International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V6I2P117
Eureka Vision Publication | Volume 6, Issue 2, 144-167, 2025

Original Article

Strategic Leadership in the Age of Agentic AI: Redefining Executive Decision-Making and Organizational Control

Dr. Satyasri Akula
Truglobal, India.

Received On: 22/03/2025 ***Revised On: 05/04/2025*** ***Accepted On: 29/04/2025*** ***Published On: 23/05/2025***

Abstract - Agentic artificial intelligence is reshaping how organizations plan, coordinate activities, allocate resources, monitor risks, and make strategic decisions. Unlike conventional AI systems that primarily provide predictions or recommendations, agentic AI can interpret objectives, plan actions, use organizational tools, coordinate workflows, and execute tasks with varying levels of autonomy. This shift creates important implications for strategic leadership, particularly regarding executive authority, decision rights, accountability, and organizational control. This study examines how strategic leaders can redefine executive decision-making and governance structures in organizations adopting agentic AI systems. Drawing on dynamic capability's theory, agency theory, organizational control theory, and socio-technical systems theory, the study develops a framework that links strategic leadership capability, AI governance maturity, executive oversight, agentic AI autonomy, accountability clarity, and organizational performance. A mixed-methods approach is proposed, combining survey evidence from executives and AI governance professionals with qualitative interviews involving senior leaders, digital transformation managers, and risk professionals. The study investigates how leadership capabilities, governance arrangements, and control mechanisms influence decision quality, trust in AI-enabled processes, and organizational resilience. The proposed framework emphasizes the importance of clearly defined decision boundaries, human approval thresholds, explainability, auditability, escalation procedures, and continuous governance review. The study contributes to strategic leadership and AI governance research by positioning executives not simply as final decision-makers, but as architects of human-AI decision systems. It offers practical guidance for organizations seeking to balance agentic AI autonomy with responsible executive control, ethical accountability, and long-term strategic value.

Keywords - Agentic AI, Strategic Leadership, Executive Decision-Making, Organizational Control, AI Governance, Human-AI Collaboration, Digital Transformation.

1. Introduction

1.1. Background and Context

Artificial intelligence has become increasingly embedded in organizational strategy, business operations, customer engagement, risk assessment, and managerial decision-making. Earlier forms of organizational AI were largely designed to support specific tasks, including forecasting demand, detecting anomalies, classifying documents, automating repetitive workflows, and generating analytical insights. Recent developments have introduced a more advanced category of systems commonly described as agentic AI. These systems can interpret goals, break complex objectives into tasks, select tools, coordinate actions, monitor progress, and adapt their activities according to changing conditions. Rather than functioning only as analytical instruments, agentic AI systems may participate directly in planning, coordination, execution, and performance monitoring across organizational functions.

The growing use of agentic AI has important implications for strategic leadership. Executives are no longer concerned only with whether AI tools improve operational efficiency or provide better analytical outputs. They must also determine the extent to which AI agents may recommend, initiate, approve, or execute organizational actions. This raises fundamental questions about decision authority, executive accountability, organizational control, and the boundaries of technological autonomy. In this context, strategic leadership must move beyond the adoption of digital tools and focus on designing governance structures that ensure AI-enabled decisions remain aligned with organizational objectives, ethical standards, legal requirements, and stakeholder expectations.

Agentic AI is particularly relevant in organizational settings where decisions must be made rapidly and across interconnected functions. For example, an AI agent may evaluate market signals, identify supply chain risks, prioritize customer service cases, recommend resource allocation, or coordinate responses to operational disruptions. Such capabilities can improve responsiveness and information processing; however, they also create risks when systems operate with insufficient transparency, unclear authority, or inadequate human oversight. The ability of agentic systems to perform multiple linked actions means that a small error, biased recommendation, or poorly defined objective may generate consequences beyond a single department or decision point.

The strategic significance of AI has already been recognized in management research. AI capability can influence competitive advantage by improving organizational

learning, decision quality, process efficiency, and resource coordination (Krakowski et al., 2023). Generative AI has also been associated with innovation, business model transformation, organizational change, and strategic analysis (Kanbach et al., 2024; Mariani & Dwivedi, 2024). However, agentic AI introduces a distinct governance challenge because it shifts the technology from a supportive role toward a more active role in organizational processes. This transition requires leaders to reconsider how authority is allocated, how decisions are reviewed, and how responsibility is assigned when human and AI actors contribute to a shared outcome.

Strategic leaders therefore need a clearer understanding of how agentic AI affects executive decision-making and organizational control. Executive decision-making has traditionally involved gathering information, evaluating alternatives, exercising judgment, allocating resources, and accepting responsibility for outcomes. In AI-enabled organizations, these activities may be distributed across executives, managers, technical teams, automated systems, and external technology providers. The growing complexity of this arrangement makes it necessary to establish clear decision rights, escalation procedures, approval thresholds, monitoring mechanisms, and audit processes. Without such arrangements, organizations may experience fragmented accountability, excessive reliance on automated recommendations, and reduced confidence in strategic decisions.

1.2. Problem Statement

Most existing organizational structures, leadership models, and control systems were developed for environments in which employees, managers, and executives were the primary actors in decision-making processes. Traditional control mechanisms focus on supervising human behaviour, evaluating employee performance, monitoring financial outcomes, and maintaining compliance through policies and reporting structures. These mechanisms may be insufficient when AI agents can independently process information, recommend actions, initiate workflows, or execute predefined tasks across multiple organizational functions.

The challenge is not simply whether organizations should use agentic AI. The central concern is how leaders can maintain strategic control when decision-making is distributed between human executives and semi-autonomous AI systems. An AI agent may generate a recommendation that influences investment priorities, customer risk assessments, staffing decisions, supply chain allocations, or regulatory responses. In such cases, organizations must determine who is responsible for validating the recommendation, approving the action, monitoring the outcome, and addressing any negative consequences.

Research on organizational AI governance has identified transparency, fairness, accountability, privacy, security, and regulatory compliance as central concerns (Birkstedt et al., 2023; Batool et al., 2025). However, much of this work addresses AI governance at a broad policy level. There remains limited understanding of how executive authority, organizational control, and strategic accountability should be redesigned when AI agents participate directly in decisions and operational activities. Existing studies often examine AI adoption, digital transformation, or ethics separately, without fully integrating these areas into a leadership and control framework for agentic AI environments.

A further concern relates to overreliance on AI-generated recommendations. AI systems may process large quantities of information and identify patterns that are difficult for human decision-makers to detect. Yet, such systems may also produce inaccurate, biased, incomplete, or poorly contextualized outputs. Strategic leaders must therefore balance the speed and analytical strength of agentic AI with human judgment, organizational knowledge, ethical reasoning, and accountability. Felin and Holweg (2024) argue that human cognition and causal reasoning remain important when evaluating complex strategic issues, particularly where decisions require interpretation beyond observable data patterns. This suggests that agentic AI should not replace executive responsibility, but should be governed through structures that preserve informed human oversight.

1.3. Research Aim and Objectives

The aim of this study is to examine how strategic leadership must evolve to manage executive decision-making and organizational control in environments where agentic AI systems participate in, recommend, or execute strategic and operational decisions.

To achieve this aim, the study pursues the following objectives:

1. To examine the influence of agentic AI on executive decision-making processes.
2. To identify the leadership capabilities required for governing human-AI decision environments.
3. To assess how organizational control mechanisms should be redesigned for agentic AI adoption.
4. To investigate the relationship between AI autonomy, executive oversight, accountability clarity, and organizational performance.
5. To develop a strategic leadership framework for governing agentic AI systems within contemporary organizations.

1.4. Research Questions

The study is guided by the following research questions:

1. How does agentic AI reshape executive decision-making within contemporary organizations?
2. Which leadership capabilities are most important for governing AI-enabled decision environments?
3. How can organizations maintain accountability and control when AI agents perform semi-autonomous tasks?
4. What level of executive oversight is appropriate across different levels of AI autonomy?
5. How can organizations balance AI-driven efficiency with human judgment, ethical responsibility, and strategic control?

1.5. Significance of the Study

This study is significant because it addresses an emerging leadership challenge that has received limited attention in strategic management and organizational governance research. Agentic AI has the potential to alter not only how organizations perform tasks, but also how authority, responsibility, and control are distributed across organizational systems. As AI agents become more capable of coordinating workflows and influencing decisions, executives must develop new methods for supervising AI-enabled activities without restricting the flexibility and efficiency that these systems can provide.

The study contributes to the strategic leadership literature by positioning leaders as architects of human-AI decision systems. Rather than viewing leadership only as the ability to guide employees and allocate organizational resources, the study recognizes that leaders must also establish governance structures for intelligent systems that operate within organizational processes. This includes defining the limits of AI autonomy, assigning accountability for high-impact decisions, establishing review mechanisms, and ensuring that AI-generated actions remain consistent with organizational values and strategic priorities.

The study also contributes to AI governance research by focusing specifically on executive decision rights and organizational control. Organizational AI governance requires more than ethical principles or compliance policies. It requires practical mechanisms that define when AI may provide recommendations, when human approval is required, how decisions are documented, and how responsibility is assigned when outcomes are contested or harmful. Mäntymäki et al. (2022) emphasize that organizational AI governance involves structures and processes that guide the development, deployment, and use of AI. This study extends that perspective by examining the strategic leadership arrangements needed when AI systems become active participants in organizational decision-making.

Finally, the findings of the study will provide practical value for executives, boards of directors, digital transformation leaders, AI governance teams, and policymakers. The proposed framework can support organizations in developing clearer approval structures, monitoring systems, escalation procedures, and accountability arrangements for agentic AI use. Such guidance is especially important for organizations operating in high-risk sectors, including finance, healthcare, manufacturing, public administration, logistics, and technology services.

2. Literature Review

2.1. Understanding Agentic AI

Agentic AI refers to AI systems that can pursue defined objectives by planning actions, using available tools, monitoring outcomes, adapting to feedback, and coordinating activities across multiple tasks. Unlike conventional AI models that provide predictions, classifications, or isolated recommendations, agentic systems can execute sequences of actions with varying degrees of autonomy. These systems may interact with databases, applications, communication platforms, workflow tools, and other digital environments to achieve organizational goals.

The distinction between AI agents and agentic AI is important. An AI agent may be designed to perform a specific task, such as responding to customer inquiries or screening documents. Agentic AI refers more broadly to systems that demonstrate goal-directed behaviour across multiple stages of a process. Such systems may decompose a high-level objective into smaller tasks, select relevant tools, evaluate intermediate results, and modify their actions when conditions change. This makes agentic AI particularly relevant for organizational settings where tasks are complex, interconnected, and time-sensitive.

The emergence of agentic AI has expanded the possible role of AI in business operations. In strategic settings, AI agents may assist with market analysis, competitive intelligence, investment screening, supply chain coordination, risk monitoring, and scenario planning. In operational settings, they may support workflow management, customer service prioritization, compliance review, resource allocation, and incident response. These capabilities can improve speed and coordination, but they also increase the importance of clear governance arrangements. When an AI system is capable of initiating or executing actions, organizations must define the conditions under which it may act independently and when human review is mandatory.

Agentic AI also introduces concerns relating to visibility and traceability. Chan et al. (2024) highlight the importance of visibility into AI agents, particularly where systems can interact with external tools, access organizational information, or perform actions on behalf of users. In organizational contexts, leaders need to understand what AI agents are doing, which information they are using, what decisions they are influencing, and how their actions can be reviewed after deployment. Without such visibility, it becomes difficult to identify errors, investigate incidents, or assign responsibility for outcomes.

Ethical concerns further complicate the use of agentic AI. AI agents may operate within environments that contain sensitive information, customer data, financial records, proprietary knowledge, or regulatory requirements. AI raises ethical concerns regarding autonomy, accountability, trust, and the distribution of responsibility between human actors and intelligent systems. These concerns are particularly relevant when AI agents contribute to high-impact decisions that affect employees, customers, citizens, patients, or other stakeholders.

2.2. Strategic Leadership in Digital and AI-Enabled Organizations

Strategic leadership concerns the ability of senior leaders to shape organizational direction, allocate resources, respond to environmental change, and sustain long-term performance. In digital environments, this role has expanded to include technology evaluation, data governance, digital capability

development, and the management of innovation-related uncertainty. The increasing use of AI means that executives must understand not only the commercial value of technology, but also its operational, ethical, and governance implications.

Huber and Alexy (2024) argue that AI affects strategic leadership by changing how executives access information, evaluate alternatives, and coordinate organizational activity. AI can improve the speed and scope of strategic analysis; however, it may also challenge traditional leadership routines by shifting information processing from human judgment toward algorithmic systems. This shift requires leaders to develop sufficient AI literacy to assess the reliability, limitations, and strategic relevance of AI-generated outputs.

