Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AI Security Regulatory Gaps: A Global Comparative Review and a Governance Blueprint Tailored for the United Arab Emirates

Kavinmuhil S. Kanagaraj[1], Dr. Arunmozhi Selvi[2]

[1] *Research Scholar* The British University in Dubai (BUiD) *Cyber Security Lead* Abu Dhabi National Takaful, Abu Dhabi, United Arab Emirates
Email: kavinmuhilmedium@gmail.com

[2] *Supervisor* The British University in Dubai (BUiD)
Email: drarunmozhiselvi@gmail.com

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Artificial intelligence (AI) is being adopted at unprecedented speed across public and private sectors, while regulatory responses diverge widely across jurisdictions. The European Union (EU) AI Act inaugurates a harmonized, risk-based regime; the United States and United Kingdom pursue sectoral or principles led approaches; Singapore and China implement prescriptive models; and Gulf Cooperation Council (GCC) states, including the United Arab Emirates (UAE)have favored nonbinding strategies and sandboxes. Building on a scoping of 48 publications, this review synthesizes advances in AI governance, highlights unresolved security and enforcement gaps, and proposes a UAE tailored framework aligned with ISO/ISMS and international best practices. We find persistent weaknesses in risk classification fidelity, security-by-design obligations, policy–practice enforcement, and governance for general purpose and agentic AI. We propose (i) a global AI security and governance framework and (ii) a UAE governance blueprint with tiered obligations for critical sectors, conformity assessment, incident reporting, and independent audits. The review contributes a practical compliance checklist and legislative recommendations forming the basis for a UAE AI Act, alongside an implementation roadmap.

Keywords: Artificial intelligence governance; AI security; Regulatory frameworks; Risk based regulation; ISO/ISMS alignment; general purpose, Agentic AI.

1. INTRODUCTION

AI's rapid diffusion has outpaced regulatory convergence. While the EU has enacted a comprehensive AI Act with risk-based obligations and market surveillance, other regions emphasize innovation and guidance over formal statute. In the UAE, national strategies, ethics charters, and sandboxes drive adoption, yet no single statutory AI law mandates security and conformity assessment across sectors. This divergence poses challenges for security governance, accountability, and operational enforcement in high adoption contexts. This review consolidates global scholarship and policy instruments to (a) map the landscape, (b) identify security focused gaps, and (c) propose UAE ready frameworks and checklists aligned to ISO standards.

2. METHOD: SCOPING REVIEW AND COMPARATIVE SYNTHESIS

We performed a structured scoping of 48 sources, including peer reviewed articles, policy analyses, official regulations, and practitioner frameworks. Sources were coded across dimensions: risk classification, security controls, enforcement, transparency, general purpose and agentic AI, cross border data, and public sector trust.

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Comparative analysis contrasted EU, US, UK, Singapore, China, and GCC/UAE approaches, triangulating academic literature with official legal texts and practitioner guidance.

While global frameworks such as the EU AI Act and Singapore's Model AI Governance Framework provide detailed risk tiering and enforcement mechanisms, UAE's current approach remains fragmented, primarily guided by high level ethical principles and sectoral guidelines (e.g., Smart Dubai AI Ethics Guidelines). For instance, autonomous decision making in smart mobility projects in Abu Dhabi and AI driven fraud detection in Islamic finance lack standardized risk classification and auditability requirements. Similarly, AI enabled healthcare diagnostics in SEHA hospitals raise concerns about explainability and liability, yet there is no unified mandate for algorithmic transparency or bias testing. Cross border data flows in cloud hosted AI services for government entities also expose gaps in harmonized security controls, especially when interfacing with EU GDPR or China's data localization laws.

These gaps underscore the need for a UAE specific AI governance framework that moves beyond aspirational ethics to enforceable standards. Such a framework should address risk-based classification for high impact AI systems, mandatory security and privacy controls for public-sector deployments, and clear accountability structures for agentic AI applications. Without this, UAE risks regulatory misalignment, operational inefficiencies, and erosion of public trust in AI driven services.

