Int. J. Adv. Res. in Artificial Intelligence and Machine Learning Reviews
Volume 2, Issue 1 - 2026, Pg. No. 1-13
Peer Reviewed Journal

Research Article

AI-Driven IT Management: A Framework for Strategic Implementation and Risk Mitigation

Anushka Shashikant Bhamre

Assistant Professor, K.B.H.S.S. Trust's Indira College, Malegaon, Nashik, Maharashtra, India

INFO

E-mail Id:
anushkabhamre05@gmail.com
Orcid Id:
https://orcid.org/0009-0001-6484-3387

How to cite this article:
Bhamre A S, AI-Driven IT Management: A Framework for Strategic Implementation and Risk Mitigation. *Int J Adv Res Artif Intell Mach Learn Rev* 2026; 2(1): 1-13.

Date of Submission: 2025-12-15
Date of Acceptance: 2026-02-22

ABSTRACT

Artificial Intelligence (AI) has become a significant influence in IT management, altering strategic decision-making, automation, and risk management processes. The incorporation of AI into IT operations equips organisations with sophisticated tools to enhance efficiency, optimise resources, anticipate threats, and improve service delivery. This research examined the viewpoints of 230 participants, comprising IT professionals, managers, and decision-makers, to investigate the adoption, challenges, and risk mitigation strategies related to AI-driven IT management. The research employed demographic profiling in conjunction with four key dimensions of quantitative data analysis: (1) strategic implementation, (2) operational efficiency, (3) risk mitigation, and (4) organisational impact. The findings indicated that a structured framework that includes employee training, governance mechanisms, and scalable AI infrastructure is essential for effective implementation.

Keywords: AI in IT management; Digital transformation, organisational efficiency, strategic implementation, risk mitigation, and automation.

Introduction

The rapid development of information technology (IT) has transformed organisational processes, making IT management crucial for strategic decision-making. With the advancement of digital transformation, IT managers face the challenge of sustaining operational efficiency while managing risks related to security, compliance, and infrastructure management. Artificial Intelligence (AI) has developed into a transformative technology in this field, providing sophisticated solutions for automation, predictive analytics, and risk detection. AI-driven IT management employs machine learning algorithms, natural language processing, and intelligent automation to optimise IT operations, minimise downtime, and improve organisational agility.[1] The integration of AI and IT management represents not just a technological enhancement but a strategic imperative for organisations seeking to maintain competitiveness in a progressively digital economy.

The potential of AI to enhance operational efficiency is a significant aspect of IT management. Conventional IT management depends significantly on human oversight and manual problem-solving, leading to potential delays and inaccuracies. Artificial intelligence facilitates proactive monitoring, enhances resource utilisation, and accelerates incident resolution through predictive analytics and intelligent automation.[2] Artificial intelligence systems can predict hardware failures and autonomously redistribute workloads, thus minimising service interruptions. These applications demonstrate AI's capacity to shift IT operations from reactive to proactive models, thereby ensuring continuous service delivery.

Risk mitigation constitutes a critical component of AI integration within IT management. Cybersecurity risks, data breaches, and compliance violations pose considerable challenges for organisations.[3] argue that artificial intelligence facilitates the creation of sophisticated security systems that can identify anomalies, anticipate vulnerabilities, and react to cyber incidents in real time. Machine learning algorithms analyse extensive data streams to detect anomalous patterns indicative of cyberattacks, thus enhancing organisational resilience. Artificial intelligence functions as a catalyst for improving efficiency and is essential for risk mitigation in IT management systems.

The strategic implications of AI implementation extend beyond mere operational advantages. Organisations that incorporate AI into IT management gain competitive advantages through improved decision-making processes, increased customer satisfaction, and the promotion of innovative business models. AI-driven IT frameworks allow senior managers to align technological capabilities with long-term business objectives, ensuring that IT functions serve as facilitators of growth rather than cost centres.[4] The use of AI improves organisational agility, enabling companies to respond quickly to market fluctuations and emerging technological developments.

This study analyses the function of AI in IT management, emphasising strategic implementation and frameworks for risk mitigation. This study surveys 230 respondents from various organisational contexts to examine the adoption of AI-driven IT systems, identify encountered challenges, and explore strategies for maximising benefits while minimising risks. The results aim to improve academic discourse and practical applications by proposing a structured framework for AI-based IT management.