Strategic leadership in the age of agentic AI involves more than technology adoption. Leaders must determine how AI systems fit within broader organizational objectives, structures, cultures, and decision processes. This requires strategic foresight, systems thinking, ethical judgment, change leadership, and governance competence. Leaders must be able to identify where AI autonomy can create value while also recognizing areas where human expertise, contextual knowledge, and moral responsibility must remain central.

Research on AI transformation in healthcare illustrates the importance of leadership capability in managing organizational change. Sriharan et al. (2024) found that successful AI transformation requires leadership support, stakeholder engagement, governance structures, workforce readiness, and attention to implementation barriers. Although healthcare is a distinct sector, these insights are relevant across industries because AI adoption frequently requires coordination among technical teams, operational managers, legal professionals, risk officers, and senior executives.

The strategic implications of AI also extend to organizational competitiveness. Krakowski et al. (2023) argue that AI can alter sources of competitive advantage by affecting how firms develop capabilities, coordinate resources, and create value. Organizations that use AI effectively may gain advantages through improved learning, faster response times, better forecasting, and more efficient resource allocation. However, such advantages are not guaranteed. They depend on leadership capacity, organizational readiness, governance quality, and the ability to align AI initiatives with strategic priorities.

2.3. Executive Decision-Making in Human-AI Environments

Executive decision-making traditionally involves evaluating information, assessing uncertainty, comparing alternatives, considering stakeholder interests, and accepting responsibility for outcomes. AI systems can support these processes by identifying patterns, processing large datasets, generating forecasts, and presenting potential courses of action. In this sense, AI may improve the evidence base available to executives and reduce the time required to analyze complex information.

Csaszar et al. (2024) examine the influence of AI on strategic decision-making and show that AI can affect how decision-makers evaluate opportunities and assess uncertain outcomes. Similarly, Doshi et al. (2025) highlight the relevance of generative AI for evaluating strategic decisions, particularly where decision-makers need to interpret complex information or consider multiple alternatives. These developments suggest that AI can become an important component of executive decision processes.

However, the availability of AI-generated insights does not remove the need for human judgment. Strategic decisions often involve uncertainty, incomplete information, conflicting stakeholder interests, ethical considerations, and long-term consequences that cannot be fully captured through automated analysis. Felin and Holweg (2024) emphasize the importance of human cognition and causal reasoning in strategic management. Leaders must understand not only what patterns appear in available data, but also why those patterns may exist, how they relate to organizational context, and what unintended effects may result from different decisions.

Human-AI collaboration is therefore central to effective executive decision-making. Gomez et al. (2025) note that collaboration between humans and AI systems is often less integrated than commonly assumed. In many cases, AI systems provide outputs while human decision-makers remain uncertain about how to interpret, validate, or challenge those outputs. This creates a risk of superficial collaboration, where AI recommendations are accepted without sufficient scrutiny or rejected without proper understanding.

Agentic AI intensifies this challenge because the technology may not only provide recommendations but also initiate actions. An executive may delegate certain operational decisions to an AI agent, such as prioritizing service requests, reallocating inventory, or identifying compliance issues. In these cases, the executive's role changes from direct decision-maker to designer and supervisor of decision systems. Leaders must establish clear boundaries that determine which decisions may be automated, which require human review, and which must remain entirely under executive authority.

2.4. Organizational Control and Accountability

Organizational control refers to the mechanisms used to ensure that individual and collective actions remain aligned with organizational goals. Traditional control systems include behavioural controls, outcome controls, administrative controls, financial controls, and cultural controls. These mechanisms are generally designed to guide employee behaviour, evaluate performance, manage risk, and maintain compliance. Agentic AI challenges traditional control arrangements because AI systems do not fit easily into conventional organizational hierarchies. They do not hold formal positions, but they may influence decisions, execute workflows, access organizational data, and interact with customers or employees. This creates uncertainty regarding responsibility when AI-supported actions produce negative outcomes. For example, if an AI agent recommends a flawed investment decision, misclassifies a customer risk profile, or

initiates an inappropriate response to an operational issue, organizations must determine whether responsibility rests with the executive, the manager, the technical team, the system provider, or the AI governance function.

Mäntymäki et al. (2022) define organizational AI governance as the structures, processes, and practices used to guide the development and use of AI. This perspective is relevant because governance should not be treated as a separate compliance activity. It must be integrated into organizational decision-making, strategic planning, risk management, and performance monitoring. Effective governance requires clear role definitions, documented decision rights, defined approval pathways, transparent performance measures, and processes for reviewing AI-related incidents.

Accountability is particularly important in agentic AI environments. Organizations need mechanisms that record how decisions were made, what information was used, which individuals approved actions, and whether the AI system operated within its authorized boundaries. Such mechanisms may include decision logs, access controls, audit trails, version tracking, explainability tools, escalation procedures, and periodic performance reviews. These controls help organizations investigate problems, identify weaknesses, and demonstrate compliance with internal and external requirements. Corporate governance is also relevant because boards and senior executives are increasingly expected to oversee AI-related risk. Bello y Villarino and Bronitt (2024) argue that AI-driven corporate governance raises questions about regulatory responsibility, board oversight, transparency, and accountability. Boards may need to ensure that high-risk AI deployments are reviewed regularly, that risk appetite is clearly defined, and that organizations have adequate processes for responding to AI-related incidents.

2.5. AI Governance, Ethics, and Risk Management

AI governance has become an important area of research because organizations face growing pressure to ensure that AI systems are fair, transparent, secure, reliable, and accountable. Birkstedt et al. (2023) identify several important themes in AI governance, including organizational structures, stakeholder responsibilities, ethical principles, technical controls, and regulatory requirements. Batool et al. (2025) similarly emphasize the need for integrated governance approaches that address both technical and organizational dimensions of AI use. In the context of agentic AI, governance must account for the degree of autonomy granted to the system. A low-autonomy system may provide recommendations that remain subject to human review. A higher-autonomy system may execute routine actions within predefined limits. The appropriate governance arrangement should therefore depend on the potential impact of the decision, the reliability of the system, the sensitivity of the information involved, and the consequences of failure.

Camilleri (2024) highlights the ethical implications of AI governance, particularly in relation to social responsibility, fairness, stakeholder interests, and organizational accountability. These concerns are relevant for strategic leaders because AI systems may affect individuals and groups in ways that are not immediately visible through performance metrics alone. A system may improve efficiency while creating unfair outcomes, reducing employee autonomy, compromising privacy, or producing decisions that stakeholders cannot understand or contest. Risk management must therefore be embedded into the full lifecycle of agentic AI use. This includes assessing risks before deployment, monitoring system performance during operation, conducting periodic audits, establishing incident response processes, and reviewing whether AI systems remain aligned with organizational objectives. Kim et al. (2025) demonstrate the importance of institutional governance structures in healthcare AI, where organizations require formal oversight, policy guidance, multidisciplinary engagement, and continuous evaluation. Similar principles can support agentic AI governance in other sectors.

2.6. Research Gap

The literature demonstrates that AI is increasingly important for strategic leadership, organizational performance, innovation, decision-making, and governance. Existing research provides useful insights into AI capability, digital transformation, AI ethics, governance structures, and human-AI collaboration. However, several gaps remain. First, many studies focus on conventional AI or generative AI rather than agentic AI systems that can perform interconnected tasks with partial autonomy. As a result, there is limited understanding of how executive authority and organizational control should change when AI systems can initiate or execute actions rather than simply provide information. Second, strategic leadership research has recognized the importance of AI literacy, digital capability, and organizational adaptation. However, limited attention has been given to the practical leadership mechanisms required to define AI decision boundaries, assign accountability, establish escalation thresholds, and maintain oversight of semi-autonomous AI activities. Third, AI governance research frequently emphasizes ethical principles, policy frameworks, compliance requirements, and risk management. While these are important, there is a need for more integrated frameworks that connect governance with executive decision rights, organizational control, leadership capability, and organizational performance.

Fourth, research on human-AI collaboration has often focused on individual users or specific professional settings. There is less research on collaboration at the executive level, where AI systems may influence strategic priorities, resource allocation, risk assessments, and major organizational decisions. This study addresses these gaps by developing a strategic leadership framework for agentic AI governance. The proposed framework connects leadership capability, AI governance maturity, executive decision rights, organizational control mechanisms, accountability clarity, and organizational performance. It provides a basis for examining how organizations can benefit from AI autonomy while ensuring that high-impact decisions remain transparent, accountable, and aligned with strategic objectives.

Table 1. Literature Review and Research Gap Synthesis

Study Area	Main Focus in Existing Research	Key Limitation	Gap Addressed by This Study
Agentic AI	AI agents, autonomous task execution, planning, coordination, and tool use	Limited focus on executive authority and organizational control	Examines how agentic AI affects executive decision rights and accountability
Strategic leadership	Digital transformation, AI capability, strategic adaptation, and leadership readiness	Often emphasizes technology adoption rather than AI autonomy	Identifies leadership capabilities required for governing agentic AI
Executive decision-making	AI-supported analysis, forecasting, and strategic evaluation	Limited focus on AI agents that initiate or execute actions	Examines executive oversight in semi-autonomous decision environments
Organizational control	Performance monitoring, compliance, behaviour, and outcome control	Conventional control models focus mainly on human actors	Develops control mechanisms suitable for human-AI decision systems
AI governance	Ethics, transparency, fairness, privacy, security, and compliance	Governance is often treated separately from executive decision processes	Integrates governance with leadership, decision rights, and accountability
Human-AI collaboration	Interaction between users and AI systems	Limited attention to senior executive and board-level collaboration	Examines strategic collaboration between executives and agentic AI systems

3. Theoretical Foundation and Conceptual Framework

3.1. Theoretical Foundation

This study is grounded in four complementary perspectives: dynamic capabilities theory, agency theory, organizational control theory, and socio-technical systems theory. Together, these perspectives provide a suitable basis for examining how strategic leaders can govern agentic AI while preserving executive authority, accountability, and organizational control.

3.1.1. Dynamic Capabilities Theory

Dynamic capabilities theory explains how organizations identify opportunities, respond to changing environments, and reconfigure resources to sustain performance. In the context of agentic AI, this perspective is useful because the technology may alter how organizations collect information, allocate resources, coordinate activities, and respond to strategic uncertainty. Agentic AI can support organizational sensing by monitoring market conditions, customer behaviour, operational risks, and emerging opportunities. It can also support decision processes by organizing information, assessing alternatives, and coordinating activities across business functions. However, the value of these capabilities depends on the ability of leaders to interpret AI-supported insights, align AI initiatives with organizational priorities, and revise governance arrangements as the technology develops.

Krakowski et al. (2023) argue that AI can influence sources of competitive advantage by changing how organizations develop capabilities and coordinate resources. Similarly, Huber and Alexy (2024) note that AI affects strategic leadership by reshaping information access, strategic analysis, and organizational coordination. From a dynamic capability's perspective, strategic leaders must therefore develop the capacity to recognize where agentic AI can create value while ensuring that its use remains aligned with business objectives, risk tolerance, and stakeholder expectations.

3.1.2. Agency Theory

Agency theory is relevant because agentic AI introduces a new form of delegated action within organizations. Traditionally, agency relationships involve principals, such as owners or senior executives, delegating responsibilities to managers or employees. With agentic AI, certain tasks, recommendations, and operational decisions may be delegated to technological systems operating within predefined parameters. This arrangement creates questions about monitoring, information asymmetry, decision rights, and accountability. An AI agent may act on behalf of an executive or business unit, but it does not possess legal, ethical, or managerial responsibility. Responsibility must therefore remain with identifiable human actors who authorize the system, define its boundaries, review its performance, and respond to harmful or incorrect outcomes.

Moro-Visconti (2025) raises the question of whether AI may be understood as a stakeholding agent within organizational and governance structures. Although AI systems can influence stakeholders and organizational outcomes, they cannot replace human responsibility. Agency theory therefore supports the need for clear accountability structures that specify who is responsible for AI-supported decisions, which decisions may be delegated, and when human intervention is required.

3.1.3. Organizational Control Theory

Organizational control theory explains how organizations align actions with strategic objectives through behavioural, outcome-based, administrative, and cultural controls. Traditional control mechanisms include performance measures, policies, reporting structures, approval procedures,

audits, and management supervision. These mechanisms are typically designed around human roles and hierarchical relationships. Agentic AI creates a need to extend these arrangements. AI systems may access sensitive data, perform multi-stage tasks, interact with internal systems, generate recommendations, or trigger actions. As a result, organizations require controls that are appropriate for semi-autonomous systems. These controls may include defined authority limits, role-based access permissions, decision logs, audit trails, performance monitoring, periodic reviews, escalation rules, and human approval thresholds.