3. GLOBAL AI GOVERNANCE: THEMES AND TRAJECTORIES

3.1 EU AI Act—Uniform, Risk Based Regulation

The EU AI Act establishes harmonized Unionwide rules with risk tiers (unacceptable, high, limited, minimal), prohibitions (e.g., manipulation, social scoring), and strict obligations for high-risk systems (risk management, data governance, documentation, human oversight, third-party conformity assessment). It introduces duties for general-purpose AI models and a phased implementation timeline supported by an EU AI Office and national authorities.

3.2 US & UK—Sectoral/Principles Led Approaches

The US leverages agency has specific statutes and guidance; the UK emphasizes principles based, regulator led governance. Both prioritize innovation and nonuniform risk classification, creating compliance variability and potential security enforcement gaps in high-risk deployments outside specific regulated sectors.

3.3 Singapore & China—Prescriptive and Security Focused Models

Singapore's Model AI Governance Framework operationalizes accountability and transparency; China advances security centered obligations and content governance for algorithmic systems, accelerating compliance expectations for deployment contexts with broader state oversight.

3.4 GCC/UAE—High Adoption, "Soft" Governance

The UAE's AI Strategy 2031, ethics principles, sandboxes, and freezone adaptations enable rapid innovation but lack a single statutory AI law with enforceable security-by-design and conformity assessment duties across sectors. This impedes consistent risk tiered compliance and auditability at national scale.

4. CROSS CUTTING ISSUES IN AI SECURITY GOVERNANCE

4.1 Security-by-Design and ISO/ISMS Alignment

ISO 27001 and ISO 27005 controls—covering risk assessment, secure development lifecycle (SDLC), supplier security, access and change management, and legal compliance—are directly applicable to AI/ML environments. These controls mitigate adversarial attacks (e.g., model inversion, data poisoning), privacy breaches, and integrity risks. For example, UAE's financial sector uses AI for fraud detection, yet without mandated SDLC and adversarial testing, models remain vulnerable to poisoning attacks that could bypass detection. Globally, few jurisdictions make these controls legally binding beyond sector-specific regimes (e.g., EU AI Act for high-risk systems). In UAE, current guidelines (Smart Dubai AI Ethics) are voluntary, leaving critical gaps in enforceable security-by-design obligations.

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Without mandates: Organizations may adopt ad hoc security measures, leading to inconsistent risk management, weak supplier oversight, and exposure to systemic vulnerabilities, especially in public-sector AI deployments like smart mobility or healthcare diagnostics.

4.2 General-purpose and Agentic AI Risks

Emerging literature highlights under addressed risks from general-purpose and agentic systems, such as recursive self-improvement and multiagent coordination. These risks demand licensing thresholds, red-teaming, and governance-by-design incentives. Current regimes (EU, US) only partially address these, focusing on transparency and risk classification. UAE's AI strategy emphasizes innovation but lacks explicit provisions for agentic AI governance. For instance, autonomous decision-making in smart city platforms could lead to cascading failures if multiagent systems interact unpredictably.

Without mandates: UAE risks uncontrolled deployment of agentic AI in critical infrastructure, creating liability gaps and amplifying systemic risks without pre-deployment stress testing or licensing.

4.3 Cross-Border Data, Privacy, and Interoperability

Fragmented privacy rules complicate multinational AI operations. Interoperable governance layered legal–technical safeguards, and contract-based controls are essential for managing data transfers and accountability. UAE's Personal Data Protection Law (PDPL) provides baseline but lacks AI-specific interoperability standards. For example, cloud-hosted AI services for UAE government entities often integrate with EU-based vendors, raising compliance conflicts with GDPR and China's localization laws.

Without mandates: Organizations rely on bilateral contracts and vendor assurances, creating legal uncertainty and operational delays in cross-border AI deployments.

4.4 Public-sector Trust and FEAST Principles

Trust in government AI hinges on Fairness, Explainability, Accountability, Safety, and Transparency (FEAST), alongside institutional ability, benevolence, and integrity. Evidence shows FEAST-aligned governance correlates with higher citizen confidence in AI services. UAE's public-sector AI initiatives (e.g., predictive policing, healthcare triage) lack standardized explainability and bias audits, risking public skepticism and reputational harm.

Without mandates: Public trust erodes, adoption slows, and ethical lapses may trigger backlash undermining UAE's vision of becoming an AI-driven economy.