Review of Literature

Research on the application of artificial intelligence (AI) to IT management has accelerated over the last decade as organisations confronted exponentially larger streams of operational data and more complex service environments. The term 'AIOps' — Artificial Intelligence for IT Operations — emerged to describe the combination of big-data platforms, machine learning, and analytics to automate and improve IT operations tasks such as event correlation, anomaly detection, root-cause analysis, and automated remediation.[5] Gartner's conceptualisation underlined how scale (volume, variety, velocity) of telemetry from modern systems rendered manual practices insufficient and how algorithmic approaches promised to move IT from reactive troubleshooting toward proactive, predictive operations. Reports from industry and academia have documented initial production deployments of AIOps workflows that have shown measurable improvements in incident classification and reduced mean time to resolution.[6] Levin et al. discussed insights gained from the development of an AIOps platform for a substantial cloud object storage service, highlighting the engineering challenges associated with heterogeneous data ingestion, the limited availability of labels for supervised models, and the necessity of incorporating human-in-the-loop processes to maintain operational effectiveness.[6]

Applying predictive analytics to logs, telemetry, and sensor data enables organisations to foresee component degradation and take corrective actions prior to failures, thereby transitioning maintenance from a reactive approach to a condition-based strategy.[7] refer to recent surveys on predictive monitoring). The predictive maintenance framework utilising machine learning showed potential for cost reduction; however, it encountered practical challenges. These included the necessity for representative historical failure data, meticulous feature engineering, and ongoing retraining to maintain accuracy across diverse workloads and system configurations. Model management and data management pose significant operational challenges for model shifting, observability AND lifecycle management of AI systems in IT environments.[6,7] The focus of research in the field of cyber, cybersecurity, is the evaluation of artificial intelligence methodology in practical IT operating environments. Seriously, early applications, such as MIT's artificial intelligence system, combined unsupervised outlier detection with analyst feedback to efficiently sort millions of log lines per day. This method significantly decreased human workload and effectively identified a considerable number of authentic attacks.[8] Such hybrid human-machine systems illustrated the practical value of augmenting — rather than replacing — security analysts, since attackers and benign operational patterns both evolve over time.

In addition to operational performance, a substantial body of literature has explored human-automation interaction, governance, and ethical considerations that are pivotal to the adoption of AI in IT management. Foundational work on automation highlighted that the benefits and hazards of automation depend strongly on what functions are automated and at what level, and that poor design choices can produce automation surprises, skill degradation, and coordination problems.[9] Contemporary AI systems intensify these challenges owing to their diminished transparency and heightened adaptability in relation to conventional automation. Organisations must consider model interpretability, explainability, and the allocation of responsibility when automated decisions affect critical services. Research on ethics and policy emphasises that the dual-use risks, potential for misuse, and systemic vulnerabilities linked to AI require the development of governance frameworks, standards, and collaboration among diverse stakeholders.[3,10] The works contend that technical solutions are inadequate; institutional frameworks – encompassing defined accountability, human oversight, and effective incident response mechanisms – are essential for mitigating emerging risks.

The strategic and economic effects of artificial intelligence on organisations have been investigated using empirical and analytical methods. Macro and industry studies indicate that investments in AI can lead to significant productivity enhancements; however, the actual benefits are largely contingent upon complementary assets such as data availability, skilled personnel, organisational processes, and managerial commitment.[4] Successful AI-driven IT management necessitates alignment with business objectives, financial investment in tools and personnel, and a cultural shift to incorporate AI outputs into decision-making processes. Both academic and practitioner analyses of AIOps implementations indicate that the technology's value is typically realised when there is support from senior leadership for adoption, governance frameworks are established to ensure responsible use, and frontline teams receive retraining to collaborate effectively with algorithmic assistants.[4,6]

Research on the malicious applications of AI and system vulnerabilities.[3] highlights the potential for adversaries to weaponise AI tools, automate reconnaissance, and design attacks that specifically target and confuse predictive models. Deployment case studies highlight the practical advantages organisations can achieve by effectively integrating algorithmic detection, human judgement, and strong governance.[8,6] The synthesis of prior work, therefore, points to a balanced research agenda: one that investigates technical methods for robust anomaly detection and predictive maintenance; organisational pathways for aligning AI projects with strategy and skills; and governance mechanisms that mitigate ethical, security, and operational risks.[11] This paper builds on those threads by empirically examining practitioner perspectives on strategic implementation and risk mitigation for AI-driven IT management and by proposing a framework that integrates technical, human, and governance dimensions.[12]

Research Objectives

- To investigate the impact of AI adoption on the strategic implementation of IT management systems.
- To assess the impact of AI on improving operational efficiency in IT departments.
- To examine the role of AI in enhancing risk mitigation within IT management practices.
- To examine the effects of AI adoption at the organisational level, focusing on productivity, decision-making, and customer satisfaction.
- To examine demographic variations in the perception and acceptance of AI-driven IT management frameworks.

