Detecting Governance Risk In Generative AI Adoption: A Predictive Analysis Of Organizational Misalignment And AI Failure Signals

Ahmad Jamal[1] , Zeeshan Akbar[2] , Salman Akbar[3] , Sikander Niaz[4] , Fatima Tauseef[5]

[1]MBA- Business Analytics King Graduate School- Monroe University 434 Main St, New Rochelle, NY, 10801 ajamal7503@monroeu.edu
[2]Raymond A Mason School of Business William and Mary University, ukropway 101, Williamsburg, Virginia, Zakbar@wm.edu
[3]Master research fellow State university of NewYork, Albany,USA salman.akbar@fulbrightmail.org
[4]Master of cybersecurity (MSCIA) Virginia University of Science & Technology 2070 Chain Bridge Road, Suite G100 Vienna, VA 22182, United States Sniaz362@vust.edu
[5]MBA-IT Department of Business Administration and Management Washington University of Science and Technology 2900 Eisenhower Ave, Alexandria, VA 22314 ftauseef.student@wust.edu

Abstract

Generative artificial intelligence is rapidly being implemented in organizations, but the governance systems tend to build slowly than the implementation. This builds up growing alarm about governance risk, especially where poor supervision, absence of accountability, and inadequate compliance preparedness and novel AI breakdown indicators influence responsible adoption. In that regard, the investigation of the impact of organizational circumstances and warning signs of operations on governance risk has gained a significant research priority. This research paper explores the relationship between the signs of AI failure and organizational aspects of governance as predictors of governance risk in adoption of generative AI. The study particularly aims to reveal the governance preparedness, interplay between the governance processes and the indicators of failure, as well as to determine the most predictive of the governance risk factors. The quantitative cross-sectional design was followed with primary data being gathered by way of structured questionnaire. There were 100 participants in the study who were selected across various industries, including technology, healthcare, retail, finance, education and the public sector. The analysis and interpretation of data were done in SPSS through descriptive statistics, Cronbach alpha reliability test, Pearson correlation and multiple linear regression. The results indicate that in general, organizations were only moderately ready to adopt generative AI. The governance risk was also mitigated using better governance practices that included clarity in policy, support of leadership, accountability structure, human control, compliance preparedness, and alignment of strategy. Conversely, AI failure indicators, especially, low user trust, bias/fairness issues, risk of misuse, and disruption of workflow were related to greater governance risk. The findings also reveal that good governance environments are likely to have low levels of failure-signals. The paper finds that the governance risk in the use of generative AI is quantifiable and controllable. It provides useful guidance to managers and compliance teams as well as policy designers interested in ensuring that the governance frameworks are tougher and that the adoption of AI is less damaging, more compliant, and less risky.

Keywords Generative AI, AI governance, Governance risk, organizational misalignment, AI failure signals, predictive analytics, regression analysis.

1.0. Introduction

Generative artificial intelligence has emerged as a valuable component of digital transformation in organizations very fast. In their generative AI applications across technology, healthcare, finance, retail, education and the public sector, organizations are progressively implementing AI generative technology to automate routine work, aid decision-making, improve customer interaction, improve content creation and bolster operational effectiveness. It is a trend with high popularity mainly due to the belief that it can be used to enhance productivity, lower expenditures, hasten the innovation process and generate competitive advantage. To most organizations, generative AI is no longer regarded as an experimental facility but as a business asset that has the capacity to redefine business operations and knowledge work (Parvez et al., 2022).

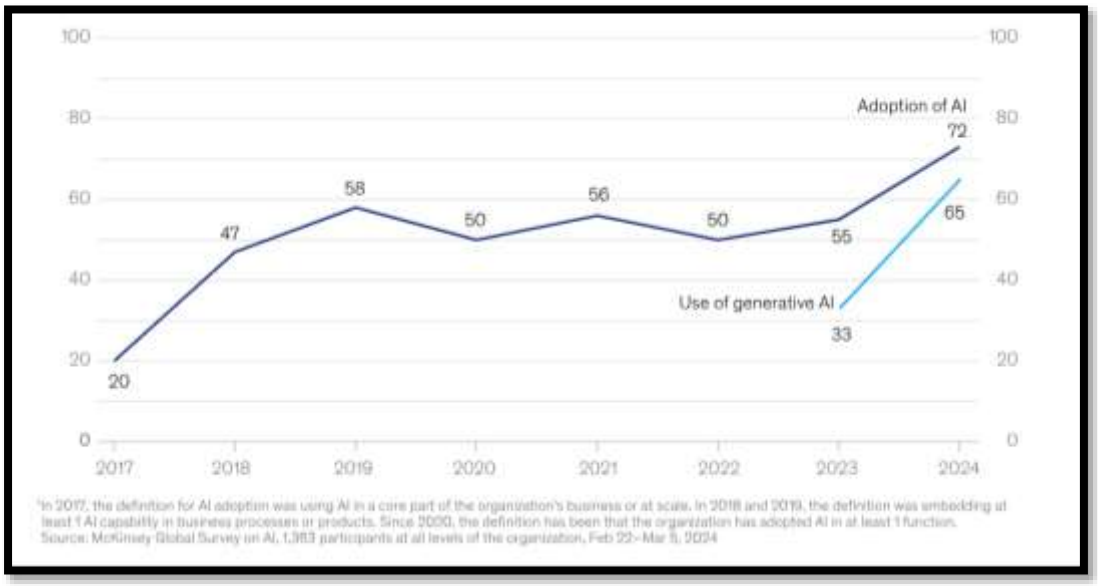


Figure 1: Organizations that have adopted AI in at leats 1 Business Functions

Source: (Singla et al., 2024)

Nonetheless, there are also significant governance issues that have arisen due to the swift development of the generative AI use. Though organizations are keen on reaping the merits of the technology, most of them are deploying it in their systems without having proper governance arrangements. Successful AI governance should have clear policies, adequate accountability frameworks, human supervision, compliance preparedness, ethical review, privacy provisions, and perpetual risk monitoring (De Almeida, dos Santos and Farias, 2021). In the absence of these controls, organizational objectives, regulatory expectations, and trust in generative AI may be generated in a way that is inconsistent with life in organizations. Consequently, governance has become a major concern of successful implementation of generative AI.

The main issue is that the rate of technology adoption is usually higher than the rate of governance development. Most organizations adopt or ramp generative AI without fully comprehending the strength of the internal structures to cope with the risks as they arise. Such imbalance may result in various failure indicators, such as hallucinated outputs, bias or fairness issues, misuse or unauthorised use, low user trust, workflow interference and the development of shadow AI practices that are non-formally regulated (Duke, 2023). These problems not only have an impact on the technical performance, but can also point to underlying organizational misalignment, a lack of strategic control and deficient governance maturity. In this regard, governance risk is to be interpreted as the possibility that the use of generative AI will produce an operational, ethical, compliance, or strategic issue due to the incompleteness or inefficiency of governance arrangements.

Despite the growing academic and professional discussion on the topic of responsible AI, AI ethics, and governance structures, there is still a deficit of empirical research that anticipates governance risk on the organizational level. A lot of the current discourse is normative and conceptual and aims at the suggested principles as opposed to experimenting with which governance-related conditions and AI failure indicators are the ones that correspond to most risk in reality (Wirtz, Weyerer and Kehl, 2022). This, in turn, necessitates conducting evidence-based research that will explore whether it is possible to use measurable organizational conditions as indicators of early signs of governance failure in the implementation of generative AI.

This paper fills that gap by analysing the degree to which the organizational conditions related to governance and AI failure indicators forecast the presence of governance risk during the adoption of generative AI. The study is also important as it offers empirical information regarding the way in which the issue of governance weaknesses is revealed within the organizational context and how the risk can be detected prior to the significant AI-related breakdowns. It is anticipated that the findings will assist in improving governance decision-making and ensure that managers, compliance departments, and organizational leaders are aware of the high-risk situations early, reinforce governance mechanisms, and lower the chance of misalignment of the organization towards generative AI implementation.

1.1. Research Aim

To investigate how effectively the organizational conditions associated with governance and AI failure cues are predictors of the presence of governance risk in AI adoption (generative AI).

1.2. Research Objectives

- To determine the degree of governance preparedness in organizations that adopt generative AI.
- To test the association between the variables related to governance and AI failure signals.
- To find the primary predictors of the existence of governance risk in the adoption of generative AI.

1.3. Research Question

What organizational governance-related predictors and AI failure indicators are substantially predictive of organizational governance risk in generative AI use?

2.0. Literature Review

2.1. Generative AI adoption in organizations

Generative artificial intelligence has in only a short time transitioned out of the experimentation phase into real application in businesses across a very diverse range of functions. A recent survey by McKinsey has indicated that 65 percent of the people surveyed indicated that their organizations were already using generative AI in at least one activity regularly in early 2024, which is indicative of an abrupt increase in enterprise use (Kumar, 2023). This diffusion is observed within operations, customer service, software development, document generation, analytics, and decision support, with organizations perceiving generative AI as the way to enhance productivity, speed up the process of task execution, and augment the innovation potential. It is not just the automation or the fact that the technology will aid in the knowledge-intensive work, which previously absolutely relied on human promise, that makes the technology attractive.