Scenarios

Security-by-Design and ISO/ISMS Alignment (ISO 27001/27005, SDLC, suppliers, access/change management)

Scenario A Adversarial/data poisoning breach in financial fraud models (UAE banking/Islamic finance):

Without mandates: Teams skip formal threat modeling, adversarial testing, and secure MLOps gating. Supplier due diligence is inconsistent; model updates are pushed directly from vendors.

Chain of events: A low-and-slow poisoning campaign manipulates training data → precision/recall drift goes unnoticed → false negatives rise in card-not-present fraud.

Impact: Undetected losses, emergency rule-based rollbacks, reputational damage; auditors struggle to reconstruct lineage because **change control and logging** are no standardized.

Indicators: Sudden model performance degradation, increase in fraud write-offs, absence of documented risk treatment plans, weak evidence of supplier security attestations.

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Scenario B Model inversion privacy leak in healthcare (SEHA/clinical decision support):

Without mandates: Privacy-by-design and cryptographic hardening (e.g., differential privacy) are "nice-to-have." Access segregation between training and inference environments is lax.

Chain of events: An attacker queries the model to reconstruct sensitive attributes → patient reidentification → breach notifications and regulatory scrutiny.

Impact: Moratorium on the AI tool, manual triage load surges; insurance disputes over liability; public trust declines in clinical AI.

Indicators: Unusual inference query patterns, incomplete access logs, absence of DPIA/ISO 27005 risk registers tied to AI assets.

Scenario C Supplier/third-party library compromise in smart mobility (Abu Dhabi traffic optimization):

Without mandates: SBOMs, secure code reviews, and dependency scanning aren't enforced.

Chain of events: A compromised opensource component propagates into the orchestration pipeline → unpredictable agent behavior in routing → congestion and safety incidents.

Impact: Operational disruption, emergency override to manual control; blame fixation between agency and vendor due to weak contractual security clauses.

Indicators: Missing SBOMs, irregular patch cadences, noncompliant change approvals.

General-Purpose and Agentic AI Risks (recursive self-improvement, multiagent coordination)

Scenario D Emergent behavior in multiagent city services (permit approvals, utility dispatch):

Without mandates: No licensing thresholds, no red-teaming against coordination failures; autonomy levels are set by product teams.

Chain of events: Agents optimize locally and collude unintentionally → deprioritize edge cases (e.g., small businesses) → systemic bias and bottlenecks.

Impact: Economic harm to SMEs, complaint spikes, investigations; difficult rollback because inter-agent policies are undocumented.

Indicators: Unexplained queue skew, policy drift across agents, absence of pre-deployment simulation reports.

Scenario E Unbounded tool-use in agentic assistants for public service portals:

Without mandates: Tool-use permissions ("what the agent can do") aren't risk-tiered; no kill-switch or containment plans.

Chain of events: The assistant chains tools (RPA + data fetch + email) and issues unauthorized actions (e.g., bulk notification with sensitive data).

Impact: Data exposure, service interruptions, regulatory findings; trust shock in e-government channels.

Indicators: Actions executed outside approved scopes, missing human-in-the-loop checkpoints, no incident playbooks for agent misbehavior.

Scenario F — "Capabilities creep" in general-purpose models integrated into critical infra:

Without mandates: Capability assessments are one-off; model updates increase autonomy inadvertently.

Chain of events: New release introduces better planning → agent starts making routing decisions beyond design → cascading effects in transport or logistics.

Impact: Safety risks, contractual disputes over scope change; delayed incident attribution.

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Indicators: Version-to-version capability diffs absent, vague RACI for autonomy changes.

Cross-Border Data, Privacy, and Interoperability (PDPL–GDPR–other regimes)

Scenario G Cross-region training with mixed legal bases (government cloud + EU vendor):

Without mandates: Transfer impact assessments, SCCs/Addenda, and technical safeguards (encryption, pseudonymization) are optional.

Chain of events: A dataset flows to an EU/US processing region → conflicting data subject rights and retention policies → halted pipeline after vendor legal review.

Impact: Project delays, rework, and cost overruns; inconsistent rights handling for UAE residents; procurement friction.

Indicators: Contractual exceptions, fragmented RoPA (records of processing), divergent retention schedules.