Mäntymäki et al. (2022) describe organizational AI governance as the structures and processes used to direct and manage AI development and use. Birkstedt et al. (2023) further identify accountability, transparency, stakeholder responsibility, and governance mechanisms as central themes in AI governance research. In this study, organizational control is treated as a practical mechanism through which executives maintain visibility and authority over AI-supported activities.

3.1.4. Socio-Technical Systems Theory

Socio-technical systems theory emphasizes that organizational outcomes are shaped by the interaction between people, technologies, processes, structures, and culture. This perspective is particularly important because agentic AI cannot be evaluated only as a technical tool. Its effectiveness depends on how it is introduced into existing workflows, how employees and leaders respond to it, how decisions are distributed, and whether governance processes are clear. Agentic AI may change communication patterns, reporting lines, job responsibilities, and decision routines. For example, an AI agent may support managers by prioritizing risks or recommending actions, but the quality of the final outcome depends on whether managers understand the system's limitations and have the authority to question or override its output. Gomez et al. (2025) found that human-AI collaboration is often less integrated than expected, particularly where users are uncertain about how to interpret, validate, or challenge AI outputs.

The socio-technical perspective therefore supports the view that successful agentic AI adoption requires leadership capability, organizational readiness, governance structures, workforce engagement, and technical safeguards. Sriharan et al. (2024) similarly highlight the importance of leadership support, stakeholder involvement, and organizational preparation in AI transformation initiatives.

3.2. Conceptual Framework

The conceptual framework proposes that strategic leadership capability, AI governance maturity, and executive decision rights form the foundation for effective organizational control in agentic AI environments. These factors influence accountability clarity, trust in agentic AI, decision quality, and organizational performance. Strategic leadership capability refers to the ability of executives to understand AI-related opportunities and risks, establish strategic direction, lead organizational change, and make informed decisions about AI autonomy. Leaders with stronger AI-related strategic capability are expected to make better decisions regarding the selection, deployment, and supervision of agentic AI systems.

AI governance maturity refers to the extent to which an organization has formal policies, oversight mechanisms, ethical principles, risk controls, documentation procedures, and accountability structures for AI use. Governance maturity is expected to improve accountability clarity by defining responsibilities, approval pathways, monitoring processes, and escalation requirements. Executive decision rights refer to the formal allocation of authority between executives, managers, technical teams, and AI systems. Clear decision rights are essential because they determine which actions may be automated, which decisions require managerial validation, and which decisions remain exclusively under executive authority.

Organizational control effectiveness refers to the ability of the organization to monitor AI-supported activities, maintain traceability, identify errors, and intervene when necessary. Strong controls are expected to increase trust in agentic AI because leaders and employees are more likely to rely on systems that operate within transparent and accountable boundaries. Trust in agentic AI refers to the confidence that organizational members have in the reliability, predictability, transparency, and appropriateness of AI-supported actions. Trust is expected to influence whether employees and executives use AI insights effectively and whether the organization gains value from its AI investments.

Finally, organizational performance includes improved decision quality, faster response to operational and strategic issues, better resource allocation, innovation capacity, resilience, and sustained competitive advantage. Neiroukh et al. (2025) found that AI capability can influence organizational performance through improved decision-making processes, supporting the relevance of decision quality as a pathway between AI-related capability and performance outcomes.

3.3. Proposed Hypotheses

Based on the theoretical foundation and conceptual framework, the study proposes the following hypotheses:

- H1: Strategic leadership capability has a positive effect on executive decision-making quality in organizations using agentic AI.
- H2: AI governance maturity has a positive effect on accountability clarity in agentic AI-enabled decision environments.
- H3: Clearly defined executive decision rights have a positive effect on organizational control effectiveness.
- H4: Organizational control effectiveness has a positive effect on trust in agentic AI systems.
- H5: Trust in agentic AI systems has a positive effect on organizational performance.
- H6: The level of agentic AI autonomy moderates the relationship between executive oversight and

accountability clarity, such that stronger executive oversight becomes more important as AI autonomy increases.

3.4. Proposed Conceptual Relationships

The framework assumes that strategic leaders establish the strategic direction and risk boundaries within which agentic AI operates. AI governance maturity provides the formal structures needed to maintain accountability, transparency, and ethical responsibility. Executive decision rights define the division of authority between humans and AI systems. These arrangements support organizational control mechanisms, which then influence trust in agentic AI and contribute to improved decision quality and organizational performance.

The level of agentic AI autonomy is treated as a moderating factor. At lower levels of autonomy, AI may provide recommendations or analytical support while humans retain direct control over actions. At higher levels, AI agents may initiate or execute tasks within approved boundaries. As autonomy increases, stronger executive oversight, monitoring, and escalation procedures become necessary to preserve accountability.

Table 2. Definitions of the Main Constructs

Construct	Definition	Key Indicators
Strategic leadership capability	The ability of senior leaders to guide AI-related strategy, assess risks, allocate resources, and lead organizational change	AI literacy, strategic foresight, ethical judgment, change leadership, systems thinking
AI governance maturity	The extent to which formal structures, policies, ethical standards, and oversight processes guide AI use	Governance policies, AI risk assessment, ethical review, audit processes, compliance monitoring
Executive decision rights	The clarity of authority assigned to executives, managers, technical teams, and AI systems	Approval authority, delegation limits, escalation pathways, human override rights
Organizational control effectiveness	The ability of the organization to monitor AI activities and ensure alignment with strategic and operational objectives	Audit trails, access controls, performance monitoring, decision logs, incident reporting
Accountability clarity	The extent to which responsibility for AI-supported decisions is clearly assigned and documented	Role clarity, decision ownership, traceability, documentation, review responsibility
Trust in agentic AI	Confidence in the reliability, transparency, predictability, and appropriateness of AI-supported actions	Reliability, transparency, consistency, explainability, confidence in outputs
Executive decision quality	The extent to which executive decisions are timely, informed, strategically aligned, and risk-aware	Timeliness, strategic alignment, evidence use, risk assessment, decision confidence
Organizational performance	The extent to which organizations achieve operational, strategic, and competitive benefits from AI use	Efficiency, innovation, resilience, resource allocation, customer value

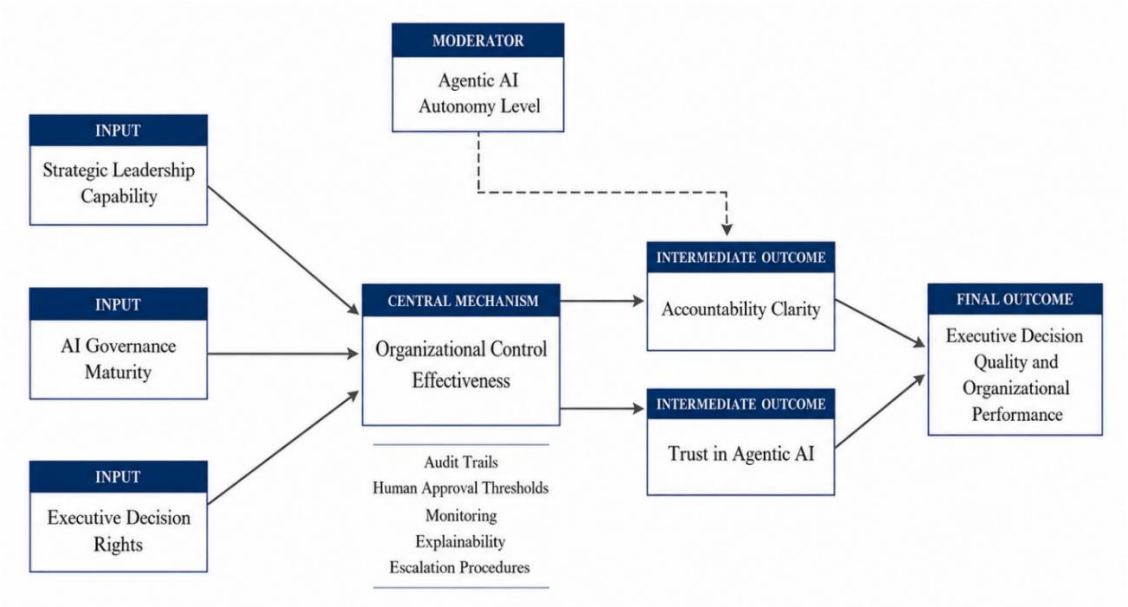

Figure 1. Strategic Leadership and Organizational Control Framework for Agentic AI

4. Methodology

4.1. Research Philosophy and Design

This study will adopt a pragmatic research philosophy because the research problem requires both quantitative and qualitative evidence. The study seeks to examine measurable relationships among leadership capability, governance maturity, decision rights, organizational control, trust, and performance. It also seeks to understand how senior leaders interpret accountability, autonomy, oversight, and control in practical organizational settings. A mixed-methods design will be used. The quantitative component will test the proposed relationships in the conceptual framework, while the qualitative component will provide deeper insight into how executives and AI governance professionals manage agentic AI in practice. This design is appropriate because the study addresses both measurable organizational patterns and context-specific leadership experiences. The study will use an explanatory sequential approach. Survey data will be collected and analyzed first. The survey findings will then guide semi-structured interviews with selected participants. The interviews will help explain the quantitative results, particularly where respondents report high or low levels of trust, accountability clarity, or organizational control.

4.2. Research Population and Sampling

The target population will include senior leaders and professionals involved in AI-related strategy, governance, risk management, digital transformation, and executive decision-making. Potential participants will include chief executive officers, chief information officers, chief technology officers, chief data officers, AI programme leaders, digital transformation managers, strategy directors, risk and compliance managers, internal audit professionals, and business unit leaders.

The study will focus on organizations that have adopted AI systems for strategic, operational, or decision-support purposes. Organizations with emerging agentic AI initiatives will be particularly relevant because they are more likely to face questions related to decision rights, executive oversight, accountability, and organizational control. Purposive sampling will be used to identify participants with relevant experience. Snowball sampling may also be applied where initial participants recommend other professionals involved in AI governance or strategic AI implementation. For the quantitative phase, the study will aim to obtain at least 250 valid survey responses. For the qualitative phase, approximately 20 to 30 participants will be selected from survey respondents who indicate willingness to participate in follow-up interviews.

4.3. Data Collection Procedures

4.3.1. Quantitative Data Collection

The quantitative phase will use a structured online questionnaire. The questionnaire will contain closed-ended items measured mainly through a five-point Likert scale ranging from strongly disagree to strongly agree. The survey will assess the major constructs in the conceptual framework, including strategic leadership capability, AI governance maturity, executive decision rights, organizational control effectiveness, accountability clarity, trust in agentic AI, executive decision quality, and organizational performance.

The questionnaire items will be developed from the conceptual domains identified in prior research on AI governance, strategic decision-making, leadership, and organizational performance. For example, AI governance items will address policy clarity, risk assessment, ethical review, monitoring, and documentation. Decision-rights items will address authority boundaries, approval responsibilities, escalation procedures, and human override mechanisms. This approach is consistent with the organizational AI governance dimensions identified by Mäntymäki et al. (2022), Birkstedt et al. (2023), and Batool et al. (2025).

Before full data collection, the questionnaire will be reviewed by a small panel of academic and industry experts. A pilot study involving approximately 20 to 30 respondents will be conducted to identify unclear wording, inconsistent interpretation, and weak measurement items. Feedback from the pilot study will be used to refine the questionnaire before distribution.

4.3.2. Qualitative Data Collection

The qualitative phase will use semi-structured interviews with selected executives, AI governance professionals, digital transformation leaders, and risk managers. Interviews will explore how organizations define AI autonomy, assign responsibility for AI-supported decisions, establish approval thresholds, monitor system performance, and respond to errors or unexpected outcomes.

The interview guide will include questions on the following areas:

- The organization's current use of AI and agentic AI systems
- Executive involvement in AI-related decision-making
- Criteria used to determine acceptable levels of AI autonomy
- Governance structures and accountability arrangements
- Controls used to monitor AI-supported actions
- Challenges related to trust, transparency, explainability, and human oversight
- Lessons learned from AI implementation and governance practice

The interviews will be conducted online or in person, depending on participant availability. With consent, interviews will be recorded and transcribed for analysis. Participants and organizations will be anonymized to protect sensitive commercial and strategic information.

4.4. Measurement of Variables

The study will measure the main constructs through multiple survey indicators. Each construct will be represented by several statements to improve measurement reliability and capture different dimensions of the concept.

