

Governance of Artificial Intelligence Deployment in the Administrative Work of the Islamic Affairs Department in the Emirate of Sharjah

Omar Darwish Ahmed Mahmoud Alameeri, Mohd Hafiz Bin
Mohd Dasar

Academy of Islamic Civilization, Faculty of Social and Islamic Sciences, Universiti Teknologi
Malaysia, Malaysia

Email: darwishahmed@graduate.utm.my, mohdhafiz.md@utm.my

DOI Link: <http://dx.doi.org/10.6007/IJARBSS/v16-i10/29211>

Published Date: 27 October 2026

Abstract

This study examines the governance of Artificial Intelligence (AI) deployment in the administrative work of the Islamic Affairs Department in the Emirate of Sharjah, against the backdrop of accelerated technological developments across government institutions and the increasing shift toward leveraging smart technologies to enhance administrative performance and service quality. The primary research problem addresses the imperative to establish controls and operational requirements that guarantee the responsible deployment of AI while mitigating associated organizational, technical, and ethical risks. The study aims to delineate the concept, significance, and application domains of AI governance in public administration; analyze the governing regulatory and ethical principles; identify key implementation challenges and prerequisites; and propose operational mechanisms to strengthen AI governance within the Islamic Affairs Department in Sharjah. Employing a descriptive-analytical methodology, the study reviews relevant scholarly literature, analyzing key concepts, controls, and administrative frameworks. The findings reveal that effective AI governance hinges on establishing explicit institutional policies, assigning clear lines of accountability, reinforcing human oversight, protecting data privacy, and upskilling personnel. Furthermore, the study underscores the necessity of aligning smart technology deployment with Islamic values and Sharia objectives (*Maqasid al-Shariah*) within religious government entities. The paper recommends formulating a comprehensive institutional AI governance framework that classifies applications based on risk profiles and systematically evaluates their performance. Methodologically, the study contributes a proposed organizational and ethical framework designed to advance AI governance practices within the Department.

keywords: AI Governance, Administrative Work, Islamic Affairs, Algorithmic Accountability, Risk Classification.

Introduction

The contemporary public sector is undergoing profound structural transformation driven by rapid advancements in Artificial Intelligence (AI). Across diverse administrative contexts, AI systems are increasingly deployed to automate administrative workflows, optimize data processing, enhance predictive decision support, and streamline public service delivery. Consequently, governmental entities actively pursue institutional mechanisms to embed AI technologies within broader digital modernization agendas. However, the acceleration of algorithmic deployment presents systemic administrative, legal, and ethical challenges, particularly regarding algorithmic bias, opacity, data sovereignty, privacy infringement, and the attenuation of discretionary accountability (Mustafa, 2026). In response, AI governance has emerged as an indispensable institutional architecture to direct, regulate, and audit algorithmic ecosystems, ensuring that automated systems remain aligned with the public interest.

While a substantial body of scholarship examines AI governance in public administration, existing literature predominantly focuses on secular, technocratic, or commercially driven public settings (e.g., healthcare registries, judicial analytics, and municipal tax administration). Current global frameworks such as the OECD AI Principles, the European Union's risk-based regulatory classifications, and standard administrative accountability paradigms rely almost exclusively on Western-derived administrative values, secular ethical matrices, or generic procedural compliance checklists. These standard paradigms remain conceptually ill-equipped to address the normative, spiritual, and socio-religious complexities intrinsic to faith-based governmental authorities. Specifically, prevailing governance models fail to account for how institutional legitimacy in religious public bodies is intrinsically tied to divine jurisprudence, public moral stewardship, and normative community trust.

This scholarly omission is acutely evident in specialized administrative bodies such as the Islamic Affairs Department in the Emirate of Sharjah. While the Department shares general public-sector objectives such as procedural efficiency, operational optimization, and digital citizen engagement its administrative remit is fundamentally differentiated by its religious mandate. This mandate demands governance architectures that guarantee not merely algorithmic fairness and technical data protection, but also strict ontological alignment with Islamic ethical tenets and jurisprudence. Conventional governance frameworks offer little operational guidance on reconciling automated administrative outputs with traditional mechanisms of human moral accountability and religious propriety (Oglu, 2025).