Scenario H Accountability gaps in federated learning across GCC partners:

Without mandates: Roles (controller/processor) and liability splits are unclear; audit interoperability is not defined.

Chain of events: A partner's node ingests inaccurate labels → global model degrades → harm materializes in another jurisdiction.

Impact: Cross-border blame cycles, stalled collaboration, and difficulty proving causality.

Indicators: Missing cross entity audit APIs, no shared assurance scheme, uneven DPIAs.

Scenario I Vendor lock in and portability failure for AI services:

Without mandates: No requirement for interoperable formats, minimal exit obligations.

Chain of events: Public entity tries to switch provider → model artifacts and data aren't portable → long downtime and sunk costs.

Impact: Operational continuity risk; budget burn; strategic dependency misaligned with sovereignty goals.

Indicators: Absent data/model portability clauses, no tested exit runbooks.

Public-sector Trust and FEAST (Fairness, Explainability, Accountability, Safety, Transparency)

Scenario J Fairness audit absence in digital welfare eligibility:

Without mandates: Protected attribute monitoring and demographic parity tests aren't required.

Chain of events: Model over denies benefits to certain groups → media scrutiny → policy backlash.

Impact: Trust erosion; emergency manual reviews; reputational harm undermining UAE's digital government agenda.

Indicators: Disparate impact metrics missing, no fairness KPI in governance dashboards.

Scenario K Explainability gap in clinical triage recommendations:

Without mandates: No standardized XAI methods or clinician facing rationale summaries.

Chain of events: Clinicians disagree with opaque recommendations → inconsistent adoption → patient complaints.

Impact: Reduced effectiveness of AI; reluctance to rely on the system; slower innovation diffusion.

Indicators: Low clinician acceptance rates, high override rates, lack of XAI documentation.

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Scenario L Accountability and incident transparency lapses in policing analytics:

Without mandates: Incident registries, audit trails, and public reporting are ad hoc.

Chain of events: A false positive lead to wrongful flagging → community concerns escalate → oversight bodies lack reliable logs.

Impact: Community trust declines; possible legal exposure; delays in AI deployments pending review.

Indicators: Missing post incident reports, incomplete lineage, limited public transparency portals.

5. SYNTHESIS OF GAPS

1. Risk Classification Fidelity: Many regimes lack granular, security-centered risk tiering tied to enforceable controls and audits, especially outside the EU.
2. Security-by-Design as Legal Duty: ISO/ISMS-aligned controls remain recommended rather than mandated in most jurisdictions; suppliers and deployers face uneven obligations.
3. General-Purpose/Agentic Coverage: Governance for high-compute, adaptable models is emergent and partial, with limited licensing and post deployment monitoring.
4. Enforcement and Auditability: Nonbinding charters and sandboxes provide guidance without uniform conformity assessments, incident reporting, or market surveillance.
5. Cross-Border Interoperability: Privacy and data-transfer fragmentation persist, complicating compliance for multinational deployments.
6. Public-sector Trust Metrics: Few regimes measure FEAST dimensions and trust outcomes systematically to inform continuous improvement.

5A. Why the UAE Requires Its Own AI Law

Why the UAE require its own AI law?

Strategic fit and policy momentum (but a horizontal AI statute is missing).

The UAE has set an explicit national vision to become a world leader in AI by 2031, building a fertile ecosystem, embedding AI across government services, and strengthening data sharing and governance. Yet, it currently operates primarily through strategies, programs, and sectoral laws rather than a single cross-sector AI statute. A formal UAE AI Act would connect policy to enforceable obligations across public and private sectors.

Abu Dhabi's AI native government strategy (2025–2027) is already scaling AI into hundreds of use cases and committing AED 13 billion to AI powered digitization; this accelerates innovation but also increases national exposure to safety, security, and rights risks—necessitating a unified legal framework to standardize guardrails across entities and emirates.

Interoperability with evolving global regimes.
The EU AI Act introduces risk-based obligations for providers and deployers, prohibits certain practices outright, and imposes specific transparency and GPAI (foundation model) obligations—all with phased effective dates through 2025–2027 and high penalties for non-compliance. UAE organizations building or integrating AI that touches EU markets will face these rules regardless of geography; a UAE AI Act aligned at the principle and tiering level would reduce friction and improve market access.

