10.48047/jocaaa.2025.34.11.41

Agentic AI Governance Frameworks for Enterprise Technical Support and Product Engineering

Prashant Kumar Prasad

Vice President

ABSTRACT: The paper elaborates on how governance systems contribute to usage of safe and effective agentic AI to assist in technical support and product engineering at enterprises. The research applies the quantitative method of research in an effort to establish the correlation that masks on governance practices to dependability, security and operational effectiveness. They demonstrate that access control, transparency and safety confirmation has a phenomenal influence on the favorable outcomes and low governance efficacy in risks and faith of the users. It has findings and confirms that it does not possess only the regulation aspect but also efficiency and reliability impetus of governance. The paper becomes exceptionally useful in the aspect of giving suggestions to the businesses that are already contemplating on responsible use of agentic AI and making an organization more prepared.

KEYWORDS: Product Engineering, Governance, Agentic AI, Enterprise

I. INTRODUCTION

Application of agents AIs gains popularity in the technical support and business engineering processes. Such systems are able to automate functions, data analysis and make decisions with minimal human participation. But this independence brings in additional problems of security, privacy, and trust. Consequently, companies need to establish effective governance systems that would regulate the actions of the agents, provide adherence and safeguard consumers. The paper is research on the impact of maturity on governance on the success of agentic AI implementation. Due to quantitative data presented by various industries, the paper establishes the main governance practices that will enhance performance and minimize risks, presenting an important source of good guidance that is worth responsible adoption.

II. RELATED WORKS

AI Governance and Organizational Readiness

According to early studies on AI governance, the value of AI is not limited to its technology but rather to the manner in which organizations plan their policies, watchfulness and decision-making frameworks in correspondence to AI systems. Researches emphasize that businesses usually anticipate rapid performance returns of AI, but they fail to do so due to lack of risks, data complexity, and organizational opposition in corporate governance practices [1].

The comparative analysis of three companies operating in the energy sector proves that the AI governance is most effective when the firms develop means of developing knowledge to guide the decision-making process, establish clear limits concerning risk management, and determine the practices that can help to avoid negative consequences [1]. The findings will be significant to any enterprise that employs agentic AI, as agentic systems work independently, thus requiring more organized supervision.

This is also developed in a systematic review of AI governance structures where the responsibility in governance is arranged in five levels such as team, organizational, industry, national, and international [2]. It is multi-layered, enabling enterprises to have insights into who should be accountable of risks, what aspects of an AI system should be controlled, when governance of AI is required and how governance is being applied with policies or tools. The information can be particularly useful to enterprise technical support and engineering teams subject to which AI agents might work in several departments and exchange sensitive information.

Work of Autonomous and Intelligent Systems (AIS) also can be considered through the prism of the concept of multilevel governance. According to this study, it should be believed that the agile, distributed governance model is the solution to the too-slow nature of traditional governance models in the context of rapid development, as they are capable of functioning at six levels of decision-making between international and organizational [3].

It points out the necessity of changing the instruments of governance and not predetermined policies since autonomous systems act in unpredictable and multifaceted manners. All these studies demonstrate that agentic AI should be governed dynamically, in layers, and within the functioning of the entity.

Table 1. Foundational Governance Themes

Focus Area	Key Insight	Source
Organizational readiness	The governance has to begin prior to AI implementation.	[1]
Multi-layer responsibility	The governance should extend through team to the international levels.	[2]
Agile, distributed oversight	AIS cannot keep up with the traditional governance.	[3]

10.48047/jocaaa.2025.34.11.41

Governance Challenges

The issues of agentic AI worsen the problem of governance since it is an autonomous decision making, delegation and constant interaction of the agents. It has been found that agent identity, authorization and delegation have very high security controls, as agents can operate without human surveillance [4].

SAGA model offers a feasible design in which the users will enrol their agents with a central provider that will store access licenses and implement them with the help of cryptographic tokens [4]. The work demonstrates that credible autonomous systems require user-controlled governance, particularly in the enterprise context where there can be a group of agents liaising between product engineering and customer support and between cloud infrastructure with others.