To bridge this critical empirical and conceptual void, this study proposes a tailored governance framework that synthesizes public-sector administrative accountability, risk-based operational governance, and the foundational teleological objectives of Islamic jurisprudence (*Maqāṣid al-Sharī'ah*). Unlike mainstream governance models that treat risk purely through procedural compliance or statistical utility, this triadic integration reconceptualizes algorithmic risk and accountability through both institutional stewardship and substantive ethical preservation specifically safeguarding faith (*ḥifẓ al-dīn*), human dignity and intellect (*ḥifẓ al-'aql*), societal welfare (*ḥifẓ al-naḥs*), and institutional trust.

Employing a descriptive-analytical methodology, this research delineates the operational prerequisites structural, technical, and human capital necessary to deploy AI within the

Islamic Affairs Department in Sharjah. By operationalizing *Maqāṣid al-Sharī'ah* alongside rigorous risk-tiering and administrative oversight mechanisms, the paper establishes an original institutional model that advances beyond generic ethical AI declarations, offering an actionable blueprint for ethical, context-sensitive technology adoption in faith-based public institutions (Al-Sharif, 2025).

Concept and Importance of AI Governance in Public Sector Administrative Development

In recent years, public sector entities have witnessed rapid adoption of modern digital technologies, with AI standing out as a primary tool for elevating administrative efficiency and service delivery. AI offers advanced capabilities in data processing, information analytics, workflow automation, and decision support. However, expanding technology integration necessitates clear governance frameworks to ensure these systems are utilized responsibly without compromising individual rights, administrative justice, transparency, or institutional accountability. Thus, AI governance has become a foundational requirement for safe, ethical public sector technology adoption (Al-Muwaiqri, 2025).

AI Governance is defined as *the comprehensive set of organizational policies, regulatory rules, procedural controls, and oversight mechanisms that govern the design, selection, deployment, and performance monitoring of AI systems within an institution*. This framework ensures alignment with organizational objectives, statutory frameworks, and professional ethical standards. AI governance extends beyond technical operational parameters and data security; it establishes clear lines of authority, mandates human-in-the-loop oversight, and manages risk profiles associated with automated or semi-automated administrative outputs. Consequently, AI governance provides a holistic administrative architecture designed to harmonize technological innovation with core public governance principles (Hussein & Muhammad, 2024).

AI governance carries unique importance in public sector institutions due to their public trust obligations and direct impact on societal welfare. Deploying intelligent systems to evaluate service applications, classify beneficiaries, or generate administrative recommendations can directly alter service accessibility and procedural equity. Establishing a transparent governance framework mitigates algorithmic bias, technical error rates, and data misuse. Furthermore, it ensures that high-stakes administrative decisions remain subject to human review and explainability, thereby reinforcing public trust in digital government services (Qutieshat et al., 2026).

Additionally, AI governance optimizes operational efficiency by channeling smart systems toward high-value administrative domains. AI tools can dramatically reduce transaction processing times, eliminate routine administrative burdens, optimize human and financial resource management, and improve data processing precision. However, capturing these benefits requires institutional policies that explicitly distinguish between administrative tasks suitable for automation and complex functions requiring direct human judgment, supported by systematic, periodic system performance evaluations (Hijazi & Emad, 2026).

A vital dimension of AI governance is reinforcing administrative transparency and accountability. Lines of responsibility for administrative actions must remain explicit, even when utilizing smart systems to generate decision recommendations or analyze complex

datasets. Technology integration must never obscure operational liability or erode institutional oversight. Governance mandates thorough process documentation, output auditing, grievance redress mechanisms, and strict personal data privacy controls considerations that gain heightened importance in entities handling sensitive social, personal, or religious data (Dhafiri, 2024).