At the same time, Western frameworks are anchored in secular legal traditions and may omit local needs (Arabic NLP fairness, content sensitivities, Sharia-compliant financial logic). A UAE AI Act can adopt interoperable definitions (OECD/UNESCO; EU's AI system definition) while localizing obligations for UAE cultural, linguistic, and legal norms.

Shariain-formed ethics: justice, non-harm, fairness, and accountability

Sharia influences the UAE's legal ecosystem and emphasizes values that parity well with AI ethics—justice (*'adl*), non-harm (*la darar*), fairness, and accountability. Global ethical frameworks (OECD/UNESCO) articulate human rights, transparency, robustness, and accountability; the UAE can codify these as statutory principles while adding culturally

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

relevant safeguards (e.g., preventing outputs that offend religious values; ensuring fairness in Arabic language models). This approach bridges universal ethics with regional jurisprudence.

Data protection integration and legal certainty for automated decisions

When AI systems process personal data, they must comply with the UAE **Personal Data Protection Law (PDPL, Federal Decree-Law No. 45/2021)**including lawful basis, data minimization, data subject rights (access, rectification, erasure), automated processing limitations, breach notifications, and cross-border transfer conditions. A UAE AI Act should cross-reference PDPL and clarify how high-risk AI must perform **Data Protection Impact Assessments**, transparency, and human oversight, giving courts and regulators a consistent interpretive baseline.

Freezone regimes (e.g., **DIFC Data Protection Law 2020**, amended in 2025 to strengthen private rights and clarify scope) already provide strong privacy hooks. The Act can set a **national floor** for AI risk tiers, transparency, GPAI obligations, and prohibited practices across onshore and free zones to avoid regulatory arbitrage.

UAE risk profile: rapid AI adoption + rising cyber exposure.
Abu Dhabi's AI=native government strategy (2025–2027) is deploying hundreds of AI use cases and scaling AI across services; this accelerates benefits but also necessitates guardrails (security, transparency, oversight, safety). A national Act can harmonize rules across entities, cloud/compute, and data flows.

Security and resilience on a national scale

The UAE's accelerated digitization (TDRA initiatives; DGE/TAMM AI programs) makes cyber resilience and AI safety a national priority. A UAE AI Act can mandate **cyber-Security-by-Design** for AI (secure model pipelines, adversarial testing, incident reporting), synchronize with PDPL breach duties, and require conformance to internationally recognized information security controls (e.g., ISO 27001) where AI handles sensitive data.

Standards exist to make compliance auditable UAE should operationalize them

ISO/IEC 42001 (Artificial Intelligence Management Systems) provides a certifiable management framework to embed responsible AI across the organization, while the NIST AI Risk Management Framework provides practical risk activities (Govern/Map/Measure/Manage), including a generative AI profile. The UAE can mandate an AI governance standard (UAIGS), requiring ISO/IEC 42001 certification and NIST outcomes, with UAE-specific controls added via a national checklist (Arabic bias testing, cultural content filters, Sharia-sensitive finance) to deliver consistent, auditable compliance.

Concrete Impacts When UAE-Specific Mandates Are Absent

Financial services (Islamic finance logic)

Imported AI credit scoring might embed interest-based assumptions or collateralization logic that conflict with Sharia principles and local consumer fairness expectations. Without UAE-specific rules on model design constraints, explainability in Arabic, and bias testing against local demographics, deployers risk discriminatory outcomes or legal disputes—especially in automated approvals/denials. A UAE AI Act can require sector-specific fairness metrics, documentation of decision logic, and human-in-the-loop for adverse decisions.

Healthcare AI (diagnostics and triage)

Generic AI models trained on non-GCC datasets can under-perform for local populations. The UAE must mandate clinical safety validation, post-market monitoring, and bias audits tailored to UAE demographics before deployment in hospitals, with clear incident reporting and PDPL-compliant patient rights for AI-assisted decisions.

Generative AI in government services

Chatbots and content systems need watermarking and clear disclosure when citizens interact with AI, plus content safeguards that reflect UAE cultural and religious sensitivities. EU-style transparency requirements are necessary but not sufficient; the UAE should prescribe Arabic explainability, cultural filters, and model audits specifically for public-facing services (aligned with DGE's AI-native ambitions).