Research Methodology

A cross-sectional survey research design was employed to investigate the strategic implementation and risk mitigation capabilities related to AI-driven IT management. This design was deemed suitable as it facilitated the gathering of varied perspectives from IT professionals and decision-makers across multiple sectors at a particular moment. The research included a sample of 230 participants, comprising IT managers, administrators, senior leaders, AI specialists, and consultants from organisations of varying sizes: small, medium, and large. This provided a comprehensive examination of viewpoints regarding the integration of AI into IT management.

A stratified random sampling method was employed to ensure equitable representation across various demographic factors, including age, education, work experience, and organisational size. This technique facilitated a thorough examination of varied viewpoints regarding the use of AI and its associated risks among individuals from different professional and organisational contexts. The use of random selection within each stratum effectively reduces bias and improves the analysis of ideas specific to each group.

The methodology used structured online surveys, enabling an efficient, comprehensive and economical approach to data collection. The study employed descriptive and inferential statistical methods. The examination of demographic patterns and trends in AI adoption employed descriptive statistics for summarisation, while inferential tests were utilised to explore relationships and differences among demographic groups. Reliability analysis and factor analysis were then performed to validate constructs related to AI acceptance, competence, risk management, and organisational outcomes.

The proposed hypotheses for this investigation are outlined as follows:

Hypothesis 1

- **H_0**: "There exists no significant correlation between the adoption of AI and the strategic execution of IT management."
- **H_1**: "A notable correlation exists between the adoption of AI and the strategic execution of IT management."

Hypothesis 2

- **H_0**: "The implementation of AI-driven IT management does not yield a statistically significant enhancement in operational efficiency."
- **H_1**: "AI-driven IT management leads to a notable enhancement in operational efficiency."

Hypothesis 3

- **H_0**: "There exists no significant correlation between the adoption of AI and the mitigation of risk within the realm of IT management."
- **H_1**: "A significant relationship exists between the adoption of AI and the mitigation of risks in IT management."

Hypothesis 4

- **H_0**: "There are no significant demographic differences in perceptions of AI-driven IT management."

- **H_1**: "Significant demographic differences exist in the perceptions of AI-driven IT management."

Empirical Results

Section A: Demographic Questions

Interpretation

The largest proportion of respondents (35.65%) belonged to the age group of 26–35 years, indicating that early- to mid-career professionals were the primary contributors to the study. A smaller but significant group (23.48%) were aged 36–45 years, suggesting participation from experienced professionals. Respondents above 55 years made up only 7.39%, reflecting limited engagement from senior-most practitioners (table 1).

Interpretation

Males accounted for 53.91% of the total respondents, while females represented 45.65%. Only one respondent (0.43%) identified as "Other", reflecting minimal representation of non-binary categories. The nearly balanced gender distribution demonstrates inclusivity in perspectives(table2).

Interpretation

Respondents with a bachelor's degree constituted the largest group at 38.70%, followed by those holding a master's degree at 33.91%. A smaller proportion, 8.26%, had completed doctorates, showing some representation from highly qualified professionals. This educational spread indicates that the study attracted participants with substantial academic backgrounds in IT(table 3).

Interpretation

The majority of respondents had between 6 and 10 years of IT experience (31.30%), followed closely by those with 2–5 years (29.13%). This indicates strong participation from mid-level professionals. Respondents with over 15 years of experience were only 10.43%, suggesting fewer contributions from veteran experts (table 4).

Table 1.Age Group of Respondents

Age Group	Frequency	Percentage	Valid Percentage	Cumulative Percentage
18–25 years	46	20.00%	20.00%	20.00%
26–35 years	82	35.65%	35.65%	55.65%
36–45 years	54	23.48%	23.48%	79.13%
46–55 years	31	13.48%	13.48%	92.61%
Above 55 years	17	7.39%	7.39%	100.00%
Total	230	100.00%	100.00%	

Table 2.Gender Distribution of Respondents

Gender	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Male	124	53.91%	53.91%	53.91%
Female	105	45.65%	45.65%	99.57%
Other	1	0.43%	0.43%	100.00%
Total	230	100.00%	100.00%	

Table 3.Educational Qualification

Educational Qualification	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Diploma/Certification in IT	27	11.74%	11.74%	11.74%
Bachelor's Degree	89	38.70%	38.70%	50.43%
Master's Degree	78	33.91%	33.91%	84.35%
Doctorate/PhD	19	8.26%	8.26%	92.61%
Others	17	7.39%	7.39%	100.00%
Total	230	100.00%	100.00%	

Table 4.Work Experience in IT Sector

Work Experience	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Less than 2 years	28	12.17%	12.17%	12.17%
2–5 years	67	29.13%	29.13%	41.30%
6–10 years	72	31.30%	31.30%	72.61%
11–15 years	39	16.96%	16.96%	89.57%
More than 15 years	24	10.43%	10.43%	100.00%

Total	230	100.00%	100.00%	

Interpretation

IT managers/team leads formed the largest group of respondents (26.96%), followed by administrators/ technicians (23.04%). Data scientists/AI specialists accounted for 17.83%, reflecting notable participation from emerging technology professionals (table 5). Senior management and consultants were represented equally at 16.09%.

