by Artificial Intelligence (AI) enhances productivity while simultaneously reducing operational costs. In addition, AI systems demonstrate exceptional capabilities in swiftly processing and analyzing large volumes of data, thereby generating actionable insights that facilitate informed and timely decision-making across all levels of the organization. This data-driven approach fosters more efficient resource utilization, strengthens customer relationships,

and elevates an organization's competitiveness in increasingly dynamic and complex market environments (Kassa & Worku: 2025).

Government organizations can also leverage AI to deliver personalized public services and streamline administrative processes. Effective adoption of AI in the public sector can generate benefits that are significantly larger than typically anticipated for national economies. Some applications can directly strengthen government finances—such as using advanced analytics to detect fraud, prevent incorrect disbursements in grant and transfer programs, or identify tax evasion, all of which are major sources of fiscal leakage. Beyond financial gains, many public-sector AI use cases enhance service quality and societal outcomes. Personalized, predictive, and preventive solutions in domains such as education, transportation planning, and emergency response can create broader economic multipliers, as they not only reduce public expenditure but also improve productivity for citizens and businesses (Berglind, Fadia, Isherwood: 2022). Integrating AI into government operations represents a strategic step toward building more resilient and adaptive public services. When deployed effectively, AI enables public servants to redirect their efforts toward higher-value tasks, thereby enhancing the quality, consistency, and reliability of services delivered to citizens (Marshall: 2025).

AI plays an increasingly central role in both business and government organizations by automating routine tasks, enhancing decision-making, and personalizing services to improve efficiency and outcomes. In the business sector, AI supports marketing, operations, and innovation, whereas in the public sector, it strengthens service delivery and resource allocation. In response to these developments, this paper introduces AI Management as a new and emerging subfield within management science by proposing a structured AI Management framework that guides the effective management of AI across business and government contexts, ensuring that AI initiatives are deployed and executed in a strategic, well-managed, ethical, and secure manner.

Literature Review

Artificial Intelligence (AI) is rapidly becoming a critical driver of organizational value and growth. Yet, despite its transformative potential, many organizations fail to realize meaningful outcomes from AI initiatives, as a significant number of projects collapse in the early stages due to insufficient guidance, inadequate management practices, and the absence of structured best-practice frameworks (Uba, Lewandowski, Böhmann: 2023). Effective implementation of artificial intelligence requires strategic execution rather than aspirational intent. Evidence shows that nearly 83% of Fortune 500 organizations struggle to achieve successful AI-driven digital transformation, primarily due to inadequate automation capabilities, talent shortages, data quality challenges, and ineffective customer-facing AI systems. Achieving meaningful outcomes, therefore, necessitates a clear strategy, robust real-time analytics, a strong supporting infrastructure, and effective management of AI initiatives (Craig: 2025). In 2025, AI project failure rates have escalated significantly, with approximately 42% of organizations abandoning most of their AI initiatives. The central issue is no longer the transformative potential of AI, but its persistent inability to deliver meaningful outcomes at scale. A primary driver of these failures is the strategic misalignment between business leadership and technical teams. Initiatives often deteriorate because executives misinterpret the underlying problem AI is intended to address, establish unrealistic expectations, or pursue emerging technologies without a well-defined business rationale (Krishnamohan:2025). Governments are also facing significant challenges in adopting AI, with skills shortages and limited access to high-quality, shareable data emerging as the most pervasive barriers. Despite increasing experimentation, most public-sector AI initiatives remain in pilot phases, struggling to scale due to fragmented data governance, inadequate technical guidance, and outdated digital infrastructure. Risk aversion, unclear regulatory interpretations, and overreliance on vendors further impede progress. Evidence indicates a lack of systematic monitoring of pilots and limited documentation of lessons learned, weakening continuity and institutional learning. To advance beyond experimentation, governments must strengthen implementation capacity through robust data strategies, clearer cross-cutting and sector-specific guidance, and mechanisms that balance innovation with responsible risk management (OECD:2025).

The other side of the picture tells that for effective governance of AI, five major standards and frameworks provide the most authoritative global guidance. At the foundational level, the OECD AI Principles provide an internationally endorsed set of values for responsible AI. At the same time, UNESCO's recommendation on the Ethics of Artificial Intelligence addresses the broader societal and