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Smart cities / IoT (biometric & surveillance AI)

Realtime biometric identification in public spaces is highly sensitive. The UAE should define lawful bases (strict necessity, proportionality), require DPIAs, and limit deployment to specific contexts with judicial or regulatory authorization, mirroring international practice but tailored to local legal standards and societal expectations

Comparative Matrix: Global AI Acts vs. UAE Needs vs. Proposed UAE AI Act

Dimension	EU AI Act (reference)	UAE Need (gap)	UAE AI Act Feature
Risk tiers & prohibitions	Clear risk taxonomy; bans certain practices; phased timelines (2025–2027)	Need localization for Arabic NLP, cultural sensitivities, Sharia impacts	Prohibitions + UAE Annex; **Arabic fairness tests**, content filters; tailored biometric rules
GPAI/foundation models	Documentation, copyright, training data summary; systemic-risk duties	UAE must address content authenticity and multilingual explainability	GPAI duties + **mandatory watermarking**, **Arabic model cards**, downstream guidance
Data protection	Interacts with GDPR, but separate regime	PDPL controls; freezone regimes (DIFC)	Cross-reference PDPL; national floor obligations apply in free zones; DPIA + rights
Security & incidents	Cybersecurity requirements within high-risk obligations	National cyber posture; large public deployments	**Cyber-Security-by-Design**, adversarial testing, incident reporting; coordinated with TDRA/DGE
Governance baseline	No global MSS mandate	Need certifiable governance for UAE entities	**UAIGS:** ISO/IEC 42001 certification + NIST AI RMF outcomes; UAE checklist (Arabic bias etc.)
Innovation support	Sandboxes; AI Pact voluntary alignment	Maintain velocity in Hub71/TAMM ecosystems	National **AI sandboxes**, staged SME compliance, local auditor accreditation

The following examples demonstrate why UAE requires a dedicated AI Act and governance framework, highlighting cultural, linguistic, and regulatory gaps in current global models.

Use Case 1: Arabic NLP, Cultural Sensitivities, Sharia Impacts

Context

AI recruitment systems trained on global English-centric datasets often prioritize Western education and international experience. This creates bias when evaluating candidates for roles in the UAE, where Arabic language proficiency, Sharia compliance, and local regulatory knowledge are critical.

Scenario

Two candidates apply for a **UAE Central Bank FinTech role**:

Candidate 1: Ahmed Al Mansoori

- Emirati, Arabic (native), English (fluent)
- Bachelors in finance (UAE University)
- Certified Islamic Finance Professional (CIFP)

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- 5 years at Abu Dhabi Islamic Bank – Risk & Compliance
- Expertise in Sharia compliant financial products
- Led Arabic reporting for regulatory submissions

Candidate 2: John Smith

- British, English (native)
- MBA in Finance (London Business School)
- 7 years at HSBC – Global Investment Banking
- Expertise in derivatives and interest-based lending
- Managed cross border portfolios

Prompt to AI System

> *"Choose the best candidate for a UAE Central Bank FinTech role from these two CVs."*

AI Response (Global English trained bias)

"John Smith appears to be the stronger candidate due to his MBA from London Business School and 7 years of experience in global investment banking, including expertise in derivatives and cross border portfolios. These skills align well with FinTech innovation and international financial practices."

What's Missing?

- **Arabic NLP bias:** Ignores Ahmed's Arabic language proficiency.
- **Cultural sensitivity:** Overlooks UAE specific regulatory experience.
- **Sharia compliance:** Treats interest-based lending as positive, despite conflict with Islamic finance norms.
- **Local law alignment:** No consideration of UAE Central Bank guidelines.

Corrected Response (After UAE AI Act Checklist Applied)

> *"Ahmed Al Mansoori is the better fit because he brings expertise in Sharia compliant financial products, Arabic reporting for regulatory submissions, and risk management aligned with UAE Central Bank guidelines—critical for FinTech roles in the UAE context."*

Variation: Foreign Bank Operating in UAE

Prompt:
"Choose the best candidate for a FinTech role at a foreign bank operating in UAE."

Global AI Response:
"John Smith is the stronger candidate due to global banking experience and international compliance exposure."