In the context of the United Arab Emirates (UAE), public sector AI governance supports the national vision for responsible digital transformation and modern public service delivery. This applies directly to the Islamic Affairs Department in Sharjah, where administrative workflows must reflect legal, organizational, and value-based standards. The success of AI integration in such institutions should not be evaluated solely by processing speed or cost reductions, but by adherence to administrative justice, data privacy, information accuracy, and public trust. Ultimately, AI governance serves as an operational imperative ensuring technology elevates institutional performance while preserving human accountability and public service values (Al-Jazairi & Hamid, 2025).

Areas and Applications of AI in Administrative Work

The rapid evolution of AI technologies offers diverse administrative applications across government entities. AI capabilities extend far beyond technical operations to encompass human resource management, transaction workflows, institutional planning, and public service delivery. Specific integration areas vary depending on an institution's statutory mandate, technical infrastructure, organizational readiness, and strategic objectives (Michel, 2023).

Automation of Administrative Procedures and Transactions

AI tools excel at processing administrative workflows by categorizing incoming applications, parsing unstructured documents, verifying preliminary data completeness, and routing files to designated departments. Automating these routine tasks reduces processing times, eliminates manual entry errors, and streamlines internal operations. Furthermore, AI systems can draft routine correspondence, generate initial report outlines, and track file progress across departments. In the Islamic Affairs Department in Sharjah, these applications can organize internal correspondence, manage digital archives, and process service requests—provided all automated outputs undergo mandatory human review prior to official issuance (Al-Jazairi & Hamid, 2025).

Human Resource Management and Optimization

AI offers strategic value in public sector HR management by analyzing workforce skill gaps, identifying employee training needs, evaluating performance metrics, and building tailored professional development plans. Intelligent tools can also optimize shift scheduling and task distribution based on operational workloads. While these applications maximize human capital utilization, HR governance must enforce objectivity, transparency, and non-discrimination, ensuring that automated metrics never serve as the sole basis for career-impacting personnel decisions.

Administrative Planning and Decision Support

AI enhances organizational planning by analyzing historical data, identifying operational patterns, and generating predictive forecasts that assist executive leadership in resource

allocation and strategic prioritization. Intelligent models can monitor operational plan execution, generate progress reports, and flag emerging workflow bottlenecks. In multi-departmental government bodies, these analytics provide valuable decision support; however, algorithmic projections remain advisory tools that must augment never replace human professional judgment and executive accountability (Jalili & Payandeh, 2026).

Public Service Enhancement and Citizen Communication

Virtual assistants and automated response systems streamline public communication by answering routine inquiries, guiding citizens through service requirements, and explaining application procedures. These tools lower administrative barriers, reduce staff workloads, and accelerate response times. Within religious entities like the Islamic Affairs Department in Sharjah, virtual assistants can handle general administrative inquiries regarding working hours, service locations, and submission procedures. However, a strict operational boundary must be enforced: public inquiries concerning specialized religious rulings (*Fatwas*) must be automatically routed to qualified human scholars rather than processed by AI tools (Al-Jazairi & Hamid, 2025).

Knowledge Management, Archiving, and Risk Analysis

AI supports organizational knowledge management by classifying digital files, extracting archived data, summarizing complex administrative documentation, and identifying procedural inefficiencies. Additionally, intelligent models can monitor policy compliance and detect unusual operational anomalies that warrant internal audit. The Islamic Affairs Department in Sharjah can leverage these tools based on a thorough needs assessment to ensure clear administrative utility, robust data security, accurate processing, and continuous human oversight.

Regulatory and Ethical Principles Governing AI Deployment

Establishing clear regulatory and ethical principles forms the cornerstone of AI governance in public administration. Capturing technology benefits requires a structured regulatory framework that aligns system usage with statutory laws, institutional policies, civil rights, and public interest. As AI systems increasingly process sensitive data, generate administrative reports, and support executive choices, public entities must establish explicit rules governing the interaction between intelligent systems and human administrators (Hussein, 2026).

Transparency and Algorithmic Explainability

The principle of transparency mandates clear disclosure regarding where and how AI systems are integrated into administrative workflows, alongside explainable logic behind automated recommendations affecting individual rights. Algorithms must not function as unreviewable "black boxes" that obscure decision rationale or prevent citizens from understanding procedures that affect their interests. Furthermore, systems must be transparent regarding their operational limits, ensuring automated recommendations are never presented as infallible truths—particularly given that generative systems can produce inaccurate or uninterpretable outputs without expert human verification (Qutieshat et al., 2026).