Interpretation

The highest proportion of respondents were from medium enterprises (25.65%), while large and very large enterprises each contributed more than 22%. Government and non-profit organisations represented 11.74%, indicating some engagement from the public sector. This distribution shows the study's coverage across varied organisational types(table 6).

Section B: Quantitative Questions

Category I: Strategic Implementation of AI in IT Management

Interpretation

A majority of respondents (35.22% agreed and 22.61% strongly agreed) indicated that their organisations had a clear AI adoption roadmap, making up more than half the sample. About one-fifth remained neutral (20.43%), and 21.74% disagreed to varying degrees, suggesting that while strategic clarity exists in most organisations, gaps remain in certain cases(table 7).

Interpretation

Nearly 59.13% of respondents agreed that AI adoption aligns with long-term strategy, with 24.78% strongly agreeing. A smaller group (23.04%) expressed disagreement, showing that alignment is not uniform across all organisations(table8).

Table 5.Current Role in Organization

Current Role	Frequency	Percentage	Valid Percentage	Cumulative Percentage
IT Administrator/ Technician	53	23.04%	23.04%	23.04%
IT Manager/Team Lead	62	26.96%	26.96%	50.00%
Senior Management/ Director	37	16.09%	16.09%	66.09%
Data Scientist/AI Specialist	41	17.83%	17.83%	83.91%
Consultant/Other	37	16.09%	16.09%	100.00%
Total	230	100.00%	100.00%	

Table 6.Organization Type

Organization Type	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Small Enterprise (<100)	41	17.83%	17.83%	17.83%
Medium Enterprise (100–499)	59	25.65%	25.65%	43.48%
Large Enterprise (500–1000)	52	22.61%	22.61%	66.09%
Very Large Enterprise (>1000)	51	22.17%	22.17%	88.26%
Government/Non-profit	27	11.74%	11.74%	100.00%
Total	230	100.00%	100.00%	

Table 7.My organization has a clear AI adoption roadmap for IT management

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	52	22.61%	22.61%	22.61%
Agree	81	35.22%	35.22%	57.83%
Neutral	47	20.43%	20.43%	78.26%
Disagree	34	14.78%	14.78%	93.04%
Strongly Disagree	16	6.96%	6.96%	100.00%

Total	230	100.00%	100.00%	

Table 8.AI adoption in IT is aligned with our long-term business strategy

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	57	24.78%	24.78%	24.78%
Agree	79	34.35%	34.35%	59.13%
Neutral	41	17.83%	17.83%	76.96%
Disagree	36	15.65%	15.65%	92.61%
Strongly Disagree	17	7.39%	7.39%	100.00%
Total	230	100.00%	100.00%	

Interpretation

Management support for AI was evident, with 57.39% of respondents agreeing or strongly agreeing. However, 23.48% reported disagreement, suggesting that leadership backing is inconsistent across organisations(table 9).

Interpretation

A combined 51.30% of respondents agreed that AI adoption was well-integrated into IT governance. Meanwhile, almost one-fourth (23.91%) were neutral, and another quarter (24.78%) disagreed, indicating mixed maturity levels in governance integration(table 10).

Interpretation

While 47.39% agreed that adequate resources are allocated, a large portion (25.65%) remained neutral, and 26.96% disagreed. This suggests budgetary constraints are a concern in many organisations(table 11)

Interpretation

Only 46.52% agreed that employees receive adequate training for AI-driven IT solutions, while a notable 26.09% were neutral and 27.39% disagreed. This highlights training as a key area needing improvement in AI adoption(table 12).

Table 9.Senior management actively supports AI initiatives in IT operations

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	49	21.30%	21.30%	21.30%
Agree	83	36.09%	36.09%	57.39%
Neutral	44	19.13%	19.13%	76.52%
Disagree	36	15.65%	15.65%	92.17%
Strongly Disagree	18	7.83%	7.83%	100.00%
Total	230	100.00%	100.00%	

Table 10.AI adoption has been well-integrated into our IT governance structure

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	42	18.26%	18.26%	18.26%
Agree	76	33.04%	33.04%	51.30%
Neutral	55	23.91%	23.91%	75.22%
Disagree	38	16.52%	16.52%	91.74%
Strongly Disagree	19	8.26%	8.26%	100.00%
Total	230	100.00%	100.00%	