human rights implications of AI deployment. Building on these high-level norms, three technical and operational standards translate ethical commitments into implementable practices: the U.S. National Institute of Standards and Technology (NIST) AI Risk Management Framework, the ISO/IEC 42001 international standard for AI governance, and the IEEE 7000-2021 standard for the design of ethically aligned systems. Collectively, these five frameworks form a comprehensive foundation for designing, deploying, and governing AI systems in a responsible and ethically robust manner (Leopard & Epstein: 2025). Several additional frameworks shape contemporary AI governance. The EU AI Act introduces a legally binding, risk-based regulatory model that bans high-risk practices such as social scoring and imposes stringent compliance obligations on sectors like healthcare and finance. The UK's pro-innovation AI framework offers a non-statutory, principle-based approach centered on fairness, transparency, accountability, safety, and contestability. In the United States, federal oversight is guided by Executive Orders 14110 and the 2025 update, EO 14179, alongside earlier principles introduced in the AI Bill of Rights. State-level regulations, such as Colorado's AI Act and proposed legislation in California, further address algorithmic discrimination and accountability in automated decision-making. At the international level, the G7 Code of Conduct provides voluntary guidance for the safe and responsible development of foundation and generative AI systems (AI21:2025).

Postulation

The reviewed literature clearly reveals a persistent and widening gap between the transformative promise of artificial intelligence and its practical realization within organizations. Despite the accelerating adoption of AI and the availability of numerous governance frameworks—ranging from ethical principles to risk-management standards—most AI initiatives continue to fall short of successful deployment. Empirical evidence indicates that organizations frequently struggle with strategic misalignment, inadequate execution capabilities, fragmented data infrastructures, and the absence of coherent managerial practices that effectively translate theoretical guidance into operational success. This contrast between extensive governance frameworks and consistently poor implementation outcomes suggests a fundamental void: there is no unified, accepted theory of AI Management that integrates strategy, governance, organizational design, capability development, and operationalization into a single, applicable managerial discipline. Consequently, there is a critical need to develop a structured AI Management theory that can guide businesses and governments in achieving effective, scalable, and sustainable AI integration.

The postulation of this paper encompasses the critical organizational factors required to initiate, execute, sustain, and continuously improve AI initiatives. These factors include AI Leadership, AI Strategy, AI Transformation, AI Operationalization, AI Security, Data Governance for AI, AI Governance, AI Culture, AI Risk Management, and AI Performance & Value Management.

1: AI Leadership

AI leadership is the strategic capability to oversee the ethical adoption and management of artificial intelligence within organizations, aligning technological initiatives with long-term business objectives. An AI Leader understands both AI technologies and their impact on people and organizational culture. AI leaders leverage data, automation, and intelligent systems to drive performance improvements while upholding ethical standards and promoting employee well-being. By integrating innovation, governance, and human judgment, they ensure that AI serves as a responsible and effective tool for organizational advancement (Jones:2025). While IT departments are proficient in managing the technical dimensions of AI systems, the strategic deployment of AI requires leadership that accounts for both human and business implications. Effective AI leadership involves integrating AI into core organizational strategy and decision-making processes, ensuring alignment with broader objectives. Successful AI adoption extends beyond technical understanding to cultivating a culture of change, innovation, and continuous learning. Leaders play a critical role in guiding teams through technological transformation, fostering adaptability, and securing organizational commitment to AI-driven initiatives (Odilov: 2024). The successful implementation of AI typically requires a dedicated leadership structure, such as an AI steering committee or a Chief AI Officer, reporting directly to the CEO or board of directors. These leaders are responsible for defining a clear AI vision aligned with organizational objectives and ensuring the allocation of necessary resources, including budgets, data, and technology. They also establish strategic priorities for AI deployment, identifying areas—such as customer experience or operational efficiency—where AI can create the most value while maintaining alignment with the overall business strategy (Eddy:2025).

2. AI Strategy

An AI strategy is a structured approach to planning artificial intelligence initiatives that achieve strategic business objectives (Pratt:2024). Developing an AI strategy in isolation, without alignment to organizational goals, can lead to suboptimal or even negative outcomes. To maximize AI's potential, it must be closely integrated with the company's overall strategy and long-term goals. Consequently, the initial step in crafting an AI strategy is a thorough analysis of the company's strategic priorities. An AI strategy serves as a framework to orchestrate and guide initiatives that harness AI's transformative potential across the organization. Its foundation should be grounded in generating business value, with key objectives including enhancing productivity, profitability, accuracy, and innovation. A comprehensive AI strategy outlines how AI will drive innovation, improve operational efficiency, and create measurable value, while also addressing risk management, ethical adoption, regulatory compliance, governance, change management, and scalability for future growth (Bashir:2024). In the public sector, an AI strategy provides a structured basis for addressing key decision-making questions such as which applications should be prioritized, which technologies are most appropriate, how the value of AI can be communicated to the workforce, how AI initiatives should be governed, and whether talent should be developed internally, sourced externally, or pursued through a hybrid model. An effective AI strategy aligns technological choices with the government's overarching strategic direction and integrates insights from previous technological transformations by incorporating both technical and managerial considerations. Such a comprehensive approach ensures coherence with broader organizational objectives as well as national or federal priorities for AI adoption (Eggers, Mendelson, Chew & Kishnani:2019).