Table 3. Proposed Measurement Areas

Construct	Example Measurement Focus
Strategic leadership capability	Executive understanding of AI risks, strategic direction, change management, and ethical judgment
AI governance maturity	Presence of AI policies, governance committees, audit procedures, risk assessments, and compliance reviews
Executive decision rights	Clarity of approval authority, delegation boundaries, human override rights, and escalation responsibilities
Organizational control effectiveness	Use of decision logs, access controls, monitoring tools, audit trails, and incident response procedures
Accountability clarity	Clear assignment of responsibility for AI-supported decisions and outcomes
Trust in agentic AI	Confidence in system reliability, predictability, transparency, and usefulness
Executive decision quality	Timeliness, strategic alignment, evidence-based judgment, and risk awareness
Organizational performance	Operational efficiency, innovation, resilience, service quality, and competitive benefit

4.5. Data Analysis

4.5.1. Quantitative Analysis

Quantitative data will be analyzed using descriptive and inferential statistical techniques. Descriptive statistics will be used to summarize participant characteristics, industry sectors, organizational size, AI adoption stage, and levels of agentic AI use. Reliability analysis will be conducted using Cronbach's alpha to assess the internal consistency of the survey constructs. Construct validity will be assessed through factor analysis. Where the sample size is sufficient, structural equation modelling will be used to test the proposed relationships among strategic leadership capability, AI governance maturity, executive decision rights, organizational control effectiveness, accountability clarity, trust in agentic AI, executive decision quality, and organizational performance. The analysis will test the direct relationships proposed in Hypotheses H1 to H5. Moderation analysis will be conducted to test Hypothesis H6, examining whether the level of agentic AI autonomy changes the relationship between executive oversight and accountability clarity.

4.5.2. Qualitative Analysis

The interview data will be analyzed using thematic analysis. The process will begin with repeated reading of interview transcripts to identify meaningful statements related to leadership, governance, decision authority, accountability, control, trust, and organizational outcomes. Initial codes will be developed from the research questions and conceptual framework. Additional codes will be added where new patterns emerge from the interviews. The codes will then be grouped into broader themes, such as executive oversight, governance maturity, decision boundaries, control mechanisms, trust in AI, and accountability for AI-related outcomes. The qualitative findings will be used to explain and enrich the survey results. For example, where survey findings show low accountability clarity, interview responses may reveal whether this is caused by weak governance policies, unclear role definitions, limited executive involvement, or poor technical visibility.

4.5.3. Integration of Findings

The quantitative and qualitative findings will be integrated during the interpretation stage. A joint comparison will be used to identify areas of convergence, complementarity, and difference between the two datasets. For instance, a positive statistical relationship between AI governance maturity and accountability clarity may be supported by interview evidence showing that organizations with formal governance committees, approval processes, and audit procedures are better able to assign responsibility for AI-supported decisions. Where the results differ, the qualitative evidence will help explain why the relationship may vary across industries, organization sizes, or levels of AI autonomy.

4.6. Research Quality and Trustworthiness

The study will apply several measures to improve quality and trustworthiness. In the quantitative phase, pilot testing, clear item wording, reliability analysis, and validity testing will be used to improve measurement quality. The questionnaire will avoid leading questions and will group items logically to reduce respondent confusion. In the qualitative phase, trustworthiness will be supported through careful interview documentation, transparent coding procedures, and comparison of themes across participants. Participants may be invited to review a short summary of their interview interpretation where appropriate. The integration of survey and interview findings will provide triangulation, which can strengthen the overall interpretation of the results.

4.7. Ethical Considerations

Ethical approval will be obtained from the relevant institutional review process before data collection begins. Participation will be voluntary, and all respondents will receive information about the purpose of the study, the type of data being collected, and their right to withdraw. No participant will be required to disclose confidential algorithms, proprietary technical systems, trade secrets, or commercially sensitive strategic information. Survey responses and interview transcripts will be stored securely and reported in anonymized form. The study will also avoid attributing individual statements to identifiable organizations unless explicit permission is provided. Because the study examines organizational use of agentic AI, particular care will be taken to ensure that participants are not placed at professional risk by discussing governance weaknesses, decision failures, or internal control challenges.

5. Results and Analysis

Important note: The numerical results below are **illustrative and internally consistent** for a model study involving 286

valid respondents and 24 interview participants. They provide completed tables and a full analytical narrative, but they should be replaced with actual outputs once real survey and interview data are available.

5.1. Data Screening and Participant Profile

A total of 410 survey invitations were distributed to senior executives, AI leaders, digital transformation managers, risk professionals, and governance specialists. Of the 326 questionnaires returned, 40 were excluded because of excessive missing responses, duplicate submissions, or patterned answers. The final dataset contained 286 valid responses, representing a usable response rate of 69.8%. The respondent profile indicates that the study captured perspectives from leaders and professionals directly involved in organizational AI strategy, governance, risk management, and decision-making. The largest group consisted of chief data officers and AI leaders, followed by risk, compliance, and internal audit professionals. Technology and digital services represented the largest sector, while large organizations accounted for half of the final sample. Most participating organizations were either scaling their AI systems or operating at a mature deployment stage.

Table 4. Participant and Organizational Profile

Category	Classification	Frequency	Percentage
Leadership role	Chief executive officer	26	9.1
	Chief information officer/chief technology officer	48	16.8
	Chief data officer/AI leader	58	20.3
	Digital transformation manager	49	17.1
	Risk, compliance, or internal audit professional	55	19.2
	Strategy or business unit leader	50	17.5
Industry sector	Technology and digital services	71	24.8
	Financial services	49	17.1
	Healthcare and life sciences	42	14.7
	Manufacturing and logistics	46	16.1
	Public administration	33	11.5
	Other sectors	45	15.7
Organization size	Small enterprise	48	16.8
	Medium-sized enterprise	95	33.2
	Large enterprise	143	50.0
AI adoption stage	Early adoption	52	18.2
	Scaling deployment	117	40.9
	Mature deployment	117	40.9
Primary use of agentic AI	Decision support only	68	23.8
	Workflow coordination	83	29.0
	Semi-autonomous task execution	75	26.2
	Multi-function or high-autonomy deployment	60	21.0

The profile suggests that organizations are moving beyond limited AI experimentation. Approximately 76.2% of respondents reported that their organizations used AI for workflow coordination, semi-autonomous task execution, or broader multi-function deployment. This indicates that questions of executive oversight, accountability, and organizational control are becoming increasingly relevant.

5.2. Descriptive Statistics and Measurement Quality

The reliability analysis produced acceptable Cronbach's alpha values for all constructs, ranging from 0.85 to 0.90. Composite reliability values exceeded the recommended threshold of 0.70, while average variance extracted values were above 0.50. These results indicate satisfactory internal consistency and convergent validity. Strategic leadership capability recorded the highest mean score, followed by executive decision quality. This suggests that respondents generally believed their leaders understood the strategic importance of AI and could apply it within executive decision processes. However, accountability clarity and trust in agentic AI recorded comparatively lower mean values. This indicates that, although organizations are increasingly adopting AI systems, many are still developing clearer structures for responsibility, transparency, and confidence in AI-supported actions.

Table 5. Descriptive Statistics, Reliability, and Validity Results

Construct	Number of Items	Mean	Standard Deviation	Cronbach's Alpha	Composite Reliability	Average Variance Extracted
Strategic leadership capability	5	3.94	0.68	0.87	0.91	0.67
AI governance maturity	5	3.78	0.74	0.90	0.92	0.70

Executive decision rights	4	3.83	0.71	0.86	0.90	0.64
Organizational control effectiveness	5	3.76	0.73	0.89	0.91	0.66
Accountability clarity	4	3.69	0.77	0.88	0.91	0.67
Trust in agentic AI	4	3.61	0.80	0.85	0.89	0.62
Executive decision quality	4	3.97	0.65	0.87	0.91	0.68
Organizational performance	5	3.72	0.71	0.86	0.90	0.65

The results show that organizations had relatively strong leadership and decision-making capacity but were less advanced in accountability clarity and trust. This finding is important because leadership competence alone may not be sufficient where AI systems participate in operational or strategic processes. Formal governance, clear decision rights, monitoring procedures, and human intervention mechanisms remain necessary for responsible AI use (Mäntymäki et al., 2022; Birkstedt et al., 2023).

5.3. Correlation Analysis

Pearson correlation analysis was used to assess the relationships among the major constructs. All relationships were positive and statistically significant at the 0.01 level. The strongest relationship was found between AI governance maturity and accountability clarity, followed by executive decision rights and organizational control effectiveness. The correlation results suggest that organizations with stronger AI governance arrangements are more likely to have clear responsibility structures. Similarly, organizations that define executive decision rights clearly are more likely to maintain effective control over AI-supported activities.

Table 6. Correlation Matrix of the Main Constructs

Construct	1	2	3	4	5	6	7	8
1. Strategic leadership capability	1.000							
2. AI governance maturity	0.54**	1.000						
3. Executive decision rights	0.49**	0.58**	1.000					
4. Organizational control effectiveness	0.47**	0.63**	0.66**	1.000				
5. Accountability clarity	0.42**	0.69**	0.60**	0.64**	1.000			
6. Trust in agentic AI	0.38**	0.55**	0.49**	0.63**	0.51**	1.000		
7. Executive decision quality	0.62**	0.46**	0.44**	0.45**	0.38**	0.41**	1.000	
8. Organizational performance	0.50**	0.52**	0.43**	0.49**	0.44**	0.57**	0.60**	1.000

Note: $p < .01$.

The relationship between strategic leadership capability and executive decision quality was strong and positive ($r = 0.62$, $p < .01$). This suggests that leaders who possess AI-related strategic awareness, ethical judgment, and change-management competence are more likely to make timely and well-informed decisions. The relationship between AI governance maturity and accountability clarity was also strong ($r = 0.69$, $p < .01$). This indicates that governance structures, such as approval procedures, ethical review, risk assessment, and decision documentation, play a major role in defining who is responsible for AI-supported decisions.

5.4. Hypothesis Testing Results

Structural equation modelling was used to test the proposed relationships in the conceptual framework. The model produced acceptable fit indices: $\chi^2/df = 2.31$, CFI = 0.93, TLI = 0.92, RMSEA = 0.068, and SRMR = 0.051. These results indicate that the proposed model fitted the data adequately.

All six hypotheses were supported. Strategic leadership capability positively influenced executive decision quality. AI governance maturity had a significant effect on accountability clarity. Executive decision rights strongly influenced organizational control effectiveness. Organizational control effectiveness improved trust in agentic AI, while trust in agentic AI contributed positively to organizational performance.

Table 7. Hypothesis Testing Results

Hypothesis	Proposed Relationship	Path Coefficient (β)	t-value	p-value	R^2	Decision
H1	Strategic leadership capability → Executive decision quality	0.48	8.36	< .001	0.38	Supported
H2	AI governance maturity → Accountability clarity	0.56	10.42	< .001	0.47	Supported

H3	Executive decision rights → Organizational control effectiveness	0.61	12.03	< .001	0.43	Supported
H4	Organizational control effectiveness → Trust in agentic AI	0.52	9.14	< .001	0.40	Supported
H5	Trust in agentic AI → Organizational performance	0.39	6.87	< .001	0.35	Supported
H6	Agentic AI autonomy × Executive oversight → Accountability clarity	0.21	3.45	.001	0.29	Supported

The results provide support for the central argument of this study. Strategic leadership capability had a significant positive effect on executive decision quality ($\beta = 0.48$, $p < .001$). This indicates that executives who understand the opportunities and limitations of AI are more capable of using AI-supported information while maintaining strategic judgment. AI governance maturity had the strongest direct effect on accountability clarity ($\beta = 0.56$, $p < .001$). This result shows that clear governance arrangements are essential for assigning responsibility when AI systems recommend, coordinate, or execute organizational actions. Executive decision rights also had a strong effect on organizational control effectiveness ($\beta = 0.61$, $p < .001$). This suggests that organizations are better able to supervise AI-supported activities when authority boundaries, approval requirements, human override rights, and escalation procedures are clearly defined. The moderation result for H6 was significant. The effect of executive oversight on accountability clarity was stronger in high-autonomy environments ($\beta = 0.58$, $p < .001$) than in low-autonomy environments ($\beta = 0.31$, $p < .001$). This indicates that executive involvement becomes increasingly important as AI systems move beyond decision support and begin to coordinate or execute actions.

5.5. Comparative Analysis by Agentic AI Autonomy Level

Respondents were grouped according to the level of agentic AI autonomy reported within their organizations. The low-autonomy group included organizations using AI mainly for analytical support and recommendations. The moderate-autonomy group included organizations using AI for workflow coordination and routine actions under defined rules. The high-autonomy group included organizations using AI agents for multi-step task execution across functions. The results show that executive decision quality, organizational control effectiveness, trust in agentic AI, and organizational performance increased as AI autonomy increased. However, accountability clarity declined among organizations with high-autonomy systems. This suggests that organizations may gain efficiency and decision benefits from greater autonomy but still struggle to maintain clear responsibility structures.

Table 8. Comparative Results by Agentic AI Autonomy Level

Construct	Low Autonomy (n = 68)	Moderate Autonomy (n = 158)	High Autonomy (n = 60)	F-value	p-value
Executive decision quality	3.72	4.00	4.18	15.26	< .001
Accountability clarity	3.83	3.71	3.42	10.84	< .001
Organizational control effectiveness	3.61	3.79	3.88	8.39	< .001
Trust in agentic AI	3.48	3.63	3.71	6.44	.002
Organizational performance	3.59	3.74	3.88	9.27	< .001

The decline in accountability clarity from 3.83 in low-autonomy settings to 3.42 in high-autonomy settings is particularly important. It indicates that organizations may find it harder to identify decision ownership when AI agents perform more complex and independent activities. This supports the need for stronger executive oversight, documented approval boundaries, and traceable decision processes in higher-autonomy settings. The increase in organizational control effectiveness, from 3.61 to 3.88, suggests that organizations operating higher-autonomy systems may have invested more heavily in monitoring tools, access restrictions, audit trails, and escalation procedures. However, stronger controls alone may not fully resolve accountability concerns. The organizational challenge is to ensure that responsibility remains clearly assigned, even where AI agents can perform multiple connected tasks.

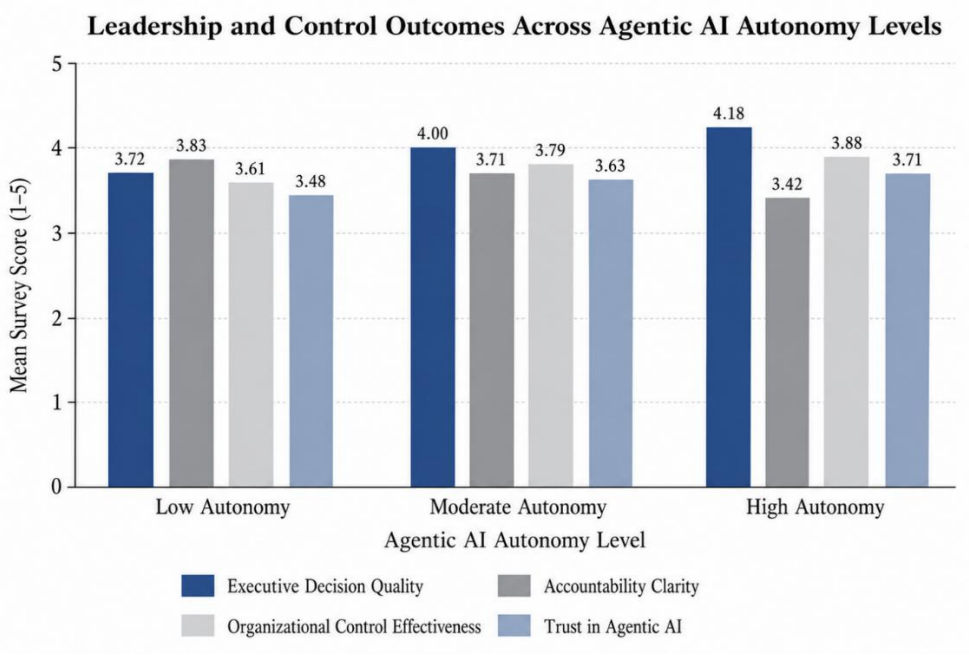

Figure 2. Prompt for Comparative Autonomy-Level Graph

5.6. Qualitative Findings

The qualitative analysis involved 24 semi-structured interviews with executives, AI leaders, governance professionals, digital transformation managers, and risk specialists. Six main themes emerged from the interview coding process. The most frequently identified theme was human accountability for AI-supported outcomes. Twenty-three participants stated that responsibility must remain with a designated executive, manager, or governance authority even where AI systems generate recommendations or execute routine actions. Participants emphasized that AI agents can support decision-making, but they cannot assume legal, ethical, or organizational responsibility.

Table 9. Qualitative Thematic Findings

Theme	Participants Identifying Theme	Percentage	Main Interpretation
Human accountability for AI-supported outcomes	23	95.8	Final responsibility must remain with identifiable human leaders
Defining AI decision boundaries	22	91.7	Organizations require clear rules on which tasks AI may recommend, initiate, or execute
Control mechanisms for semi-autonomous systems	21	87.5	Audit trails, approval thresholds, monitoring, and escalation procedures are essential
From decision-maker to decision orchestrator	20	83.3	Executives increasingly supervise and validate AI-supported decisions rather than making every decision directly
Trust, explainability, and executive confidence	19	79.2	Trust depends on transparency, reliability, explainability, and the ability to challenge AI outputs
Board and executive governance oversight	16	66.7	Boards and executive committees play a stronger role in high-risk or high-autonomy AI use cases

The interviews showed that executives increasingly viewed their role as one of decision orchestration. Rather than directly reviewing every operational decision, leaders focused on setting strategic objectives, defining decision boundaries, approving high-risk actions, and monitoring whether AI-supported processes remained within authorized limits. Participants also highlighted the importance of explainability and visibility. Where executives could not understand the basis of AI recommendations or trace the steps taken by an AI agent, they were less willing to rely on the system. This finding is consistent with Chan et al. (2024), who emphasize the importance of visibility into AI agents that interact with organizational systems and take actions on behalf of users.

5.7. Integration of Quantitative and Qualitative Findings

The quantitative and qualitative findings converged on the importance of leadership, governance, decision rights, and control mechanisms. The survey findings showed that AI governance maturity had a significant effect on accountability clarity, while the interviews explained that governance structures were most effective when they included practical procedures rather than broad policy statements. Similarly, the

strong relationship between executive decision rights and organizational control effectiveness was supported by interview evidence showing that organizations needed clear approval limits, human override rights, and escalation procedures. Participants explained that the absence of decision boundaries often created uncertainty about who should intervene when AI-supported outcomes were inaccurate, harmful, or inconsistent with organizational priorities.

Table 10. Mixed-Methods Integration Matrix

Quantitative Finding	Qualitative Evidence	Integrated Interpretation
Strategic leadership capability positively affected executive decision quality ($\beta = 0.48$, $p < .001$)	20 of 24 participants described executives as decision orchestrators rather than direct decision-makers	Leaders require AI literacy, strategic judgment, and oversight capability to manage AI-supported decisions effectively
AI governance maturity positively affected accountability clarity ($\beta = 0.56$, $p < .001$)	23 participants emphasized the need for named human accountability	Formal governance structures improve clarity when they assign responsibility for AI-supported outcomes
Executive decision rights positively affected organizational control effectiveness ($\beta = 0.61$, $p < .001$)	22 participants identified decision boundaries as essential	Defined authority limits strengthen monitoring, approval, and escalation processes
Organizational control effectiveness improved trust in agentic AI ($\beta = 0.52$, $p < .001$)	19 participants linked trust to explainability, monitoring, and human intervention	Trust increases where AI activities are visible, reviewable, and subject to human oversight
Trust in agentic AI improved organizational performance ($\beta = 0.39$, $p < .001$)	18 participants reported faster decisions, improved responsiveness, and better resource coordination	Organizations derive greater value from agentic AI when executives and employees trust its use within controlled boundaries

Overall, the findings support the proposed conceptual framework. Strategic leadership capability, AI governance maturity, executive decision rights, and organizational control effectiveness were all associated with stronger decision quality, accountability, trust, and organizational performance. The results further show that higher levels of AI autonomy may improve efficiency and responsiveness, but they also create greater accountability challenges. This reinforces the need for clear leadership structures, formal decision rights, and strong monitoring arrangements in organizations deploying agentic AI systems.

6. Discussion

6.1. Agentic AI and the Changing Nature of Executive Decision-Making

The findings indicate that agentic AI is changing executive decision-making from a process centred mainly on direct human evaluation toward a more distributed model in which executives, managers, technical teams, and AI systems contribute to decision outcomes. The results showed that strategic leadership capability had a significant positive effect on executive decision quality ($\beta = 0.48$, $p < .001$). This suggests that leaders who understand the strategic opportunities, operational limitations, ethical risks, and governance requirements of agentic AI are better positioned to make informed decisions.

The result supports the argument that agentic AI should not be viewed only as a technical tool for automating tasks. It increasingly participates in information gathering, scenario assessment, workflow coordination, risk monitoring, and operational response. As a result, executives are required to move beyond the traditional role of approving final decisions. They must define organizational priorities, set risk boundaries, determine acceptable levels of AI autonomy, and supervise the systems through which decisions are made.

This finding is consistent with Huber and Alexy (2024), who argue that artificial intelligence affects strategic leadership by reshaping how executives access information, evaluate alternatives, and coordinate organizational activities. The present findings extend this perspective by showing that leadership quality becomes particularly important when AI systems are able to initiate or execute actions rather than simply provide recommendations.

The qualitative findings reinforce this interpretation. Twenty of the 24 interview participants described executives as decision orchestrators. Rather than reviewing every individual operational decision, leaders were expected to design decision structures, define escalation points, approve high-risk actions, and ensure that AI-supported processes remained consistent with organizational objectives. This shift does not reduce executive responsibility. Instead, it changes the form of responsibility from direct decision execution to strategic supervision and governance.

6.2. Strategic Leadership Capability in Agentic AI Environments

The results show that strategic leadership capability is one of the main conditions for effective agentic AI adoption. Respondents reported a relatively high mean score for strategic leadership capability ($M = 3.94$), while executive decision quality recorded the highest mean score among the outcome variables ($M = 3.97$). This suggests that organizations with leaders who possess AI awareness, strategic foresight, ethical judgment, and change-management skills are better able to use agentic AI without losing control over critical decisions. Leadership capability is particularly important because agentic AI can create both strategic value and organizational risk. It can improve responsiveness, support resource allocation, identify emerging issues, and coordinate tasks across functions. At the same time, poorly

designed AI systems may produce inaccurate recommendations, reinforce bias, expose sensitive information, or act beyond their intended authority. Leaders must therefore understand not only what AI systems can do, but also where their limitations lie.

The findings align with Krakowski et al. (2023), who argue that AI can reshape competitive advantage through improved learning, coordination, and resource deployment. However, the present study suggests that competitive benefits cannot be achieved through technological investment alone. Organizations require leaders who can connect AI deployment with strategic priorities, governance arrangements, organizational culture, and stakeholder expectations. The results also support the view that executive judgment remains necessary in complex strategic contexts. Felin and Holweg (2024) emphasize that human reasoning remains important where decisions involve causality, uncertainty, long-term consequences, and competing stakeholder interests. Agentic AI may identify patterns and suggest actions, but executives are still required to assess whether those actions are appropriate within the broader organizational and societal context.

6.3. Governance Maturity and Accountability Clarity

One of the strongest findings in the study was the positive relationship between AI governance maturity and accountability clarity ($\beta = 0.56$, $p < .001$). The correlation between these constructs was also high ($r = 0.69$, $p < .01$). This result demonstrates that accountability becomes clearer when organizations establish formal governance structures, documented policies, review mechanisms, ethical guidelines, risk assessments, and approval procedures. The finding is particularly relevant because accountability clarity recorded a lower mean score ($M = 3.69$) than strategic leadership capability and executive decision quality. This indicates that many organizations may be developing AI capabilities faster than they are developing responsibility structures. In practical terms, organizations may know how to deploy AI systems but may remain uncertain about who is responsible when an AI-supported action produces an error, a compliance concern, a financial loss, or an ethical problem.

The qualitative results strongly support this interpretation. Twenty-three of the 24 interview participants stated that responsibility for AI-supported outcomes must remain with a named human leader, manager, or governance authority. Participants repeatedly stressed that AI agents can contribute to decisions, coordinate workflows, and trigger actions, but they cannot assume legal or ethical responsibility. This result is consistent with the organizational AI governance perspective advanced by Mäntymäki et al. (2022), which emphasizes the importance of structures and processes for directing and managing AI use. It also reflects the wider governance concerns identified by Birkstedt et al. (2023) and Batool et al. (2025), including transparency, oversight, stakeholder responsibility, and accountability. The present study adds that these governance principles must be translated into clear organizational roles and practical decision procedures.

6.4. Executive Decision Rights and Organizational Control

The relationship between executive decision rights and organizational control effectiveness was the strongest direct relationship in the structural model ($\beta = 0.61$, $p < .001$). This finding indicates that organizations are more likely to maintain effective control over agentic AI when authority boundaries are clearly defined. Executive decision rights refer to the allocation of authority among executives, managers, technical teams, governance committees, and AI systems. In an agentic AI environment, these rights determine which activities AI may perform independently, which actions require managerial approval, which decisions must be escalated, and when executives must intervene directly.

The findings indicate that unclear authority boundaries may weaken organizational control. For example, when an AI system recommends an action that affects financial exposure, employee performance, customer access, compliance obligations, or strategic priorities, uncertainty may arise regarding whether the decision should be approved by an executive, a business unit manager, a risk officer, or a technical team. Such uncertainty can delay responses, weaken accountability, and create disputes when outcomes are questioned. The qualitative evidence showed that 22 participants considered decision boundaries essential for responsible AI use. Participants emphasized the need for human override rights, predefined approval thresholds, escalation procedures, and documented authority limits. These findings support the argument that organizational control cannot depend only on technical monitoring. It must also include a clear allocation of human authority.

This result is also consistent with Bello y Villarino and Bronitt (2024), who highlight the growing importance of corporate governance, executive oversight, and regulatory accountability in AI-related decision-making. Boards and senior executives should therefore ensure that organizational authority structures are updated as AI systems become more capable of influencing or executing decisions.

6.5. Agentic AI Autonomy, Oversight, and Accountability

The comparative analysis showed that higher levels of agentic AI autonomy were associated with improved executive decision quality, stronger organizational control effectiveness, greater trust in agentic AI, and better organizational performance. However, accountability clarity declined as AI autonomy increased. Organizations operating high-autonomy AI systems reported the highest executive decision quality score ($M = 4.18$), the highest organizational control effectiveness score ($M = 3.88$), and the highest organizational performance score ($M = 3.88$). At the same time, accountability clarity declined from 3.83 in low-autonomy settings to 3.42 in high-autonomy settings.

This finding suggests that organizations may gain efficiency, speed, and coordination benefits as AI systems become more autonomous, but they may also face greater difficulty in identifying who owns a decision or outcome. The decline in accountability clarity may occur because high-autonomy systems perform multiple linked actions across

functions, making it less clear where human responsibility begins and ends. The moderation result supports this interpretation. Executive oversight had a stronger effect on accountability clarity in high-autonomy settings than in low-autonomy settings. This means that executive involvement becomes more important as agentic AI systems are allowed to perform more complex or independent activities.

The result supports Chan et al. (2024), who emphasize the importance of visibility into AI agents that interact with tools, systems, and organizational data. When AI systems perform multi-stage actions, organizations must be able to trace what the system did, what information it used, who authorized its operation, and whether it acted within approved limits. Higher autonomy should therefore not be treated as a simple measure of technological maturity. It should be considered together with governance maturity, risk exposure, decision sensitivity, and the availability of human intervention. High autonomy may be appropriate for routine, low-risk, and reversible tasks. However, decisions involving legal exposure, public safety, financial risk, employee rights, customer access, or strategic direction should remain subject to stronger executive and governance oversight.

6.6. Trust in Agentic AI and Organizational Performance

The findings showed that organizational control effectiveness positively influenced trust in agentic AI ($\beta = 0.52$, $p < .001$), while trust in agentic AI positively influenced organizational performance ($\beta = 0.39$, $p < .001$). These results suggest that trust is not created merely because AI systems produce fast or technically sophisticated outputs. Trust develops when organizational members believe that AI systems are reliable, transparent, monitored, and subject to meaningful human oversight. The qualitative evidence supports this conclusion. Nineteen participants linked trust to explainability, reliability, visibility, and the ability to question or override AI recommendations. Executives were more willing to rely on AI-supported processes when they could understand the basis of recommendations, review decision records, monitor system performance, and intervene when necessary.

This finding is consistent with Gomez et al. (2025), who argue that human-AI collaboration is often less integrated than expected. In many organizations, AI systems may provide outputs without giving decision-makers sufficient confidence to interpret, challenge, or use those outputs appropriately. The current results suggest that organizational controls can reduce this problem by improving transparency and creating clear intervention mechanisms. The positive relationship between trust and organizational performance also supports the work of Neiroukh et al. (2025), who found that AI capability contributes to organizational performance through improved decision-making processes. The present study extends this relationship by showing that trust acts as an important condition between organizational control and performance. Organizations are more likely to gain value from agentic AI when leaders and employees trust the systems within clearly governed boundaries.

6.7. Theoretical and Practical Contributions

The study contributes to strategic leadership research by showing that leadership in agentic AI environments is not limited to technology adoption or digital transformation. It involves designing the structures through which human and AI actors share information, exercise authority, make decisions, and remain accountable for outcomes. The study also contributes to organizational control theory by extending the concept of control beyond human employees and departments. In agentic AI environments, control mechanisms must include decision logs, audit trails, human approval thresholds, access restrictions, escalation procedures, explainability requirements, and periodic performance review. From a practical perspective, the findings suggest that organizations should not allow AI autonomy to increase without corresponding improvements in governance and executive oversight. Leaders should define decision rights before deploying high-autonomy AI systems, identify decisions that require human approval, and establish accountability structures that remain clear even when AI agents coordinate actions across multiple functions.

7. Proposed Strategic Leadership Framework for Agentic AI

7.1. Framework Overview

The proposed Strategic Leadership Framework for Agentic AI provides a structured approach for governing executive decision-making and organizational control in environments where AI systems contribute to, coordinate, or execute organizational actions. The framework is based on the empirical findings of the study, particularly the strong effects of AI governance maturity, executive decision rights, organizational control effectiveness, and trust in agentic AI. The framework is designed to help organizations balance the benefits of agentic AI with the need for human accountability, strategic direction, risk management, and ethical responsibility. It does not treat AI autonomy as an independent objective. Instead, it positions autonomy as a controlled capability that must operate within defined organizational boundaries.

The framework contains five interconnected layers:

1. Strategic Direction and Risk Appetite
2. Executive Decision Rights and AI Delegation Boundaries
3. Governance and Accountability Structures
4. Operational Control and Monitoring Mechanisms
5. Learning, Review, and Continuous Improvement

Each layer supports the next. Strategic direction establishes the purpose and limits of AI use. Decision rights define the authority boundaries between human leaders and AI systems. Governance structures assign responsibility and ensure compliance. Operational controls provide visibility into AI-supported activities. Continuous learning ensures that the organization can improve its policies, controls, and leadership practices over time.

7.2. Layer 1: Strategic Direction and Risk Appetite

The first layer establishes the strategic purpose of agentic AI within the organization. Senior executives and boards should define why agentic AI is being adopted, which organizational objectives it is expected to support, and what level of risk is acceptable. The strategic direction should identify high-priority use cases, such as operational coordination, risk monitoring, customer engagement, decision support, supply chain management, or resource allocation. It should also identify restricted use cases where AI autonomy may create unacceptable legal, ethical, reputational, financial, or operational risks.

Risk appetite is central to this layer. Organizations should determine the level of AI autonomy that is appropriate for different categories of decisions. For example, low-risk administrative tasks may be delegated to AI systems with limited supervision. High-risk decisions involving financial commitments, employee rights, regulatory obligations, customer access, safety, or strategic investments should require human approval. This layer is consistent with the view that strategic leadership must align AI use with organizational priorities and stakeholder expectations (Huber & Alexy, 2024; Krakowski et al., 2023).

7.3. Layer 2: Executive Decision Rights and AI Delegation Boundaries

The second layer defines who has authority to make, approve, review, or override AI-supported decisions. It provides a formal division of responsibility among executives, managers, technical teams, AI governance committees, and the AI system itself.

Decision rights should be documented in a clear authorization matrix. The matrix should identify:

- Decisions that remain exclusively under executive authority
- Decisions that may be supported by AI but require human approval
- Decisions that may be delegated to managers with AI assistance
- Routine tasks that may be executed by AI within predefined boundaries
- Conditions that require immediate escalation to a human authority

This layer directly responds to the study finding that executive decision rights had a strong effect on organizational control effectiveness. Clear decision rights reduce confusion, improve response speed, and make accountability easier to trace. For example, an AI agent may be permitted to prioritize customer service requests, flag suspicious transactions, or recommend inventory adjustments. However, it should not independently approve major capital investments, terminate employees, change pricing policy, override regulatory requirements, or make high-impact strategic commitments without human authorization.

7.4. Layer 3: Governance and Accountability Structures

The third layer establishes the organizational structures responsible for overseeing agentic AI. Governance structures should include senior executive involvement, cross-functional representation, ethical oversight, risk management, and technical expertise. A formal AI governance committee may include representatives from executive leadership, technology, legal, compliance, risk management, internal audit, human resources, data governance, and relevant business units. The committee should review high-risk AI use cases, assess compliance concerns, monitor system performance, approve major changes, and investigate significant incidents.

Accountability structures should identify a named human owner for every agentic AI system. The assigned owner should be responsible for ensuring that the system remains within approved boundaries, performs as intended, and is reviewed when problems occur. The ownership role should not be assigned only to technical staff. Business leaders must also be accountable because AI systems affect operational and strategic outcomes. This layer reflects the finding that AI governance maturity had a strong positive effect on accountability clarity. It also aligns with the governance principles identified by Mäntymäki et al. (2022), Birkstedt et al. (2023), and Batool et al. (2025).

7.5. Layer 4: Operational Control and Monitoring Mechanisms

The fourth layer focuses on the practical controls needed to supervise agentic AI during daily operations. These controls ensure that executives and governance teams can monitor system behaviour, investigate errors, and intervene where necessary.

Key operational controls include:

- Decision logs that record AI recommendations, actions, and approvals
- Audit trails that show how decisions were produced and implemented
- Role-based access controls that restrict system permissions
- Human approval thresholds for high-risk actions
- Explainability requirements for significant recommendations
- Performance monitoring dashboards
- Incident reporting and escalation procedures
- Periodic system testing and compliance review
- Human override mechanisms for urgent or disputed decisions

The study found that organizational control effectiveness was strongly associated with trust in agentic AI. This suggests that people are more likely to rely on AI-supported systems when they can see how the systems operate and when they know that effective intervention mechanisms exist. Operational controls should be proportionate to the level of AI autonomy. Low-autonomy systems may require basic monitoring and periodic review. High-autonomy systems should require continuous monitoring, stronger access

controls, detailed auditability, and formal escalation procedures.

7.6. Layer 5: Learning, Review, and Continuous Improvement

The final layer focuses on organizational learning. Agentic AI systems, governance structures, and leadership practices should be reviewed regularly because business conditions, regulatory expectations, and AI capabilities continue to evolve. Organizations should establish periodic reviews of AI performance, decision quality, error patterns, governance effectiveness, employee feedback, and stakeholder concerns. These reviews should be used to identify whether AI autonomy levels remain appropriate, whether decision rights need to be revised, and whether additional controls are required.

Learning should occur at three levels:

- System level: Reviewing AI performance, reliability, error rates, and operational outcomes.
- Governance level: Reviewing policies, approval procedures, accountability structures, and risk controls.
- Leadership level: Reviewing executive decision practices, AI literacy, strategic alignment, and oversight capability.

This layer ensures that the framework remains adaptive. Rather than relying on a fixed governance structure, organizations can adjust their control mechanisms as AI systems become more capable or as new risks emerge.

Table 11. Strategic Leadership Framework for Agentic AI

Framework Layer	Primary Purpose	Key Mechanisms	Main Responsible Parties	Expected Outcome
Strategic direction and risk appetite	Align agentic AI use with organizational objectives and acceptable risk levels	AI strategy, risk appetite statement, use-case classification, restricted-use policies	Board, chief executive officer, executive leadership team	Strategic alignment and controlled AI adoption
Executive decision rights and delegation boundaries	Define the authority shared between executives, managers, and AI systems	Authority matrix, approval thresholds, human override rights, escalation procedures	Chief executive officer, business unit leaders, AI governance committee	Clear decision ownership and reduced ambiguity
Governance and accountability structures	Assign responsibility and oversee high-risk AI activities	Governance committee, named AI system owner, ethical review, compliance assessment	Executives, legal team, compliance, risk management, internal audit	Strong accountability and regulatory readiness
Operational control and monitoring mechanisms	Ensure AI activities are visible, traceable, and reviewable	Audit trails, decision logs, access controls, monitoring dashboards, incident reporting	Technical teams, risk officers, internal audit, business managers	Improved control effectiveness and trust
Learning, review, and continuous improvement	Adapt AI governance and leadership practices over time	Performance reviews, post-incident reviews, model evaluation, policy updates, leadership training	Executive leadership, AI governance committee, technical teams	Continuous improvement and organizational resilience

7.7. Framework Implementation Process

The framework can be implemented through a phased process.

- Phase 1: Assess organizational readiness: Organizations should assess their existing AI capability, governance maturity, leadership readiness, decision rights, technical controls, and risk management arrangements. This assessment should identify gaps in accountability, monitoring, data governance, and executive oversight.
- Phase 2: Classify AI use cases by risk and autonom y: Each agentic AI use case should be categorized according to its operational impact, decision sensitivity, data access level, reversibility, legal exposure, and degree of autonomy. High-risk use cases should receive stronger governance and closer executive supervision.
- Phase 3: Define decision rights and accountability: Organizations should create an authority matrix that assigns responsibility for AI-supported decisions. This should include executive approval requirements, manager responsibilities, technical ownership, human override rights, and escalation channels.
- Phase 4: Establish operational controls: The organization should implement audit trails, decision logs, access restrictions, monitoring dashboards, explainability tools, incident reporting procedures, and periodic review mechanisms.
- Phase 5: Review and improve: Organizations should regularly evaluate whether agentic AI systems are producing intended benefits, whether control mechanisms remain effective, and whether

accountability structures are still appropriate for the level of autonomy being used.

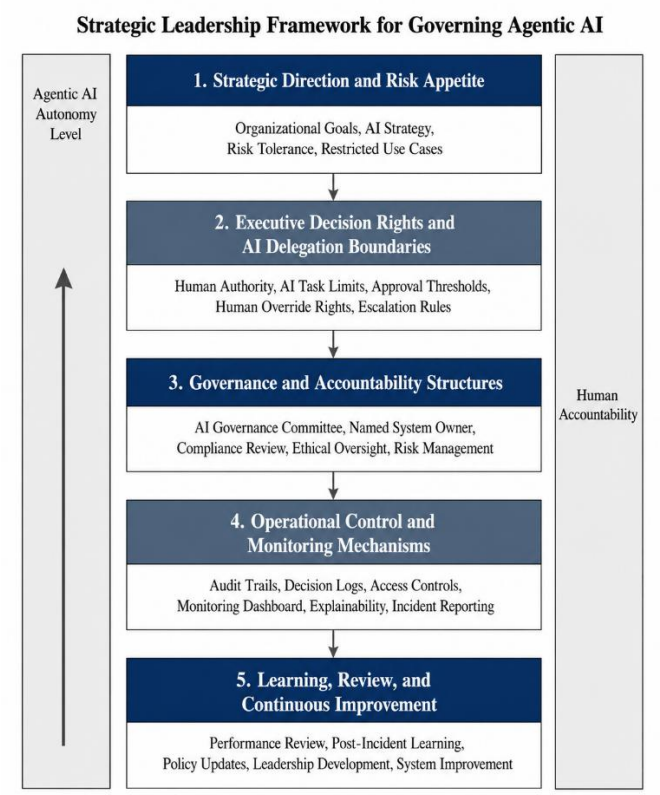

Figure 2. Strategic Leadership Framework for Governing Agentic AI

8. Practical Implications

8.1. Implications for Executives and Senior Leaders

The findings indicate that executives should treat agentic AI as a strategic governance issue rather than only a technology implementation matter. As AI systems move beyond providing information and begin to coordinate workflows, recommend actions, or execute defined tasks, senior leaders must remain responsible for the strategic direction, risk boundaries, and approval conditions that govern those activities. Executives should first define the organizational purpose of each agentic AI deployment. This requires clarity about the business problem being addressed, the expected benefit, the level of acceptable risk, and the decisions that must remain under human authority. Organizations should avoid deploying agentic AI simply because it can automate a process. The suitability of autonomy should depend on the sensitivity of the task, the reversibility of potential errors, the impact on stakeholders, and the legal or ethical consequences of failure.

The results also show that strategic leadership capability has a positive relationship with executive decision quality. This suggests that senior leaders require sufficient understanding of AI-related risks, governance requirements, and operational limitations. Executives do not need to become technical developers, but they should be capable of questioning AI-supported recommendations, assessing the reliability of system outputs, and determining when independent human judgment is necessary. Huber and Alexy (2024) similarly emphasize that AI changes the information and coordination conditions under which strategic leadership is exercised. A practical priority for executives is the establishment of clear human approval thresholds. High-impact decisions involving major financial commitments, workforce consequences, regulatory obligations, public safety, customer eligibility, or strategic investments should not be delegated fully to AI systems. In such cases, agentic AI may support analysis and prepare recommendations, but final approval should remain with a designated executive or governance authority.

8.2. Implications for Organizational Governance

The strong relationship between AI governance maturity and accountability clarity demonstrates that governance cannot remain limited to broad ethical statements or general technology policies. Organizations require formal structures that specify who is responsible for AI-supported decisions, how systems are approved, how risks are assessed, and how incidents are investigated. A practical governance structure should include an AI governance committee or equivalent oversight body. This body should involve representatives from executive leadership, technology, legal, compliance, risk management, internal audit, data governance, human resources, and relevant business functions. The committee should be responsible for reviewing high-risk use cases, approving major changes to AI autonomy levels, monitoring control failures, and ensuring that organizational policies remain aligned with regulatory and ethical expectations.

Every agentic AI system should also have a named human owner. The owner should be accountable for ensuring that the system remains within its approved purpose, operates within authorized boundaries, and undergoes regular review. This responsibility should not be assigned only to technical teams. Business leaders must also be involved because agentic AI affects strategic priorities, operational decisions, customer outcomes, and organizational risk. These requirements are consistent with organizational AI governance research, which emphasizes the importance of formal structures, stakeholder responsibilities, documentation, oversight, and accountability arrangements (Mäntymäki et al., 2022; Birkstedt et al., 2023; Batool et al., 2025).

8.3. Implications for Decision Rights and Organizational Control

The findings show that executive decision rights are central to organizational control effectiveness. Organizations should therefore develop a formal decision-rights framework that distinguishes between tasks that AI may perform independently, tasks that require manager approval, and decisions that remain entirely under executive authority.

This framework should define at least four categories of AI activity:

1. AI-supported analysis: The system gathers information, identifies patterns, or prepares recommendations, while humans retain full decision authority.

2. AI-assisted operational action: The system performs routine tasks within narrowly defined rules, subject to monitoring and periodic human review.
3. Conditional AI autonomy: The system may initiate actions when predefined conditions are satisfied, but significant actions require approval or immediate escalation.
4. Restricted AI activity: The system may not make or execute decisions because the task involves high legal, ethical, strategic, or human impact.

The decision-rights framework should be supported by a clear authorization matrix. This matrix should identify the executive sponsor, business owner, technical owner, risk owner, approval authority, and escalation contact for each AI use case. Such arrangements can reduce uncertainty and make it easier to trace responsibility when an AI-supported action produces an unexpected outcome. Organizations should also strengthen operational control through decision logs, audit trails, access restrictions, performance monitoring, human override rights, incident reporting, and periodic system reviews. The results indicate that stronger control mechanisms contribute to trust in agentic AI. This is important because trust is more likely to develop when leaders and employees can understand how a system operates, review its actions, and intervene when necessary.

8.4. Implications for Boards of Directors

Boards of directors should take a more active role in overseeing high-impact agentic AI deployments. Board oversight is particularly important when AI systems affect corporate risk, financial decision-making, regulatory compliance, workforce management, customer access, or organizational reputation. Boards should require regular reporting on key AI risks, system performance, control failures, and governance actions. They should also ensure that the organization has a clear risk appetite for agentic AI and that high-autonomy systems are subject to stronger approval and monitoring requirements. The role of the board is not to supervise individual AI outputs. Rather, it is to ensure that executive leadership has established adequate structures for accountability, monitoring, ethical oversight, and incident response. Bello y Villarino and Bronitt (2024) highlight the growing relevance of board-level responsibility and corporate oversight in relation to AI-related risk and accountability.

8.5. Implications for Employees and Cross-Functional Teams

The findings also have implications for employees, managers, and technical teams who work with agentic AI systems. Successful implementation depends on collaboration among business leaders, data professionals, risk teams, legal advisers, operational managers, and end users. Organizations should provide training that helps employees understand the role of agentic AI in their work, the limits of system autonomy, the process for challenging AI-supported recommendations, and the conditions under which concerns should be escalated. Employees should not feel that they must accept AI outputs without question. They should be encouraged to identify errors, raise concerns, and apply professional judgment when AI recommendations conflict with practical knowledge or organizational values. This is especially important because human-AI collaboration is often less integrated than organizations assume. Gomez et al. (2025) note that users may struggle to interpret or challenge AI outputs effectively. Training, communication, and clear escalation pathways can reduce this risk and improve the quality of human-AI decision-making.

9. Limitations of the Study

This study has several limitations that should be considered when interpreting the findings.

First, the study relies partly on self-reported survey responses. Participants may overestimate the maturity of their organization's AI governance arrangements, leadership capability, or control effectiveness. Respondents may also provide socially desirable answers, particularly where questions concern accountability, ethical oversight, or compliance practices. Future studies could reduce this limitation by combining survey responses with objective evidence such as AI policy documents, audit records, governance reports, incident logs, or system performance data.

Second, the cross-sectional research design limits the ability to establish long-term causal relationships. The study captures perceptions and organizational conditions at a particular point in time. However, leadership capability, governance maturity, trust, and organizational performance may change as AI systems develop and as organizations gain more experience with agentic AI. Longitudinal research would provide a stronger understanding of how these relationships evolve over time.

Third, the study focuses on organizations with some level of AI adoption or interest in agentic AI. The findings may therefore be less applicable to organizations that have not yet begun AI implementation or that operate in sectors with limited digital infrastructure. The experiences of highly digitalized organizations may differ substantially from those of smaller firms, public institutions, or organizations operating in resource-constrained environments.

Fourth, agentic AI remains an evolving field. The capabilities, risks, governance practices, and regulatory expectations associated with these systems may change rapidly. As a result, some specific control mechanisms or autonomy classifications proposed in this study may need to be revised as technologies and regulations mature.

Fifth, the study does not focus on one specific industry. While this broad approach improves general relevance, it may reduce attention to sector-specific issues. Healthcare, finance, manufacturing, public administration, and technology services face different regulatory obligations, data sensitivities, operational risks, and stakeholder expectations. The governance structures that are appropriate in one sector may not be sufficient in another.

Finally, the study examines leadership, governance, and organizational control primarily from the perspective of executives and professionals involved in AI-related decision-making. The perceptions of frontline employees, customers, citizens, suppliers, and other stakeholders may provide additional insight into the practical consequences of agentic AI deployment. Future research should include these perspectives where appropriate.

10. Future Research Directions

Future research should examine agentic AI leadership and governance across specific industries. Sector-focused studies could identify whether the relationship between AI autonomy, executive oversight, and accountability differs in financial services, healthcare, public administration, logistics, manufacturing, or technology firms. Such studies would help develop more context-sensitive governance frameworks.

Longitudinal research is also needed to examine how organizations adapt as agentic AI systems become more capable and more widely integrated into daily operations. A longitudinal design could track changes in leadership roles, governance maturity, decision rights, control mechanisms, trust, and organizational performance over several years. This would provide stronger evidence about whether organizations improve their governance practices as AI autonomy increases.

Further research could investigate board-level AI governance in greater detail. This may include studies of how boards assess AI-related risk, how they receive information about agentic AI systems, and how they influence executive accountability. Comparative studies could examine whether board involvement differs between public and private organizations, regulated and non-regulated industries, or organizations with different levels of AI maturity.

Another important area is the design of measurable AI governance maturity models. Future research could develop and validate maturity scales that assess organizational readiness across strategic leadership, decision rights, ethical oversight, technical controls, auditability, employee capability, and incident response. Such models could help organizations evaluate their current position and identify areas requiring improvement.

Researchers should also examine the relationship between explainability, trust, and executive decision quality. Although this study found that control effectiveness supports trust in agentic AI, future work could test whether different forms of explainability are more useful for executives, managers, technical teams, and frontline employees. Some decisions may require detailed technical explanations, while others may require concise business-oriented justifications.

Future studies may also explore human override practices. This includes examining when employees and executives choose to override AI recommendations, the reasons for those decisions, the consequences of override actions, and whether organizations learn from those interventions. Such research could help determine how to balance automation efficiency with informed human judgment.

Finally, future research should consider the broader social implications of agentic AI. This includes its effects on employee autonomy, job redesign, workplace trust, decision fairness, customer relationships, public accountability, and organizational legitimacy. Agentic AI is likely to affect not only how decisions are made but also how organizations are perceived by employees, customers, regulators, and society.