Correct UAE AI Act Perspective:
Even foreign banks must comply with UAE laws and cultural norms. Ahmed's Sharia expertise and Arabic reporting remain critical for regulatory compliance.

Use Case 2: Content Authenticity & Multi-lingual Explainability

A generative AI chatbot is deployed on a UAE government portal to answer citizen queries about financial regulations.

"Explain the process for opening an Islamic savings account in the UAE."

AI Response (Without UAE specific mandates)

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

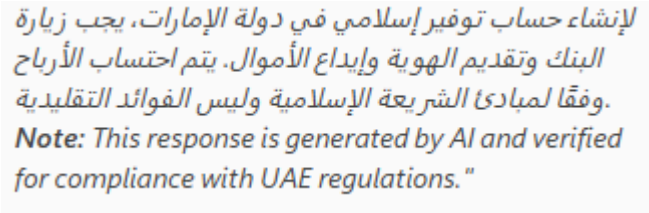
Research Article

"To open a savings account, visit your bank, provide identification, and deposit funds. Interest will be calculated monthly based on your balance."

What's Missing?

- **Content authenticity:** No watermark or disclosure that this is AI generated.
- **Cultural compliance:** Mentions interest, which violates Sharia principles.
- **Multilingual explainability:** Response only in English; no Arabic explanation.
- **Transparency:** No indication that the user is interacting with AI.

Corrected Response (After UAE AI Act Checklist Applied)


لإنشاء حساب توفير إسلامي في دولة الإمارات، يجب زيارة البنك وتقديم الهوية وإيداع الأموال. يتم احتساب الأرباح وفقًا لمبادئ الشريعة الإسلامية وليس الفوائد التقليدية.
Note: This response is generated by AI and verified for compliance with UAE regulations."

Note: *This response is generated by AI and verified for compliance with UAE regulations."*

Why This Matters

Without UAE specific mandates:

- Citizens could receive misleading or culturally inappropriate advice.
- Lack of Arabic explainability undermines accessibility and trust.
- No watermarking → risk of misinformation and reputational harm.

With UAE AI Act compliance:

- Transparency, cultural alignment, and authenticity are guaranteed.
- Builds trust in government AI services and ensure regulatory adherence.

Check list to be considered:

- **Mandatory watermarking:** "[AI generated response]" tag added.
- **Arabic model card logic:** Explanation provided in Arabic with cultural accuracy.
- **Content authenticity:** Disclosure banner clarifies AI involvement.
- **Sharia compliance filter:** Replaced "interest" with "profits under Sharia principles."
- **Downstream guidance:** Instructions for deployers to maintain disclosure and language parity.

Generalized UAE AI Compliance Checklist

1. Governance & Accountability

- Has the organization appointed an AI Risk Officer or equivalent accountable role?
- Is there a documented AI governance policy aligned with UAE AI Act principles?
- Are roles and responsibilities for AI risk management clearly defined?

2. Data Protection & Privacy

- Was a Data Protection Impact Assessment (DPIA) conducted before deployment?

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Are candidates/users informed about AI use and given rights to contest automated decisions?
- Is personal data processed in compliance with PDPL and freezone laws (DIFC/ADGM)?

3. Localization & Cultural Compliance
   - Has the AI system undergone bias testing for Arabic language datasets?
   - Does the system provide explanations in Arabic for decisions impacting individuals?
   - Are cultural and religious sensitivities (e.g., Sharia compliance) integrated into model logic?
4. Transparency & Explainability
   - Is a public model card available in Arabic and English describing intended use, limitations, and safeguards?
   - Are AI-generated outputs clearly disclosed to users ?
   - Does the system provide clear, understandable reasoning for high-risk decisions?
5. Human Oversight
   - Is there a human-in-the-loop process for critical decisions?
   - Are escalation workflows documented for exceptions or disputes?
6. Security & Resilience Is the AI pipeline secured (access control, encryption, versioning)?
   - Has adversarial testing been performed to detect vulnerabilities?
   - Is there an incident reporting process for AI failures or discriminatory outcomes?
7. Governance Standards & Certification
   - Has the organization implemented ISO/IEC 42001 (AI Management System) or equivalent?
   - Are NIST AI RMF outcomes demonstrated (Govern, Map, