Issues in Information Systems
Volume 26, Issue 1, pp. 171-184, 2025

DOI: https://doi.org/10.48009/1_iis_113

Artificial Intelligence Compliance: Perceptions within Organizations

Carol Springer Sargent, *Mercer University, sargent_cs@mercer.edu*
Alex Koohang, *Middle Georgia State University, alex.koohang@mga.edu*
Christopher Tsavatewa, *Middle Georgia State University, chris.tsavatewa@mga.edu*
Kevin Floyd, *Middle Georgia State University, kevin.floyd@mga.edu*
Salome Svanadze, *Caucasus International University, salomea.svanadze@gmail.com*

Abstract

This paper investigated employee perceptions regarding three categories of AI compliance: organizational, technical, and ethical/legal, with a focus on gender, age, and job level within organizations. An instrument was designed to measure AI compliance in these categories. A professional Internet survey company distributed the instrument to sample participants from various organizations in the USA. A total of 152 usable surveys were completed. Three separate analyses of variance (ANOVA) tests were used to analyze the data. Gender differences emerged, with males consistently rating the importance of compliance higher than females in all categories, suggesting a need for further exploration into the underlying reasons. Age-related trends indicated that the older participants exhibited higher opinions about the importance of AI compliance in two AI compliance categories. Regarding job levels, the mean scores increased significantly from entry-level to intermediate and middle management, and then decreased from middle to senior management in two AI compliance categories. The implications of the findings are discussed, emphasizing the urgent need for proactive governance strategies and effective compliance mechanisms to address the rapidly evolving risks associated with AI. It is suggested that leadership engagement and the implementation of Compliance-as-a-Service (CaaS) may enhance adherence to AI risk management practices. Conclusion and recommendations for future research complete the paper.

Keywords: Artificial intelligence, AI, AI compliance, risk, organizational, technical, ethics, legal, user perspectives

Introduction

The rapid advancement of AI, accompanied by its associated risks and benefits, has led to a need to address the safety, good governance, and risk management of these powerful systems. Computer scientists are collaborating with social scientists and lawyers on pressing policy issues posed by new AI abilities (Hacker et al., 2022). The far-reaching potential harms from quality-of-service to social impacts of AI systems are coming into focus, alerting practitioners to consider ways to address these AI consequences (Shelby et al., 2023). Understanding and anticipating AI system risks enables a healthy debate about which risks are most important to address and what practices are necessary to mitigate them.

Organizations such as the NIST's AI Risk Management Framework (NIST, 2023) and the ISO/IEC 42001 international standard (ISO, 2023) offer guidance on best practices to help protect organizations and society from the unintended consequences of AI systems or irresponsible AI actors. The European Union's

Artificial Intelligence Act is the world's first attempt to regulate the development and operations of AI systems. It offers a range of methods to ensure trustworthy and responsible AI (EU, 2024).

What is unknown is how effectively AI developers and users of AI systems address the guidance. If organizations implement AI controls as part of their risk management plan, how strong is compliance with the extensive list of policies and controls? We add to the literature by reporting what users signal as the more critical areas for compliance monitoring. This helps AI developers, AI vendors, and organizations with AI systems allocate their resources to the most vital compliance areas.

AI compliance, in general, is the adherence to standards and policies in the design, development, deployment, and use of AI systems (IBM, 2024; NIST, 2023; Australian Government, 2024; EU, 2024; The White House, 2022). Based on our literature review, we categorized AI compliance into three main areas: organizational, technical, and legal/ethical. Table 1 presents the three categories of AI compliance, along with their associated items, definitions, and sources.

Table 1. Categories of AI Compliance and its three categories

AI Compliance - Organizational
1. *AI Governance Framework*, where a clear and well-defined AI governance framework guides the development and deployment of AI systems (Hirsch et al., 2024). 2. *Compliance Program*, where a robust compliance program ensures adherence to relevant AI regulations and ethical guidelines (Bogucka et al., 2024). 3. *Training and Awareness*, where organizations' employees receive adequate training and awareness on AI ethics, compliance, and responsible AI development (Australian Government, 2024; EU, 2024). 4. *Risk Management*, where risks are effectively identified, assessed, and mitigated in developing and deploying AI systems (Bogucka et al., 2024; Cappelli & Di Marzo Serugendo, 2024; NIST, 2023).
AI Compliance - Technical
1. *Data Governance*, where strong data governance practices are in place, ensures data quality, security, and ethical use for AI development (de-Lima-Santos et al., 2024; Pichai, 2018). 2. *Model Monitoring*, where the performance and behavior of AI models are monitored in real time to detect and address potential issues (AI HLEG, 2019; The White House, 2022). 3. *Model Auditing*, where regular and thorough audits are conducted to assess AI models' accuracy, fairness, and compliance within an organization (Cappelli & Di Marzo Serugendo, 2024; Wang et al., 2020) 4. *Explainable AI (XAI) Techniques*, where XAI techniques are utilized to enhance the transparency and interpretability of AI models (de-Lima-Santos et al., 2024; Deloitte AI Institute, 2024; Hirsch et al., 2024; Taylor & Taylor, 2021). 5. *Security Measures*, where adequate security measures are in place to protect AI systems from cyberattacks and data breaches (IBM, 2024; NIST, 2023).
AI Compliance – Ethical/Legal
1. *Data Privacy*, where data privacy and adhering to relevant data protection regulations are prioritized (Pichai, 2018; The White House, 2022). 2. *Bias and Fairness*, where bias is actively mitigated to ensure fairness in AI systems (Hirsch et al., 2024; The White House, 2022). 3. *Transparency/Explainability*, where transparency/explainability is required in developing and deploying AI systems (Deloitte AI Institute, 2024; Lekadir et al., 2024; Pichai, 2018). 4. *Accountability/Responsibility*, where clear lines of accountability/responsibility are established for AI's ethical and responsible use (AI HLEG, 2019; The White House, 2022).

The purpose of this study is to investigate users' opinions on the importance of AI compliance within organizations, with a focus on the variables of gender, age, and job level. Users' opinions about the importance of AI compliance may help prioritize allocating resources to AI risks. Furthermore, by understanding where users are most focused, AI developers, vendors, and implementing teams can communicate risk-mitigating strategies to internal and external parties, thereby enhancing AI compliance and potentially leading to improved AI adoption within organizations. Studying the differences between gender, age, and job level is crucial for identifying how potential disparities in organizational experience and roles impact perceptions of AI compliance. Understanding how these demographic and hierarchical factors influence attitudes and behaviors related to AI compliance may impact organizations' proactive efforts to address what is needed to adhere to the standards and policies in each AI compliance category, which in turn may contribute to building trust and transparency in AI adoption and enhance organizational efficiency and innovation (Koohang et al., 2023). Based on the purpose of the study, we ask the following research questions:

RQ1: *Is there a significant mean difference between the independent variable of gender and the dependent variables (AI Compliance: Organizational, Technical, and Ethical/Legal) separately?*

RQ2: *Is there a significant mean difference between the independent variable of age and the dependent variables (AI Compliance: Organizational, Technical, and Ethical/Legal) separately?*

RQ3: *Is there a significant mean difference between the independent variable of job level and the dependent variables (AI Compliance: Organizational, Technical, and Ethical/Legal) separately?*

Literature review

Addressing AI risk

We are now beginning to use a shared language surrounding the range of possible harms from an AI system that outgrows its own code ("learning"). The literature has articulated some common themes with elevated levels of concern around human oversight (Deloitte AI Institute, 2024), data privacy (de-Lima-Santos et al., 2024), fairness (Badal et al., 2023; Hagendorff, 2019), explainability (Lekadir et al., 2024), model robustness (NIST, 2023), transparency (Hirsch et al., 2024), and non-maleficence (Jang et al., 2022). Organizations that do not anticipate and surround AI systems with risk-mitigating strategies will lose trust. Trust is an essential lubricant for adopting complicated systems where few comprehend the full range of potential harms (Hirsch et al., 2024).

Organizations that adopt AI need risk-reducing practices. However, the industry has not coalesced around a standardized framework for assessing AI risk. Bogucka et al. (2024) reported 38 distinct AI impact assessment methods to help companies anticipate AI risk and address consequences. The authors encourage thoughtful diversity rather than reducing the variety of risk-sensing practices. Instead, they encourage AI actors to move towards agreement on the taxonomy of AI system risk *themes*, which may be higher or lower for a particular AI use case.

Awareness and understanding of risks have been growing with the conviction that AI developers and organizations implementing AI systems need to be involved in mitigating risks (ISO, 2023). Typically, risk assessments and the adoption of controls to mitigate those risks are vetted within the organization, with traditional concerns centering around the correctness of the output. AI system risk, however, has wider tenacles than technical failures where AI did not *perform-as-designed,* causing disruption of operations (Hacker et al., 2022). Consumers and citizens are becoming increasingly aware that decisions affecting

them were guided by AI, exposing those using AI in their operations to a wide range of people seeking redress (Hayes, 2022). AI developers and those managing AI systems may need to enhance governance over AI by incorporating community-driven engagement to identify, address, and communicate risks beyond technical competence (Shelby et al., 2023). With the widespread adoption of AI use cases and the growing concern about unintended consequences, ensuring that AI systems adhere to legal, ethical, technical, and safety principles is a significant concern for external parties (Bourgne et al., 2023; Cappelli & Di Marzo Serugendo, 2024).

Compliance with AI risk-mitigating policies

Companies struggle not just with creating AI risk management policies but also with compliance. Non-compliance can pose serious consequences, making AI compliance a key issue (Cappelli & Di Marzo Serugendo, 2024). Organizations have challenges raising awareness of AI risk issues and training staff on responsible AI behavior. Businesses purchasing AI solutions need to set expectations for the vendor and the staff deploying the system to ensure clear accountability for AI-enabled decisions and settings (Australian Government, 2024).