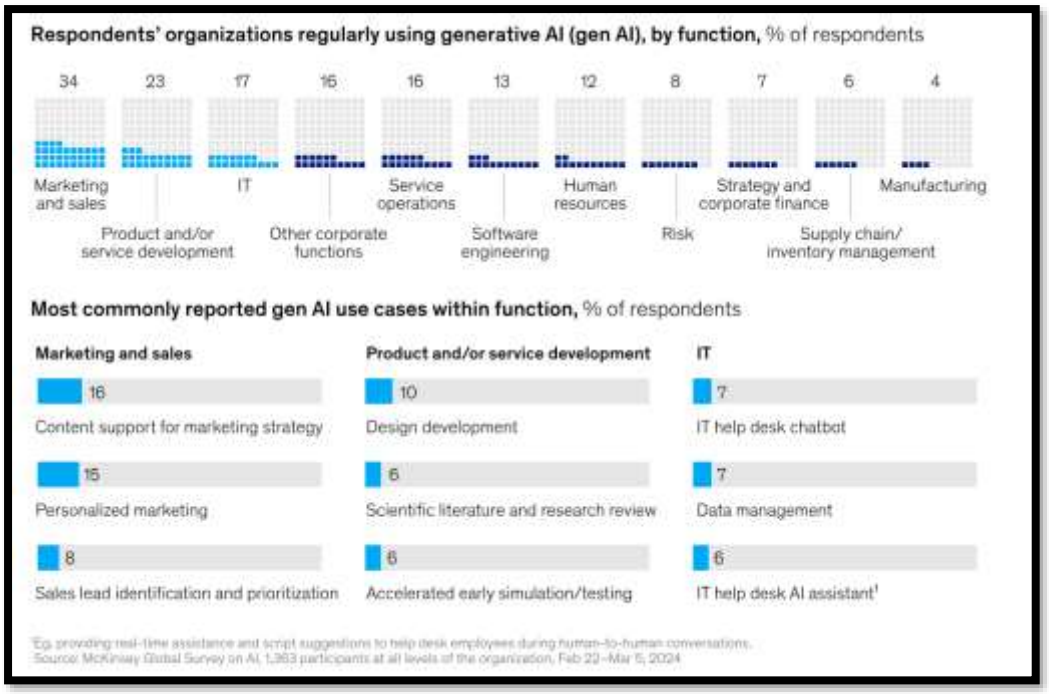


Figure 2: Respondents' Organizations Regularly Using Generative AI

Source: (Singla et al., 2024).

Nevertheless, the rate of adoption has created an equivalent governance challenge. Generative AI Profile by NIST points out that the risks presented by generative AI are of a different magnitude and different types than a variety of other previous digital tools, such as confabulation or hallucination, harmful bias, privacy risks, information integrity issues, insecure integration, and misuse (Janjeva et al., 2023). This indicates that adoption should not be perceived as a mere technology implementation problem; it is also a control problem in the organization. The literature seems to indicate with growing consensus that the value of generative AI should be determined by the ability of organizations to keep pace with governance maturity with deployment speed. Practically, such balance is usually poor, as adoption is often influenced by competitive factors, experimentation and productivity benefits before strong control systems are established as institutions.

The significance of this tension in the current study is that it provides a justifiable reason in investigating the opportunities, as well as the conditions of governance of adoption. In the case of generative AI being integrated into the fundamental business processes, the organizational performance is influenced not only by model capacity but also internal organizational structures (such as policy transparency, leadership vision, education, supervision, and responsibility). The literature thus justifies the need to consider the adoption of generative AI as a socio-technical process whereby the operational advantages and governance risks co-exist.

2.2. AI governance and organizational alignment

AI governance denotes the frameworks, policies, functions, and controls and supervision systems, by which organisations direct the design, deployment, use, and monitoring of AI systems. Both the AI Risk Management Framework and the Generative AI profile by NIST view governance as an organizational capability that deals with accountability, risk identification, monitoring, human oversight, and response procedures. In a comparable fashion, OECD contents addressing the principles of AI and AI privacy governance emphasize that credible AI must be transparent, accountable, strong, privacy-oriented, and respectful toward human rights (Mike, 2023). Stated otherwise, governance is not a policy document but a system of organizational arrangements that coordinate the alignment of technology use and institutional goals as well as normative expectations.

The variables in the current research are directly supported by this literature. Clarity of policies is important since misunderstood policies provide ambiguity as to whether something is acceptable to use or not. accountability structure is important since organizations should be aware of who will be held accountable whenever mistakes, abuse or damages are committed. The role of human supervision is

also very critical as even high-performing generative systems may issue false or misleading results and to eliminate such errors, human intervention is indispensable in high-stakes environments. The preparedness to adhere to all standards and the privacy protection are also not less significant since organizations should ensure that the usage of AI is consistent with legal and regulatory frameworks, particularly in cases when personal data or sensitive information are used. Ethical review practices help in another layer by making sure that the deployment decisions are made through fairness, impact to society and protection of harm and strategic alignment to guarantee that AI implementation is supportive and not distorting the organizational priorities (Shneiderman, 2020).

The role of organizational alignment is particularly important since technically successful AI systems do not always work on the organizational level as they do not accommodate governance frameworks, organizational processes, decision-making authority, or compliance requirements. Recent papers in Policy and Society posit that the issue of governance of generative AI should not be construed as a regulatory problem but rather as an organizational one that is defined by institutions, power, complexity, and adaptive decision-making (Wach, 2023). In this regard, a loose fit between the implementation of AI and organizational governance will have unstable results, divided responsibility, and unnecessary risk. This is what makes the current research consider the factors related to governance as a predictive condition and not as an abstract principle.

2.3. Governance risk in AI implementation

The risk of governance in the AI implementation can be interpreted as the possibility that the implementation of AI will result in operational, strategic, ethical, legal, or reputational issues due to the lack of completeness, clarity, or effectiveness in governance arrangements (Wirtz, Weyerer and Kehl, 2022). It is a strategic risk as it can cause harm to the legitimacy of the organization, jeopardize trust, and subject the firms to regulatory oversight. It is also in operation due to day-to-day applications of generative AI relies on understandable policies, paths of escalation, quality checks, and processes of monitoring. In case such mechanisms are weak or absent the organizations tend to be susceptible to project drift, bad decision making, covert usage and uncontrolled harms.

The cases of governance risk constantly recur in the literature: absence of policy, ambiguity on ownership of AI decisions, weak auditability, ineffective monitoring, weak training of employees and poor compliance processes. According to the guidance by NIST, monitoring and post deployment management is also vital since new or unfamiliar risks might arise in the course of use. OECD resources also focus on the fact that privacy and data governance risks may occur at various points of the AI lifecycle, but not only when training the model but also by deployment and daily operation (Shahriar et al., 2023). This is because, in the context of organization, there are hardly any instances where governance failure is a one-time occurrence; more often, it is a consequence of weak accumulating control.

This is also one of the reasons why AI project breakdown can also be due to governance failure. Unless organizations are able to guarantee reliable use, responsibility, misuse, and trust, then generative AI will no longer be considered a strategic asset and rather a source of disruption. The literature thus justifies the logic of the dependent variable of this study, the governance risk, as a result of a multiplicity of conditions of governance and failure as opposed to a single condition.

2.4. AI failure signals

According to literature various problems that can be observed may act as precursors to underlying governance weaknesses. One of the most well-known issues of generative AI is the cases of hallucinations, as computers might generate fake but accurate text. Confabulation or hallucination is an explicit and significant AI risk identified by NIST, which makes it a very valuable signal of failure in the organization (Freudenreich, 2020). Issues of bias and fairness are also of central concern, as both OECD and NIST point to discrimination and detrimental bias as potentially material risks that can occur in the behavior of models or how data is used or deployed downstream.

Another significant indicator is misuse or unauthorized usage especially in cases where employees become users of tools that are not in the approved workflows or they end up using tools in a manner that goes round the controls. This relates well to the concept of shadow AI, where AI systems operate in an informal manner with no formal visibility, record keeping, or oversight. Though shadow AI is not selected as that specific term in the texts of policies, the wider literature of monitoring, accountability, and uncontrolled deployment suggests that the absence of tracking implicates a substantial governance issue due to a lack of visibility and control. Unstable workflow and user distrust are also significant

pointers (Wycislak, 2022). In case generative AI generates confusion, duplications, inconsistencies, and diminished trust in the users, it might be a sign that the organization is poorly aligned and managed. These problems cannot then be taken to be mere user level problems; they could be an indication of weak structural governance.

A combination of these variables constitutes a consistent failure-Signal construct. This opinion is backed by the literature as such signals are not independent technical glitches, but pragmatic expressions of more fundamental governance failures. The study is based on that rationale, including hallucination incidents, bias or fairness incidents, risk of misuse, disruption of workflow, lack of user trust, and shadow AI use as predictors of governance risk.

2.5. Empirical gap

There is an evident empirical gap in the literature. Generative AI governance has much conceptual, normative, or policy-focused work. It describes the appearance of responsible governance, but less frequently, it examines what the state of affairs in an organization predicts governance risk. The recent academic literature has recognized legal, organizational, political, and social governance risks, but continues to have a relative deficiency of primary quantitative research that theorizes governance risk in terms of organizational-level measures (Zhang and Welch, 2022). Little literature also exists that combines both variables of governance strength with failure-signal variables under a single predictive model.

This research fills this gap by relying on primary quantitative data to explain the hypothesis that governance-related factors and AI failure signals both predict governance risk. By so doing, it will transform the literature on the macro-level governance debate to a more practical and quantified framework of misalignment within organizations in the implementation of generative AI.

2.6. Conceptual direction and hypotheses

According to the literature, the research presupposes that the governance risk is determined by two general factors, including the effectiveness of governance systems and the severity of AI failure indicators. Better governance, in turn, is to minimize chances of misalignment, whereas better risk of failure should be associated with higher chances of governance risk (Gordon et al., 2021). Moreover, more resilient governance arrangements ought to be linked to less intense failure-signalling due to the possibility to mitigate uncontrolled or adverse use, through enhanced monitoring, control, accountability, and policy transparency. The following hypotheses are caused by these relationships:

- **H1**: There is a strong impact of factors related to governance on the governance risk of generative AI adoption.
- **H2**: AI failure indicators have a strong impact on the governance risk in the adoption of generative AI.
- **H3**: More robust governance mechanisms are related to a weak signal of failure.

These hypotheses offer the conceptual gap between the literature review and the study model. They also explain the inclusion of the governance variables and failure-signal variables as predictors of governance risk in the empirical analysis.

Figure 3: Conceptual Framework
Source: Author

3.0. Results / Findings

3.1. Respondent profile

The study was analysed on the basis of 100 valid responses, and there were no MI cases reported on the main categorical variables. The sample was carefully heterogeneous in both sector, organizational size, job role, experience, and generative AI adoption stage to enable the study to provide a general cross-sectional view of the situation in governance in different organizational settings.