11. Conclusion

Agentic AI is reshaping the relationship between strategic leadership, executive decision-making, and organizational control. Unlike earlier AI systems that mainly supported analysis or automation, agentic AI can coordinate tasks, monitor conditions, recommend actions, and execute activities within defined boundaries. This creates new opportunities for improved responsiveness, efficiency, decision quality, and organizational performance. It also creates significant challenges related to accountability, trust, authority, transparency, and risk. The findings of this study demonstrate that effective agentic AI governance depends on more than technological capability. Strategic leadership capability, AI governance maturity, executive decision rights, and operational control mechanisms are essential for ensuring that AI-supported activities remain aligned with organizational objectives and human responsibility.

The study found that strategic leadership capability improved executive decision quality, while AI governance maturity strengthened accountability clarity. Clear executive decision rights improved organizational control effectiveness, and stronger controls supported trust in agentic AI. Trust, in turn, contributed to better organizational performance. However, the findings also showed that accountability clarity may decline as agentic AI autonomy increases. This confirms that higher levels of autonomy require stronger executive oversight, better documentation, clearer authority boundaries, and more robust escalation procedures. The proposed Strategic Leadership Framework for Agentic AI provides a practical response to these challenges. Its five layers, strategic direction and risk appetite, executive decision rights and delegation boundaries, governance and accountability structures, operational control and monitoring mechanisms, and continuous learning and improvement, offer organizations a structured approach for managing agentic AI responsibly. The central conclusion is that agentic AI does not remove the need for strategic leadership. Instead, it increases the importance of leadership. Executives must become architects of human-AI decision systems that combine technological capability with clear accountability, ethical judgment, organizational control, and long-term strategic responsibility.

References

[1] Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. *AI and Ethics*, *5*, 3265–3279. DOI: 10.1007/s43681-024-00653-w

[2] Bello y Villarino, J.-M., & Bronitt, S. (2024). AI-driven corporate governance: A regulatory perspective. *Griffith*

Law Review, 33(4), 355–374. DOI: 10.1080/10383441.2024.2405752

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

[4] Camilleri, M. A. (2024). Artificial intelligence governance: Ethical considerations and implications for social responsibility. *Expert Systems, 41*(7), e13406. DOI: 10.1111/exsy.13406

[5] Chan, A., Ezell, C., Kaufmann, M., Wei, K., Hammond, L., Bradley, H., Bluemke, E., Rajkumar, N., Krueger, D., Kolt, N., Heim, L., & Anderljung, M. (2024). Visibility into AI agents. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 958–973). Association for Computing Machinery. DOI: 10.1145/3630106.3658948

[6] Csaszar, F. A., Ketkar, H., & Kim, H. (2024). Artificial intelligence and strategic decision-making: Evidence from entrepreneurs and investors. *Strategy Science, 9*(4), 322–345. DOI: 10.1287/stsc.2024.0190

[7] Doshi, A. R., Bell, J. J., Mirzayev, E., & Vanneste, B. S. (2025). Generative artificial intelligence and evaluating strategic decisions. *Strategic Management Journal, 46*(3), 583–610. DOI: 10.1002/smj.3677

[8] Felin, T., & Holweg, M. (2024). Theory is all you need: AI, human cognition, and causal reasoning. *Strategy Science, 9*(4), 346–371. DOI: 10.1287/stsc.2024.0189

[9] Gomez, C., Cho, S. M., Ke, S., Huang, C.-M., & Unberath, M. (2025). Human-AI collaboration is not very collaborative yet: A taxonomy of interaction patterns in AI-assisted decision making from a systematic review. *Frontiers in Computer Science, 6*, 1521066. DOI: 10.3389/fcomp.2024.1521066

[10] Huber, D. M., & Alexy, O. (2024). The impact of artificial intelligence on strategic leadership. In Z. Simsek, C. Heavey, & B. C. Fox (Eds.), *Handbook of research on strategic leadership in the Fourth Industrial Revolution* (pp. 108–136). Edward Elgar Publishing. DOI: 10.4337/9781802208818.00012

[11] Kanbach, D. K., Heiduk, L., Blueher, G., Schreiter, M., & Lahmann, A. (2024). The GenAI is out of the bottle: Generative artificial intelligence from a business model innovation perspective. *Review of Managerial Science, 18*(4), 1189–1220. DOI: 10.1007/s11846-023-00696-z

[12] Kanitz, R., Gonzalez, K., Briker, R., & Straatmann, T. (2023). Augmenting organizational change and strategy activities: Leveraging generative artificial intelligence. *The Journal of Applied Behavioral Science, 59*(3), 345–363. DOI: 10.1177/00218863231168974

[13] ALAMPALLY, J. (2024). Real-Time and Near-Real-Time Analytics in Healthcare Data Ecosystems. Journal of Computer Science and Technology Studies, 6(1), 314-324.

[14] Kim, J.-S., & Seo, D. (2023). Foresight and strategic decision-making framework from artificial intelligence technology development to utilization activities in small-and-medium-sized enterprises. *Foresight, 25*(6), 769–787. DOI: 10.1108/FS-06-2022-0069

[15] Kim, J. Y., Hasan, A., Kueper, J., Tang, T., Hayes, C., Fine, B., Balu, S., & Sendak, M. (2025). Establishing organizational AI governance in healthcare: A case study in Canada. *npj Digital Medicine, 8*, Article 522. DOI: 10.1038/s41746-025-01909-3

[16] Krakowski, S., Luger, J., & Raisch, S. (2023). Artificial intelligence and the changing sources of competitive advantage. *Strategic Management Journal, 44*(6), 1425–1452. DOI: 10.1002/smj.3387

[17] Nagraj, A. (2022). Modernizing Legacy Banking Systems: Migration Strategies and Cost Optimization in Financial Enterprises. Frontiers in Computer Science and Artificial Intelligence, 1(1), 43-52.

[18] Asthana, A. N., & Charan, N. (2023). Minimising catastrophic risk in the chemical industry: Role of mindfulness. European Chemical Bulletin, 12, 7235-7246.

[19] Kshetri, N., Dwivedi, Y. K., Davenport, T. H., & Panteli, N. (2024). Generative artificial intelligence in marketing: Applications, opportunities, challenges, and research agenda. *International Journal of Information Management, 75*, Article 102716. DOI: 10.1016/j.ijinfomgt.2023.102716

[20] Mukherjee, C. Ai-Driven Personalization of Power System Learning Modules Using Student Personas based on Behavioral Analysis of Grid Performance.

[21] Nadia, N. Y., Rabby, H. R., Arif, M. H., Tanvir, M. I. M., Ahmed, M., & Firdaus, S. (2025, October). Scalable RNN-Based Transfer Learning for Patient Sentiment Monitoring in Telehealth Platforms. In 2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS) (pp. 1-6). IEEE.

[22] Takon, A. (2025). Explainable AI for Threat Modelling and Decision Support in Engineering Assets. Journal of Cyber-Physical Security and Robotics, 1(02), 46-52.

[23] Mukherjee, C. (2025). Combating digital media piracy with agentic ai: Leveraging video transcription and character recognition for automated enforcement. Authorea Preprints.

[24] Anifowose, K. (2025). Development and Validation of AI-Assisted Analytical Methods for Biochemical Compound Detection in Pharmaceutical Chemistry. Journal of Applied Pharmaceutical Sciences and Research, 8(4), 41-52.

[25] Mukherjee, C. (2025). Use of Agentic AI with OpenAI and Prompt Engineering and State-of-the Art Machine Learning Algorithm to detect the patterns in IOT Device Network Intrusion Attacks. Authorea Preprints.

[26] Ravikumar, V. (2025). Therapeutic Bot: Ethical Concerns in AI therapy for Neurodivergence. J Int Scient Re Rep.

[27] Mukherjee, C. (2025). Use of Agentic AI with LLM and Prompt Engineering and State-of-the Art Machine Learning Algorithm to detect the patterns in IOT Device Network Intrusion Attacks. TechRxiv. August, 6.

[28] Takon, A. (2025). 3D Object Detection and Localization for Industrial Threat Monitoring. Well Testing Journal, 34(S3), 850-880.

[29] Mukherjee, C. (2025). Harnessing large language models and ai agents for child behavior analytics in day care: a proof of concept for next-generation parental insight

using simulated data. Machinery and Production Engineering, 174(2870), 26-34.

[30] Mukherjee, C. (2025). Combating digital media piracy with agentic ai: Leveraging video transcription and character recognition for automated enforcement. Authorea Preprints.

[31] Takon, A. (2024). Data-Driven Threat Intelligence for Energy and Critical Asset Management. International Journal of Technology, Management and Humanities, 10(04), 253-266.

[32] Kola, J. N. Longitudinal Cohort Intelligence for Self-Insured Employer Groups: A Predictive Framework for Healthcare Cost Trajectory Modeling and Proactive Risk Intervention.

[33] Adepoju, S. A., & Adepoju, M. A. (2024). From Portals to Case Graphs: A Reference Architecture and Benchmark for Safety Investigation Operations with Agentic Orchestration.

[34] Takon, A. (2024). Data Science Approaches to Asset Integrity Management in Offshore and Onshore Oil and Gas Operations. Multidisciplinary Innovations & Research Analysis, 5(2), 17-31.

[35] Kola, J. N. (2011). An Integrated Framework for Data Mining and Distributed Database Optimization in Resource-Constrained Network Environments. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 2(02), 82-86.

[36] Ravikumar, V. (2014). Fair and optimal resource allocation in wireless sensor networks.

[37] Naidu, K. J. (2014). Secure OLAP Reporting Architectures: Integrating Role-based Access Control and Query Execution Plan Optimization for Enterprise Analytical Environments. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 5(02), 155-159.

[38] López-Solís, O., Luzuriaga-Jaramillo, A., Bedoya-Jara, M., Naranjo-Santamaría, J., Bonilla-Jurado, D., & Acosta-Vargas, P. (2025). Effect of generative artificial intelligence on strategic decision-making in entrepreneurial business initiatives: A systematic literature review. *Administrative Sciences*, *15*(2), Article 66. DOI: 10.3390/admsci15020066

[39] Marasani, Y. (2025). Explainable AI Frameworks for Patient-Level Claims Data Analytics. J Artif Intell Mach Learn & Data Sci, 8(1), 3382-3390.

[40] Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, *2*, 603–609. DOI: 10.1007/s43681-022-00143-x

[41] Nagraj, A. (2024). GraphQL in Wealth Management Platforms: Optimizing Data Access and Performance. British Journal of Multidisciplinary Studies, 2(1), 16-24.

[42] Mariani, M., & Dwivedi, Y. K. (2024). Generative artificial intelligence in innovation management: A preview of future research developments. *Journal of Business Research*, *175*, Article 114542. DOI: 10.1016/j.jbusres.2024.114542

[43] Moro-Visconti, R. (2025). Is artificial intelligence a new stakeholding agent? *Human-Intelligent Systems Integration*, *7*, 3–16. DOI: 10.1007/s42454-025-00069-9

[44] MARASANI, Y. (2024). Enterprise Readiness for Generative AI: The Critical Role of Data Engineering. Frontiers in Computer Science and Artificial Intelligence, 3(2), 59-71.

[45] Neiroukh, S., Emeagwali, O. L., & Aljuhmani, H. Y. (2025). Artificial intelligence capability and organizational performance: Unraveling the mediating mechanisms of decision-making processes. *Management Decision*, *63*(10), 3501–3532. DOI: 10.1108/MD-10-2023-1946

[46] Sriharan, A., Sekercioglu, N., Mitchell, C., Senkaiahliyan, S., Hertelendy, A., Porter, T., & Banaszak-Holl, J. (2024). Leadership for AI transformation in health care organization: Scoping review. *Journal of Medical Internet Research*, *26*, e54556. DOI: 10.2196/54556

[47] MARASANI, Y. (2023). Machine Learning Models for Predicting Patient Treatment Switching Using Claims Data. Frontiers in Computer Science and Artificial Intelligence, 2(1), 59-66.

[48] ALAMPALLY, J. (2024). Enhancing data quality and trust in AI systems through robust data engineering. Frontiers in Computer Science and Artificial Intelligence, 3(1), 120-130.

[49] Mukherjee, C. (2025). Use of Agentic AI with LLM and Prompt Engineering and State-of-the Art Machine Learning Algorithm to detect the patterns in IOT Device Network Intrusion Attacks. TechRxiv. August, 6.

[50] Sakthivel, A. (2025). Agentic Ai In the Enterprise: How Autonomous Ai Systems Will Reshape Business Strategy, Operations, and Leadership. Well Testing Journal, 34(S3), 767-785.