Table 11.Adequate budget and resources are allocated for AI-driven IT projects

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	38	16.52%	16.52%	16.52%
Agree	71	30.87%	30.87%	47.39%
Neutral	59	25.65%	25.65%	73.04%
Disagree	42	18.26%	18.26%	91.30%
Strongly Disagree	20	8.70%	8.70%	100.00%
Total	230	100.00%	100.00%	

Table 12.Employees are trained to adapt to AI-driven IT solutionss

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	41	17.83%	17.83%	17.83%
Agree	66	28.70%	28.70%	46.52%
Neutral	60	26.09%	26.09%	72.61%
Disagree	40	17.39%	17.39%	90.00%
Strongly Disagree	23	10.00%	10.00%	100.00%
Total	230	100.00%	100.00%	

Category 2: Operational Efficiency through AI in IT

Interpretation

A majority of respondents (59.13%) agreed or strongly agreed that AI reduced the time to resolve IT issues, while only 22.17% expressed disagreement. The findings suggest AI significantly accelerates IT problem resolution, though a small fraction of respondents remain unconvinced (table 13).

Interpretation

Over half of the respondents (58.26%) believed AI helps in optimising IT resources. Nearly one-fifth (19.57%) stayed neutral, while 22.18% disagreed. This reflects broad confidence in AI's role in resource utilisation, though a minority remain skeptical (table 14).

Interpretation

More than half of the respondents (56.52%) acknowledged that predictive analytics improved IT maintenance, while 23.48% opposed this view. The remaining 20% stayed neutral, indicating that although predictive AI is widely valued, its application may not be uniformly adopted across organisations (table 15).

Interpretation

Just over half the respondents (53.91%) agreed or strongly agreed that automation reduced IT costs. However, more than one-fifth (21.30%) were neutral, and 24.78% disagreed, showing that while cost benefits exist, they may not be realised equally across organisations (table 16).

Table 13.AI has reduced the time required to resolve IT-related issues

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	54	23.48%	23.48%	23.48%
Agree	82	35.65%	35.65%	59.13%
Neutral	43	18.70%	18.70%	77.83%
Disagree	34	14.78%	14.78%	92.61%
Strongly Disagree	17	7.39%	7.39%	100.00%
Total	230	100.00%	100.00%	

Table 14.AI systems help in optimizing IT resources (e.g., servers, storage)

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	48	20.87%	20.87%	20.87%
Agree	86	37.39%	37.39%	58.26%
Neutral	45	19.57%	19.57%	77.83%
Disagree	33	14.35%	14.35%	92.17%
Strongly Disagree	18	7.83%	7.83%	100.00%
Total	230	100.00%	100.00%	

Table 15.Predictive analytics powered by AI has improved IT maintenance

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	53	23.04%	23.04%	23.04%
Agree	77	33.48%	33.48%	56.52%
Neutral	46	20.00%	20.00%	76.52%
Disagree	36	15.65%	15.65%	92.17%

pISSN :3117-4795
eISSN :3117-4809

Strongly Disagree	18	7.83%	7.83%	100.00%
Total	230	100.00%	100.00%	

Table 16.Automation through AI has lowered operational costs in IT management

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	44	19.13%	19.13%	19.13%
Agree	80	34.78%	34.78%	53.91%
Neutral	49	21.30%	21.30%	75.22%
Disagree	38	16.52%	16.52%	91.74%
Strongly Disagree	19	8.26%	8.26%	100.00%
Total	230	100.00%	100.00%	

Interpretation

A total of 57.39% believed AI enhances service desk operations. Yet, 24.79% disagreed and 17.83% were neutral, reflecting that while most organisations observe improvements, user experience with AI-driven service desks may vary (table 17).

Interpretation

Most respondents (57.39%) confirmed that AI enhances real-time monitoring, with only 24.35% expressing disagreement. The results highlight AI's growing value in system oversight, though some organisations still face challenges in full implementation (table 18).

Category 3: Risk Mitigation through AI in IT

Interpretation

Nearly 59.13% of respondents agreed or strongly agreed that AI enhances real-time cybersecurity threat detection. Around one-fifth (19.57%) were neutral, while 21.30% disagreed, indicating that while most organisations value AI in cybersecurity, some still struggle with its consistent performance (table 19).

Table 17.AI improves service desk operations by resolving queries faster

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	50	21.74%	21.74%	21.74%
Agree	82	35.65%	35.65%	57.39%
Neutral	41	17.83%	17.83%	75.22%
Disagree	39	16.96%	16.96%	92.17%
Strongly Disagree	18	7.83%	7.83%	100.00%
Total	230	100.00%	100.00%	

Table 18.AI tools enhance real-time IT system monitoring

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	47	20.43%	20.43%	20.43%
Agree	85	36.96%	36.96%	57.39%
Neutral	42	18.26%	18.26%	75.65%
Disagree	37	16.09%	16.09%	91.74%
Strongly Disagree	19	8.26%	8.26%	100.00%
Total	230	100.00%	100.00%	

Table 19.AI improves the detection of cybersecurity threats in real time

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	59	25.65%	25.65%	25.65%
Agree	77	33.48%	33.48%	59.13%
Neutral	45	19.57%	19.57%	78.70%
Disagree	32	13.91%	13.91%	92.61%
Strongly Disagree	17	7.39%	7.39%	100.00%
Total	230	100.00%	100.00%	

pISSN :3117-4795
eISSN :3117-4809

Interpretation

A majority (58.26%) agreed that AI reduces human error in IT management, but 23.48% expressed disagreement. The neutral group (18.26%) indicates that while many organisations observe benefits, the effectiveness of AI in error reduction may not yet be fully realised everywhere(table 20).

Interpretation

More than half (55.22%) agreed that AI strengthens disaster recovery planning and execution, while 24.79% disagreed. The neutral stance of 20% suggests that disaster recovery integration with AI is progressing but still not universally robust (table 21).

Interpretation

A combined 54.78% agreed that AI aids compliance and regulatory adherence, though 23.91% disagreed and 21.30% were neutral. This suggests AI plays a growing but uneven role in supporting IT compliance processes (table 22).

Interpretation

A majority (56.52%) agreed that AI strengthens IT risk forecasting. However, 24.79% disagreed, highlighting that while AI tools enhance foresight, some organisations may not yet rely on AI fully for infrastructure-related risk planning (table 23).

Interpretation

More than half (56.52%) believed AI helps minimise data breaches through anomaly detection, though 24.79% disagreed. With 18.70% neutral, the results show that while AI-driven security is widely acknowledged, challenges remain in its universal application (table 24).

Table 20.AI-driven systems reduce the chances of human error in IT management

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	53	23.04%	23.04%	23.04%
Agree	81	35.22%	35.22%	58.26%
Neutral	42	18.26%	18.26%	76.52%
Disagree	36	15.65%	15.65%	92.17%
Strongly Disagree	18	7.83%	7.83%	100.00%
Total	230	100.00%	100.00%	

Table 21.AI enhances disaster recovery planning and execution

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	48	20.87%	20.87%	20.87%
Agree	79	34.35%	34.35%	55.22%
Neutral	46	20.00%	20.00%	75.22%
Disagree	39	16.96%	16.96%	92.17%
Strongly Disagree	18	7.83%	7.83%	100.00%
Total	230	100.00%	100.00%	

Table 22.AI contributes to compliance and regulatory requirements in IT

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	44	19.13%	19.13%	19.13%
Agree	82	35.65%	35.65%	54.78%
Neutral	49	21.30%	21.30%	76.09%
Disagree	36	15.65%	15.65%	91.74%
Strongly Disagree	19	8.26%	8.26%	100.00%
Total	230	100.00%	100.00%	

Table 23.AI strengthens risk forecasting for IT infrastructure

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	52	22.61%	22.61%	22.61%
Agree	78	33.91%	33.91%	56.52%
Neutral	43	18.70%	18.70%	75.22%
Disagree	39	16.96%	16.96%	92.17%
Strongly Disagree	18	7.83%	7.83%	100.00%

Total	230	100.00%	100.00%	

Table 24.AI tools minimize data breaches by identifying unusual behavior

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	50	21.74%	21.74%	21.74%
Agree	80	34.78%	34.78%	56.52%
Neutral	43	18.70%	18.70%	75.22%
Disagree	37	16.09%	16.09%	91.30%
Strongly Disagree	20	8.70%	8.70%	100.00%
Total	230	100.00%	100.00%	

Category 4: AI-Driven Decision-Making in IT Management

Interpretation

A combined 59.57% agreed or strongly agreed that AI adoption has significantly boosted IT department productivity. Neutral responses accounted for 18.70%, while about 21.74% disagreed, showing that although AI is widely perceived as beneficial, its full potential may not yet be realised across all organisations.

Interpretation

Nearly 60% of respondents believed AI integration improves managerial decision-making, while 18.26% remained neutral and 21.74% disagreed. This reflects growing confidence in AI's analytical role but also indicates caution among some managers who may still rely on traditional approaches.

Interpretation

More than half of respondents (56.96%) agreed that AI enhances customer satisfaction in IT services, but 23.92% disagreed and 19.13% were neutral. This shows that while AI-driven IT management improves user experiences for many, organisations must still address concerns around service consistency and personalization (table 27).

Interpretation

Almost 60% agreed that AI-driven IT management provides a competitive advantage, while 17.83% remained neutral and 22.61% disagreed. This suggests that although AI is increasingly seen as a driver of strategic advantage, some organisations may still lack the maturity to translate AI adoption into tangible business competitiveness (table 28).

Table 25.AI adoption has increased overall productivity within the IT department

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	56	24.35%	24.35%	24.35%
Agree	81	35.22%	35.22%	59.57%
Neutral	43	18.70%	18.70%	78.26%
Disagree	32	13.91%	13.91%	92.17%
Strongly Disagree	18	7.83%	7.83%	100.00%
Total	230	100.00%	100.00%	

Table 26.AI integration improves decision-making at managerial levels

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	61	26.52%	26.52%	26.52%
Agree	77	33.48%	33.48%	60.00%
Neutral	42	18.26%	18.26%	78.26%
Disagree	32	13.91%	13.91%	92.17%
Strongly Disagree	18	7.83%	7.83%	100.00%
Total	230	100.00%	100.00%	

Table 27.AI adoption enhances customer/end-user satisfaction in IT services

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	52	22.61%	22.61%	22.61%
Agree	79	34.35%	34.35%	56.96%
Neutral	44	19.13%	19.13%	76.09%

Disagree	37	16.09%	16.09%	92.18%
Strongly Disagree	18	7.83%	7.83%	100.00%
Total	230	100.00%	100.00%	

Table 28.AI-driven IT management provides a competitive advantage to the organization

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	55	23.91%	23.91%	23.91%
Agree	82	35.65%	35.65%	59.56%
Neutral	41	17.83%	17.83%	77.39%
Disagree	33	14.35%	14.35%	91.74%
Strongly Disagree	19	8.26%	8.26%	100.00%
Total	230	100.00%	100.00%	

Interpretation

A total of 56.52% felt that AI adoption has encouraged IT team innovation, while 25.22% disagreed and 18.26% were neutral. This indicates that while AI fosters creative problem-solving in many cases, the perception of innovation varies depending on organisational culture and resource availability(table 29).

Interpretation

More than half (56.52%) reported that ROI from AI adoption is positive, though 24.78% disagreed and 18.70% were neutral. This suggests that AI investment is generally paying off, but the degree of financial return may vary based on how effectively organisations implement and integrate AI systems (table 30).

Hypothesis Testing

Hypothesis I

Interpretation

The association between AI adoption and strategic implementation of IT management was examined using the Chi-Square Test of Independence. The Pearson Chi-Square value of 42.156 with 4 degrees of freedom yielded a p-value of 0.000, which is below the 0.05 threshold. This indicates a statistically significant association between AI adoption and strategic IT implementation. Organisations with clear AI adoption roadmaps and management support reported higher alignment with strategic IT goals. Therefore, H_0 is rejected, and H_1 is accepted (table 31).

Table 29.AI integration has encouraged innovation within the IT team

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	49	21.30%	21.30%	21.30%
Agree	81	35.22%	35.22%	56.52%
Neutral	42	18.26%	18.26%	74.78%
Disagree	39	16.96%	16.96%	91.74%
Strongly Disagree	19	8.26%	8.26%	100.00%
Total	230	100.00%	100.00%	

Table 30.The overall return on investment (ROI) from AI adoption is positive

Response	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Agree	47	20.43%	20.43%	20.43%
Agree	83	36.09%	36.09%	56.52%
Neutral	43	18.70%	18.70%	75.22%
Disagree	36	15.65%	15.65%	90.87%
Strongly Disagree	21	9.13%	9.13%	100.00%
Total	230	100.00%	100.00%	

Table 31.Chi-Square Test for Association Between AI Adoption and Strategic Implementation of IT Management

Value	df	Asymp. Sig.
Pearson Chi-Square	42.156	4
Likelihood Ratio	45.321	4
N of Valid Cases	230	

Hypothesis 2

Interpretation

A one-way ANOVA was conducted to assess operational efficiency improvements due to AI-driven IT management across different levels of AI adoption. The F-value of 12.134 with p = 0.000 indicates statistically significant differences in efficiency. Respondents reporting strong AI integration (e.g., predictive analytics and automation) reported higher operational efficiency than those with limited AI adoption. Hence, H_0 is rejected, and H_1 is accepted(table 32).

Hypothesis 3

Interpretation

Regression analysis indicated that AI adoption had a significant positive effect on risk mitigation in IT management ($\beta = 0.621$, $p = 0.000$). AI-driven tools such as real-time monitoring, anomaly detection, and predictive analytics significantly contributed to reducing cybersecurity threats and minimising human error ($\beta = 0.462$, $p = 0.000$). The inclusion of cybersecurity measures as a mediator increased the explained variance in risk mitigation ($R^2 = 0.448$), confirming that AI adoption substantially strengthens IT risk management. H_0 is rejected, and H_1 is accepted(table 33).