When it comes to the type of organization, the highest percentages of respondents were associated with Retail (19%) and Technology (19%), then Public Sector (13%), Manufacturing (12%), Healthcare (11%), Consulting (10%), Education (9%) and Finance (7%). It means that the sample was not skewed towards one industry and the respondents were recruited in areas where the adoption of generative AI is not only strategically important, but also operationally evident. On the issue of the size of the organization, 41% of the respondents had to be in a medium-sized organization, 30% in a large organization, and 29% in a small organization, which suggested a relatively balanced representation across the business scales.

There was also a reasonable variation in the role distribution. The proportion of Compliance Officers, Managers, and Operations Officers was 16 percent each, and the rest were AI Practitioners (15 percent), IT Staff (14 percent), Team Leads (12 percent), and Business Analysts (11 percent). The reason why this distribution comes in handy is the fact that the issue of AI governance crosscuts functions, technical, and managerial duties. In terms of professional experience, the highest number was 46 years (33%), 76 years (20%), 16 years (29%), 10+ years (18%). This indicates that the sample consisted of relatively young professionals in their careers and experienced individuals who might have been exposed to governance and compliance matters.

Regarding the stage of AI adoption, 33% of the respondents said that they were in the Early Deployment stage, 24% in the Scaled Deployment stage, 23% Planning stage, and 20% Pilot stage. This implies that the majority of the organizations sampled were beyond first thought and were already venturing into implementation issues. The distribution also justifies the application of a bar chart of adoption stage in the findings chapter because it clearly displays that the governance risk is being evaluated at multiple levels of adoption and not at a limited range of implementation level. Also, the governance risk category revealed that 55 percent of respondents were in the Moderate risk segment, 31 percent in Low risk and 14 percent in the High risk. On the same note, the dichotomous categorization revealed that 14 percent of the cases were classified as high risk. These indicators imply that there is a significant minority of organizations that are vulnerable to governance even though the majority of organizations seem to be in the moderate-risk middle ground.

3.2. Descriptive statistics of study variables

All the governance variables, failure-signal variables, and composite scores were calculated using descriptive statistics (Potter et al., 2021). With the ten indicators on governance matters, the average scores were cantered around the middle of the scale indicating that the respondents considered governance preparedness to be moderate, and not strong. The mean of governance items with the highest rank was Data_ Privacy_Safeguards (M = 3.2800, SD = 0.85375) and then there was Leadership Support (M = 3.2200, SD = 1.01085) and Strategic Alignment (M = 3.1700, SD = 0.87681). On the other hand, the lowest governance means were recorded in Risk_Monitoring_Procedures (M = 2.9400, SD = 0.88557), Accountability_Structure (M = 2.9800, SD = 0.90988) and Ethical_Review_Practices (M = 2.9900, SD = 0.94810). Such statistics show that, though organizations might have a sense of viable assistance in the strategic and privacy-related angles, weak points exist in the formal responsibility, adherence, and morality fees.

In the case of the six variables of failure-signals, the means were once again clustering towards the middle of the scale which showed that the failure-signals existed in moderate intensity but were not trivial. Hallucination_Incidents (M = 3.1500, SD = 0.93609), Shadow_AI_Use (M = 3.1100, SD = 1.01399) and Workflow_Disruption (M = 3.0700, SD = 0.91293) have the highest mean of failure-signals with a close second behind. Bias or Fairness Incidents had the lowest mean (M = 2.9200, SD = 0.99168), but it is still very close to the mean. In general, the results indicate that the sample organizations were undergoing significant measures of AI-related risk indicators, particularly, hallucinations and shadow usage, which are especially applicable to the collapse of governance (Vipula Rawte et al., 2023).

The Governance Strength Score used the means of 3.0740 and the standard deviation of 0.66113, and the Failure Signal Score used the means of 3.0389 and the standard deviation of 0.72180. Governance Risk Score which is the main dependent variable had a means of 3.5874 and a standard deviation of 0.94820 meaning that there were moderate to high levels of governance risk throughout the sample. Offering a histogram of Governance Risk Score would be beneficial in the chapter as it would indicate whether the risk is clustered in the middle or the distribution is skewed towards higher levels of risk (Thompson et al., 2021).

3.3. Reliability analysis

The reliability analysis was done to evaluate the internal consistency of the governance and failure-signal scales. The governance predictor scale used ten items and resulted in a Cronbachs alpha of 0.906, and the standardized alpha of 0.907. This shows a very high degree of internal consistency and this implies that the items related to governance do work very well as a uniform construct.

Failure-signal scale which is a 6-item scale yielded a Cronbachs alpha of 0.852, which is good reliability. This finding indicates that the number of incidents of hallucinations, incidents of bias, or fairness, risk of misuse, workflow interference, low user trust, and use of the shadow AI is a sufficiently large set to utilize in further correlational and regression analysis. Altogether, the results of reliability indicate that both scales can be used in the model and interpretation of the empirical data.

3.4. Correlation analysis

The Pearson correlation indicated that the composite variables and the governance risk had a very strong relationship. Governance Strength Score was found to have a negative and significant correlation with Governance Risk Score ($r = -0.961$, $p = 0.000$) whereby a stronger governance condition is correlated with reduced governance risk significantly. Failing to this, Failure_Signal_Score had a very strong and positive correlation with Governance_Risk_Score ($r = 0.982$, $p = 0.000$) indicating that the greater the AI failure signals, the larger the governance risk. Moreover, Governance strength score was also significantly and negatively related to Failure signal score ($r = -0.896$, $p = 0.000$), which means that stronger governance is more likely to be associated with less failure signals. The three findings are direct evidence of the rationality of the study framework and empirical evidence of the anticipated relationships between governance conditions, the intensity of failures and the governance risk.

In the individual-variable level, the governance variables were found to be negatively related to Governance_Risk_Score with the failure-signal variables being positively related. The good negative correlations between variables of governance and governance risk were Leadership_Support ($r = -0.753$), AI_Training_Adequacy ($r = -0.734$), Ethical_Review_Practices ($r = -0.733$), and Compliance_Readiness ($r = -0.720$). The variables of the failure-signals, which showed the strongest positive correlations with the governance risk, were Bias or Fairness Incidents ($r = 0.777$), Misuse or Unauthorized Use Risk ($r = 0.752$), Workflow Disruption ($r = 0.741$), Low User Trust ($r = 0.713$) and Shadow AI Use ($r = 0.802$). The relationship of governance strength versus governance risk and governance strength versus failure signals would then be clearly illustrated in scatterplots of the two variables.

3.5. Regression analysis

Multiple linear regression involving Governance_Risk_Score as the dependent variable was applied in the core analysis (Antunes et al., 2023). The regression model was refined and had 13 predictors: Policy_Clarity, Leadership_Support, AI_Training_Adequacy, Accountability_Structure, Human_Oversight, Compliance_Ready, Risk_Monitoring_Procedures, Ethical_Review_Practices, Strategic_Alignment, Bias or Fairness Incidents, Misuse or Unauthorized Use Risk, Workflow Disruption, and Low User Trust.

The model yielded a very high fit with R: 0.990, R 2: 0.980, and Adjusted R 2: 0.977, which is to say that the predictors included in it explained 98.0 percent of the variation in the governance risk. The statistical significance of the outcome of the ANOVA was as follows: $F(13, 86) = 326.793$, $p = 0.000$, which indicated that the model in its entirety contributed significantly to the prediction of governance risk.

The results of the coefficient indicated that a number of variables of governance had a significant negative impact on governance risk and failure-signal variables had a significant positive impact. Among others, Accountability_Structure, Human_Oversight, Leadership_Support, Compliance_Readiness, Strategic_Alignment, Ethical_Review_Practices, Risk_Monitoring_Procedures, and Policy_Clarity had significant negative coefficients with the others

(B = -0.123, p = 0.000; B = -0.098, p = 0.013; B = -0.094, p = 0.013; B = -0.075, p The value of AI_Training Adequacy was also negative, but insignificant at the 5 percent level (B = -0.047, p = 0.081).

The remaining predictors, which were statistically significant and positive, were all Low_User_Trust (B = 0.212, Beta = 0.207, p = 0.000), Bias_or_Incidents_Fairness (B = 0.190, Beta = 0.199, p = 0.000), Misuse_or_Unauthorized_Use (B = 0.159, p = 0.000), and Workflow_Disruption (B = These results suggest that the increase in user distrust and perceived fairness issues formed some of the most significant constructive predictors of governance risk in the last model. In general, the regression findings indicate that both sides of the framework are important: more powerful governance mechanisms minimize risk, and more powerful AI failure signals maximize it.

3.6. Summary of key findings

To conclude, the sample was representative of a wide range of organizational environments, the majority of the responded were in the retail, technology, and public-sector environments and in the early stage of deployment and in the scaled deployment stage. Descriptive statistics indicated moderate governance strength levels, intermediate AI failure signals levels and moderately high mean governance risk levels. The governance scale and the failure-signal scale were both sound. The analysis based on correlation showed that high governance was correlated strongly with low governance risk and low failure signal intensity, and weak governance risk was correlated with the high intensity of failure signals. Lastly, the regression model established a strong prediction of the governance risk of having a mix of governance weaknesses and AI failure signals, with low user trust, fairness concerns, misuse risk, and workflow disruption, enhancing the risk, and accountability, oversight, leadership support, compliance readiness, and strategic alignment decreasing it.

4.0. Discussion

4.1. Governance readiness and organizational risk

The results indicate that the sample organizations were moderately ready instead of being completely ready to adopt generative AIs. The descriptive results support this interpretation as the governance variables including data privacy protection, leadership support, and strategic alignment have only moderate mean scores, the accountability structure, risk monitoring process, and ethical review practices were weaker (Chau et al., 2020). The trend shows that lots of organizations have been starting to lay the groundwork of governance, yet these frameworks are not at a developed state to allow low-risk deployment at scale. This conclusion is further supported by the fact that the moderate category of governance risk dominated the sample. Most organizations do not seem to be experiencing total failure of governance but seem to be functioning on a middle ground where they are adopting but are yet to achieve full maturity in governance. This is also in line with the broader governance literature that tends to posit that organizations tend to adopt generative AI more rapidly than they come up with the institutional structures that are necessary to control its risks.