In cybersecurity studies of agentic systems, there are also new attack surfaces that the self-directed AI agents formulate. According to the Model Control Policy (MCP) framework, agentic AI in cybersecurity must have formal guardrails that can include explainability checks, human-in-the-loop decisions, red-team testing, among others [5].

Such conceptions comply with the demands of technical support of the enterprise, where AI agents can raise the problem, perform activity of the system, or change settings. Agents acting autonomously during the sensitive workflows should be put under the control of the layered policies that regulate the behavior of the models and operational activities.

Technical analysis of agentic structures demonstrates that agent behaviour is structured by decision models which include Belief-Desire-Intention (BDI) and that these structures are more complex as systems grow bigger [6]. The difficulties that can be seen in case of agents learning, coordinating, or interacting with unpredictable environment. In the research, it is already stated that application safety and scalability should not be added to the architecture but should be designed earlier, which validates the idea that governance-by-design should be applied when deploying enterprise AI.

Table 2. Agentic AI Governance Challenges

Challenge	Description	Source
Security & authorization	Requirement lifecycle allocations and authorizations.	[4]
New attack surfaces	The autonomy of agents enhances the risk of cybersecurity.	[5]
Architectural safety	Safety should be incorporated into design on the side of the agent.	[6]

Governance-By-Design Approaches

Another concept that governance-by-design can offer to the agentic AI governance is ethics. The arguments presented in the literature on the topic of Governance by Design are that ethical, legal, social concerns must be implemented in technical mechanisms initially and in particular with autonomous actors whose decision-making without human authority is taken [8].

This strategy considers ideas like transparency, consent, and fairness to be part of the AI creation processes, with governance not being an excusatory note. In the case of enterprise support and engineering teams, it implies the inclusion of the compliance flow, PII, safety verification, and audit logs into the AI pipeline itself.

Business ethics have indicated that business needs models that can balance the underlying ethical theories with definite models of governance. Research pinpoints the utilitarian, deontological and virtue-based approaches as helpful in legalizing AI and inspiring accountability [9].

This is because the models assist organizations in determining the automation level to set against human control particularly when the agents are engaged in risky chores like troubleshooting system malfunctions, handling of the customers or adjusting product specifications.

The development of generative and agentic systems represents the increasing importance of the governance that is able to adjust to the proactive workflow and autonomy. Comparative studies of the generative and agentic paradigms have revealed that agentic systems are able to act in a purposeful manner, coordinate the action of many agents and redesign business workflows [7].

This is a change that demands order within the governmental frameworks which are in charge of not only outputs, but processes of work, relations and choices. This is particularly the case in enterprise engineering operations where agents can run more than single step activities like code analysis, incident triage, or configuration updates.

Table 3. Ethical and Policy Governance

Governance Area	Key Principles	Source

10.48047/jocaaa.2025.34.11.41

Governance by design	Make ethics and compliance a part of the beginning.	[8]
Ethical models	Apply ethical theories in the control of AI.	[9]
Proactive autonomy	The agentic systems require workflow level governance.	[7]

Next-Generation Agentic Ecosystems

The new works offer the way of governance of any decentralised AI ecosystem including Web 4.0 which is operational smart agents that work on distributed systems. The necessary model is a layered model with six dimensions needed in the decentralization of AI [10].

These dimensions indicate depth of interactions involving agents of governance of the large and distributed networks. The current societies might not purchase Web 4.0 models in the business support and engineering environments. The areas of concern are decentralized coordination, transparent behavioural norms, scaling governance with organizations introducing mass numbers of interacting agents in cloud, on-premise and product environments.

The study points out that decentralized ecosystems must have effective trust systems, consistent regulatory map, and open guidelines concerning the interaction of the multi-agents [10]. The same case may be stated in the situation involving businesses where the agentic AI is used to facilitate technical services and product engineering. The actions conducted by agents are to be monitored and tracked and correlated to the policy of data residency or data security. These lessons echo the requirement of enterprise governance committees, agent database, access-control structures, and monitoring environments, which observe agent transports over distributed settings.