Verification of a system's compliance can be done manually or automatically. Manual controls, for instance, mock interactions with the system, offering some assurance of compliance (Australian Government, 2024; Cappelli & Di Marzo Serugendo, 2024). Manual verification that systems are avoiding harm, ensuring consumer trust, and acting responsibly is also difficult (Cappelli & Di Marzo Serugendo, 2024). General Data Protection Regulation (European Parliament, 2016) requires human oversight of major decisions, but what if humans are rubber-stamping the AI system (Hacker et al., 2022; Hayes, 2022)? Manual audits are generally inadequate because of the frequent changes to AI systems (Knoblauch & Großmann, 2023).

Semi-automated tools to monitor AI systems are an emerging strategy to monitor compliance. Data mining processes that scan system logs and sequence activities can help reveal the system's processes, allowing comparison with reference standards (Cappelli & Di Marzo Serugendo, 2024; Wang et al., 2020). Continuous auditing and semi-automated software to supervise AI systems have been proposed, but these tools are not yet vetted and widely available (Cappelli & Di Marzo Serugendo, 2024). Another approach, proactively designing compliance during AI development, requires substantial expertise. For instance, converting ethical norms and de-biasing routines into computational algorithms understandable to the system is complex, especially with evolving criteria for ethical and unbiased sensibilities (Cappelli & Di Marzo Serugendo, 2024). More importantly, developers find it challenging to manage AI impacts after they sell the product and are no longer involved in deploying the AI system (Australian Government, 2024). The placement of accountability for AI's unintended or unanticipated actions is a new legal domain, with "freedom from errors" having a new meaning, not just that it worked as designed (Hacker et al., 2022). For instance, will vendors selling AI solutions accept responsibility for more than proper system setup? Will vendors need customers to document their understanding of system limitations and untested/untrained aspects (Australian Government, 2024; Hacker et al., 2022)?

The European Union (EU) Artificial Intelligence (AI) Act has published the first legislative framework, indicating the required compliance to mitigate AI risks. Most compliance obligations fall on those placing AI on the market or into service (EU, 2024). In particular, the regulation distinguishes between prohibited systems (those with unacceptable levels of risk), high-risk systems (e.g., those that provide a safety component or profile individuals), and general-purpose AI (which completes a distinct, known task). The act imposes higher requirements for those providing "high-risk AI systems," requiring a risk management system, data governance, technical documentation, record-keeping, instructions for use, human oversight, accuracy, robustness, and cybersecurity, and a quality management system to verify compliance.

Compliance-as-a-Service (CaaS) enables the outsourcing of AI risk compliance, reducing upfront costs and simplifying budgeting for these requirements (Wu & Liu, 2023). AI compliance costs are a considerable burden, especially for AI startups, which are often weighed down by high research and development costs, making it challenging to determine whether they will dedicate adequate resources to compliance (Wu & Liu, 2023). It is early to find compliance with AI policies in the literature, likely due to technology novelty and AI implementations' proprietary nature. That is, companies rarely share compliance struggles with outside parties.

Methodology

Instrument

We used the literature review from Table 1 to design the instrument for the present study, which measures users' opinions about the importance of AI compliance in organizations, categorized into three areas: AI compliance: organizational, AI compliance: technical, and AI compliance: ethical/legal. The items for each category are listed below.

AI Compliance – Organizational *(Hirsch et al., 2024; Bogucka et al., 2024; Australian Government, 2024; EU, 2024; Cappelli & Di Marzo Serugendo, 2024; NIST, 2023)*

1. AI Governance Framework: A clear and well-defined AI governance framework that guides the development and deployment of AI systems.
2. Compliance Program: A robust compliance program that ensures adherence to relevant AI regulations and ethical guidelines.
3. Training and Awareness: Organizations' employees receive adequate training and awareness on AI ethics, compliance, and responsible AI development.
4. Risk Management: Effectively identify, assess, and mitigate the risks of developing and deploying AI systems.

AI Compliance – Technical *(de-Lima-Santos et al., 2024; Pichai, 2018; AI HLEG, 2019; The White House, 2022; Cappelli & Di Marzo Serugendo, 2024; Wang et al., 2020; Deloitte AI Institute, 2024; Hirsch et al., 2024; Taylor & Taylor, 2021; IBM, 2024; NIST, 2023)*

1. Data Governance: Having strong data governance practices in place that ensure the quality, security, and ethical use of data for AI development.
2. Model Monitoring: Effectively monitor the performance and behavior of AI models in real time to detect and address potential issues.
3. Model Auditing: Conduct regular and thorough audits to assess AI models' accuracy, fairness, and compliance within any organization.
4. Explainable AI (XAI) Techniques: Utilizing XAI techniques to enhance the transparency and interpretability of AI models.
5. Security Measures: Having adequate security measures to protect AI systems from cyberattacks and data breaches.

AI Compliance – Ethical/Legal *(Pichai, 2018; The White House, 2022; Hirsch et al., 2024; Deloitte AI Institute, 2024; Lekadir et al., 2024; Pichai, 2018; AI HLEG, 2019)*

1. Data Privacy: Prioritizing data privacy and adhering to relevant data protection regulations.
2. Bias and Fairness: Actively mitigate bias and ensure fairness in AI systems.

3. Transparency/Explainability: Striving for transparency/explainability in developing and deploying AI systems.
4. Accountability/Responsibility: Establishing clear lines of accountability/responsibility for AI's ethical and responsible use.

The 5-point Likert-type instrument includes the following scale: 5 = Very important, 4 = Moderately important, 3 = Neutral, 2 = Slightly important, and 1 = Not at all important.

Participants

Participants were employees from various organizations in the USA recruited by a professional Internet survey company. After completing the consent form approved by the Institutional IRB board, they responded to the survey items on the instrument described above. Of the 155 responses, one was eliminated because of incomplete data, and two were eliminated based on the outlier test. This yielded 152 final participants. Refer to Table 2 for the participant demographics and characteristics.

Table 2. Participant characteristics

Company's AI priority			Proficiency with AI			Employees in Company		
	N	%		N	%		N	%
High	39	25.7	High	22	14.5	0-50	48	31.6
Moderate	57	37.5	Somewhat	44	28.9	51-500	47	30.9
Low	56	36.8	Moderate	32	21.1	501-2000	27	17.8
			Limited	54	35.5	2001-10000	18	11.8
						Over 10000	12	7.9

The company's activity			*Region*		
	N	%		N	%
Manufacturing	29	19.1	East North Central	29	19.1
Banking/Financial Services	12	7.9	East South Central	12	7.9
Insurance	20	13.2	Middle Atlantic	16	10.5
Tech/Computer Software	11	7.2	Mountain	6	3.9
Healthcare/Medical	12	7.9	New England	10	6.6
Retail	24	15.8	Pacific	21	13.8
Government	3	2.0	South Atlantic	33	21.7
Services	4	2.6	West North Central	15	9.9
Education	21	13.8	West South Central	10	6.6
Other	16	10.5			

Data Analysis

We used SPSS™ version 29 to analyze the collected data. First, the data were analyzed to obtain the instrument's reliability for all three constructs using Cronbach's Alpha. Second, once the acceptable reliability was obtained, the data were analyzed using three separate one-way analyses of variance (ANOVA). The ANOVA test shows the effect of one independent variable on one dependent variable. The F test establishes the significance of the groups. Mertler and Vannatta (2001) stated that before the ANOVA test is conducted, the following assumptions must be met: 1) the dependent variables are continuous, and the independent variables include two or more independent groups; 2) there is no relationship between the observations in each group or between the groups; and 3) data should be tested to eliminate significant outliers. Once these assumptions are met, the data must be tested for homogeneity of variances, i.e., Levene's test for homogeneity of variances. If Levene's test is not significant at the .05 level, then the standard ANOVA is used. If Levene's test for homogeneity of variances is equal to or less than .05, the

Welsh ANOVA is used. The F test in ANOVA determines the significance of the groups. Post hoc analysis is conducted for groups with more than two levels. Finally, descriptive analyses show each independent variable's means and standard deviation with the dependent variable.

Results

The outlier procedure was conducted to ensure the dataset is free of outliers. Two outliers were eliminated. We conducted reliability tests for the three AI compliance constructs, verifying that the data collected is dependable and not subject to random fluctuations, thus ensuring the accuracy and trustworthiness of the results. A generally accepted reliability value is above 0.7. A value between 0.8 and 0.9 is considered "very good" and values above 0.9 are considered excellent reliability. The reliability results were as follows: AI compliance: Organizational = .913, AI compliance: Technical = .930, and AI compliance: Ethics/Legal = .901.

RQ1: Is there a significant mean difference between the independent variable of gender and the dependent variables (AI Compliance: Organizational, Technical, and Ethical/Legal) separately?

The ANOVA assumptions were met, i.e., the dependent variables for the data set were continuous, the independent variables included two or more independent groups, there was no relationship between the observations in each group or between the groups, and the outliers were eliminated from the dataset. Levene's test results yielded a significant p-value for AI compliance: organizational and AI compliance: technical; therefore, Welsh ANOVA was used. Levene's test for AI compliance: ethics/legal yielded a non-significant p-value greater than .05; therefore, standard ANOVA was used.

Table 3 shows the results of the ANOVA, which indicate a significant difference for AI compliance: Organizational and gender ($F_{1, 150} = 4.537$, $p = .035$), AI compliance: Technical and gender ($F_{1, 150} = 5.549$, $p = .020$), and AI compliance: Ethics/Legal and gender ($F_{1, 150} = 5.298$, $p = .023$).

Table 4 shows descriptive results. In all AI compliance categories (i.e., organizational, technical, and ethical/legal), male subjects scored higher, indicating that they had higher opinions about the importance of AI compliance than females.

Table 3. ANOVA for Gender and the three AI compliance categories

Gender		Sum of Squares	df	Mean Square	F	Sig.
Organizational	Between Groups - (Combined)	5.525	1	5.525	4.537	**.035**
	Within Groups	182.653	150	1.218		
	Total	188.178	151			
Technical	Between Groups - (Combined)	6.414	1	6.414	5.549	**.020**
	Within Groups	173.379	150	1.156		
	Total	179.793	151			
Ethics/legal	Between Groups - (Combined)	6.016	1	6.016	5.298	**.023**
	Within Groups	170.344	150	1.136		
	Total	176.360	151			

Table 4. Descriptives - Gender and the three AI compliance categories

Gender		Organizational	Technical	Ethics/Legal
Female	Mean	3.5301	3.6193	3.6837
	N	83	83	83
	Std. Deviation	1.22437	1.18306	1.15233
Male	Mean	3.9130	4.0319	4.0833
	N	69	69	69
	Std. Deviation	.93721	.92839	.95068

RQ2: Is there a significant mean difference between the independent variable of age and the dependent variables (AI Compliance: Organizational, Technical, and Ethical/Legal) separately?

The ANOVA assumptions were met, i.e., the dependent variables for the data set were continuous, the independent variables included two or more independent groups, there was no relationship between the observations in each group or between the groups, and the outliers were eliminated from the dataset. Levene's test results for all three AI compliance categories yielded a non-significant p-value greater than .05; therefore, standard ANOVA was used.

Table 5 shows the results of the ANOVA. There were no significant differences between AI compliance: organizational and age ($F_{3, 148} = 2.330$, $p = .077$). However, the results indicated a significant difference for AI compliance: Technical and age ($F_{3, 148} = 5.646$, $p = .002$), and AI compliance: Ethics/Legal and age ($F_{3, 148} = 4.976$, $p = .003$). Post hoc comparisons analysis showed group differences between AI compliance: technical and age for groups 18-29 & 60 and above, $p = .005$, and AI compliance: Ethics/Legal and age for groups 18-29 & 60 and above, $p = .004$.

Table 6 shows descriptive results. The mean scores for AI compliance: technical and AI compliance: ethical/legal increased as age increased, i.e., 60 above > 45 – 60 > 30 – 44 > 18 – 29. The older participants exhibited a higher opinion about the importance of AI compliance for technical and ethical/legal.

Table 5. ANOVA for age and the three AI compliance categories

Age		Sum of Squares	df	Mean Square	F	Sig.
Organizational	Between Groups - (Combined)	8.488	3	2.829	2.330	.077
	Within Groups	179.690	148	1.214		
	Total	188.178	151			
Technical	Between Groups - (Combined)	16.937	3	5.646	5.131	**.002**
	Within Groups	162.856	148	1.100		
	Total	179.793	151			
Ethics/Legal	Between Groups - (Combined)	16.159	3	5.386	4.976	**.003**
	Within Groups	160.202	148	1.082		
	Total	176.360	151			

Table 6. Descriptives - Age and the three AI compliance categories

Age		Organizational	Technical	Ethics/Legal
18 - 29	Mean	3.3281	3.2938	3.3125
	N	32	32	32
	Std. Deviation	1.02870	.97714	1.10898
30 - 44	Mean	3.6908	3.6263	3.7829
	N	38	38	38
	Std. Deviation	1.11415	1.06459	1.00198
45 - 60	Mean	3.6824	3.9892	4.0068
	N	37	37	37
	Std. Deviation	1.11593	.90301	.86500
60 above	Mean	4.0000	4.1733	4.2111
	N	45	45	45
	Std. Deviation	1.12941	1.18674	1.14807

RQ3: Is there a significant mean difference between the independent variable of job levels and the dependent variables (AI Compliance: Organizational, Technical, and Ethical/Legal) separately?

The ANOVA assumptions were met, i.e., the dependent variables for the data set were continuous, the independent variables included two or more independent groups, there was no relationship between the observations in each group or between the groups, and the outliers were eliminated from the dataset. Levene's test results for all three AI compliance categories yielded a non-significant p-value greater than .05; therefore, standard ANOVA was used.

Table 7 shows the results of the ANOVA. Significant differences existed between job level and AI compliance: organizational ($F_{3, 148} = 4.081$, $p = .008$) and job level and AI compliance: technical ($F_{3, 148} = 2.717$, $p = .047$).

The results for AI compliance: ethics/legal and job level yielded no significant group difference ($F_{3, 148} = 1.538$, $p = .207$). Post hoc comparisons analysis showed group differences between AI compliance: organizational and job level for middle and senior management groups, $p = .001$.

Table 8 shows descriptive results for all AI compliance categories and job levels. The mean scores increase from entry-level to intermediate to middle management. However, they decrease from middle management to senior management.

Table 7. ANOVA for job level and the three AI compliance categories

Job level		Sum of Squares	df	Mean Square	F	Sig.
Organizational	Between Groups - (Combined)	14.377	3	4.792	4.081	**.008**
	Within Groups	173.801	148	1.174		
	Total	188.178	151			
Technical	Between Groups - (Combined)	9.384	3	3.128	2.717	**.047**
	Within Groups	170.409	148	1.151		
	Total	179.793	151			
Ethics/Legal	Between Groups - (Combined)	5.334	3	1.778	1.538	.207
	Within Groups	171.027	148	1.156		
	Total	176.360	151			

Table 8. Descriptives - Job level and the three AI compliance categories

Job level		Organizational	Technical	Ethics/Legal
Entry Level	Mean	3.5833	3.5852	3.6852
	N	27	27	27
	Std. Deviation	1.15192	1.15549	1.16147
Intermediate	Mean	3.6652	3.8357	3.8750
	N	56	56	56
	Std. Deviation	1.09262	1.07609	1.04989
Middle management	Mean	4.1369	4.1381	4.1250
	N	42	42	42
	Std. Deviation	.81000	.78459	.81945
Senior Management	Mean	3.2315	3.4519	3.6204
	N	27	27	27
	Std. Deviation	1.34079	1.34117	1.35585
Total	Mean	3.7039	3.8066	3.8651
	N	152	152	152
	Std. Deviation	1.11634	1.09119	1.08072

Discussion

Theoretical Implications

This exploration contributes to the literature by reporting employee perceptions of the importance of compliance in reducing AI risks in three important areas: organizational, technical, and ethical/legal. Overall, workers reported compliance in mitigating AI risks as moderately to very important (means above 3.5 on a Likert scale of 1-5, with 5 = very important), especially men and those with more life and work experience (over 29 years old and beyond entry-level job positions). This confirms the literature that citizens are becoming more aware that AI can lead to unintended adverse technical outcomes and ethical or legal issues impacting organizations (Hacker et al., 2022; Hayes, 2022; Shelby et al., 2023). That is, there is a general sense that AI needs governance to avoid a range of negative impacts (Bourgne et al., 2023; Cappelli & Di Marzo Serugendo, 2024).

This study also contributes to the literature by investigating whether gender, age level, or job level were associated with respondents' ratings of the importance of AI compliance in organizational, technical, and ethical/legal areas. The finding for gender indicated that males rated the importance of AI compliance higher than females in all three areas, organizational, technical, and ethical/legal. The literature has not explored why gender may increase the reported importance of mitigating AI risks, making this finding an area for further study.

For the age level, the level of importance increased with age, with the youngest group, 18-29 years old, rating the importance of AI compliance lower than other age groups in all three areas: organization, technical, and ethics/legal. It is possible that younger individuals and those just starting their work lives have not been exposed to AI risks or best practices for mitigating them. This is an area that warrants further study.

For job level, the rating increased as the job level rose, with middle management rating the importance of AI compliance higher than other job levels. In an unexpected result, senior management rated AI compliance related to organizational risks as the lowest in importance. Further work is needed to examine whether senior management has visibility over risks and, therefore, rates the importance of governance structure, training, and risk assessment lower than those without special access to current governance practices.

Practical Implications

The risks associated with AI and strategies for mitigating them are evolving rapidly. The overall high importance rating by nearly all respondents highlights that many seem to take the need to comply with AI risk mitigation practices seriously. While limited, tools that can monitor AI sequencing, compare processing against standards, and de-bias data are starting to be designed and vetted (Cappelli & Di Marzo Serugendo, 2024), offering more strategies to help mitigate AI risks. Given the general agreement on the importance of mitigating and governing these robust systems, these may be excellent proactive projects.

Leaders who set expectations for workers may also help to focus efforts on accountability for AI-related decisions and settings during design and implementation (Australian Government, 2024; Hacker et al., 2022), mitigating risks. Another strategy is Compliance-as-a-Service (CaaS), which has external experts assume the considerable burden of conducting due diligence and monitoring compliance (Wu & Liu, 2023). Even with a well-developed AI risk management system, non-compliance with AI policies may mirror non-compliance with other technology risks. Organizations effective in increasing compliance with other IT risks, such as cybersecurity, may have an advantage with compliance habits already in place for addressing AI risks (Nord et al., 2022), an area for future research.

With the emergence of numerous new use cases, it is too early to establish comprehensive compliance practices. Tracking the risk itself is a considerable challenge, especially with the current level of experimentation. Identifying risks occurs before forming strategies to mitigate them, so compliance practices will lag behind the creation and sharing of AI enterprise management. The first legislative framework on compliance with AI risks was recently published by the European Union (EU, 2024), requiring a risk management system. Other regulators will likely follow with similar themes, including human oversight, transparency, robust testing, cybersecurity measures, and quality management. Prior work on information security policy compliance suggests that leadership that values compliance provides a supportive culture and engages workers so that they value their role in safeguarding the organization, tends to comply with policies (Nord et al., 2022). Leaders who adopt best practices for technology compliance may benefit from a workforce already adhering to technology policies.

Conclusion and Future Research

This study concludes that there is a significant and growing recognition of the importance of AI compliance across organizational, technical, and ethical/legal dimensions. The findings for gender indicated a significant difference for all three categories of AI compliance: organizational, technical, and ethical/legal. Male subjects scored higher than female subjects, indicating that they held more positive opinions about the importance of AI compliance. There was no significant difference between age and AI compliance: organizational. However, the findings indicated significant differences between age and AI compliance: technical and AI compliance: ethical/legal. In both categories, the older participants exhibited higher opinions about the importance of AI compliance. Furthermore, significant differences were reported between job level and AI compliance: organizational and AI compliance: technical. The mean scores increase from entry-level to intermediate to middle management. However, they decrease from middle management to senior management. No significant difference was reported for job level and AI compliance: ethics/legal.

These findings point to several promising research directions. Future research should delve deeper into the gender differences in the perceived importance of AI compliance. Qualitative studies examining the specific experiences and perspectives of male and female employees regarding AI risks and compliance could provide valuable insights. The gender gap in perceived importance merits deeper investigation into

whether this reflects different levels of AI exposure, risk tolerance, or other factors. Longitudinal studies tracking the perceptions of younger workers as their exposure to AI technologies increases would also be beneficial in understanding the evolution of their views on AI compliance.

The disconnect between senior management and other job levels regarding organizational compliance raises questions about visibility into current governance practices and resource allocation priorities. Further investigation into the unexpectedly lower ratings from senior management regarding organizational AI compliance is warranted. Exploring their specific understanding of these risks and their approaches to mitigation could reveal crucial insights into leadership perspectives. Future studies could employ qualitative methods to explore the reasoning behind these differences and develop more effective approaches to building organization-wide consensus on AI governance.

Additionally, future research could explore the effectiveness of different governance strategies and compliance mechanisms, including the implementation and impact of Compliance-as-a-Service (CaaS) models on organizational adherence to AI risk management practices. Investigating the relationship between organizational culture, training programs, and employee perceptions of AI compliance would also provide valuable practical implications for fostering a more risk-aware and compliant workforce. Furthermore, the instrument for this study was designed based on a literature review and is a first step in measuring users' opinions about AI compliance in organizations. Given that the instrument used in this study was researcher-generated and represents an initial step in measuring user opinions on AI compliance, future studies should prioritize its validation and refinement. Furthermore, expanding the scope of this research to include diverse industries and larger sample sizes would enhance the generalizability of the findings.

Finally, for organizations implementing AI systems, these findings underscore the importance of developing comprehensive compliance strategies that engage employees across all demographic groups. Special attention should be given to raising awareness among younger employees and potentially recalibrating senior management's understanding of organizational compliance needs. As regulatory frameworks continue to evolve globally, organizations that cultivate strong compliance cultures may be better positioned to navigate the complex landscape of AI risks and requirements. By understanding and addressing demographic variations in compliance perceptions, organizations can develop more effective governance structures that protect against AI risks while maximizing benefits.

Acknowledgements

The authors acknowledge the utilization of the Grammarly App throughout this paper for language improvement (i.e., grammar, spelling, punctuation, and style).

References

AI HLEG. (2019). *Ethics guidelines for trustworthy AI*. High-level expert group on artificial intelligence.

Australian Government. (2024). *Testing the AI Ethics Principles*. Department of Industry, Science and Resources. https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-principles

Badal, K., Lee, C. M., & Esserman, L. J. (2023). Guiding principles for the responsible development of artificial intelligence tools for healthcare. *Communications Medicine*, *3*(1), 47–47. https://doi.org/10.1038/s43856-023-00279-9

Bogucka, E., Constantinides, M., Šćepanović, S., & Quercia, D. (2024). *Co-designing an AI Impact Assessment Report Template with AI Practitioners and AI Compliance Experts*. https://doi.org/10.48550/arxiv.2407.17374

Bourgne, G., Ganascia, J.-G., Paschke, A., & Satoh, K. (2023). Preface of Special Issue on International Workshop on AI compliance mechanism (WAICOM 2022). *The Review of Socionetwork Strategies*, *17*(2), 215–216. https://doi.org/10.1007/s12626-023-00150-2

Cappelli, M. A., & Di Marzo Serugendo, G. (2024). A semi-automated software model to support AI ethics compliance assessment of an AI system guided by ethical principles of AI. *Ai and Ethics (Online)*. https://doi.org/10.1007/s43681-024-00480-z

de-Lima-Santos, M.-F., Yeung, W. N., & Dodds, T. (2024). Guiding the way: A comprehensive examination of AI guidelines in global media. *AI & Society*. https://doi.org/10.1007/s00146-024-01973-5

Deloitte AI Institute. (2024). *Toward humanity's brightest future with generative AI*. www.deloitte.com/us/AIInstitute

EU. (2024). *EU artificial intelligence act high-level summary*. European Union.

European Parliament. (2016). *General data protection regulation*. https://gdpr-info.eu/

Hacker, P., Naumann, F., Friedrich, T., Grundmann, S., Lehmann, A., & Zech, H. (2022). AI Compliance – Challenges of Bridging Data Science and Law. *ACM Journal of Data and Information Quality*, *14*(3), 1–4. https://doi.org/10.1145/3531532

Hagendorff, T. (2019). The Ethics of AI Ethics—An Evaluation of Guidelines. *arXiv.Org*. ProQuest Central; ProQuest One Academic. https://doi.org/10.1007/s11023-020-09517-8

Hayes, K. (2022). Beware the Algorithm: Understanding AI Compliance. *ITNow*, *64*(3), 58–59. https://doi.org/10.1093/combul/bwac099

Hirsch, Dennis., Bartley, Timothy., Chandrasekaran, Aravind., Norris, Davon., Parthasarathy, Srinivasan., & Turner, P. Norris. (2024). *Business Data Ethics: Emerging Models for Governing AI and Advanced Analytics* (1st ed. 2024.). Springer International Publishing. https://doi.org/10.1007/978-3-031-21491-2

IBM. (2024). *What is AI ethics?* IBM. www.ibm./topics/ai-ethics

ISO. (2023). *ISO/IEC 42001:2023 Information technolog—Artificial intelligence—Management system*. ISO. iso.org/standard/81230.html

Jang, Y., Choi, S., & Kim, H. (2022). Development and validation of an instrument to measure undergraduate students' attitudes toward the ethics of artificial intelligence (AT-EAI) and analysis of its difference by gender and experience of AI education. *Education and Information Technologies*, *27*(8), 11635–11667. https://doi.org/10.1007/s10639-022-11086-5

Knoblauch, D., & Großmann, J. (2023). Towards a Risk-Based Continuous Auditing-Based Certification for Machine Learning. *The Review of Socionetwork Strategies*, *17*(2), 255–273. https://doi.org/10.1007/s12626-023-00148-w

Koohang, A., Sargent, C. S., Zhang, J. Z., & Marotta, A. (2023). Big data analytics: From leadership to firm performance. *Industrial Management and Data Systems*, *123*(12), 2976–2996. https://doi.org/10.1108/IMDS-06-2023-0415

Lekadir, K., Frangi, A. F., Porras, A. R., Glocker, B., Cintas, C., Langlotz, C. P., ... & Starmans, M. P. (2025). FUTURE-AI: international consensus guideline for trustworthy and deployable artificial intelligence in healthcare. *arXiv.Org*. *bmj*, 388.

Mertler, C. A., & Vannatta, R. A., (2001). Advanced and multivariate statistical methods: Practical application and interpretation. Routledge.

NIST. (2023). *Artificial intelligence risk management framework (AI RM 1.0)*. U.S. Department of Commerce.

Nord, J., Sargent, C. S., Koohang, A., & Marotta, A. (2022). Predictors of Success in Information Security Policy Compliance. *The Journal of Computer Information Systems*, *62*(4), 863–873. https://doi.org/10.1080/08874417.2022.2067795

Pichai, S. (2018). *AI at Google: Our principles*. https://blog.google/technology/ai/ai-principles/

Shelby, R., Rismani, S., Henne, K., Moon, A., Rostamzadeh, N., Nicholas, P., ... & Virk, G. (2023, August). Sociotechnical harms of algorithmic systems: Scoping a taxonomy for harm reduction. *In Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 723-741). https://doi.org/10.1145/3600211.3604673

Taylor, J. E. T., & Taylor, G. W. (2021). Artificial cognition: How experimental psychology can help generate explainable artificial intelligence. *Psychonomic Bulletin & Review*, *28*(2), 454–475. https://doi.org/10.3758/s13423-020-01825-5

The White House. (2022). *Blueprint for an AI bill of rights: Making automated systems work for the American people*.

Wang, K., Zipperle, M., Becherer, M., Gottwalt, F., & Zhang, Y. (2020). An AI-Based Automated Continuous Compliance Awareness Framework (CoCAF) for Procurement Auditing. *Big Data and Cognitive Computing*, *4*(3), 23. https://doi.org/10.3390/bdcc4030023

Wu, W., & Liu, S. (2023). Why Compliance Costs of AI Commercialization May Be Holding Startups Back. *Kennedy School Review*, *23*, 16.