This moderate-readiness pattern is significant as it indicates that the issue of governance risk does not occur only in organizations that are not managed by controls whatsoever. It may also manifest itself in places in which partial controls are not yet whole, deeply unco-ordinated, and/or not yet deeply entrenched in daily practice. Practically, this implies that companies can mistakenly believe that few policy reports or informal control would suffice to govern AI generative application. The findings fail to show it: in the presence of certain governance factors, the governance risk is still high in the case of inconsistencies in core control domains. This helps to hold the perception that generative AI regulation is not a dichotomy of the presence or absence of something but the strength of capability and integration and constant surveillance.

4.2. Role of governance mechanisms in reducing risk

The results of the regression demonstrate that the governance mechanisms are not symbolic forms of control, but are functional risk mitigating variables. Policy clarity, leadership support, accountability structure, human oversight, compliance readiness, strategic alignment, ethical review practices, and risk monitoring procedures were all found to be negatively related with governance risk with many having their relationship being statistically significant in the final model (Samans and Nelson, 2022). This implies that in case companies provide a better sense of direction in terms of AI implementation, delegate responsibility more efficiently, enhance control, and align adoption to compliance and strategic

goals, there is a reduction in governance risk. The most powerful impacts in the model especially on accountability structure, human oversight, leadership support, and compliance preparedness indicate that organizations mitigate risk in the best way when governance is not only embedded in managerial authority but also operational control instead of remaining an abstract ethical aspiration.

These results are also consistent with the Generative AI Profile offered by NIST which suggests the governance, mapping, measurement, and management as the fundamental functions of handling the generative AI risk. They are also consistent with OECD work on relating trustworthy AI to accountability, transparency, privacy protection and human-centered protection. The current research contributes some tangible weight on these frameworks by demonstrating that such aspects of governance are not only normatively good but statistically related to reduced risk. In this regard, the results reinforce the thesis that the capacity of organizational governance is a determining factor in the adoption of responsible AI.

4.3. Failure signals as early indicators of misalignment

The findings further reveal that failure signals can be used as some sort of early warning of greater organizational misalignment. The actual top positive predictors of governance risk in the regression model were low user trust, bias or unfair cases, misuse or unauthorized use risk, and workflow disruption, and correlation findings also indicated that there were strong positive relations between failure-signal intensity and the governance risk (Parimi and Yallavula, 2023). This suggests that the apparent AI-related issues cannot be translated into merely a few operational inconveniences. More likely, they are indicators of deeper institutional flaws in the system of governance, its regulation and monitoring. In the case of non-trust of outputs in users, disruption of workflow, and increased chances of unauthorized use, the organization has already been showing signs of a lack of proper governance.

The extended generative AI literature agrees with this interpretation highly. Hallucination, harmful bias, information integrity problem, and risk of misuse are the main areas of generative AI concern listed by NIST. The World Economic Forum also emphasizes the lack of accountability, stakeholder-related issues, and the changing governance need as the key topics in strong generative AI governance. In that sense, the signals of failure, i.e. hallucinations, shadow AI usage, disruption of the workflow, and low trust, should be regarded as managerial intelligence. They show where the governance structures are not performing properly and where the controls are not up to date in the organization. This line of reasoning is supported by the negative relationship between the level of governance and the intensity of the failure-signals in the current study, which display that the closer the governance environment is, the fewer the warnings signs would manifest.

4.4. Comparison with prior studies

The results are largely consistent with the available literature that was reviewed above. Earlier research and governance publications have reiterated that the adoption of generative AI will only be successful when the policy is clear, accountable, human responsibility, monitoring, privacy protection, and ethical review (Ghosh and Lakshmi, 2023). The current findings are in line with that argument, especially in demonstrating that leadership support, compliance preparedness, accountability structure, and human oversight mitigate the governance risk. They also contribute to the literature on the harmfulness of generative AI by demonstrating that the risk of bias, lack of trust, and misuse are not only peripheral, but also key predictors of vulnerability in governance.

Simultaneously, the research adds value to the existing knowledge. The existing literature is much conceptual, regulatory or principle based. The paper is also empirical as it reveals predictive relationship among governance variables, predicty factors and governance risk based on primary quantitative data. Specifically, it introduces the governance strength and the intensity of failure in a single model and does not consider them as different dialogues. It is a valid addition to the literature since it demonstrates that the symptoms of governance weakness and failure areas should be evaluated as a unit when gauging the organizational preparedness to adopt generative AI.

4.5. Practical implications

The practical implications of the findings are obvious: organizations cannot view the adoption of generative AI only as the technical implementation process. Continuous policy formulation, the commitment of the leader, supervision, the preparation of compliance, monitoring, and the review of ethics need to be maintained in case the governance risk should be maintained within bounds (Eyinade, Ezeilo and Ogundeji, 2021). To managers, this implies that AI governance should be part of operational strategy as opposed to being assigned to technical teams. In the case of compliance teams, the findings

indicate that proactive privacy, accountability, and acceptable use control systems must be developed before the use of AI can become even larger. To the AI governance boards or oversight committees, the findings indicate that the indicators of failure like low trust, workflow disruption, and misuse risk are to be observed as the signs of the underlying governance weakness but not as individual complaints. To policy designers, the article reaffirms the need to have realistic governance structures that help in implementation, rather than high principle ethical values.

In general, the discussion suggests that generative AI adoption has a governance risk, which is preventable and measurable. The ability to build governance capacity early on can help organizations reduce negative signs of failure and prevent more profound organizational misalignment. On the other hand, in the situation where there is partial or reactive governance, even potentially generative AI initiatives can cause a growing operational and strategic risk.

5.0. Conclusion

This paper investigated whether the organizational conditions and AI failure indicators, which relate to governance, are predictive of generative AI adoption governance risk. The study was made based on the increasing application of generative AI within organizations and the alarm over the fact that implementation is usually going ahead much faster than the creation of proper governance frameworks. The research thus aimed at comprehending the interaction between the governance preparedness and the signs of operation in defining the general governance risk.

The results indicate that the organizations of the sample were typically only moderately ready to use generative AI. Even though the evidence of certain governance foundations was present, especially regarding areas like leadership support, data privacy protection, weaknesses could still be seen in the accountability foundations, risk oversight processes, and ethical review practices. The findings further presented that both the governance conditions and AI failure signals significantly influenced the governance risk. Better governance mechanisms were linked to less governance risk whereas greater user trust to low level, issues of fairness, misuse risk and workflow disruption were linked to increased governance risk. Moreover, the better the governance environments, the more there were less signals of failures, which implies that the ability of governance and the stability of its operations are inseparable.

The importance of these findings is that they indicate that the governance risk in the adoption of generative AI is not by chance. It is detectable based on quantifiable organizational situations and visible warning signs. This is of practical significance to organizations interested in scaling generative AI in a responsible manner because it implies that the governance issue should be regarded as a strategic capability and not a secondary compliance problem. Adoption can only be effective when the technical performance is coupled with a robust policy, oversight, accountability and risk management structures.

In general, this analysis shows that effective adoption of generative AI goes beyond the need to implement new technologies. It demands powerful and combined governance systems that can mitigate organizational misalignment and identify risks before significant failures in AI situations can take place.

6.0. Recommendations

Considering the results, it is possible to make a number of recommendations that will help to make the adoption of generative AI more responsible and less risky. To begin with, before expanding to the scale of deployment, organizations must have formal generative AI governance policies. Clear policies are needed to establish a definition of acceptable use, roles, less ambiguity, and aligning AI practices with organizational objectives. Second, responsibility and control systems of humans should be enhanced. The results show that the governance risk is reduced when organizations delegating AI-related decisions have a clear responsibility and when the outputs and use cases are reviewed and reviewed by human specialists.

Third, companies are to enhance the training and awareness of AI among employees. Generative AI tools should be not merely explained on how to use them, but also be discussed in the context of ethical use, privacy concerns, bias issues, and escalation processes. Fourth, the introduction of periodic surveillance of failure indicators, especially hallucinations, misuse, lack of user trust, workflow interference, and shadow AI use, should be introduced in organizations. These signals must be perceived as early signals of operational vulnerability instead of being solitary operational issues.

Lastly, the protection of privacy, compliance preparedness, and ethical scrutiny ought to be inculcated into the implementation processes at an early stage. The issue of governance cannot be incorporated

when expansion of adoption has already increased. Rather it must be incorporated in the planning, piloting, deployment and post-deployment review. Combined, these suggestions imply that companies should have an active and organized way of governance in order to achieve the advantages of generative AI and reduce the possibility of misalignment and failure as much as possible.

7.0. Limitations and Future Research

This research can be characterized by a number of limitations. To start with, the number of respondents (100) is adequate to conduct the current analysis, but it is quite small, and thus, restricts the generalizability of the results. Second, the research employed a cross-sectional design, that is, the data are based on the perceptions at one time only and cannot indicate the changing governance risk as the adoption of generative AI becomes a fact. Third, the results are based on self-reported responses which could be subject to perception, recall or subjectivity of the respondents. Lastly, the sample consisted of individuals who lived and worked in various industries and organizational settings and, thus, the results might not be applicable to all industries and nations equally.

These limitations can be overcome in future studies in a number of ways. The review of larger samples would enhance statistical soundness and enhance generalizability. Industry-specific comparisons, in turn, may help give a deeper analysis of the differences between governance risk among industries, including healthcare, finance, or the public sector. Moreover, longitudinal research would be of use to investigate the effect of governance readiness and failure signs through time. Lastly, the next-generation research might utilize more sophisticated machine learning algorithms with actual organizational data to enhance the predictive ability and go beyond the survey-based estimation to more dynamic governance risk identification.

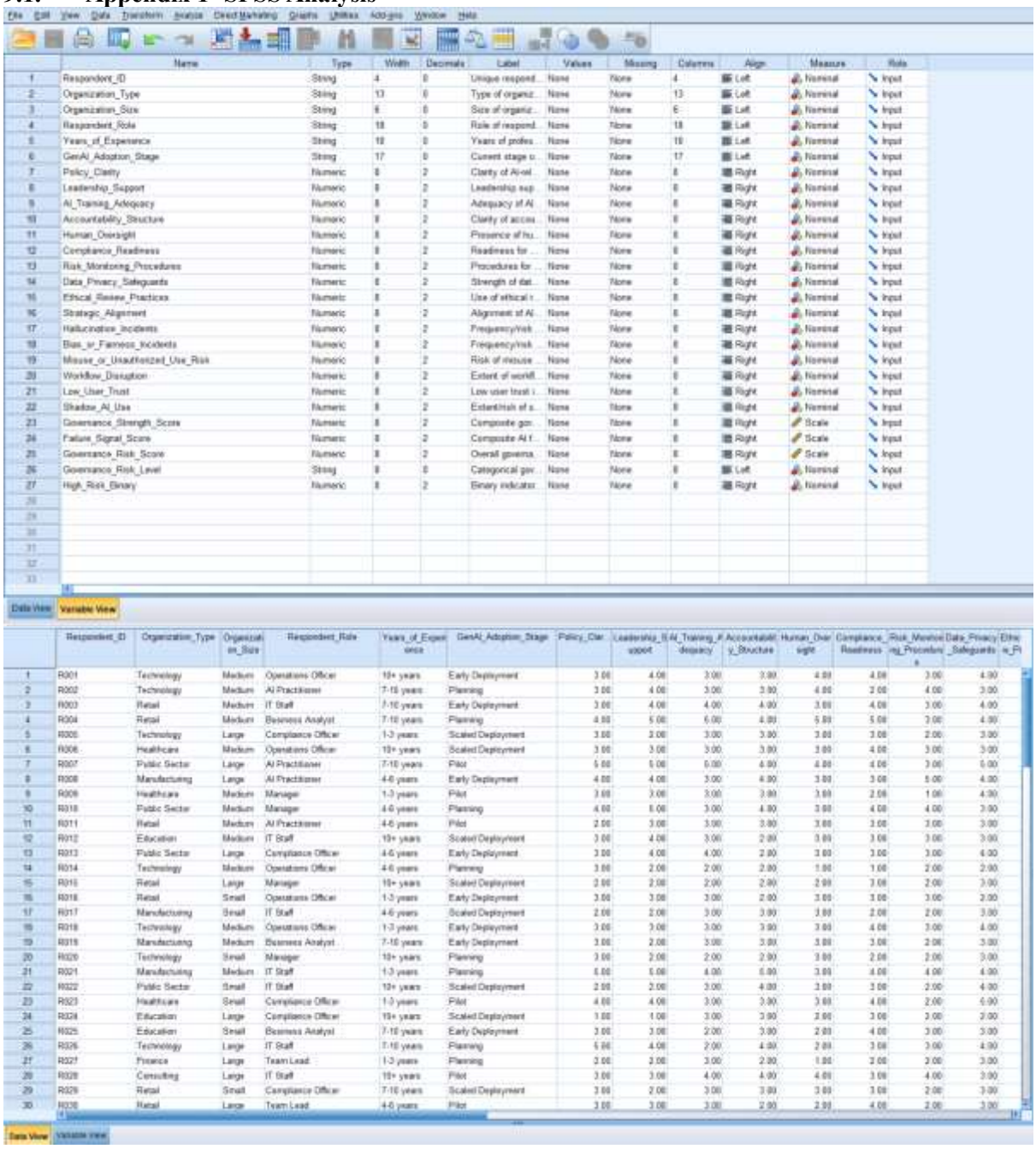
8.0. References

1. Antunes, J., Wanke, P., Fonseca, T. and Tan, Y. (2023). Do ESG Risk Scores Influence Financial Distress? Evidence from a Dynamic NDEA Approach. Sustainability, 15(9), p.7560. doi:https://doi.org/10.3390/su15097560.
2. Chau, D.C.K., Ngai, E.W.T., Gerow, J.E. and Thatcher, J.B. (2020). The Effects of Business-IT Strategic Alignment and IT Governance on Firm Performance: A Moderated Polynomial Regression Analysis. MIS Quarterly, 44(4), pp.1679–1703. doi:https://doi.org/10.25300/misq/2020/12165.
3. De Almeida, P.G.R., dos Santos, C.D. and Farias, J.S. (2021). Artificial Intelligence Regulation: a Framework for Governance. Ethics and Information Technology, [online] 23(3), pp.505–525. doi:https://doi.org/10.1007/s10676-021-09593-z.
4. Duke, T. (2023). Building Responsible AI Algorithms. Apress eBooks. doi:https://doi.org/10.1007/978-1-4842-9306-5.
5. Eyinade, W., Ezeilo, O.J. and Ogundeji, I.A. (2021). An Internal Compliance Framework for Evaluating Financial System Integrity Under Changing Regulatory Environments. International Journal of Multidisciplinary Research and Growth Evaluation, [online] 2(1), pp.927–934. doi:https://doi.org/10.54660/.ijmrge.2021.2.1.927-934.
6. Freudenreich, O. (2020). Psychotic Disorders. Current Clinical Psychiatry. Cham: Springer International Publishing. doi:https://doi.org/10.1007/978-3-030-29450-2.
7. Ghosh, A. and Lakshmi, D. (2023). Dual Governance: The intersection of centralized regulation and crowdsourced safety mechanisms for Generative AI. [online] arXiv.org. doi:https://doi.org/10.48550/arXiv.2308.04448.
8. Gordon, I.M., Hrazdil, K., Jermias, J. and Li, X. (2021). The Effect of Misalignment of CEO Personality and Corporate Governance Structures on Firm Performance. Journal of Risk and Financial Management, [online] 14(8), p.375. doi:https://doi.org/10.3390/jrfm14080375.
9. Janjeva, A., Harris, A., Mercer, S., Kasprzyk, A.M. and Gausen, A. (2023). The rapid rise of generative AI : assessing risks to safety and security - WRAP: Warwick Research Archive Portal. Warwick.ac.uk. [online] doi:https://wrap.warwick.ac.uk/id/eprint/196398/1/GenAI.pdf.
10. Kumar, V. (2023). Digital Enablers. Management for professionals, pp.1–110.
11. Mike, N. (2023). European Privacy by Design - BCE Doktori disszertációk. Uni-corvinus.hu. [online] doi:https://phd.lib.uni-corvinus.hu/1254/1/Mike_Nimrod_den.pdf.

12. Parimi, S.K. and Yallavula, R. (2023). Enterprise Risk Intelligence: Machine Learning Models for Predicting Compliance, Fraud, and Operational Failures. International Journal of Emerging Trends in Computer Science and Information Technology, [online] 4(2). doi:https://doi.org/10.63282/3050-9246.ijetcsit-v4i2p117.
13. Parvez, M.O., Arasli, H., Ozturen, A., Lodhi, R.N. and Ongsakul, V. (2022). Antecedents of human-robot collaboration: theoretical extension of the technology acceptance model. Journal of Hospitality and Tourism Technology, ahead-of-print(ahead-of-print). doi:https://doi.org/10.1108/jhtt-09-2021-0267.
14. Potter, E.L., Rodrigues, C.H.M., Ascher, D.B., Abhayaratna, W.P., Sengupta, P.P. and Marwick, T.H. (2021). Machine Learning of ECG Waveforms to Improve Selection for Testing for Asymptomatic Left Ventricular Dysfunction. JACC. Cardiovascular imaging, [online] 14(10), pp.1904–1915. doi:https://doi.org/10.1016/j.jcmg.2021.04.020.
15. Samans, R. and Nelson, J. (2022). Corporate Governance and Oversight. Sustainable Enterprise Value Creation, [online] pp.103–140. doi:https://doi.org/10.1007/978-3-030-93560-3_4.
16. Shahriar, S., Allana, S., Hazratifard, S.M. and Dara, R. (2023). A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle. IEEE Access, [online] 11, pp.61829–61854. doi:https://doi.org/10.1109/ACCESS.2023.3287195.
17. Shneiderman, B. (2020). Bridging the Gap between Ethics and Practice. ACM Transactions on Interactive Intelligent Systems, 10(4), pp.1–31. doi:https://doi.org/10.1145/3419764.
18. Singla, A., Sukharevsky, A., Yee, L. and Chui, M. (2024). The state of AI in early 2024: Gen AI adoption spikes and starts to generate value. [online] McKinsey & Company. Available at: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024?utm.
19. Thompson, J.R. J., Feng, L., Reesor, R.M. and Grace, C. (2021). Know Your Clients' Behaviours: A Cluster Analysis of Financial Transactions. Journal of Risk and Financial Management, 14(2), p.50. doi:https://doi.org/10.3390/jrfm14020050.
20. Vipula Rawte, Chakraborty, S., Pathak, A., Sarkar, A., Islam, T., Chadha, A., Sheth, A.P. and Das, A. (2023). The Troubling Emergence of Hallucination in Large Language Models - An Extensive Definition, Quantification, and Prescriptive Remediations. doi:https://doi.org/10.18653/v1/2023.emnlp-main.155.
21. Wach, K. (2023). The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT. Entrepreneurial Business and Economics Review, [online] 11(2), pp.7–30. Available at: https://www.ceeol.com/search/article-detail?id=1205845.
22. Wirtz, B.W., Weyerer, J.C. and Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. Government Information Quarterly, 39(4), p.101685. doi:https://doi.org/10.1016/j.giq.2022.101685.
23. Wycislak, S. (2022). From real-time visibility to operational benefits – tensions on unfinished paths. The International Journal of Logistics Management, 34(5). doi:https://doi.org/10.1108/ijlm-03-2022-0126.
24. Zhang, F. and Welch, E.W. (2022). Explaining Public Organization Adaptation to Climate Change: Configurations of Macro- and Meso-Level Institutional Logics. Journal of Public Administration Research and Theory, 33(2). doi:https://doi.org/10.1093/jopart/muac027.

