JPS Journal of Policy Studies

J. Policy Stud. 2026;41(1):41-57
https://doi.org/10.52372/jps.250358
pISSN 2799-9130 eISSN 2800-0714

Article

Governing artificial intelligence risks for effective public administration: the case of Kuwait

Shahad Altammar
Kuwait University, Kuwait City, Kuwait

Received: December 12, 2025
Revised: January 29, 2026
Accepted: February 8, 2026

Corresponding author
Shahad Altammar
Tel: +965-24988582
E-mail: dr.sha.alt@ku.edu.kw

ORCID
Shahad Altammar
https://orcid.org/0009-0004-9716-7006

Competing interests
No potential conflict of interest relevant to this article was reported.

Funding sources
Not applicable.

Acknowledgements
Not applicable.

Availability of data and material
Upon reasonable request, the datasets of this study can be available from the corresponding author.

Abstract

Governance of Artificial Intelligence (AI) is increasingly discussed within public administration, yet risk centred conceptualisations remain more developed than empirical evidence in contexts where digital infrastructure is still lagging. This research examines residents' perceptions of AI related risks in Kuwait across the four domains of economic, organisational, social and technical, and considers what these patterns imply for governance priorities in public administration. A nationally representative survey of 679 respondents identifies heightened social risks, particularly related to job security and freedom of expression, alongside moderate economic and organisational risks and variable technical risks. Regression analysis indicates that males perceive lower economic but higher social risks, and that respondents aged 41+ perceive lower economic and technical risks. Education has only a marginal effect on social risk perception. The findings underscore the need for stronger, risk informed governance attention, as residents' evaluations signal where trust pressures and safeguarding expectations are likely to concentrate as digital public services expand. The research concludes by calling for a stakeholder-led governance mission to ensure that innovation is balanced against social welfare in Kuwait.

Keywords: public administration, artificial intelligence, governance, risks, policy

Introduction

Artificial intelligence (AI) governance is increasingly discussed within public administration, yet much of the literature remains focused on general principles rather than on empirical evidence that can guide administrative action (Batool et al., 2025). This gap is especially evident in contexts where digital infrastructure and institutional capacity are still developing. It matters because AI enabled tools are no longer peripheral to government activity. They are becoming embedded in citizen facing services and routine administrative processes, where questions of accountability, legitimacy and trust are practical rather than abstract.

Kuwait provides a relevant setting for examining these issues. As of 2024, Kuwait ranked 68th out of 133 countries in innovation outputs, which include scientific research, investment and technological adoption (WIPO, 2025). Although this represented an improvement from 2021 (73rd), it remained

below its position in 2022 (66th) and 2023 (65th). Kuwait has expanded digital public services through platforms such as Sahil and Sihity (Altammar, 2025), alongside wider private sector uptake in areas such as ecommerce and gaming. At the same time, the most recent Ministry of Interior reporting records substantial losses associated with cybercrime (MOI, 2023), reinforcing that digital transformation expands opportunity while also widening exposure to governance risks that can affect citizens directly.

In public administration terms, AI governance concerns how governments set rules, allocate responsibility and maintain oversight for technologies that shape service delivery and citizen experience. Wilson's (1887) foundational argument was not a celebration of government in the abstract. It was, instead, a claim that administration is the practical work of government and must be understood in relation to its political environment. In contemporary digital settings, this implies that service modernisation must be matched with administrative arrangements that protect the public interest and sustain public confidence. AI governance thus refers to the policies and mechanisms through which AI systems are designed, deployed and overseen responsibly, with attention to transparency and the safeguarding of rights (Cath, 2018; Taeihagh, 2021).

The empirical focus of this study intends to be specific, whereby rather than claiming to test causal governance mechanisms, the research uses residents' evaluations of AI related risks to infer governance priorities for public administration. In other words, the evidence speaks more directly to which risks are prominent to users of AI enabled services and how these perceptions vary across demographic groups. These patterns are then interpreted as signals for where safeguards, administrative capacity and oversight functions are most urgently needed as digital public services expand. This approach is especially relevant in settings where AI adoption is progressing faster than the development of governance routines that can reassure the public and support consistent service performance.

As such, the research examines perceived AI related risks in Kuwait across the four domains of economic, organisational, social and technical—identified through an in depth literature review and refined through expert validation to reflect the Kuwaiti context. It also triangulates survey findings with executive level interviews to clarify how policymakers interpret the risk profile and its governance consequences. The study addresses the following research questions:

RQ1: How do residents in Kuwait evaluate AI related risks across the economic, organisational, social and technical domains in the context of public and private digital services?

RQ2: To what extent do risk perceptions differ by gender, age and education?

RQ3: What governance and policy priorities for public administration are implied by these risk perceptions, particularly in relation to transparency, accountability and socially responsive digital service delivery?

RQ4: How do executive policymakers interpret the survey patterns in terms of likely consequences and governance priorities if AI risks remain insufficiently addressed?

Through the process of responding to these questions, the study contributes empirical evidence from an under researched Gulf context and provides a risk informed basis for strengthening the

https://doi.org/10.52372/jps.250358

governance of AI enabled digital public services. It concludes by calling for a stakeholder-led governance mission that balances innovation with social welfare in Kuwait.

Literature Review

In public administration, governance is widely understood as the set of decisions, arrangements and practices that both constrain and enable service provision (Hill & Lynn Jr., 2004). Governance is therefore not limited to formal rules, as it includes the practical capacities through which public organisations coordinate activity and secure compliance in the delivery of services. In Kuwait, governance enhancement efforts have often concentrated on the private corporate sector (Dalwai et al., 2015; Shehata, 2015), while broader modernisation has occurred through policy adjustments that facilitate market entry and through partnerships where implementation is managed by private entities. At the strategic level, New Kuwait 2035 established nine national development goals, each of which relies on effective governance and the productive use of technology (SCPD, 2025). This strategic context matters for AI because digital public services are expanding while administrative systems are still adapting to new forms of risk, accountability and citizen expectation.