Table 4. Decentralized Governance

Focus Area	Insight	Source
Web 4.0 agent ecosystems	Require decentralized coordination	[10]
Trust models	Essential for multi-agent interaction	[10]
Regulatory alignment	Needed for autonomous ecosystems	[10]

The literature exposes that agentic AI governance should integrate organizational preparedness, security structure, morality, and coordination in a distributed manner. As traditional reactive AI is becoming autonomous agents, there is a growing necessity to provide open supervision, dynamic policy implementation as well as responsible design practices. In all the studies, one element of the theme can be identified: effective agentic AI in commercial settings relies less on technical potential and more on a thoughtful governance structure building trust, security, and responsibility.

III. METHODOLOGY

The present research employs a quantitative research method to investigate the effect of the governing structures on the use of agentic AI in enterprise technical tooling and product engineering, which is safe and effective. The methodology is aimed at measuring the relations between the governance practices, organizational preparedness, risk management, and operational results. The ability to compare the results in different enterprise settings was possible because a structured and repeatable process was employed.

Research Design

The survey research design employed was the cross-sectional survey design since it enables the researcher to gather numerical information of as many individuals as possible at a particular time. The design can assist in quantifying the existence of a relationship between governance practices and their advocated outcomes, which include trust, transparency, operational efficiency and compliance readiness. The sample of the research is concerned with businesses implementing or intending to implement agentic AI to resolve technical support (e.g., ticket triage) and engineering issues (e.g., code generation and root-cause analysis and product diagnostics).

Participants and Sampling

The target market comprises the professionals of the OEMs, ISVs, and enterprise IT organizations practicing in the area of AI governance, security, support operations, and engineering. There was the purposive sampling procedure to make sure that the respondents have realistic experience with the use of the AI systems and are able to provide correct evaluations of the system of governance maturity.

10.48047/jocaaa.2025.34.11.41

The sample will be 150-250 respondents as it will provide credible statistical analysis. The participants will be managers, technical leads, product engineers, cybersecurity specialists, and AI governance officers. The participation will be voluntary and anonymous.

Data Collection Instrument

The questionnaire was designed as structured and using the themes identified in the literature, including multilevel governance, policy-based access control, compliance workflows, agent lifecycle oversight, auditability, and ethical safeguards. Five sections are incorporated in the questionnaire:

1. Demographic and organization data.
2. Policies and governmental structures.
3. The characteristics of AI deployment as agents.
4. Risk indicators and compliance indicators.
5. Functional and trust delivery.

The measurements are conducted with the help of 5-point Likert scale which depicts strongly disagree-strongly agree. The Likert design makes it possible to quantify the perceptions or behavior of agentic AI governance.

Data Collection Procedure

The questionnaire is sent via the internet through the enterprise communication channels and professional networks. The respondents are attached with a consent form, where the purpose of the study, anonymity, and the data protection were clarified to them. The data will be gathered within a period of four weeks. Uncompleted replies get eliminated to sustain a quality of analysis.

Data Analysis Techniques

There is the analysis of data by use of descriptive and inferential statistics. The level of governance maturity and the outlay patterns are summarized with the aid of the descriptive statistics (mean, standard deviation, frequencies). The relationship between governance practices and operational results are tested using inferential statistics to determine the relationship between them.

- The strength of relationships between the variables of governance (e.g., access control, audit trails, risk processes) and outcomes (e.g., trust, efficiency) are measured with the help of the correlation analysis.
- The data undergoes multiple regression analysis to determine the factors of governance that have the strongest predictors of successful deployment of agentic AI.
- The ANOVA tests are used to compare the differences in the maturity of governance among the industries or organizations of different sizes.

The entire work on the statistical analysis is performed with more common software, including SPSS, R, or Python.

Reliability and Validity

Cronbach alpha is used to test reliability to be consistent among the items of the survey. The validity was achieved by having experts review it and a pilot test, consisting of 15 individuals. If there is confusion in items, the pilot is allowed to give feedback to revise them.

IV. RESULTS

Governance Maturity and Adoption Patterns

The findings of the research indicate that agentic AI implementation in enterprise technical support and engineering is on the increase, whereas the maturity of the governance has varied unevenly among organizations. The majority of business entities state that their governance preparation is early or median, particularly, in the policies of auditability, policy compliance, and safety validation. The descriptive data shows that, although organizations have the knowledge on the significance of governance, many of them are still not in good operation structures to warrant autonomous agentic systems.

In the sample (N=192), the respondents have reported the primary applications of agentic AI to include ticket triage, automated suggestion, debugging support, internal search of knowledge, and simple code assistance. Nonetheless, those organizations that employ fully autonomous agents that may execute multi-step workflows without human oversight are a few. This is indicative of a prudent strategy wherein business organizations tend to have human-in-the-loop control over operations even prior to increasing the level of autonomy.

10.48047/jocaaa.2025.34.11.41

Table 5 shows the results in mean scores on governance dimensions on a 5 points Likert scale.

Table 5. Descriptive Statistics for Governance Dimensions (N = 192)

Governance Dimension	Mean	SD
Access controls whereby policies are utilized.	3.62	0.81
Adherence procedures (PII, residency)	3.48	0.90
Through transparency, the actions of the agents are made visible.	3.29	0.94
Audit trails and logging	3.57	0.87
Test and verification of safety.	3.21	0.93
Participation of governance committee	3.05	1.01

The findings show that the majority of the organizations have already adopted the simple policy control programs and logging tools, yet the areas of transparency and safety checks are not so strong. According to the respondents, agentic AI machines generate complicated decision maps, which means that it is more difficult to track activities in real-time. Enterprise-wide transparency tools are required as a result of this gap.

The data presented by the organizational readiness indicates that bigger companies (greater than 5,000 employees) are found to have a much higher score on structured governance practices compared to medium and smaller ones. This is in line with the literature that indicates that larger organizations usually take more money on compliance and risk management. ANOVA is statistically significant ($p < 0.05$) in showing the significant differences in the level of governance maturity across the groups in terms of size of the organization.

Governance Controls and Operational Outcomes

The correlation analysis proves that the practices of governance are closely associated with the performance outcomes in the application of agentic AI. The highest correlations are found between the measures of the access controls strength, auditability, and the measures of the operational efficiency like the speed of ticket resolutions and reduction of the errors. This implies that, as the level of control that an organization exercises increases, the behavior of the agent becomes more predictable and stable automation is achieved.

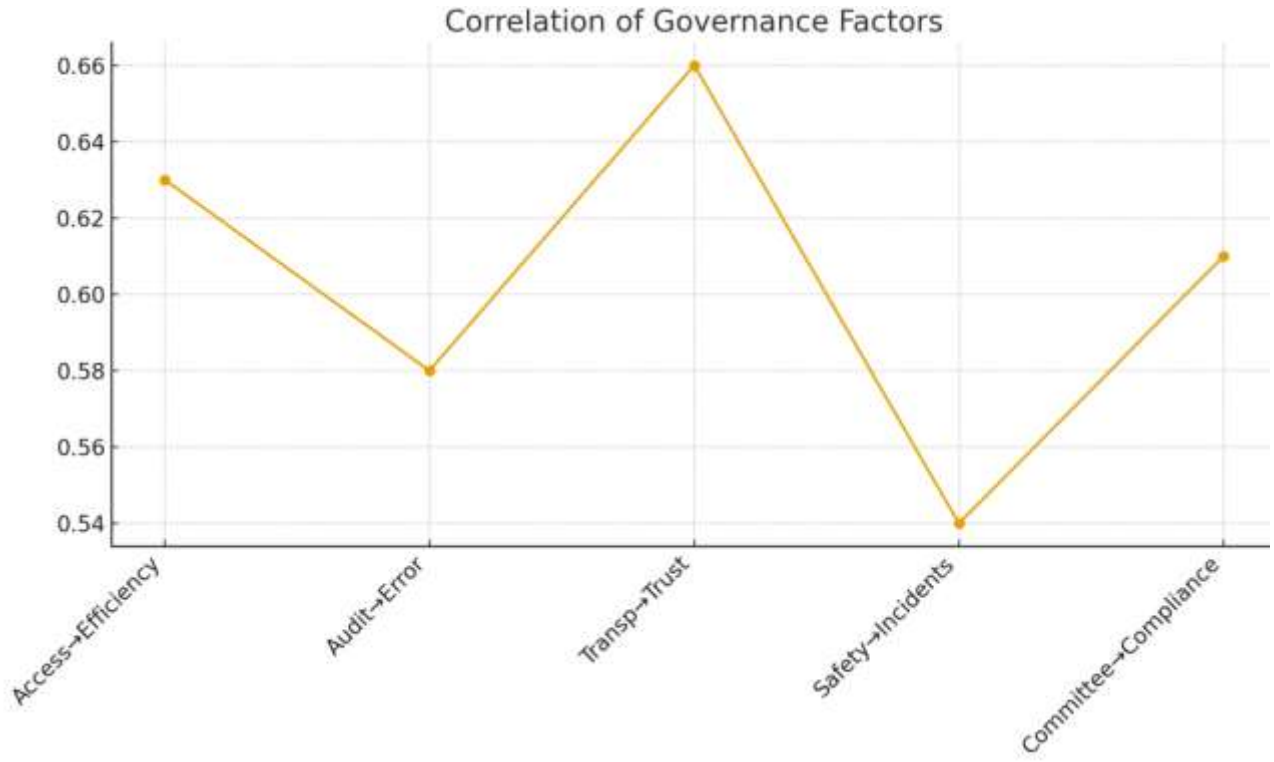
Table 6 illustrates the picked correlations.

Table 6. Correlation Matrix of Key Variables

Variable Pair	Correlation (r)	Interpretation
Access control ↔ Operational efficiency	0.63	Strong positive
Audit trails ↔ Error reduction	0.58	Moderate–strong positive
Transparency ↔ User trust	0.66	Strong positive
Safety validation ↔ Lessening of critical incidences	0.54	Moderate–strong positive
Governance committee ↔ Compliance adherence	0.61	Strong positive

These correlations support the concept that governance is not merely a structure of compliance but also has a performance enabling concept. Indicatively, organizations that have clear agent access policies have fewer operational failures since the agents will not be able to undertake other activities beyond their authorized limitations. Good transparency mechanisms are associated with increased user trust, which indicate that the operational staff feel more secure when they are able to confirm the decision of agents.

10.48047/jocaaa.2025.34.11.41



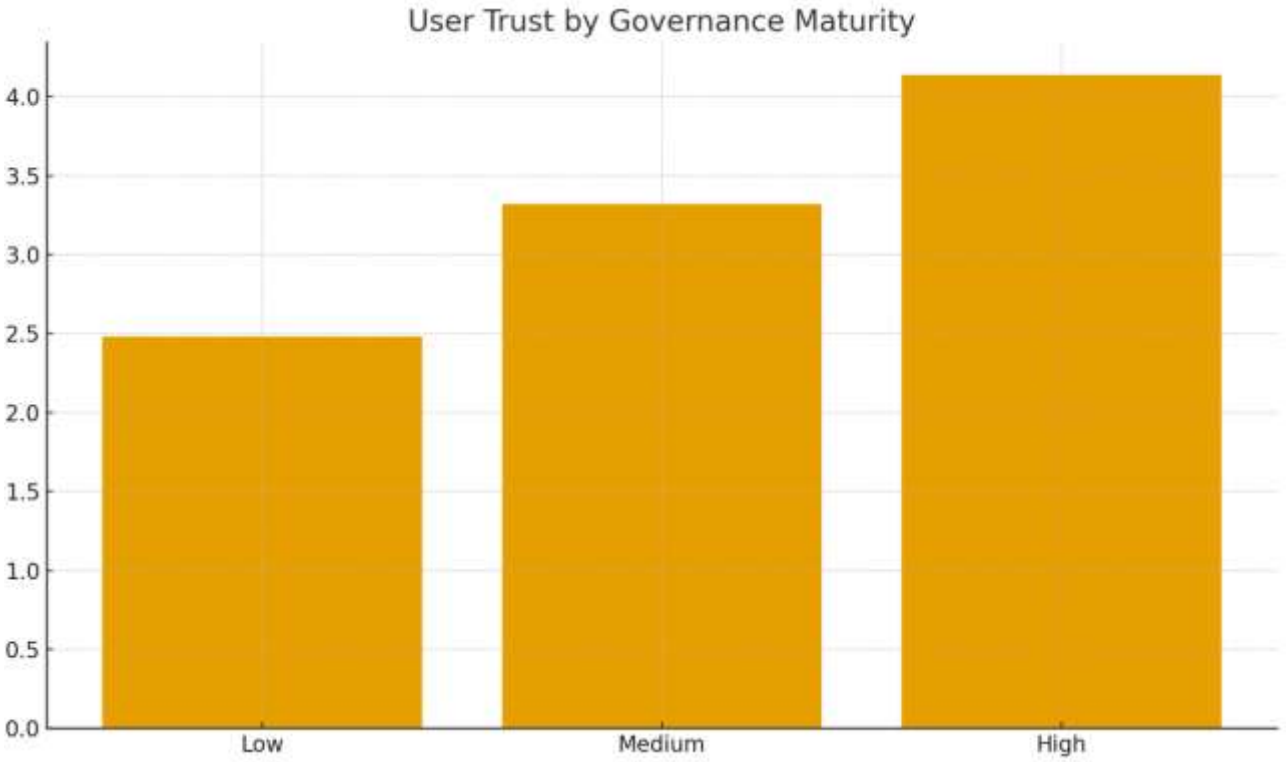
In more detail, regression analysis is offered. The model indicates that three governance variables involved in the model, which include access control, transparency, and safety validation help determine 57 percent of the variance in operational performance (R^2=0.57). This implies that these governance systems are significantly involved in establishing the provision of agentic AI with actual value. The transparency and safety checks should also be included to the policy controls.

It is also indicated in the findings that the enterprises that have data handling policies of greater maturity (PII and residency controls) mention fewer compliance problems when implementing AI agents. This is significant since agentic systems usually deal with logs, customer messages, product telemetry, and configuration files that might have a sensitive content. Data governance is powerful in offsetting unintended policy breaches.

Decision-Making Reliability

A large portion of the research is devoted to the effect of governance practices on user trust and perceived system safety. Findings indicate that trust is enhancing in cases where the user believes that agents are manageable, comprehensible, and foreseeable. The more mature organizations are in the governance level, the fewer concerns the users have about unintended actions of the agents.

10.48047/jocaaa.2025.34.11.41



The information demonstrates that the level of trust (scaling on 5 points) is significantly different between the high and low governance maturity organizations (mean difference=1.12, $p<0.01$). This proves the association between governance and user confidence. Respondents state that where agents are limited in terms of boundaries, logs and audit trails, agents are more and more willing to grant an agent to carry out more autonomous tasks in support and engineering work processes.

Table 7 presents an overview of the user trust and safety perception scores because of the governance maturity group.

Table 7. Trust and Safety Scores

Governance Maturity Level	Mean User Trust	Mean Safety Perception	N
Low	2.48	2.39	58
Medium	3.32	3.27	81
High	4.14	4.09	53

With these results, an upward trend is observed. Organizations of high maturity are approximately twice as high with respect to trust and their perceived safety level. This trend helps to confirm that the concept of technical governance, including audit logs, policy enforcement, and risk validation, has a direct impact on human decision-making confidence.

It is also mentioned by the users that their reliance on agent recommendations increases when the mechanisms of governance are observable and simple to comprehend. Indicatively, engineers are more reliant on agents in cases where they are able to check the rationale used in code diagnosis or problem classification. The support teams have more trust in agents who are capable of checking actions taken in the process of handling tickets.

10.48047/jocaaa.2025.34.11.41

It is also discovered by the study that reduction in critical incidents is positively related to safety validation (r = 0.54). Organisations in which agents of work are periodically tested in their safety procedures experience less harmful or unintended outcome. This implies that safety validation cannot be one time only but a continuous process.

Comparative Outcomes Across Industries

There are also the findings indicating variations in agentic AI performance between industries and types of uses cases. Telecom, cloud service, and enterprise software industries are the ones that are more successful when it comes to agentic AI implementation due to more established data governance and engineering practices. By comparison, the adoption and poor results are slower in industries that have less technical infrastructure.

Analysis of the use case level suggests that agentic AI works best in the situations, which are repetitive, staged and of a high volume. These are ticket classification, log analysis, system diagnostics and code review. In such regions, controlled agents minimize the human labor, enhance promptness, and frequency of errors.

Table 8 summarises use case average performance improvements.

Table 8. Average Reported Performance Improvements

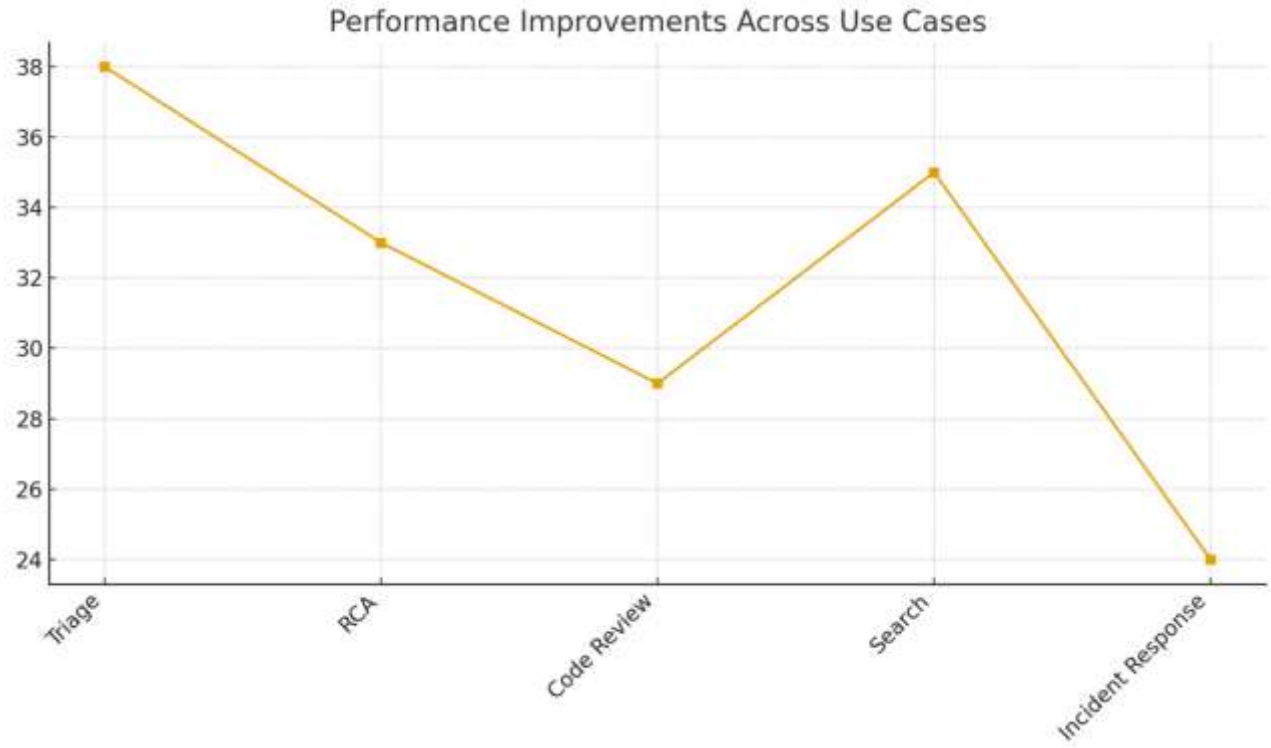
Use Case	Avg. Improvement (%)	Std. Dev.
Ticket triage automation	38%	14
Root-cause analysis support	33%	12
Recommendation on code review.	29%	11
Search and Retrievals of knowledge.	35%	13
The automation of incident response.	24%	15

Task-oriented improving takes place the most where the agentic AI is capable of analyzing logs or text at a much faster rate than a person can do so. Reductions in lower are detected in the automation of incident responses, which can be said to be the case due to higher safety risks that need human supervision.

There is also an existent interaction effect according to regression models which demonstrate that the governance maturity plays a major role towards improving use-case performance. To illustrate this, low-governance maturity organizations will have only 1520% improvement in terms of improving ticket triage and high governance maturity organizations will have an improvement that is more than 45%. This proves that agentic AI is enhanced with the help of governance.

10.48047/jocaaa.2025.34.11.41

Companies that have special AI governance committees have a lower number of case escalations and agent rollback cases. According to respondents, committees assist in ascertaining correspondence between the engineering, data governance, legal, and the support teams. This trans-functional design enhances accountability and the stability of agent workflow.



Summary of Findings

According to the quantitative data:

- The maturity of governance is a general concept that is highly predictive of agentic AI success.
- The most influential ones on the performance of the operations are access control, transparency, and safety validation.
- During governance, there is a significant increment in the level of trust and fear of unintentional acts is minimized.
- Well governed systems enhance the performance results in all the agentic AI applications.
- Companies that have well-structured governance committees get enhanced compliance and incidence cases.

V. CONCLUSION

The experiment indicates that effective agentic AI business in enterprises cannot be achieved without good governance. Companies that have well established governance practices are characterized by increased user trust, performance results and reduced cases of operations. Such fundamental mechanisms as access control, safety validation, and audit trails are important to the responsible automation. The findings also indicate that governance enhances the success of agentic workflows in different technical and support application cases. In general, governance must be perceived not as a hindrance but as a platform that allows credible, obedient, and scalable agentic AI systems.

REFERENCES

[1] Papagiannidis, E., Enholm, I. M., Dremel, C., Mikalef, P., & Krogstie, J. (2022). Toward AI Governance: Identifying Best Practices and Potential Barriers and Outcomes. Information Systems Frontiers, 25(1), 123–141. https://doi.org/10.1007/s10796-022-10251-y

[2] Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: a systematic literature review. AI And Ethics, 5(3), 3265–3279. https://doi.org/10.1007/s43681-024-00653-w

[3] Pöhler, L. D., Diepold, K., & Wallach, W. (2024). A practical multilevel governance framework for autonomous and intelligent systems. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2404.13719

10.48047/jocaaa.2025.34.11.41

[4] Syros, G., Suri, A., Ginesin, J., Nita-Rotaru, C., & Oprea, A. (2025). SAGA: A Security Architecture for Governing AI Agentic Systems. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2504.21034

[5] Suggu, N. S. K. (2025). Agentic AI Workflows in Cybersecurity: Opportunities, challenges, and governance via the MCP Model. Journal of Information Systems Engineering & Management, 10(52s), 612–624. https://doi.org/10.52783/jisem.v10i52s.10767

[6] Thoom, N. S. R. (2025). Understanding Agentic Frameworks in AI Development: A Technical analysis. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 11(1), 518–527. https://doi.org/10.32628/cseit25111249

[7] Chowdhury, N. (2025). Generative AI and Agentic Systems: driving automation and transforming operations. Preprints.org. https://doi.org/10.20944/preprints202509.0690.v1

[8] Joshi, H. (2025). AI Governance by Design for Agentic Systems: A framework for Responsible development and Deployment. Preprints.org. https://doi.org/10.20944/preprints202504.1707.v1

[9] Madanchian, M., & Taherdoost, H. (2025). Ethical theories, governance models, and strategic frameworks for responsible AI adoption and organizational success. Frontiers in Artificial Intelligence, 8, 1619029. https://doi.org/10.3389/frai.2025.1619029

[10] Gürpinar, T. (2025). Towards web 4.0: frameworks for autonomous AI agents and decentralized enterprise coordination. Frontiers in Blockchain, 8. https://doi.org/10.3389/fbloc.2025.1591907