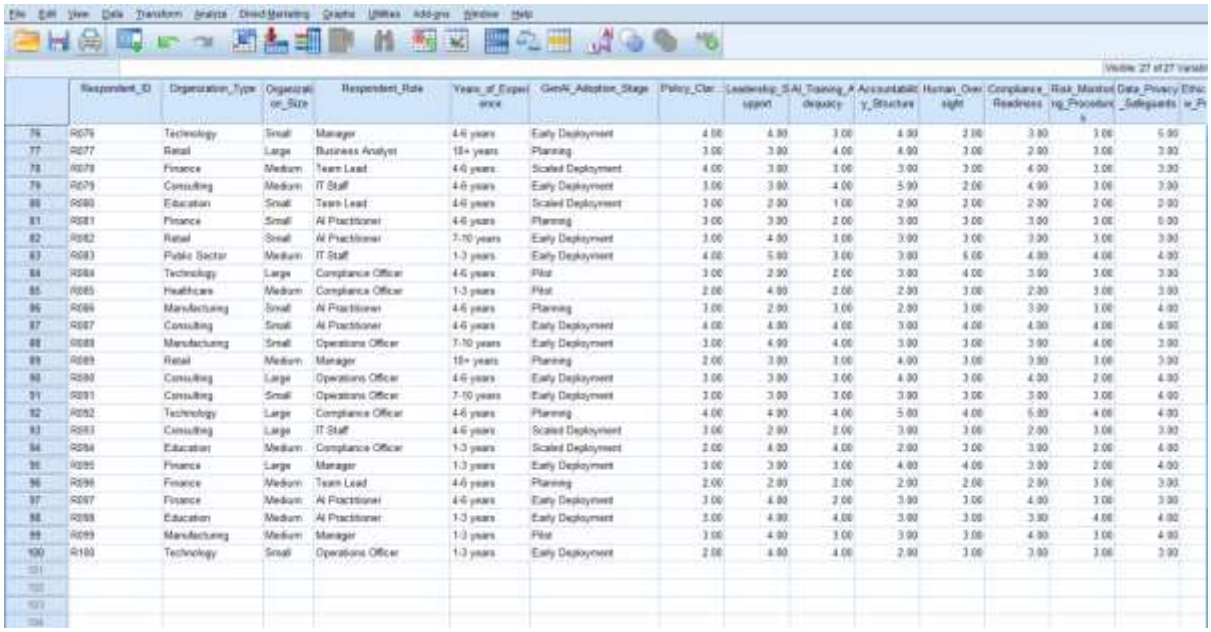
9.0. Appendices

9.1. Appendix 1- SPSS Analysis

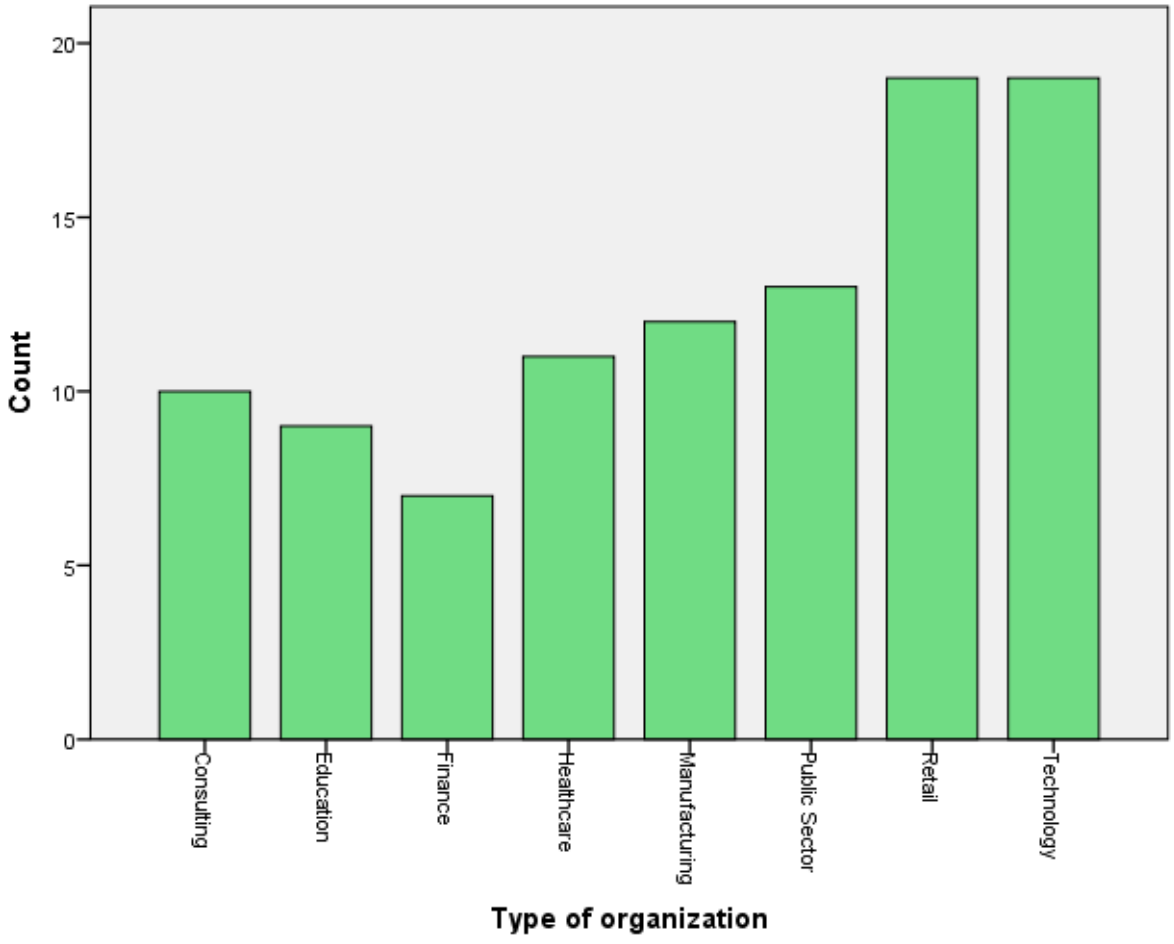


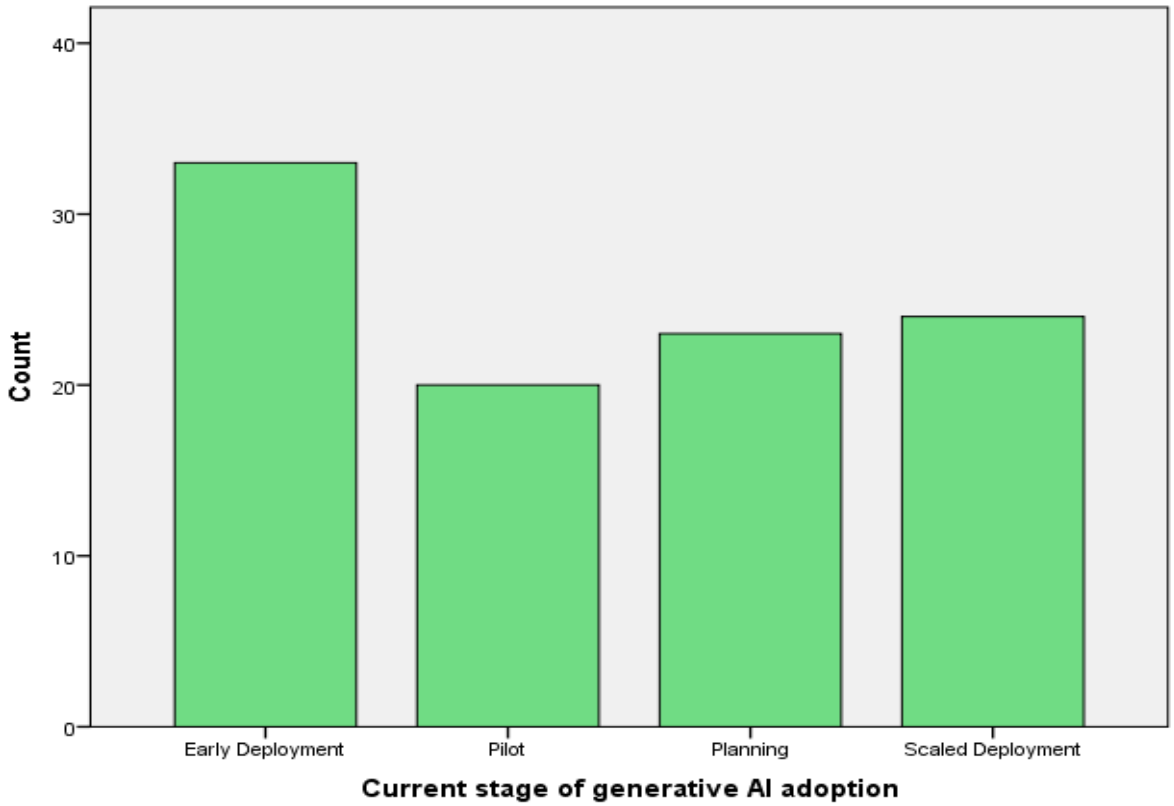
	Name	Type	Width	Decimals	Label	Values	Missing	Columns	Align	Measure	Role
1	Respondent_ID	String	4	0	Unique respond...	None	None	4	Left	Nominal	Input
2	Organization_Type	String	13	0	Type of organiz...	None	None	13	Left	Nominal	Input
3	Organization_Size	String	6	0	Size of organiz...	None	None	6	Left	Nominal	Input
4	Respondent_Role	String	18	0	Role of respond...	None	None	18	Left	Nominal	Input
5	Years_of_Experience	String	10	0	Years of profes...	None	None	10	Left	Nominal	Input
6	GenAI_Adoption_Stage	String	17	0	Current stage o...	None	None	17	Left	Nominal	Input
7	Policy_Clarity	Numeric	8	2	Clarity of AI-rel...	None	None	8	Right	Nominal	Input
8	Leadership_Support	Numeric	8	2	Leadership sup...	None	None	8	Right	Nominal	Input
9	AI_Training_Adequacy	Numeric	8	2	Adequacy of AI ...	None	None	8	Right	Nominal	Input
10	Accountability_Structure	Numeric	8	2	Clarity of accou...	None	None	8	Right	Nominal	Input
11	Human_Oversight	Numeric	8	2	Presence of hu...	None	None	8	Right	Nominal	Input
12	Compliance_Readiness	Numeric	8	2	Readiness for ...	None	None	8	Right	Nominal	Input
13	Risk_Monitoring_Procedures	Numeric	8	2	Procedures for ...	None	None	8	Right	Nominal	Input
14	Data_Privacy_Safeguards	Numeric	8	2	Strength of dat...	None	None	8	Right	Nominal	Input
15	Ethical_Review_Practices	Numeric	8	2	Use of ethical r...	None	None	8	Right	Nominal	Input
16	Strategic_Alignment	Numeric	8	2	Alignment of AI ...	None	None	8	Right	Nominal	Input
17	Hallucination_Incidents	Numeric	8	2	Frequency/risk ...	None	None	8	Right	Nominal	Input
18	Bias_or_Fairness_Incidents	Numeric	8	2	Frequency/risk ...	None	None	8	Right	Nominal	Input
19	Misuse_or_Unauthorized_Use_Risk	Numeric	8	2	Risk of misuse ...	None	None	8	Right	Nominal	Input
20	Workflow_Disruption	Numeric	8	2	Extent of workfl...	None	None	8	Right	Nominal	Input
21	Low_User_Trust	Numeric	8	2	Low user trust i...	None	None	8	Right	Nominal	Input
22	Shadow_AI_Use	Numeric	8	2	Extent/risk of s...	None	None	8	Right	Nominal	Input
23	Governance_Strength_Score	Numeric	8	2	Composite gov...	None	None	8	Right	Scale	Input
24	Failure_Signal_Score	Numeric	8	2	Composite AI f...	None	None	8	Right	Scale	Input
25	Governance_Risk_Score	Numeric	8	2	Overall governa...	None	None	8	Right	Scale	Input
26	Governance_Risk_Level	String	8	0	Categorical gov...	None	None	8	Left	Nominal	Input
27	High_Risk_Binary	Numeric	8	2	Binary indicator...	None	None	8	Right	Nominal	Input

	Respondent_ID	Organization_Type	Organizati on_Size	Respondent_Role	Years_of_Experi ence	GenAI_Adoption_Stage	Policy_Clar...	Leadership_S upport	AI_Training_A dequacy	Accountabili ty_Structure	Human_Over sight	Compliance_ Readiness	Risk_Monitori ng_Procedure s	Data_Privacy _Safeguards	Ethic s_Pr
1	R001	Technology	Medium	Operations Officer	10+ years	Early Deployment	3.00	4.00	3.00	3.00	4.00	4.00	3.00	4.00	
2	R002	Technology	Medium	AI Practitioner	7-10 years	Planning	3.00	4.00	3.00	3.00	4.00	3.00	4.00	3.00	
3	R003	Retail	Medium	IT Staff	7-10 years	Early Deployment	3.00	4.00	4.00	4.00	3.00	4.00	3.00	4.00	
4	R004	Retail	Medium	Business Analyst	7-10 years	Planning	4.00	5.00	5.00	4.00	5.00	5.00	3.00	4.00	
5	R005	Technology	Large	Compliance Officer	1-3 years	Scaled Deployment	3.00	3.00	3.00	3.00	3.00	3.00	2.00	3.00	
6	R006	Healthcare	Medium	Operations Officer	10+ years	Scaled Deployment	3.00	3.00	3.00	3.00	3.00	4.00	3.00	3.00	
7	R007	Public Sector	Large	AI Practitioner	7-10 years	Pilot	5.00	5.00	5.00	4.00	4.00	4.00	3.00	5.00	
8	R008	Manufacturing	Large	AI Practitioner	4-6 years	Early Deployment	4.00	4.00	3.00	4.00	3.00	3.00	5.00	4.00	
9	R009	Healthcare	Medium	Manager	1-3 years	Pilot	3.00	3.00	3.00	3.00	3.00	2.00	1.00	4.00	
10	R010	Public Sector	Medium	Manager	4-6 years	Planning	4.00	5.00	3.00	4.00	3.00	4.00	4.00	3.00	
11	R011	Retail	Medium	AI Practitioner	4-6 years	Pilot	2.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00	
12	R012	Education	Medium	IT Staff	10+ years	Scaled Deployment	3.00	4.00	3.00	2.00	3.00	3.00	3.00	3.00	
13	R013	Public Sector	Large	Compliance Officer	4-6 years	Early Deployment	3.00	4.00	4.00	2.00	3.00	3.00	3.00	4.00	
14	R014	Technology	Medium	Operations Officer	4-6 years	Planning	3.00	2.00	2.00	2.00	1.00	1.00	2.00	2.00	
15	R015	Retail	Large	Manager	10+ years	Scaled Deployment	2.00	2.00	2.00	2.00	2.00	3.00	2.00	3.00	
16	R016	Retail	Small	Operations Officer	1-3 years	Early Deployment	3.00	3.00	3.00	2.00	3.00	3.00	3.00	2.00	
17	R017	Manufacturing	Small	IT Staff	4-6 years	Scaled Deployment	2.00	2.00	3.00	3.00	3.00	2.00	2.00	3.00	
18	R018	Technology	Medium	Operations Officer	1-3 years	Early Deployment	3.00	3.00	3.00	3.00	3.00	4.00	3.00	4.00	
19	R019	Manufacturing	Medium	Business Analyst	7-10 years	Early Deployment	3.00	2.00	3.00	3.00	3.00	3.00	2.00	3.00	
20	R020	Technology	Small	Manager	10+ years	Planning	3.00	2.00	2.00	2.00	3.00	2.00	2.00	3.00	
21	R021	Manufacturing	Medium	IT Staff	1-3 years	Planning	5.00	5.00	4.00	5.00	3.00	4.00	4.00	4.00	
22	R022	Public Sector	Small	IT Staff	10+ years	Scaled Deployment	2.00	2.00	3.00	4.00	3.00	3.00	2.00	4.00	
23	R023	Healthcare	Small	Compliance Officer	1-3 years	Pilot	4.00	4.00	3.00	3.00	3.00	4.00	2.00	5.00	
24	R024	Education	Large	Compliance Officer	10+ years	Scaled Deployment	1.00	1.00	3.00	3.00	3.00	3.00	3.00	2.00	
25	R025	Education	Small	Business Analyst	7-10 years	Early Deployment	3.00	3.00	2.00	3.00	2.00	4.00	3.00	3.00	
26	R026	Technology	Large	IT Staff	7-10 years	Planning	5.00	4.00	2.00	4.00	2.00	3.00	3.00	4.00	
27	R027	Finance	Large	Team Lead	1-3 years	Planning	2.00	2.00	3.00	2.00	1.00	2.00	2.00	3.00	
28	R028	Consulting	Large	IT Staff	10+ years	Pilot	3.00	3.00	4.00	4.00	4.00	3.00	4.00	3.00	
29	R029	Retail	Small	Compliance Officer	7-10 years	Scaled Deployment	3.00	2.00	3.00	3.00	3.00	3.00	2.00	3.00	
30	R030	Retail	Large	Team Lead	4-6 years	Pilot	3.00	3.00	3.00	2.00	2.00	4.00	2.00	3.00	



	Respondent_ID	Organization_Type	Organizational_Size	Respondent_Role	Years_of_Experience	GenAI_Adoption_Stage	Policy_Clarity	Leadership_Support	AI_Training_Adequacy	Accountability_Structure	Human_Oversight	Compliance_Readiness	Risk_Monitoring_Procedures	Data_Privacy_Safeguards	Ethical_Practices
76	R076	Technology	Small	Manager	4-6 years	Early Deployment	4.00	4.00	3.00	4.00	3.00	3.00	3.00	5.00	
77	R077	Retail	Large	Business Analyst	10+ years	Planning	3.00	3.00	4.00	4.00	3.00	2.00	3.00	3.00	
78	R078	Finance	Medium	Team Lead	4-6 years	Scaled Deployment	4.00	3.00	3.00	3.00	3.00	4.00	3.00	3.00	
79	R079	Consulting	Medium	IT Staff	4-6 years	Early Deployment	3.00	3.00	4.00	5.00	2.00	4.00	3.00	3.00	
80	R080	Education	Small	Team Lead	4-6 years	Scaled Deployment	3.00	2.00	1.00	2.00	2.00	2.00	2.00	2.00	
81	R081	Finance	Small	AI Practitioner	4-6 years	Planning	3.00	3.00	2.00	3.00	3.00	3.00	3.00	3.00	
82	R082	Retail	Small	AI Practitioner	7-10 years	Early Deployment	3.00	4.00	3.00	3.00	3.00	3.00	3.00	3.00	
83	R083	Public Sector	Medium	IT Staff	1-3 years	Early Deployment	4.00	5.00	3.00	3.00	5.00	4.00	4.00	4.00	
84	R084	Technology	Large	Compliance Officer	4-6 years	Pilot	3.00	2.00	2.00	3.00	4.00	3.00	3.00	3.00	
85	R085	Healthcare	Medium	Compliance Officer	1-3 years	Pilot	2.00	4.00	2.00	2.00	3.00	2.00	3.00	3.00	
86	R086	Manufacturing	Small	AI Practitioner	4-6 years	Planning	3.00	2.00	3.00	2.00	3.00	3.00	3.00	4.00	
87	R087	Consulting	Small	AI Practitioner	4-6 years	Early Deployment	4.00	4.00	4.00	3.00	4.00	4.00	4.00	4.00	
88	R088	Manufacturing	Small	Operations Officer	7-10 years	Early Deployment	3.00	4.00	4.00	3.00	3.00	3.00	4.00	3.00	
89	R089	Retail	Medium	Manager	10+ years	Planning	2.00	3.00	3.00	4.00	3.00	3.00	3.00	3.00	
90	R090	Consulting	Large	Operations Officer	4-6 years	Early Deployment	3.00	3.00	3.00	4.00	3.00	4.00	2.00	4.00	
91	R091	Consulting	Small	Operations Officer	7-10 years	Early Deployment	3.00	3.00	3.00	3.00	3.00	3.00	3.00	4.00	
92	R092	Technology	Large	Compliance Officer	4-6 years	Planning	4.00	4.00	4.00	5.00	4.00	5.00	4.00	4.00	
93	R093	Consulting	Large	IT Staff	4-6 years	Scaled Deployment	3.00	2.00	2.00	3.00	3.00	2.00	3.00	3.00	
94	R094	Education	Medium	Compliance Officer	1-3 years	Scaled Deployment	2.00	4.00	4.00	2.00	3.00	3.00	2.00	4.00	
95	R095	Finance	Large	Manager	1-3 years	Early Deployment	3.00	3.00	3.00	4.00	4.00	3.00	2.00	4.00	
96	R096	Finance	Medium	Team Lead	4-6 years	Planning	2.00	2.00	2.00	2.00	2.00	2.00	3.00	3.00	
97	R097	Finance	Medium	AI Practitioner	4-6 years	Early Deployment	3.00	4.00	2.00	3.00	3.00	4.00	3.00	3.00	
98	R098	Education	Medium	AI Practitioner	1-3 years	Early Deployment	3.00	4.00	4.00	3.00	3.00	3.00	4.00	4.00	
99	R099	Manufacturing	Medium	Manager	1-3 years	Pilot	3.00	4.00	3.00	3.00	3.00	4.00	3.00	4.00	
100	R100	Technology	Small	Operations Officer	1-3 years	Early Deployment	2.00	4.00	4.00	2.00	3.00	3.00	3.00	3.00	





Statistics

		Type of organization	Size of organization	Role of respondent	Years of professional experience	Current stage of generative AI adoption	Categorical governance risk level	Binary indicator of high governance risk
N	Valid	100	100	100	100	100	100	100
	Missing	0	0	0	0	0	0	0

Frequency Table

Type of organization

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Consulting	10	10.0	10.0	10.0
	Education	9	9.0	9.0	19.0
	Finance	7	7.0	7.0	26.0
	Healthcare	11	11.0	11.0	37.0
	Manufacturing	12	12.0	12.0	49.0
	Public Sector	13	13.0	13.0	62.0
	Retail	19	19.0	19.0	81.0
	Technology	19	19.0	19.0	100.0
	Total	100	100.0	100.0	

Size of organization

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Large	30	30.0	30.0	30.0
	Medium	41	41.0	41.0	71.0
	Small	29	29.0	29.0	100.0
	Total	100	100.0	100.0	

Role of respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AI Practitioner	15	15.0	15.0	15.0
	Business Analyst	11	11.0	11.0	26.0
	Compliance Officer	16	16.0	16.0	42.0
	IT Staff	14	14.0	14.0	56.0
	Manager	16	16.0	16.0	72.0
	Operations Officer	16	16.0	16.0	88.0
	Team Lead	12	12.0	12.0	100.0
	Total	100	100.0	100.0	

Years of professional experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-3 years	29	29.0	29.0	29.0
	10+ years	18	18.0	18.0	47.0
	4-6 years	33	33.0	33.0	80.0
	7-10 years	20	20.0	20.0	100.0
	Total	100	100.0	100.0	

Current stage of generative AI adoption

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Early Deployment	33	33.0	33.0	33.0
	Pilot	20	20.0	20.0	53.0
	Planning	23	23.0	23.0	76.0
	Scaled Deployment	24	24.0	24.0	100.0
	Total	100	100.0	100.0	

[DataSet0]

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Clarity of AI-related organizational policies	100	1.00	5.00	3.1000	.85870
Leadership support for AI governance	100	1.00	5.00	3.2200	1.01085
Adequacy of AI-related training	100	1.00	5.00	3.0100	.81023
Clarity of accountability structure for AI use	100	1.00	5.00	2.9800	.90988
Presence of human oversight in AI processes	100	1.00	5.00	3.0300	.84632
Readiness for AI-related compliance requirements	100	1.00	5.00	3.0200	.95325
Procedures for monitoring AI-related risk	100	1.00	5.00	2.9400	.88557
Strength of data privacy safeguards	100	1.00	5.00	3.2800	.85375
Use of ethical review practices for AI	100	1.00	5.00	2.9900	.94810
Alignment of AI adoption with business strategy	100	1.00	5.00	3.1700	.87681
Frequency/risk of hallucination incidents	100	1.00	5.00	3.1500	.93609
Frequency/risk of bias or fairness incidents	100	1.00	5.00	2.9200	.99168
Risk of misuse or unauthorized AI use	100	1.00	5.00	3.0300	.92611
Extent of workflow disruption from AI adoption	100	1.00	5.00	3.0700	.91293
Low user trust in AI systems	100	1.00	5.00	2.9500	.92524
Extent/risk of shadow AI use	100	1.00	5.00	3.1100	1.01399
Composite governance strength score	100	1.40	4.40	3.0740	.66113
Composite AI failure signal score	100	1.33	4.83	3.0389	.72180
Overall governance risk score	100	1.42	6.02	3.5874	.94820
Valid N (listwise)	100				

Reliability

[DataSet0]

Scale: Governance Predictors

Case Processing Summary

		N	%
Cases	Valid	100	100.0
	Excluded[a]	0	.0
	Total	100	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.906	.907	10

Item Statistics

	Mean	Std. Deviation	N
Clarity of AI-related organizational policies	3.1000	.85870	100
Leadership support for AI governance	3.2200	1.01085	100
Adequacy of AI-related training	3.0100	.81023	100
Clarity of accountability structure for AI use	2.9800	.90988	100
Presence of human oversight in AI processes	3.0300	.84632	100
Readiness for AI-related compliance requirements	3.0200	.95325	100
Procedures for monitoring AI-related risk	2.9400	.88557	100
Strength of data privacy safeguards	3.2800	.85375	100
Use of ethical review practices for AI	2.9900	.94810	100
Alignment of AI adoption with business strategy	3.1700	.87681	100

Inter-Item Correlation Matrix

	Clarity of AI-related organizational policies	Leadership support for AI governance	Adequacy of AI-related training	Clarity of accountability structure for AI use	Presence of human oversight in AI processes	Readiness for AI-related compliance requirements	Procedures for monitoring AI-related risk	Strength of data privacy safeguards	Use of ethical review practices for AI	Alignment of AI adoption with business strategy
Clarity of AI-related organizational policies	1.000	.556	.434	.529	.441	.553	.486	.469	.572	.447
Leadership support for AI governance	.556	1.000	.592	.411	.535	.499	.545	.455	.563	.516
Adequacy of AI-related training	.434	.553	1.000	.562	.530	.562	.459	.434	.552	.481
Clarity of accountability structure for AI use	.529	.411	.562	1.000	.434	.525	.430	.543	.421	.469
Presence of human oversight in AI processes	.441	.535	.530	.434	1.000	.463	.531	.464	.526	.565
Readiness for AI-related compliance requirements	.553	.499	.562	.525	.463	1.000	.432	.578	.570	.491
Procedures for monitoring AI-related risk	.486	.545	.459	.430	.531	.432	1.000	.373	.556	.469
Strength of data privacy safeguards	.469	.455	.434	.543	.464	.578	.373	1.000	.556	.449
Use of ethical review practices for AI	.572	.563	.552	.421	.526	.570	.556	.556	1.000	.483
Alignment of AI adoption with business strategy	.447	.516	.481	.469	.565	.491	.469	.449	.483	1.000

Scale Statistics

Mean	Variance	Std. Deviation	N of Items
30.7400	47.709	6.91172	10

Scale: Failure Signals

Case Processing Summary

		N	%
Cases	Valid	100	100.0
	Excluded[a]	0	.0
	Total	100	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.852	.852	6

Item Statistics

	Mean	Std. Deviation	N
Frequencyrisk of hallucination incidents	3.1500	.93609	100
Frequencyrisk of bias or fairness incidents	2.9200	.99148	100
Risk of misuse or unauthorized AI use	3.0300	.92611	100
Extent of workflow disruption from AI adoption	3.0700	.91293	100
Low user trust in AI systems	2.9500	.92524	100
Extentrisk of shadow AI use	3.1100	1.01399	100

Inter-Item Correlation Matrix

	Frequencyrisk of hallucination incidents	Frequencyrisk of bias or fairness incidents	Risk of misuse or unauthorized AI use	Extent of workflow disruption from AI adoption	Low user trust in AI systems	Extentrisk of shadow AI use
Frequencyrisk of hallucination incidents	1.000	.459	.403	.437	.522	.429
Frequencyrisk of bias or fairness incidents	.459	1.000	.553	.609	.392	.581
Risk of misuse or unauthorized AI use	.403	.553	1.000	.487	.403	.599

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	87.242	13	6.711	326.793	.000[b]
	Residual	1.766	86	.021		
	Total	89.009	99			

a. Dependent Variable: Overall governance risk score

b. Predictors: (Constant), Low user trust in AI systems, Frequencyrisk of bias or fairness incidents, Clarity of accountability structure for AI use, Alignment of AI adoption with business strategy, Clarity of AI-related organizational policies, Procedures for monitoring AI-related risk, Readiness for AI-related compliance requirements, Presence of human oversight in AI processes, Extent of workflow disruption from AI adoption, Adequacy of AI-related training, Risk of misuse or unauthorized AI use, Leadership support for AI governance, Use of ethical review practices for AI

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.723	.248		15.001	.000
	Clarity of AI-related organizational policies	-.057	.024	-.052	-2.411	.018
	Leadership support for AI governance	-.094	.022	-.100	-4.341	.000
	Adequacy of AI-related training	-.047	.027	-.040	-1.767	.081
	Clarity of accountability structure for AI use	-.123	.023	-.118	-5.321	.000
	Presence of human oversight in AI processes	-.098	.024	-.088	-4.097	.000
	Readiness for AI-related compliance requirements	-.092	.022	-.092	-4.171	.000
	Procedures for monitoring AI-related risk	-.058	.023	-.054	-2.539	.013
	Use of ethical review practices for AI	-.060	.024	-.060	-2.524	.013
	Alignment of AI adoption with business strategy	-.075	.023	-.069	-3.284	.001
	Frequencyrisk of bias or fairness incidents	.190	.022	.199	8.816	.000
	Risk of misuse or unauthorized AI use	.159	.023	.155	6.753	.000
	Extent of workflow disruption from AI adoption	.115	.023	.111	5.030	.000
	Low user trust in AI systems	.212	.021	.207	10.265	.000

a. Dependent Variable: Overall governance risk score