Administrative Accountability and Liability Assignment

Transparency is intrinsically linked to administrative accountability. Institutions must establish explicit authority tiers governing AI system approval, continuous performance

monitoring, and output verification. While smart systems can generate analytical reports or process routine files, operational liability remains fully with human administrators. Utilizing AI tools can never be cited to absolve officials of their statutory duties. Effective governance demands comprehensive operation logging, formal appeal mechanisms, error remediation protocols, and clear administrative recourse for affected parties (Dhafiri, 2024).

Justice, Equity, and Non-Discrimination

Justice and non-discrimination represent vital ethical controls in public sector technology integration. AI models trained on historical or unrepresentative datasets can perpetuate systemic biases, generating inequitable outcomes in application routing, performance evaluations, or service prioritization. Responsible AI deployment requires periodic bias audits, dataset validation, and output checks to ensure equity. Administrative decisions impacting individual rights must rely on objective, verifiable standards, aligning with the fundamental principles of administrative justice (Al-Sharif, 2025).

Data Privacy, Security, and Confidentiality

Public sector bodies manage sensitive personal, professional, and institutional data. Governance policies must restrict data processing to authorized, legitimate purposes, enforce the principle of data minimization, restrict access permissions, and deploy cybersecurity measures against data breaches. Furthermore, entering confidential or classified administrative records into unvetted public cloud AI platforms must be strictly prohibited under UAE data protection and cybersecurity laws (Al-Jazairi & Hamid, 2025).

Mandatory Human Oversight and Value Alignment

AI governance requires that core administrative decisions remain subject to human discretion, particularly when impacting civil rights, personnel liabilities, or religious matters. In religious public entities, technology deployment must explicitly align with Islamic values and Sharia objectives (*Maqasid al-Shariah*) upholding justice, fiduciary trust (*Amanah*), rights preservation, harm prevention, and public benefit (*Maslahah*). Operationalizing these principles requires establishing a clear institutional AI policy that classifies tools by risk levels, defines permission tiers, trains personnel, and continuously monitors compliance.

Challenges and Risks Associated with AI Deployment in Administrative Work

While AI offers substantial operational benefits, its administrative integration entails organizational, technical, human, and ethical risks that require proactive management. Government institutions handling sensitive datasets or delivering services tied directly to public rights must establish pre-deployment risk evaluations and continuous oversight systems. This imperative is doubly vital for religious public entities, which must balance technological efficiency with preserving their foundational institutional values (Al-Muwaiqri, 2025).

Information Security and Data Leakage Risks

AI models require processing extensive datasets containing personal records, personnel files, or confidential administrative documents. This data dependence elevates vulnerabilities regarding unauthorized access, data leaks, or function creep. Utilizing unvetted external AI applications exposes sensitive institutional data to third-party environments outside direct

organizational control. Mitigating these risks requires strict data protection frameworks, defined user access tiers, and security audits of all deployed software.

Output Inaccuracy and Hallucination Risks

A critical operational challenge is the risk of AI output inaccuracy, where models generate false information, flawed logic, or unverified conclusions. In administrative contexts, uncritical reliance on inaccurate automated summaries, data analytics, or decision recommendations can lead to administrative errors, erroneous policy choices, or public misinformation. In the Islamic Affairs Department in Sharjah, ensuring complete data precision across religious and administrative matters is paramount.

Organizational and Policy Deficits

Public entities frequently face organizational challenges stemming from absent or outdated internal AI governance policies. Deploying smart tools without a formal governance structure creates overlapping departmental authorities, ambiguity regarding error liability, and procedural misalignment with existing administrative frameworks. Establishing clear institutional policies defining authorized use cases, approval tiers, and monitoring protocols is essential for structured, law-compliant technology adoption (Dhafiri, 2024).

Human Resource and Cultural Challenges

Human capital challenges significantly influence AI adoption success. Staff may struggle with new technologies due to digital skill deficits or insufficient technical training, while anxiety over potential job displacement can drive cultural resistance. Conversely, an over-reliance on automated tools risks cognitive deskilling, eroding human critical thinking, administrative discretion, and problem-solving capacities. Upskilling staff and building awareness regarding AI limitations are vital to ensuring technology augments human expertise without diminishing human leadership (Michel, 2023).

Ethical Risks and Algorithmic Bias

Ethical risks encompass unaddressed algorithmic bias, lack of explainability, and opaque decision outputs particularly when AI tools evaluate employees, categorize beneficiaries, or prioritize service requests. Unmonitored systems threaten administrative fairness and civil equity. In religious public entities, additional risks involve potential misalignment between automated outputs and Islamic principles, underscoring the absolute necessity of preventing automated systems from independently generating religious content or processing matters requiring expert human reasoning (*Ijtihad*).

Managing these risks requires the Islamic Affairs Department in Sharjah to conduct pre-deployment risk assessments, mandate continuous human-in-the-loop oversight, deliver ongoing workforce upskilling, and enforce periodic governance audits to safeguard institutional integrity (Oglu, 2025).

Administrative, Technical, and Human Resource Requirements for Implementing AI Governance

Implementing AI governance within government entities requires an integrated ecosystem of administrative, technical, and human resource prerequisites. These elements ensure the structured and responsible deployment of smart technologies, enabling public entities to achieve strategic objectives while upholding regulatory and ethical standards. Successful AI

integration relies heavily on institutional readiness and organizational adaptability to absorb technological workflows. Therefore, establishing an effective AI governance framework requires synchronization across structural, technical, and personnel dimensions to enhance operational efficiency while protecting administrative decision integrity and civil rights (Hussein & Muhammad, 2024).

Administrative Requirements

Administrative readiness mandates a clear strategic vision defining authorized AI use cases, operational priorities, and deployment scopes aligned with the entity's overarching strategic plan and operational needs. Institutions must draft internal policies, standard operating procedures, and authority matrices governing smart tools, detailing oversight and audit mechanisms. Establishing a dedicated administrative unit to oversee governance implementation and coordinate across departments ensures technological adoption aligns with existing administrative laws. The Islamic Affairs Department in Sharjah can leverage this approach by establishing a regulatory framework tailored to its administrative and religious mandate.

Leadership endorsement is paramount. Executive leadership plays a pivotal role in securing resource allocations, fostering organizational buy-in, and championing responsible digital transformation. Executive leadership must formally approve AI governance policies, oversee implementation, and ensure compliance with statutory laws and ethical guidelines. This includes enacting **Risk Management Matrices** that classify applications based on their impact severity on administrative choices and civil rights, supported by formal audit workflows to address algorithmic errors or unintended outcomes (Mustafa, 2026).

Technical Requirements

Technical readiness requires a secure digital infrastructure capable of supporting high-performance AI deployment. This includes maintaining structured databases, interoperable information systems, and robust cybersecurity protocols to prevent unauthorized access or data leaks. Furthermore, data quality management ensuring precision, completeness, and continuous dataset updates is essential, as poor training data produces flawed outputs that compromise administrative efficiency. Thus, **Data Governance** forms an indispensable pillar of AI governance.

Technical prerequisites further mandate pilot testing AI applications prior to formal operational launch to verify output accuracy and contextual appropriateness. Institutions must implement operational logging tools, performance monitoring dashboards, error-detection protocols, access control tiers, and periodic system audits. Additionally, smart tools must integrate seamlessly with existing enterprise software to avoid operational fragmentation or redundant workflows. Finally, third-party technology vendor risks must undergo rigorous pre-contractual due diligence (Hussein, 2026).

Human Resource Requirements

Human capital readiness represents the ultimate determinant of AI governance success. Personnel and administrative leadership must possess the technical literacy required to navigate smart tools responsibly. Institutions should deliver specialized training programs covering AI fundamentals, application parameters, output limits, and risk identification,

alongside building data analytics, critical thinking, and verification skills. Furthermore, organizations must foster an ethical culture that emphasizes that AI tools exist to augment human capacity and elevate output quality rather than eliminate human agency in administrative decision-making.

The researcher holds that implementing AI governance in the Islamic Affairs Department in Sharjah requires adding a distinct institutional dimension: involving Sharia, administrative, and technical experts in evaluating proposed software. This ensures alignment with Islamic values, Sharia objectives (*Maqasid al-Shariah*), and public administration standards. Success metrics must track output precision, data protection levels, human oversight efficacy, user satisfaction, and policy compliance. Harmonizing administrative, technical, and human resource requirements creates a sustainable foundation for responsible, value-aligned AI adoption (Al-Jazairi & Hamid, 2025).

Proposed Mechanisms to Enhance AI Governance in the Islamic Affairs Department in Sharjah

Strengthening AI governance within the Islamic Affairs Department in Sharjah requires adopting an integrated framework of organizational, technical, and supervisory mechanisms tailored to its statutory mandate. Capturing AI benefits requires a structured ecosystem that defines application boundaries, assigns accountability, and balances operational efficiency with Islamic values, ethical standards, and user rights. The researcher proposes the following seven mechanisms to enhance AI governance within the Department (Jalili & Payandeh, 2026):

Establishing an Institutional AI Policy and Governance Committee

The Department should enact a comprehensive AI Governance Policy detailing institutional goals, ethical principles, authorized use cases, pre-deployment review requirements, and departmental authority tiers. The researcher proposes forming a specialized **AI Governance Committee** comprising representatives from operational departments, IT, cybersecurity, legal affairs, and Sharia oversight. The committee would evaluate proposed software, conduct risk assessments, and verify alignment with Department mandates, submitting recommendations through official approval hierarchies (Hijazi & Emad, 2026).

Adopting a Risk-Based Application Classification Tiering System

Applications should be categorized based on their risk profile:

- **Low-Risk Tiers:** Automated schedule coordination, document archiving, and routine report drafting.
- **High-Risk Tiers:** Applications processing personal data, evaluating employee performance, or recommending decisions affecting beneficiary rights.

This classification dictates the level of supervisory audit required prior to deployment. High-risk systems must undergo pre-deployment evaluations verifying data integrity, output accuracy, algorithmic fairness, explainability, and human review protocols.

Strengthening Data Governance and Cybersecurity Protocols

The Department must establish clear data collection, storage, processing, and inter-departmental sharing protocols, enforcing strict user access permissions. Policy must prohibit entering confidential documents or sensitive personal data into unvetted commercial AI

platforms. Furthermore, technical vendors must demonstrate compliance with UAE cybersecurity and privacy standards, while internal teams conduct periodic audits to maintain training data accuracy and currency (Michel, 2023).

Operationalizing Human-in-the-Loop Oversight and Administrative Accountability

Governance policies must reinforce that smart systems operate strictly as decision-support tools without eliminating human administrative responsibility. High-stakes administrative, legal, or religious choices must remain subject to mandatory human review (*human-in-the-loop*). The Department should designate accountable officials responsible for auditing automated outputs prior to formal issuance, maintain operation logs, and provide formal grievance redress mechanisms for affected parties.

Building Human Capacity and Institutional Awareness

Continuous training programs tailored to leadership and administrative staff should be delivered, focusing on practical AI software operation, output verification, data security, and ethical risk identification. The researcher proposes drafting a simplified **AI Usage Guidelines Manual** detailing permissible practice, prohibited actions, and escalation protocols for system errors. This elevates institutional awareness, curbs uncritical reliance on automated outputs, and empowers staff to manage smart systems responsibly (Hussein & Muhammad, 2024).

Integrating Maqasidic Objectives and Ethical Standards

AI deployment must explicitly reflect Islamic values and Sharia objectives (*Maqasid al-Shariah*) upholding public interest (*Maslahah*), rights preservation, justice, fiduciary trust (*Amanah*), harm prevention (*Dar' al-Mafasid*), and personal privacy. In the Islamic Affairs Department in Sharjah, applications processing religious media or community services must undergo expert scholarly review prior to deployment. Automated tools must be strictly prohibited from independently generating religious rulings or official Islamic opinions (*Fatawa*).

Enacting a Continuous Assessment and Pilot Implementation Model

The Department should implement a continuous improvement framework anchored in quantitative KPIs, tracking output precision, processing velocity, data security scores, error rates, policy compliance, and user satisfaction metrics. The researcher advises adopting a **phased implementation strategy**—initiating pilot testing within low-risk administrative workflows before expanding into complex operational areas. Evaluating pilot outcomes ensures gradual, secure, and sustainable AI integration aligned with institutional values (Oglu, 2025).

Conclusion

This research demonstrated that governing Artificial Intelligence (AI) deployment in administrative work is an operational imperative for advancing public sector performance and elevating government service quality. Capturing AI capabilities requires moving beyond technical acquisition toward establishing clear institutional policies and ethical controls that guarantee safe, responsible technology adoption.

The study examined AI governance concepts, administrative applications, risk profiles, and structural requirements across organizational, technical, and human resource dimensions.

The findings underscore the necessity of reinforcing human oversight, protecting data privacy, and assigning clear administrative accountability to safeguard decision integrity.

For the Islamic Affairs Department in the Emirate of Sharjah, AI integration offers substantial operational benefits when managed through an integrated governance framework tailored to its distinct religious and societal mandate. Harmonizing technical efficiency with Islamic values and Sharia objectives supported by workforce upskilling and continuous system evaluations enhances institutional transparency, reinforces public trust, and ensures sustainable organizational development.

References

- Al-Jazairi, A. A., & Hamid, A. (2025). An Islamic perspective on the legal capacity of artificial intelligence and its role in political governance. *Governance in the Qur'an and Sunnah*, 3(3), 89–112.
- Al-Muwaiqri, N. D. F. (2025). Artificial intelligence: Its rulings and controls in Islamic Sharia. *Journal of the Faculty of Dar Al-Uloom*, 42(153), 1095–1132.
- Al-Sharif, A. A. (2025). Artificial intelligence and intelligent understanding of Islamic jurisprudence rulings. *Journal of AI Applications in Humanities and Social Sciences*, 1(1), 22–62.
- Dhafiri, M. E. (2024). The role of artificial intelligence in developing Islamic studies: Possibilities and challenges. *Ibn Khaldun Journal for Studies and Research*, 4(8).
- Hijazi, H. M. M., & Emad. (2026). Artificial intelligence and its applications in light of Islamic Sharia rulings. *Scientific Journal of the Faculty of Islamic and Arabic Studies for Boys*, 14(22), 1–104.
- Hussein, A. M. A. (2026). Ethics of artificial intelligence in light of Islamic Sharia. *Al-Asalah Journal*, 6(13), 65–81.
- Hussein, A. S., & Muhammad. (2024). Provisions of artificial intelligence and its applications in Islamic jurisprudence between grounding and analysis. *Journal of Law for Legal and Economic Research*, 1(4), 316–461.
- Jalili, S. M., & Payandeh, R. (2026). Beyond procedural AI ethics: Islamic moral reasoning for algorithmic governance. *Classical and Contemporary Islamic Studies*, Article e108859.
- Michel, G. (2023). The role of artificial intelligence in corporate governance. *International Journal of Jurisprudence, Judiciary, and Legislation*, 4(2), 397–423.
- Mustafa, A. A. A. (2026). Administrative identity in the age of artificial intelligence: An analytical study of modern management variables. *Journal of the Faculty of Arts at Port Said University*, 36(36), 991–1025.
- Oglu, A. H. (2025). Artificial intelligence companies: Sharia and applied impact. *Mesopotamia Journal for Quranic Studies*, 109–123.
- Qutieshat, E., Al Adwan, M., & Khater, M. (2026). Artificial intelligence in Islamic law: Ethics, governance, and accountability. *Journal of Sustainable Development and Regulatory Issues (JSDERI)*, 4(2), 467–714.