3: AI Transformation

AI Transformation refers to the systematic and strategic integration of Artificial Intelligence (AI) across an organization's operations, processes, and culture. It involves implementing AI-enabled systems to automate routine tasks, strengthen decision-making, optimize workflows, and stimulate innovation at scale. Beyond the adoption of individual AI tools, AI transformation signifies a deeper organizational realignment in which business models and core processes are re-engineered to harness AI's full potential. This shift enables organizations to improve efficiency, enhance competitiveness, and achieve sustainable long-term growth (Vu:2025). AI transformation involves leveraging artificial intelligence to improve data utilization, automate sophisticated tasks, support evidence-based decision-making, and enhance customer experience across the enterprise. It requires integrating intelligent technologies into key functions through a structured and strategic approach. The process begins with assessing organizational readiness—including data systems, technological capacity, human capabilities, and process maturity. Organizations then identify priority use cases that align with strategic goals and promise measurable impact. A comprehensive AI strategy, outlining objectives, governance mechanisms, technology platforms, talent development, and change management, directs implementation through targeted Minimum Viable Products (MVPs). These solutions are subsequently scaled across the organization to drive sustained operational efficiency and competitive advantage (Kajal & Clark: 2025). AI transformation extends beyond technological enhancement and represents a strategic organizational shift that demands clear vision, sustained commitment, and cross-functional collaboration. By adopting a structured approach, organizations can harness the full potential of AI and enhance their capacity for long-term, sustainable success (Mathew: 2025).

4: AI Operationalization

AI Operationalization can be defined through the definition of Gartner, which states that "AI model operationalization (ModelOps) is primarily focused on the governance and life cycle management of all AI and decision models (including models based on machine learning, knowledge graphs, rules, optimization, linguistics, and agents). In contrast to MLOps, which focuses only on the operationalization of ML models, and AIOps, which is AI for IT Operations, ModelOps focuses on the operationalization of all AI and decision models." — Gartner, Innovation Insight for ModelOps (ODSC:2021). "ModelOps (Model Operations) is a comprehensive framework for developing and managing analytical models that can rapidly transition from experimental environments to full-scale production. It emphasizes the automation of model deployment, monitoring, governance, and ongoing enhancement, ensuring that data analytics models operate reliably and continuously within the organization (Barney, Hanna, & Bernstein:2024). ModelOps represents a dynamic organizational capability that matures gradually rather than a one-time process. Organizations typically begin at a manual, fragmented stage, then progress to pipeline automation

and eventually to full CI/CD-driven lifecycle management. As automation increases, collaboration improves, model updates become more reliable, and models continuously adapt to new data. Achieving higher ModelOps maturity often requires specialized skills or external expertise to support robust lifecycle management (Doone:2024).

5: AI Security

AI security refers to the cybersecurity practices and safeguards designed to protect an organization's AI systems, data, and applications from potential threats. It involves securing the entire AI stack—from endpoints and infrastructure to models and pipelines—against cyberattacks, vulnerabilities, and data breaches. AI security also focuses on preserving the integrity of training data and preventing model corruption or poisoning. Additionally, it ensures the reliability and transparency of AI models, including LLMs and generative systems, while addressing concerns related to privacy, bias, and explainability. Finally, AI security ensures that all AI development and usage comply with relevant legal, regulatory, and organizational requirements (Habibi:2025). A compromised AI model can expose sensitive customer information, manipulate organizational decision-making, and disrupt critical operational processes. The inherent complexity of AI algorithms makes it challenging to anticipate system behavior under attack, and the rapid adoption of AI technologies often outpaces the development of corresponding security measures. Consequently, robust AI security has become essential for organizations seeking to leverage AI's benefits while mitigating emerging risks and vulnerabilities (Tariq:2025). There are AI security tools that generally concentrate on three core domains: safeguarding the data used to train and operate AI models, strengthening the models themselves against theft or manipulation, and securing the runtime environments in which models interact with users. By addressing these dimensions, such tools protect against threats including adversarial inputs, model extraction, and data poisoning (Jennings:2025).