AI governance has developed into a multidisciplinary area that is concerned with how AI systems are designed and deployed to align with public values, legal standards and institutional responsibilities (Taeihagh, 2021). In the public sector, the governance challenge is heightened since AI enabled systems largely sit within citizen facing services and environments consisting of administrative decisions. This raises questions not only about technical performance but also about transparency and accountability. A recurring concern in the governance literature is the opacity of certain AI models and their decision pathways, especially where systems function as "black boxes" that make it difficult to explain outcomes or allocate responsibility (Rahwan, 2018). For public administration, such opacity is not merely a technical characteristic, as it has implications for administrative legitimacy because citizens are more likely to accept public decisions when they perceive decision processes as fair and open to scrutiny.

Legitimacy is thus central to the governance implications of AI. Public trust in government is shaped not only by outcomes but also by whether procedures appear to be responsive and transparent (Bouckaert & van de Walle, 2003; Grimmelikhuijsen, 2012). In digital government, citizen confidence can be influenced by perceived competence, protection of user rights and how public bodies respond to failures or harms in digital services (Tolbert & Mossberger, 2006). This line of work situates AI risk governance as part of the broader administrative task of sustaining public confidence, while modernising service delivery.

Framing AI governance from a risk centred angle is well established in the literature, yet studies vary in how risks are conceptualised and prioritised. Many authors emphasise that the rapid expansion of AI introduces risks that span social, legal, organisational and technical dimensions, and that governance must be adaptive to keep pace with technological change (Floridi, 2018; Wirtz et al., 2022). Risk governance scholarship also highlights that emerging technologies require comparative and integrative governance strategies because risks cut across institutional boundaries and can escalate quickly (Linkov et al., 2018a, 2018b). This perspective is directly relevant to

AI enabled public services in which problems in one agency or platform can influence public confidence in government more broadly.

In the AI governance literature, social risks commonly include privacy invasion, exposure to harmful content, erosion of user autonomy and decline in public trust. Large scale data handling raises the likelihood of privacy breaches, especially where personal records or facial recognition are involved (Winfield & Jirotka, 2018). Also, privacy risks can become national governance concerns when data misuse undermines legitimacy and generates citizen resistance. Ethical risks are frequently connected to such issues because the use of AI in public services can intersect with citizens' rights and cultural norms and expectations (Nawi et al., 2021). Bias and discrimination represent another widely discussed social risk because AI systems depend on training data that may be incomplete or skewed (Feldstein, 2019; Weyerer & Langer, 2020). When such systems are used for recruitment or evaluation, they may produce inequitable outcomes, including disadvantage based on gender (Hall & Ellis, 2023). These concerns are not only moral, as they shape the perceived fairness of public services and therefore the soundness of administrative decision making.

Social risk discussions often connect directly to labour market disruption. Several studies argue that AI driven automation can displace jobs and affect wages, producing economic strain and social instability (Boyd & Wilson, 2017; Wright & Schultz, 2018). Acemoglu & Restrepo (2019) further explain how automation can reconfigure labour demand and reshape occupational structures. In governance terms, these debates signal that AI adoption in public services cannot be assessed only through efficiency gains. It must also consider social acceptance, perceived fairness and the political economy of employment.

Technical risks are typically framed around system robustness, reliability, cybersecurity and adversarial misuse. Cyberattacks occur even within highly defended information technology environments (Bendovschi, 2015). In Kuwait, high profile breaches in government entities illustrate that digital systems remain vulnerable, even where containment measures limit spread (Addam, 2023). The AI security literature has also emphasised adversarial machine learning and the ways in which systems can be manipulated or exploited (Biggio & Roli, 2018). Technical risks therefore intersect with public administration through the duty to protect public data, maintain service reliability and ensure that digital systems do not become a channel for harm on the larger scale. Wirtz & Müller (2019) stress that AI in public management must be integrated with safeguards that support resilience and accountability, instead of being treated as an independent technical tool.

Organisational risks relate to administrative capacity, coordination, policy coherence and implementation discipline within and across public bodies. AI systems operate within organisational environments that are dynamic and influenced by changes in infrastructure, strategy, internal rules and external market conditions (Doneda & Almeida, 2016). These shifts can undermine performance if AI systems are not monitored and updated. Gasser & Almeida (2017) further note that governance must consider layered responsibility structures because AI systems interact with multiple institutional actors and decision contexts. In practical terms, organisational risks include unclear service ownership, weak inter agency communication and the inability to manage vendor dependencies, all of which can distort accountability and create implementation gaps. These issues are particularly prominent for digital public services where citizens experience the country through

https://doi.org/10.52372/jps.250358

interfaces that appear unified, even when governance responsibilities are dispersed.

Economic risks are often discussed less significantly than technical and social risks, even though they are important for the sustainability of public service innovation. Affordability, long term resourcing, procurement decisions and the costs of maintaining security and compliance infrastructure shape whether AI enabled services remain stable and equitable. Economic constraints also influence the feasibility of investing in workforce capacity, monitoring systems and continuous system updates. In addition, cooperation across borders and learning can influence economic resilience by enabling the adoption of tested standards and governance approaches (Linkov et al., 2018a, 2018b).