Hypothesis 4

Interpretation

A one-way ANOVA assessed differences in perceptions of AI-driven IT management across age groups, gender, education, and work experience. The F-value of 6.382 with p = 0.000 indicates statistically significant differences. For instance, younger professionals (26–35 years) and mid-level managers (IT managers/team leads) perceived AI adoption more positively compared to senior management or less experienced staff. Educational qualification also influenced perception, with master's and bachelor's degree holders reporting higher satisfaction with AI-driven IT initiatives. Therefore, H_0 is rejected, and H_1 is accepted (table 34).

Table 32.Anova Test For Differences In Operational Efficiency Due To Ai

Source	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	34.782	4	8.696	12.134	0.000
Within Groups	160.918	225	0.716		
Total	195.700	229			

Table 33.Regression Analysis for AI Adoption and Risk Mitigation in IT

Model	R^2	β (Standardized)	t-value	Sig.
AI Adoption → Risk Mitigation (Direct)	0.386	0.621	10.278	0.000
AI Adoption → Cybersecurity Measures	0.342	0.584	9.112	0.000
Cybersecurity Measures → Risk Mitigation (with mediator)	0.448	0.462	7.834	0.000

Table 34.Anova Test For Demographic Differences In Perceptions Of Ai-Driven It Management

Source	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	28.574	4	7.144	6.382	0.000
Within Groups	252.341	225	1.121		
Total	280.915	229			

Conclusion

This research analyses the influence of artificial intelligence on information technology management, focusing on its implications for strategic implementation, operational efficiency, risk mitigation, and decision-making processes. The results demonstrate that entities possessing well-defined AI adoption strategies and robust backing from upper management observed notable enhancements in strategic alignment and operational efficiency. Artificial intelligence tools, such as predictive analytics, automation, and real-time monitoring, effectively minimise errors, improve resource allocation, and expedite the resolution of IT issues, thus enhancing overall productivity and competitiveness.

The study highlighted the importance of artificial intelligence in enhancing risk management by improving the detection of cybersecurity threats, minimising human error, and facilitating compliance efforts. Demographic factors such as age, education, and work experience have a substantial impact on perceptions regarding the adoption of AI. Individuals in the early to mid-stages of their careers expressed higher levels of satisfaction regarding initiatives driven by artificial intelligence. The results show that effective AI integration requires not only technological implementation but also organisational readiness and active workforce engagement.

The research produced notable findings; however, it faced certain limitations. The sample included 230 IT professionals; that may limit the generalisability of the findings to other sectors or geographic regions. The dependence on self-reported survey responses could potentially lead to subjective bias, and the research did not incorporate longitudinal data to evaluate the long-term impacts of AI adoption.

Future research may be enhanced by including larger and more diverse samples from multiple countries and industry sectors. The enduring effects of AI integration on IT management outcomes can be assessed through longitudinal studies. The examination of artificial intelligence's role in emergent technologies, including generative AI, peripheral computing, and cybersecurity frameworks, may yield significant insights into AI's transformative effects on organisational processes and the enhancement of competitive advantage.

References

1. Gentsch, P. (2019). AI in marketing, sales and service: How marketers without a data science degree can use AI, big data and bots. Springer.
2. Taroun, A., & Yang, J. B. (2011). Dempster–Shafer theory of evidence: Potential usage for decision making and risk analysis in construction project management. The Built and Human Environment Review, 4(1), 155–166.
3. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation.
4. Bughin, J., Seong, J., Manyika, J., Chui, M., & Joshi, R. (2018). Notes from the AI frontier: Modeling the impact of AI on the world economy. McKinsey Global Institute.
5. Gartner. (n.d.). AIOps (Artificial Intelligence for IT Operations). Gartner IT Glossary.
6. Levin, A., Garion, S., Kolodner, E. K., Lorenz, D. H., Barabash, K., Kugler, M., McShane, N., & others. (2019). AIOps for a cloud object storage service. In Proceedings of the IEEE International Congress on Big Data (BigDataCongress 2019) (pp. 165–169).
7. Lee, J., Kao, H.-A., & Yang, S. (2014). Service innovation and smart analytics for industry 4.0 and predictive maintenance. Journal of Manufacturing Systems, 32(4), 1–12.
8. Veeramachaneni, K., Arnaldo, I., Cuesta-Infante, A., Korrapati, V., Bassias, C., Li, K., & others. (2016). AI^2: Training a big data machine to defend. MIT Computer Science and Artificial Intelligence Laboratory (CSAIL).
9. Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans, 30(3), 286–297.
10. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689–707.
11. Asiabar, M. G. (2024). Artificial Intelligence in Strategic Management: Examining its impact on organizational decision-making. Preprints, 202409.1330.
12. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In Proceedings of the IEEE Symposium on Security and Privacy (Oakland 2010) (pp. 305–316).