6: Data Governance for AI

Data governance for AI refers to a structured system of policies, processes, and controls that ensures data used throughout AI lifecycles remains high-quality, secure, compliant, and ethically handled. While grounded in conventional data governance principles, it extends them to address the distinct requirements of machine learning and automated decision-making. The framework is typically organized around four core pillars: data quality, data privacy and security, data stewardship and ownership, and compliance and accountability. Collectively, these pillars ensure that data is reliable, protected, responsibly managed, and aligned with relevant legal and ethical obligations (Rockett:2025). Unlike traditional computing systems, AI and ML systems are far more complex, making rigorous data governance essential. Two key factors drive the need for a robust governance framework. First, AI/ML systems possess a dynamic structure that continuously adapts and learns from diverse structured and unstructured data sources. Second, their performance is closely tied to the scale and heterogeneity of the data on which they are trained. In the absence of strong governance mechanisms, these characteristics can lead to inconsistent, inaccurate, or biased model outputs (Kimachia: 2023). A comprehensive Five-Step Data Governance for AI Framework ensures secure and reliable AI operations. (1) Charter: Define data stewardship roles and policies addressing AI risks such as model bias and prompt injection. (2) Classify: Use metadata labeling and automated tools to identify sensitive or regulated data before training. (3) Control: Implement access restrictions, data minimization, and safeguards to protect sensitive information. (4) Monitor: Continuously audit data lineage, model performance, and vulnerabilities, with mechanisms to flag and contest outputs. (5) Improve: Iteratively refine governance based on audits, feedback, and evolving regulations to adapt to emerging AI risks (Mohan:2025).

7: AI Governance

AI governance is defined as a structured system of rules, practices, processes, and technological mechanisms designed to ensure that an organization's use of AI technologies is consistent with its strategic goals, objectives, and values, complies with applicable legal requirements, and adheres to the ethical AI principles followed by the organization (Birkstedt, Minkkinen, Tandon & Mäntymäki:2023). Effective governance requires policies that prioritize human-centric, trustworthy AI and safeguard health, safety, and fundamental rights. It also involves ensuring compliance with applicable legal and regulatory frameworks, such as the EU AI Act, across the jurisdictions in which organizations operate. Assigning clear responsibility for AI-driven decisions helps maintain human oversight and prevent misuse, while security and privacy measures protect data, prevent unauthorized access, and reduce potential cybersecurity risks

associated with AI systems (Farnham:2025). AI governance becomes critical when machine learning algorithms are used in decision-making processes, particularly when outcomes may adversely affect individuals. It provides structured guidance for managing situations in which AI-driven decisions could be unjust or infringe upon human rights. Biases in machine learning, such as those related to race or ethnicity, can lead to inaccurate identification of personal information, potentially resulting in the denial of essential services like healthcare or loans, or generating misleading information for law enforcement in the identification of criminal suspects (Gillis, Pour & Barney:2025).

8: AI Culture

AI culture refers to the collective values, beliefs, and behaviors that shape how individuals within an organization engage with AI and collaborate in AI-augmented environments. It is not merely a technological initiative but represents a fundamental shift in mindset, reshaping how people think, operate, and exercise leadership in the era of intelligent machines. AI culture emphasizes transforming established habits rather than simply deploying new tools. While organizations can readily invest in technology, altering ingrained mindsets is far more challenging. Without this cognitive and behavioral transformation, even the most advanced AI systems are unlikely to generate a sustainable impact (Verd:2025). In a mature workplace AI culture, teams consistently evaluate how AI should be integrated into business operations, thereby influencing the broader work environment and reinforcing organizational values (Williams:2024). Creating an AI culture requires critically examining existing assumptions, for example, questioning what the organization currently presumes about AI, whether these assumptions are shared, and how AI can be leveraged to achieve business objectives while remaining aligned with organizational values. Building an effective AI culture is not solely the responsibility of executive leadership; as with any cultural initiative, all employees should be empowered to contribute. Importantly, technical expertise in AI is not a prerequisite for meaningfully influencing AI culture; instead, a growth mindset and adaptability to change are essential for fostering an environment in which AI applications can thrive. Developing a robust AI culture requires alignment around a central vision of how AI supports the organization's goals, ensuring coherence with its assumptions, values, behaviors, and operational practices. This process demands patience, iterative learning, and openness to cultural evolution. Organizations that fail to cultivate their AI culture intentionally risk falling behind. A well-established and sustainable AI culture is a critical asset for harnessing AI's transformative potential and navigating an increasingly AI-integrated world (Soane & Newton: 2025).

9. AI Risk Management

AI risks emerge from both how these systems are designed and how they are deployed within real-world environments. As AI takes on increasingly consequential roles, it raises critical concerns related to fairness, privacy, security, and societal stability. These risks include diminished human control, exploitation by malicious actors, data-driven biases, inadequate oversight mechanisms, widespread disinformation, threats to intellectual property, and potential economic displacement. Such challenges are already becoming visible across global industries and public-sector systems, demonstrating that AI risks are immediate rather than speculative (WitnessAI:2025). Artificial intelligence (AI) risk management refers to the systematic identification, assessment, and mitigation of risks arising from the design, deployment, and use of AI systems. Unlike traditional IT risk management, AI risk management must address unique challenges, including low-quality or unrepresentative training data, model theft, algorithmic bias, and emergent or unpredictable behaviors. Given the continuously evolving nature of AI technologies, leading industry analyses emphasize that continuous risk management is necessary to ensure continuous assurance (Cardoso:2025). The National Institute of Standards and Technology (NIST) has introduced a comprehensive Artificial Intelligence Risk Management Framework (AI RMF) to support organizations in systematically identifying, assessing, and mitigating risks associated with AI systems. The framework offers a structured methodology that aligns AI initiatives with recognized best practices and emerging regulatory expectations, making it a foundational component of effective AI risk governance. It emphasizes four core functions: establishing clear governance and accountability mechanisms; mapping and contextualizing potential risks; measuring risks through qualitative and quantitative evaluation; and managing those risks through appropriate mitigation strategies. This integrated approach enables organizations to deploy AI responsibly while enhancing transparency, reliability, and trustworthiness (Pearcy:2025).

10: AI Performance and Value Management

AI Performance and Value Management (APVM) extends beyond the creation of dashboards, representing a structured governance framework that ensures AI systems are reliable, interpretable, secure, cost-efficient, and aligned with both organizational objectives and broader societal expectations. A critical component of this framework is the explicit definition of accountability: when a performance metric is breached, it must be clear who is responsible for investigating the deviation, validating the findings, and making the final decision. Organizations that establish such mechanisms proactively are better positioned to scale AI systems responsibly while maintaining stakeholder trust and confidence (Overtoom:2025). Complementing governance, AI metrics provide a rigorous, evidence-based approach to evaluating AI performance across both technical execution and business outcomes. By serving as the intersection of strategic intent and operational rigor, these metrics ensure that AI operations are reliable, transparent, and effective, supporting informed decision-making and continuous improvement (Heinig:2025).

Finally, AI ROI operationalizes the concept of value by quantifying the financial and operational benefits an organization derives from AI initiatives relative to their costs. This metric enables organizations to assess whether AI implementations deliver tangible value, including cost reductions, revenue growth, efficiency gains, improved customer experience, and risk mitigation (Thu:2025). Together, performance monitoring, metrics, and ROI form a cohesive APVM framework that links technical excellence to strategic and financial outcomes.

Conceptual Framework

This paper proposes a structured AI Management framework grounded in the postulation that encompasses the critical organizational factors required to initiate, execute, sustain, and continuously improve AI initiatives. It demonstrates complete AI Management across business and government organizations.

The AI Management Framework can be conceptualized as follows.

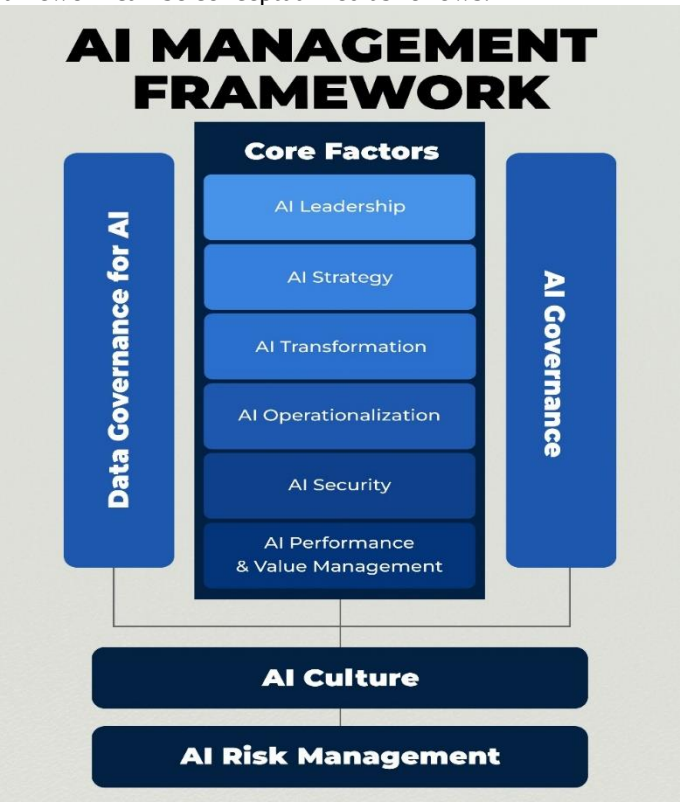

Figure 1: AI Management Framework

Core Factors – Vertical Column

1. AI Leadership

- Strategic capability to oversee ethical AI adoption and management.
- Aligns AI initiatives with long-term business objectives.

- Balances technological proficiency with understanding of organizational culture and human impact.
- Drives performance improvements via data, automation, and intelligent systems while upholding ethical standards.
- Establishes dedicated structures (e.g., Chief AI Officer, AI Steering Committee) to guide AI vision, resource allocation, and strategic priorities.

2. AI Strategy

- Structured approach to planning AI initiatives that deliver measurable business value.
- Integrates AI initiatives with overall organizational goals, enhancing productivity, innovation, efficiency, and profitability.
- Addresses risk management, ethics, regulatory compliance, governance, change management, and scalability.
- In public-sector contexts, guides prioritization, technology selection, talent sourcing, and alignment with national or organizational strategies.

3. AI Transformation

- Systematic integration of AI across operations, processes, and culture.
- Automates tasks, strengthens decision-making, optimizes workflows, and fosters innovation.
- Involves organizational realignment, re-engineering business models, and leveraging data for evidence-based decisions.
- Implementation follows assessment of readiness, prioritization of use cases, MVP deployment, and scaling for sustained competitive advantage.

4. AI Operationalization (ModelOps)

- Lifecycle management of all AI and decision models, including ML, rules-based, and optimization systems.
- Automates deployment, monitoring, governance, and continuous improvement.
- Supports reliability, adaptability, and continuous learning of AI models.
- Maturity progresses from manual, fragmented processes to CI/CD-driven lifecycle management with specialized skills or expertise as needed.

5. AI Security

- Protects AI systems, models, data, and pipelines from cyber threats and vulnerabilities.
- Preserves the integrity of training data and prevents model corruption or poisoning.
- Ensures privacy, bias mitigation, explainability, and compliance with legal/regulatory requirements.
- Focuses on safeguarding data, securing models, and protecting runtime environments against threats like adversarial inputs or data extraction.

6. AI Performance & Value Management (APVM)

- Governance framework ensuring AI systems are reliable, interpretable, secure, cost-efficient, and value-aligned.
- Explicit accountability for deviations in performance metrics.
- Uses technical and business metrics, along with ROI, to link AI execution with financial and operational outcomes.
- Supports continuous improvement and informed decision-making, aligning AI initiatives with strategic and societal goals.

Left Pillar – Data Governance for AI

- Structured policies, processes, and controls ensuring high-quality, secure, and ethical data management.
- Built on four pillars: data quality, privacy & security, stewardship & ownership, compliance & accountability.
- Addresses AI-specific challenges: dynamic learning, large-scale, heterogeneous data.

- Five-step framework: Charter → Classify → Control → Monitor → Improve, ensuring iterative risk mitigation and compliance.

Right Pillar – AI Governance

- Ensures AI use aligns with organizational goals, values, ethics, and legal frameworks.
- Prioritizes human-centric, trustworthy AI while safeguarding health, safety, and fundamental rights.
- Assigns responsibility for AI-driven decisions, mitigating bias and misuse.
- Critical when AI-driven outcomes may impact individuals' rights or essential services.

Cross-Cutting (Horizontal)

AI Culture

- Collective values, beliefs, and behaviors shaping how employees interact with AI.
- Emphasizes mindset transformation rather than only technology adoption.
- Encourages learning, adaptability, cross-functional collaboration, and value-aligned AI deployment.
- Requires organization-wide engagement; technical expertise is not mandatory, but a growth mindset and openness to change are essential.

AI Risk Management

- Systematic identification, assessment, and mitigation of AI-specific risks.
- Covers fairness, privacy, security, bias, emergent behavior, and societal impact.
- Follows structured frameworks (e.g., NIST AI RMF) emphasizing governance, risk mapping, measurement, and mitigation.
- Ensures continuous assurance, transparency, and responsible AI deployment.

This structure integrates leadership, strategy, operational execution, governance, data management, culture, and risk oversight into a unified framework, providing organizations with a comprehensive blueprint for effective, scalable, and sustainable AI adoption. From this unified framework, a complete definition of AI Management can be derived.

Definition of AI Management

This paper proposes a definition of AI Management based on the framework:
AI Management is an integrated discipline that integrates leadership, strategy, transformation processes, operational systems, performance and value management, cultural foundations, and risk oversight required to plan, build, deploy, secure, monitor, and continuously improve artificial intelligence across an organization. It ensures that AI technologies, together with supporting data governance and AI governance, remain aligned with strategic objectives, ethical principles, regulatory requirements, and broader societal expectations.

As a management field, AI Management coordinates interconnected domains:

- **AI Leadership** for vision, accountability, and strategic direction;
- **AI Strategy** for value-driven planning and prioritization;
- **AI Transformation** for organization-wide integration of AI into processes, workflows, and culture;
- **AI Operationalization** for lifecycle management of models and intelligent systems;
- **AI Security** to protect data, models, and pipelines;
- **AI Performance & Value Management** to ensure reliability, interpretability, efficiency, and measurable outcomes;

  Supported by the pillars of **Data Governance for AI** and **AI Governance**, and the cross-cutting dimensions of **AI Culture** and **AI Risk Management**.

AI Management functions as a **holistic, end-to-end management system**, ensuring that AI initiatives are trustworthy, secure, technically sound, ethically grounded, economically valuable, and operationally sustainable. It establishes the structures, competencies, and processes through which organizations can scale AI responsibly while enhancing human capability, organizational performance, and long-term societal benefit.

Impact

This paper introduces a novel management framework in the context of AI, establishing a foundation for a new subfield within the management domain. Theoretically, it provides a basis for future research, textbooks, and scholarly resources, while offering universities the opportunity to integrate AI Management into their curricula and certify professionals in this emerging field.

Practically, the framework equips organizations—both corporate and public—with a structured, sustainable, and effective approach to AI adoption. Managers can leverage this framework as a practical guideline to ensure systematic implementation, ethical alignment, and measurable value creation from AI initiatives.

Conclusion

Artificial Intelligence is reshaping business and public-sector organizations, yet its potential often remains underutilized due to strategic misalignment, fragmented governance, and limited managerial oversight. This paper introduces AI Management as a holistic subfield, providing a structured framework to guide ethical, secure, and value-driven AI adoption.

The framework integrates leadership, strategy, transformation, operationalization, security, governance, data management, culture, risk, and performance oversight into a unified model. It equips managers with actionable guidance to implement, sustain, and continuously improve AI initiatives, aligning them with organizational goals and societal expectations.

By bridging AI's transformative potential with practical execution, AI Management enables organizations to achieve measurable impact, operational excellence, and long-term sustainable value.

References

1. A., K. (2025). *AI transformation: Path to a smarter, efficient future*. USAII Insights. USAII. https://www.usaii.org/ai-insights/ai-transformation-path-to-a-smarter-efficient-future

2. AI21 Labs. (2025). *9 key AI governance frameworks in 2025*. AI21 Knowledge Hub. https://www.ai21.com/knowledge/ai-governance-frameworks

3. AIJ Guest Post. (2025). *Global AI governance: Five key frameworks explained*. The AI Journal. https://aijourn.com/global-ai-governance-five-key-frameworks-explained/

4. Barney, N., Hanna, K. T., & Bernstein, C. (2024, October 1). *What are ModelOps (model operations) analytics models?* TechTarget. https://www.techtarget.com/searchitoperations/definition/ModelOps

5. Bashir, J. (2024). *Strategic Enterprise Artificial Intelligence: The conceptual hierarchical framework. International Journal of Business & Management Studies, 5*(5). https://doi.org/10.56734/ijbms.v5n5a13

6. Berglind, N., Fadia, A., & Isherwood, T. (2022). *The potential value of AI—and how governments could look to capture it*. McKinsey & Company. https://www.mckinsey.com/industries/public-sector/our-insights/the-potential-value-of-ai-and-how-governments-could-look-to-capture-it

7. Birkstedt, T., Minkkinen, M., Tandon, A., & Mäntymäki, M. (2023). *AI governance: Themes, knowledge gaps and future agendas. Internet Research, 33*(7), 133–167. https://doi.org/10.1108/INTR-01-2022-0042

8. Cardoso, F. (2025). *What is AI risk management?* Trend Micro. https://www.trendmicro.com/en_us/what-is/ai/ai-risk-management.html

9. Craig. (2025). *Why 83% of Fortune 500 AI-Driven Digital Transformations Fail*. AskCraig.ai. https://askcraig.ai/articles/transformation/why-ai-driven-transformations-fail

10. Doone, B. (2024). *The critical importance of ModelOps in AI readiness*. 3Pillar Global. https://www.3pillarglobal.com/insights/blog/the-critical-importance-of-modelops-in-ai-readiness/

11. Eddy, N. (2025). *AI leadership: A guide to building AI strategy and governance*. *BizTech Magazine*. https://biztechmagazine.com/article/2025/11/ai-leadership-guide-building-ai-strategy-and-governance-perfcon

12. Eggers, W. D., Mendelson, T., Chew, B., & Kishnani, P. (2019). *Crafting an AI strategy for government leaders*. Deloitte Insights. https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/ai-strategy-for-government-leaders.html

13. Farnham, K. (2025). *AI governance: What it is & how to implement it*. Diligent Blog. https://www.diligent.com/resources/blog/ai-governance

14. Gillis, A. S., Hashemi-Pour, C., & Barney, N. (2025). *What is artificial intelligence (AI) governance?* SearchEnterpriseAI. TechTarget. https://www.techtarget.com/searchenterpriseai/definition/AI-governance (techtarget.com

15. Habibi, M. (2025). *What is AI security?* Trend Micro. https://www.trendmicro.com/en_us/what-is/ai/ai-security.html

16. Heinig, I. (2025). *AI metrics: How to measure and evaluate AI performance*. Sendbird Blog. https://sendbird.com/blog/ai-metrics-guide

17. Jennings, T. (2025). *Why AI security tools are different — and 9 tools to know in 2025*. Mend.io Blog. https://www.mend.io/blog/why-ai-security-tools-are-different-and-9-tools/

18. Jones, C. A. (2025). AI Leadership: Guiding Enterprises Through the Age of Intelligent Transformation. NetCom Learning Blog. https://www.netcomlearning.com/blog/ai-leadership

19. Kassa, B. Y. (2025). The mediating role of employee productivity. *Journal of Open Innovation: Technology, Market, and Complexity, 11*(1). https://www.sciencedirect.com/science/article/pii/S2199853125000095

20. Kimachia, K. (2023). *How to use data governance for AI/ML systems*. *TechRepublic*. https://www.techrepublic.com/article/data-governance-ai-systems/

21. Krishnamohan, A. (2025). *Why AI fails: The untold truths behind 2025's biggest tech letdowns*. TechFunnel. https://www.techfunnel.com/fintech/ft-latest/why-ai-fails-2025-lessons/

22. Marshall, C. (2025). *AI in government: How it's being used and future trends*. Zendesk. https://www.zendesk.com/blog/ai-in-government/

23. Mathew, A. (2025). *The AI transformation roadmap: A proven business process*. Ombrulla Blog. https://ombrulla.com/blog/ai-transformation-roadmap-business-process

24. Mayer, H., Yee, L., Chui, M., & Roberts, R. (2025). *Superagency in the workplace:Empowering people to unlock AI's full potential*. McKinsey & Company. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work

25. Mohan, P. (2025). *Data governance for AI: Framework & best practices*. Atlan. https://atlan.com/know/data-governance/for-ai/

26. Odilov, S. (2024). *AI leadership: Why AI is every leader's responsibility*. Forbes. https://www.forbes.com/sites/sherzododilov/2024/07/14/ai-leadership-why-ai-is-every-leaders-responsibility/

27. ODSC – Open Data Science. (2021). *ModelOps — AI model operationalization for the enterprise*. Medium. https://odsc.medium.com/modelops-ai-model-operationalization-for-the-enterprise-61f36213a636

28. Organisation for Economic Co-operation and Development. (2025). *Governing with artificial intelligence: The state of play and way forward in core government functions*. OECD Publishing. https://doi.org/10.1787/795de142-en

29. Overtoom, B. (2025). *AI performance management: From monitoring to managed trust*. Nemko Digital Insights. https://digital.nemko.com/insights/ai-performance-management-from-monitoring-to-managed-trust

30. Pearcy, S. (2025). *AI risk management: Effective strategies and framework*. HiddenLayer Innovation Hub. https://hiddenlayer.com/innovation-hub/ai-risk-management-effective-strategies-and-framework/

31. Pratt, M. K. (2024). *How to create a winning AI strategy for your business*. *SearchEnterpriseAI*. TechTarget. https://www.techtarget.com/searchenterpriseai/tip/How-to-formulate-a-winning-AI-strategy

32. Soane, E., & Newton, R. (2025). *Four ways to define your AI culture*. *Forbes*.

https://www.forbes.com/sites/londonschoolofeconomics/2025/01/16/four-ways-to-define-your-ai-culture/

33. Thu, H. D. (2025). *AI return on investment (ROI): Unlocking the true value of artificial intelligence for your business*. SmartDev. https://smartdev.com/ai-return-on-investment-roi-unlocking-the-true-value-of-artificial-intelligence-for-your-business/

34. Uba, C., Lewandowski, T., & Böhmann, T. (2023). *The AI-based transformation of organizations: A 3D-Model for enterprise-wide change* (Master's thesis). University of Hawai'i at Mānoa. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/bf1f654f-1b68-49e4-985c-69164ed5b415/content

35. Verd, N. (2025). *AI culture: The missing ingredient in your AI business strategy*. Medium. https://medium.com/@nickyverd/ai-culture-the-missing-ingredient-in-your-ai-business-strategy-d99d52b8b23d

36. Vu, H. (2025). *AI transformation: How top companies are revolutionizing business with AI solutions*. SotaTek Blog. https://www.sotatek.com/blogs/ai-transformation/

37. Williams, C. (2024). *5 steps to build a successful workplace AI culture*. Multiverse Blog. https://www.multiverse.io/en-GB/blog/5-steps-to-build-a-successful-workplace-ai-culture

38. WitnessAI. (2025). *Understanding AI risks: A comprehensive guide to the dangers of artificial intelligence*. WitnessAI Blog. https://witness.ai/blog/ai-risks/