Across studies, the relative importance of risk domains differs. Several lines of research prioritise technical and data risks, particularly the quality of data governance and stewardship. Media sector work (Pierson et al., 2023) and healthcare studies (Salathé et al., 2018; Zhang & Zhang, 2023) emphasise that clean data collection and responsible stewardship are prerequisites for trustworthy AI and credible governance. Reviews by Winfield & Jirotka (2018) and Batool et al. (2025) indicate that the research field has often leaned towards accessibility and privacy, at times leaving regulatory and ethical principles less developed in operational terms. In care and public service environments, scholars also caution that fully automated decision making can be inappropriate when judgement that is context sensitive is required (Dickinson et al., 2021). Without human oversight, algorithmic systems may misalign with different cases and social expectations (Cath, 2018; Couture et al., 2023). These debates collectively reinforce that AI risk governance in public administration must treat technical performance, social legitimacy and organisational capacity as intertwined rather than separable.

Despite the global growth of AI governance scholarship and the proliferation of guidelines, empirical research focused on Kuwait remains limited. Kuwait's recent acceleration in digital public services and AI enabled applications increases the need for grounded evidence that can inform administrative priorities. This study therefore contributes by operationalising AI risk governance through a four domains structure of economic, organisational, social and technical, derived from the convergence of the AI governance literature and Kuwait's administrative context. The study does not claim that perceptions alone establish objective risk levels. Instead, it treats residents' evaluations as governance relevant indicators of where trust pressures, user vulnerabilities and administrative responsibilities are likely to concentrate as digital public services expand.

Methodology

This research adopts a mixed methods design that combines a quantitative survey with qualitative interviews. The study begins with an in depth literature review to identify AI related risk domains and candidate survey factors. This was followed by a structured review of the Kuwaiti context, cross verified against the literature, which narrowed the focus to the four domains of social, organisational, technical and economic. Initially, 45 risk factors relevant to Kuwait's socio political landscape were identified. The survey items were developed through a theory informed and context specific process, rather than adopted as a complete, pre-validated scale from a single prior

framework. Candidate risk factors were first identified by synthesising recurring constructs in the AI governance and public administration risk literature (e.g., issues relating to privacy, accountability, transparency, labour market disruption, security and system reliability). These constructs were then translated into item statements that reflect how AI enabled services are encountered in Kuwait across public and private applications. The resulting pool was reviewed by academic and professional experts in governance, technology and policy to assess content relevance, clarity and domain fit, leading to the refinement of item wording and the reduction of the instrument from 45 to 37 items. This staged approach was intended to strengthen content validity while ensuring the instrument captures risk perceptions meaningful to public administration in the Kuwaiti context.

Items were measured on a four points Likert scale ranging from very poor (1.00–1.74) and poor (1.75–2.49) to good (2.50–3.24) and very good (3.25–4.00). Higher composite scores therefore indicate lower perceived risk (4=very good=low risk), while lower scores indicate higher perceived risk and, by implication, a higher governance priority. Domains were defined to reflect the primary focus of impact for public administration. First, social risks capture perceived effects on rights, norms and public trust. Second, organisational risks capture administrative and service delivery constraints within and across institutions. Third, technical risks capture perceived system integrity, reliability and safeguards. Finally, economic risks capture perceived affordability and macro level enabling conditions. Where a factor could plausibly sit in more than one domain, it was classified according to its dominant governance implication in Kuwait. For example, job security was treated as a social risk because it was framed as a social concern with implications for legitimacy and public acceptance, even though it also has economic dimensions.

The survey was administered to a gender balanced random sample of 679 residents who use AI tools through public or private sector applications. Respondents were selected from civil society at large. The aim was to assess how AI tools currently used in Kuwait are perceived by users in terms of risk. Distribution occurred via a nationwide 45 day digital campaign. A simple random sampling approach was combined with a criterion that respondents be at least 25 years old, in order to support more responses that are informed from experience. Quantitative data were analysed using descriptive statistics, demographic group comparisons and multiple regression analysis to examine whether gender, age and education were associated with variation in perceived risk across the four domains.

Quantitative results informed the qualitative component. Semi structured interviews were conducted to deepen the interpretation of the survey patterns and to capture executive level views on governance consequences and priorities. Interviews were guided by two open ended questions and were analysed using thematic analysis. Twenty five interview invitations were issued. Participants were screened using criterion sampling followed by random selection. Eligibility required that participants be department head level or above and employed in one of the following bodies: Central Agency for Information Technology (CAIT), Communication and Information Technology Regulatory Authority (CITRA), Ministry of Justice (MOJ), National Cyber Security Center (NCSC) or Ministry of Finance (MOF). These entities are central to technology administration and regulation in Kuwait. The final qualitative sample consisted of 18 executive level policymakers interviewed over two months. Coded responses were evaluated to identify recurring

https://doi.org/10.52372/jps.250358

themes and supporting suggestions (Lune & Berg, 2017). In this design, the qualitative evidence is used to contextualise and interpret the quantitative risk patterns and to strengthen the public administration implications drawn from the findings.

Data Results

In testing for reliability before administering the survey, a pilot study (N=24) was conducted. Cronbach's α values for all risk domains exceeded the acceptable threshold of 0.70. In the main research (N=679), internal consistency was again confirmed, as shown in Table 1.

As indicated in Table 1, each domain demonstrates strong internal consistency. The organisational (α=0.91), social (α=0.94) and technical (α=0.91) domains exceed 0.90, signalling high reliability. The economic domain (α=0.76) is slightly lower, possibly because it comprises fewer items, yet it still surpasses the commonly cited benchmark. The survey was therefore deemed reliable and distributed more widely. While internal consistency indicates that items within each domain move together in a coherent way, reliability alone does not establish that the domains are fully distinct constructs. In this study, the four domain structure is treated as a theory informed and expert validated classification that supports comparison of relative risk prominence for governance prioritisation. It is not presented as a definitive psychological taxonomy of risk perception. In total, 692 surveys were returned, whereby 13 incomplete responses were removed, leaving 679 valid cases. Table 2 presents the demographic profile of the sample.

Table 2 shows near gender parity, with 49.63% women and 50.37% men. Age groups are also evenly represented, whereas educational attainment is skewed towards bachelor's (49.93%) and postgraduate (40.50%) degrees, with fewer respondents holding only a school leaving certificate (9.57%). Table 3 summarises how respondents evaluated AI related risk factors across Kuwait's public and private sectors. Because the survey scale is coded such that higher values indicate more favourable evaluations, lower mean scores are interpreted as higher perceived risk. In this study,

Table 1. Domain reliability

Scale	Number of items	Cronbach's alpha	r
Economic	4	0.76	0.42
Organisational	11	0.91	0.48
Social	13	0.94	0.52
Technical	9	0.91	0.95

Table 2. Respondents' demographics

Variable	Category	Frequency	Percentage (%)
Gender	Male	342	50.37
	Female	337	49.63
Age group	25–30	159	23.42
	31–35	190	27.98
	36–40	157	23.12
	41 years and above	173	25.48
Education	High school	65	9.57
	Bachelors	339	49.93
	Postgraduate	275	40.50

Table 3. High-level artificial intelligence (AI) risks evaluation

Factor	Mean	S.D.
Economic risks domain		
International cooperation	2.78	0.96
Services affordability	2.45	0.96
Organisational risks domain		
Policy comprehensiveness	2.85	1.00
Efficiency	2.25	1.02
Social risks domain		
Social values	2.53	1.02
Freedom of expression	2.12	0.99
Content moderation	2.16	0.98
Job security	1.85	0.90
Technical risks domain		
AI usage education	2.71	1.39
User rights	2.87	1.42
Reliability	2.66	1.32
User discrimination	2.90	1.36

these risk patterns are not treated as direct measures of objective system performance. Rather, they are interpreted as indicators of where users perceive vulnerability, uncertainty or insufficient safeguards, which in turn helps identify priorities for governance attention in public administration.

Because lower mean scores denote greater perceived risk and therefore imply higher governance priority, items close to 2.00 warrant closer attention. Within the economic domain, service affordability poses a greater perceived risk (M=2.45) than international cooperation (M=2.78). Organisational items cluster around the middle range, with efficiency rated as the riskiest organisational factor (M=2.25). Several social items show notably higher perceived risk, particularly job security (M=1.85), freedom of expression (M=2.12) and content moderation (M=2.16). These results suggest that residents' concerns extend beyond service convenience to issues that touch trust, rights and the wider social implications of AI enabled services. Technical items fall in a similar middle range, but with wider standard deviations (1.32–1.42), indicating more varied experiences or expectations of technical safeguards such as AI usage education, user rights and reliability. Analysed collectively, the patterns suggest that social risks are most prominent, with economic and organisational risks moderate overall and technical perceptions more uneven across respondents and systems. Composite domain scores were then computed to enable comparisons across gender, age and education (Table 4).

As the four point Likert scale ranges from poor (1) to excellent (4), the domain with the lowest mean represents the highest risk. Table 4 shows that the social domain records the lowest mean (2.23), whereas the technical domain records the highest (2.77) but with the widest spread

Table 4. Domain scores

Risk domain	Mean	S.D.	Median
Economic	2.62	0.75	2.50
Organisational	2.69	0.73	2.73
Social	2.23	0.74	2.23
Technical	2.77	1.02	2.67

https://doi.org/10.52372/jps.250358

(S.D.=1.02), indicating more varied perceptions of technical risks. Economic (M=2.62) and organisational (M=2.69) domains fall in the moderate range with narrower spreads. Higher scores indicate lower perceived risk. Thus, respondents are generally less concerned about technical than social risks, with economic and organisational concerns situated between the two. These composite scores formed the basis for further analysis. A multiple regression (Table 5) was then carried out to determine whether gender, age and education significantly predicted perceived AI risk.

According to Table 5, gender significantly predicts both economic and social risks after controlling for demographic factors. Male respondents report a higher economic score (β=0.186, p=0.001), indicating lower perceived economic risk, and a lower social score (β=–0.158, p=0.005), indicating higher perceived social risk than females. No significant differences appear for organisational or technical risks. Age clearly influences organisational, social and technical risks. Respondents aged 36–40 perceive higher organisational risk (β=–0.216, p=0.008) and higher social risk (β=–0.199, p=0.015). Those aged 41+ also rate social risk higher (β=–0.184, p=0.022) yet perceive lower technical risk (β=0.230, p=0.040). Education plays a smaller role overall but significantly predicts social risk among postgraduates (β=–0.227, p=0.023), who perceive greater social risk than respondents with only school level qualifications. Although several effects are statistically significant, the models explain a modest share of variance (R^2=1.6%–6.0%), suggesting that factors beyond these demographics shape perceptions of AI risk.

The research also included qualitative interviews with executive policymakers from CAIT, CITRA, MOJ, NCSC and MOF. Each of the 18 interviewees first reviewed the quantitative findings, enabling more informed discussion. Table 6 presents their coded responses on the consequences of neglecting AI risk governance in Kuwait.

Ninety-four percent of interviewees stressed the importance of government oversight of digital content, warning that neglect would erode public trust and respect for authority. Illustrative comments included "inaccessibility and inefficiency of current service provision", "poor management

Table 5. Regression results

	Economic risk		Organisational risk		Social risk		Technical risk	
	Coef.	p-value	Coef.	p-value	Coef.	p-value	Coef.	p-value
Gender (male=1)	0.19**	0.001	0.07	0.217	–0.16**	0.005	0.05	0.562
Age group (base: 25–30)								
31–35	–0.10	0.226	–0.03	0.709	0.12	0.138	–0.00	0.981
36–40	–0.11	0.168	–0.22**	0.008	–0.20*	0.015	–0.20	0.074
41+	0.13	0.100	–0.01	0.882	–0.18*	0.022	0.23*	0.040
Education (base: high school)								
Bachelors	–0.03	0.750	–0.00	0.975	–0.08	0.407	–0.25	0.067
Postgraduate	–0.00	0.997	–0.00	0.986	–0.23*	0.023	–0.14	0.312
Intercept	2.56**	0.000	2.72**	0.000	2.51**	0.000	2.92**	0.000
R-squared (Adj R-sq)	0.04	0.026	0.02	0.007	0.06	0.051	0.03	0.020
F-statistic (p-value)	4.06**	0.0005	1.77	0.1031	7.12**	0.0000	3.27**	0.0035

Higher domain scores indicate "lower" perceived risk.
Coefficients represent net effects relative to the reference groups: female for gender, 25–30 for age and high school for education.
* p<0.05, ** p<0.01 (two-tailed).
Adj R-sq, adjusted R-squared; Coef., coefficient.

Table 6. Consequences summary

Item	Summary	Frequency	Percentage (%)
1	Weaker government role	17	94
2	Resources depletion	15	83
3	Prevailing underaged acts of violence	14	78
4	Digital addiction	14	78
5	Widespread psychological and social issues	12	67
6	Exposure to cybercrimes	11	61
7	Privacy violations	10	56
8	Penetrable networks and infrastructure	9	50
9	Resistance for digital transformation	9	50
N		18	100

in government sectors" and "technology with inflexible administration is not a pleasant situation for the government to be in". One interviewee remarked, "The greatest fear of most nations is an illegitimate government; it is difficult to rebuild citizens' trust once broken." The second most frequent concern (83%) was resource depletion of manpower at the organisational level, finances nationally and time individually. Interviewees cautioned that insufficient planning could result in "greater corruption", "reduced transparency" and "a national budget deficit". Seventy-eight percent cited digital addiction and potential underage violence, noting that inadequate age restrictions could expose children to harmful content. Table 7 summarises governance recommendations to mitigate these and other risks.

As Table 7 shows, 83% recommended developing web application firewalls to counter hacking and cyberthreats. Seventy-two percent urged mandatory age restrictions on all software before market entry. Sixty-one percent advocated AI specific laws and regulations. One interviewee noted that existing "one size fits all" legislation ignores workplace and service differences, so "governance of particular AI technology should vary accordingly". Government led social initiatives on digital literacy were endorsed by 56% of interviewees. Typical comments included: "We are very late in this; awareness programmes must address all segments of society"; "We need to educate people on their duties and AI risks"; "Departments should allocate part of their training budgets to digital literacy"; and "School curricula should include courses on the responsible use of AI".

Nearly half the interviewees (44%) emphasised the need for continual AI system updates to

Table 7. Recommendations summary

Item	Summary	Frequency	Percentage (%)
1	Developing application firewalls	15	83
2	Implementing age restrictions	13	72
3	Implementing AI specific laws and regulations	11	61
4	Raising social awareness through digital education	10	56
5	Updating software regularly	8	44
6	Strengthening government's cybersecurity	8	44
7	Responding to technical issues with rapid solutions	7	39
8	Hiring technical staff of a reputable caliber	5	28
9	Expanding global agreements to adopt well established development frameworks	4	22
10	Ensuring private sector's duty for use of ethical AI and consumer protection	2	11
N		18	100

https://doi.org/10.52372/jps.250358

secure user data and patch vulnerabilities. One respondent urged a review of public policies "to define individual legal responsibilities because excellent staff alone will not save us from all risks". Another advised that citizens be taught "how to identify reliable data sources and avoid unreliable AI technology" to protect their confidentiality. Although literature and survey findings confirm the importance of items 7–10, interviewees assigned even greater priority to preceding issues. Additional comments included: "Kuwait must establish an independent body to monitor AI use in government and private agencies", "Continuous inter and intra governmental communication channels would greatly aid risk mitigation" and "The government's supervisory role over AI technology across all organisations must be strengthened."

Discussion

The results in Table 4 show that the perceived risk profile of AI enabled services in Kuwait is not similar across domains. The social domain records the highest perceived risk, whereas the technical domain records the lowest perceived risk overall. This matters for public administration because digital government success is not judged only through speed or convenience. It is also judged through concerns that are legitimacy sensitive, particularly where residents feel that digital services may compromise privacy or fairness. From that context, the survey findings are best read as governance relevant signals of where public concern is concentrating, rather than as objective measures of technical compliance or actual harm. Social risk prominence is therefore a practical warning that even when services function well, public acceptance can weaken if safeguards are not visible and accountability is not clear (Burrell, 2016; Winfield & Jirotka, 2018).

Within the social domain, job security ranks as the strongest risk signal in the perceptions of respondents. This aligns with wider debates on how automation can displace jobs and widen the gap between those with technical skills and those without (Acemoglu & Restrepo, 2019). Wider public debate also continues to amplify this anxiety, particularly as AI is increasingly used for administrative and clerical functions (OECD, 2021; UN, 2023). In governance terms, the point is not that the survey can confirm job loss trends in Kuwait, but that employment related fears can shape public trust in digital reform. When residents associate AI adoption with uncertainty about jobs and equality, public administrators need to treat workforce implications as part of responsible service transformation, rather than as an external issue outside the governance agenda.

Conversely, the technical domain is perceived as less risky on average, which may reflect Kuwait's visible investments in digital services and infrastructure, alongside heightened public awareness of cybersecurity in recent years. However, the technical results also show wider dispersion, indicating that user experience and confidence are uneven across systems and across users. This variation can arise for several plausible reasons, including differences in exposure to particular services, differing levels of digital literacy, or different baselines of expectation regarding security, reliability, and user rights. For public administration, this dispersion is important, as it suggests that a "best case" technical experience is not necessarily shared across the population, and that governance should rely on baseline standards and routine monitoring rather than on assumed consistent service quality (Bendovschi, 2015; Biggio & Roli, 2018).

The regression results reveal statistically significant associations for gender and age and, to a limited extent, education, but these patterns should be interpreted cautiously. Gender significantly predicts economic and social risk perceptions, whereby male respondents report lower perceived economic risk and higher perceived social risk than female respondents. The present data do not identify the mechanisms that produce these differences, so the findings are best interpreted as signalling potential segmentation in risk prominence that governance communication and safeguards may need to address. Similarly, age group patterns show that respondents aged 36–40 report higher organisational and social risk, while respondents aged 41+ rate social risk higher yet technical risk lower. Rather than attributing this to "sensitivity", a more grounded interpretation is that age differences may reflect a combination of exposure, familiarity with digital services, confidence in navigating systems, and varying trust expectations. These mechanisms are plausible, but they are not directly measured in the dataset, so the interpretation needs to remain bounded. Education shows a limited effect overall, except that postgraduates report higher social risk. This is consistent with the idea that formal education does not, alone, determine risk perception (Said et al., 2023). Higher education may correlate with greater awareness of ethical or societal concerns, but it does not necessarily translate into lower perceived risk. In governance terms, this supports the need for broad, accessible public communication and user guidance that does not assume high levels of specialised knowledge.

This study also engages a widely cited risk in the literature, which is the risk of bias and discrimination (Feldstein, 2019; Weyerer & Langer, 2020; Wirtz et al., 2020). In this research, user discrimination is perceived as among the least risky items. This should not be interpreted as evidence that bias is absent. A more careful reading is that perceived bias risk may be less visible to users in their daily service encounters, or that residents rely on informal coping routes when they face service barriers. Given the public administration stakes in fairness and equal treatment, the finding is best positioned as a perceptual pattern warranting attention, rather than as a conclusion that discrimination risks are resolved.

Survey results are reinforced by qualitative findings in a way that strengthens the governance interpretation. Interviewees repeatedly stressed that weak oversight of digital content and safeguards could erode trust in government and weaken perceived legitimacy. This aligns closely with the survey's social risk profile and helps clarify why perceptions matter for governance. When public confidence becomes fragile, administrative reforms face resistance even when technical delivery improves. Interviewees also highlighted resource depletion and planning failures as a risk pathway which warns that digital adoption without adequate governance can increase costs, while decreasing transparency and intensifying organisational strain. In addition, interviewees' concerns around underage exposure and digital addiction reinforce the governance relevance of content and age appropriateness, alongside public education programmes. These mixed method findings support a careful claim, whereby the survey identifies which risk areas residents perceive as most pressing, while the interviews help interpret what those concerns may mean for administrative legitimacy and resource planning if risks remain insufficiently addressed. The evidence therefore speaks most directly to where governance attention is likely to be demanded, rather than to causal explanations of why each demographic group thinks as it does.

https://doi.org/10.52372/jps.250358

Finally, it is important to acknowledge a key limitation that constrains interpretation of the regression patterns. Perceptions of organisational and technical risks are likely to vary with respondents' occupational sector, the kinds of services used most frequently and the degree of AI adoption in the relevant organisational environment. These factors were not measured in the current survey, and future research should incorporate them explicitly. Doing so would strengthen causal interpretation and improve understanding of how perceived risk is shaped by institutional context and specific patterns of technology use.

Governance and Policy Implications

The findings carry direct implications for public administration in Kuwait, indicating where administrative attention is most urgently required and which governance functions need to be strengthened. Social risks emerged as the most prominent area of concern, suggesting that digital service delivery cannot be assessed solely through efficiency metrics. Administrative practice should therefore prioritise visible safeguards that protect public trust, clarify user rights and strengthen accountability for how digital services moderate content, handle personal information and affect everyday life. In practical terms, this requires a clear focus of responsibility for oversight, an explicit mandate for public engagement and a mechanism through which complaints can be escalated and acted upon. Organisational and economic risks were assessed as moderate, yet they remain consequential for implementation because they shape whether digital initiatives perform reliably over time. These results point to the importance of strengthening coordination routines across agencies, clarifying service ownership and maintaining process discipline in procurement. Public administration should treat AI enabled services as evolving programmes rather than "one off" deployments, requiring periodic review of service agreements, performance expectations and the administrative capacity needed to manage vendors and internal workflows. In addition, technical risk perceptions showed wider dispersion, which indicates uneven readiness and unequal user experience across systems. This strengthens the case for baseline requirements that standardise security posture and user facing guidance across public services, alongside continuous monitoring and rapid response protocols when issues arise.

Operationally, these governance functions can be enacted through a small set of administrative instruments that are feasible within existing structures. These include assigning clear service ownership for each AI enabled public service, setting minimum baseline requirements for security, user facing rights notices and introducing routine risk reporting that captures incidents. Procurement and vendor management processes should also require basic auditability, so that accountability extends across both public and private delivery chains. Evaluated together, these results support a risk led approach to administrative governance in which the core task is not only to expand digital services but to sustain them responsibly. A functional governance model can remain intentionally simple, in which a central coordinating function aligns priorities and reporting, assurance functions oversee technical risks and service reliability and organisational compliance functions address social risks through engagement and safeguards that maintain daily oversight. By linking empirical risk patterns to specific administrative levers, public administrators can govern

in a way that strengthens transparency, accountability and performance as digital public services expand. These implications are drawn from perceived risk patterns and executive assessments rather than from technical audits of systems, and should be refined in future research that includes occupational sector, degree of exposure and digital literacy measures.

Conclusion

This research enriches the public administration literature by positioning AI risk governance as a practical administrative function in contemporary digital service systems. By examining how residents evaluate AI related risks across economic, organisational, social and technical domains, the research provides an evidence base for identifying which areas appear most important and therefore most likely to require governance attention as digital public services expand. The findings suggest that social concerns, particularly those linked to job security and freedom of expression, carry the greatest perceived risk, while technical issues are viewed more favourably overall but with wider variation across respondents. In practice, this means that public administration cannot treat AI adoption as a purely technical upgrade or assess digital services through efficiency measures alone. Sustaining legitimacy requires visible safeguards, clear lines of accountability and ongoing engagement that protects rights and maintains public confidence as services continue to digitalise.

At the same time, the research does not claim that perceptions alone establish objective risk levels. Rather, these evaluations function as governance relevant indicators of where trust pressures, user vulnerabilities and administrative responsibilities are likely to concentrate. This strengthens the case for a risk informed approach in which Kuwait's public administration monitors emerging concerns, adapts its oversight arrangements and aligns innovation with societal welfare. Future research could replicate this study over time to track whether perceptions shift as AI enabled services mature amidst developing governance responses. Progress will depend on coordinated stakeholder effort, regulation that is fit for purpose, sustained capability building and political commitment. With these conditions in place, Kuwait can expand digital public services in a way that supports modernisation whilst maintaining public trust and safety. Ultimately, the value of risk informed AI governance lies in its ability to keep digital public services both effective and legitimate. As Kuwait accelerates digitalisation, public administration will need to treat governance as a continuous practice of monitoring and adjustment rather than a single policy response. This research offers a grounded basis for that work by indicating where governance attention is most likely to matter to the public.

References

Acemoglu, D., & Restrepo, P. (2019). Automation and new tasks: How technology displaces and reinstates labor. *Journal of Economic Perspectives, 33*(2), 3-30. https://doi.org/10.1257/jep.33.2.3

Addam, M. (2023). *Kuwait's Finance Ministry activates protection protocol after cyberattack*. Forbes Middle East. https://www.forbesmiddleeast.com/featured/politics-security/kuwaits-finance-ministry-hit-by-cyber-attack

https://doi.org/10.52372/jps.250358

Altammar, S. (2025). An evaluation of digital government services quality and extent of beneficiary satisfaction in Kuwait. *Scientific Journal of Economics and Commerce, 55*(3), 13-42. https://doi.org/10.21608/jsec.2025.459062

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

Bendovschi, A. (2015). Cyber-attacks: Trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24-31. https://doi.org/10.1016/S2212-5671(15)01077-1

Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition, 84*, 317-331.

Bouckaert, G., & van de Walle, S. (2003). Comparing measures of citizen trust and user satisfaction as indicators of 'good governance': Difficulties in linking trust and satisfaction indicators. *International Review of Administrative Sciences*, *69*(3), 329-343. https://doi.org/10.1177/0020852303693003

Boyd, M., & Wilson, N. (2017). Rapid developments in artificial intelligence: How might the New Zealand government respond? *Policy Quarterly, 13*(4), 36-43. https://doi.org/10.26686/pq.v13i4.4619

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1), 1–12. https://doi.org/10.1177/2053951715622512

Cath, C. (2018). Governing artificial intelligence: Ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180080. https://doi.org/10.1098/rsta.2018.0080

Couture, V., Roy, M. C., Dez, E., Laperle, S., & Belisle-Pipon, J. C. (2023). Ethical implications of artificial intelligence in population health and the public's role in its governance: perspectives from a citizen and expert panel. *Journal of Medical Internet Research*, *25*, e44357. https://doi.org/10.2196/44357

Dalwai, T. A. R., Basiruddin, R., & Abdul Rasid, S. Z. (2015). A critical review of relationship between corporate governance and firm performance: GCC banking sector perspective. *Corporate Governance*, *15*(1), 18-30. https://doi.org/10.1108/CG-04-2013-0048

Dickinson, H., Smith, C., Carey, N., & Carey, G. (2021). Exploring governance tensions of disruptive technologies: The case of care robots in Australia and New Zealand. *Policy and Society*, *40*(2), 232-249. https://doi.org/10.1080/14494035.2021.1927588

Doneda, D., & Almeida, V. A. F. (2016). What is algorithm governance? *IEEE Internet Computing*, *20*(4), 60-63. https://doi.org/10.1109/MIC.2016.79

Feldstein, S. (2019). The road to digital unfreedom: How artificial intelligence is reshaping repression. *Journal of Democracy*, *30*(1), 40-52. https://doi.org/10.1353/jod.2019.0003

Floridi, L. (2018). Soft ethics, the governance of the digital and the general data protection regulation. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180081. https://doi.org/10.1098/rsta.2018.0081

Gasser, U., & Almeida, V. A. F. (2017). A layered model for AI governance. *IEEE Internet Computing, 21*(6), 58-62. https://doi.org/10.1109/MIC.2017.4180835

Grimmelikhuijsen, S. (2012). Linking transparency, knowledge and citizen trust in government:

An experiment. *International Review of Administrative Sciences*, *78*(1), 50-73. https://doi.org/10.1177/0020852311429667

Hall, P., & Ellis, D. (2023). A systematic review of socio-technical gender bias in AI algorithms. *Online Information Review*, *47*(7), 1264-1279. https://doi.org/10.1108/OIR-08-2021-0452

Hill, C. J., & Lynn Jr., L. E. (2004). Governance and public management, an introduction. *Journal of Policy Analysis and Management*, *23*(1), 3-11. https://doi.org/10.1002/pam.10175

Linkov, I., Trump, B. D., Anklam, E., Berube, D., Boisseasu, P., Cummings, C., Ferson, S., Florin, M. V., Goldstein, B., Hristozov, D., Jensen, K. A., Katalagarianakis, G., Kuzma, J., Lambert, J. H., Malloy, T., Malsch, I., Marcomini, A., Merad, M., Palma-Oliveira, ... Vermeire, T. (2018a). Comparative, collaborative, and integrative risk governance for emerging technologies. *Environment Systems and Decisions, 38*, 170-176. https://doi.org/10.1007/s10669-018-9686-5

Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M. V. (2018b). Governance strategies for a sustainable digital world. *Sustainability, 10*(2), 440. https://doi.org/10.3390/su10020440

Lune, H., & Berg, B. L. (2017). *Qualitative research methods for the social sciences*. Pearson.

MOI (2023). *Cyber crimes reporting in Kuwait*. Ministry of Interior (MOI). https://www.kijls.moj.gov.kw/ar/sections/section4/sub3_section4/Releases/KIJSReleases

Nawi, A., Yaakob, M. F. M., Ren, C. C., Khamis, N. Y., & Tamuri, A. H. (2021). A preliminary survey of Muslim experts' views on artificial intelligence. *Islamiyyat*, *43*(2), 3-16. https://doi.org/10.17576/islamiyyat-2021-4302-01

OECD. (2021). *OECD AI policy observatory: Artificial intelligence.* Organisation for Economic Co-operation and Development(OECD). https://oecd.ai/en

Pierson, J., Kerr, A., Robinson, S. C., Fanni, R., Steinkogler, V. E., Milan, S., & Zampedri, G. (2023). Governing artificial intelligence in the media and communications sector. *Internet Policy Review*, *12*(1). https://doi.org/10.14763/2023.1.1683

Rahwan, I. (2018). Society-in-the-loop: Programming the algorithmic social contract. *Ethics and Information Technology, 20*(1), 5-14. https://doi.org/10.1007/s10676-017-9430-8

Said, N., Potinteu, A. E., Brich, I., Buder, J., Schumm, H., & Huff, M. (2023). An artificial intelligence perspective: How knowledge and confidence shape risk and benefit perception. *Computers in Human Behavior*, *149*, 107855.

Salathé, M., Wiegand, T., & Wenzel, M. (2018). Focus group on artificial intelligence for health. *arXiv preprint*. arXiv:*1809.04797*. https://doi.org/10.48550/arXiv.1809.04797

SCPD. (2025). *New Kuwait 2035.* Supreme Council for Planning and Development (SCPD). https://www.newkuwait.gov.kw

Shehata, N. F. (2015). Development of corporate governance codes in the GCC: An overview. *Corporate Governance*, *15*(3), 315-338. https://doi.org/10.1108/CG-11-2013-0124

Taeihagh, A. (2021). Governance of artificial intelligence. *Policy and Society*, *40*(2), 137-157. https://doi.org/10.1080/14494035.2021.1928377

Tolbert, C. J., & Mossberger, K. (2006). The effects of E-government on trust and confidence in government. *Public Administration Review*, *66*(3), 354-369. https://doi.org/10.1111/j.1540-6210.2006.00594.x

UN. (2023). The future of digital government: Trends, insights and conclusions. In *United Nations*

https://doi.org/10.52372/jps.250358

e-government survey 2022. United Nations, Department of Economic and Social Affairs (UN DESA). https://desapublications.un.org/sites/default/files/publications/2022-11/Chapter%205.pdf

Weyerer, J. C., & Langer, P. F. (2020). Bias and discrimination in artificial intelligence. In I. Lee, & R. Luppicini (Eds.), *Advances in E-business research. Interdisciplinary approaches to digital transformation and innovation* (pp. 256-283). IGI Global.

Winfield, A. F. T., & Jirotka, M. (2018). Ethical governance is essential to building trust in robotics and artificial intelligence systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical* & *Engineering Sciences*, *376*(2133), 20180085. https://doi.org/10.1098/rsta.2018.0085

Wilson, W. (1887). The study of administration. *Political Science Quarterly, 2*(2), 197–222.

WIPO. (2025). *Kuwait ranking in the global innovation index 2024*. World Intellectual Property Organization (WIPO). https://www.wipo.int/gii-ranking/en/kuwait

Wirtz, B. W., & Müller, W. M. (2019). An integrated artificial intelligence framework for public management. *Public Management Review, 21*(7), 1076-1100. https://doi.org/10.1080/14719037.2018.1549268

Wirtz, B. W., Weyerer, J. C., & Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. *Government Information Quarterly*, *39*(4), 101685. https://doi.org/10.1016/j.giq.2022.101685

Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2020). The dark sides of artificial intelligence: An integrated AI governance framework for public administration. *International Journal of Public Administration*, *43*(9), 818-829. https://doi.org/10.1080/01900692.2020.1749851

Wright, S. A., & Schultz, A. E. (2018). The rising tide of artificial intelligence and business automation: Developing an ethical framework. *Business Horizons, 61*(6), 823-832. https://doi.org/10.1016/j.bushor.2018.07.001

Zhang, J., & Zhang, Z. (2023). Ethics and governance of trustworthy medical artificial intelligence. *BMC Medical Informatics and Decision Making*, *23*(1), 7. https://doi.org/10.1186/s12911-023-02103-9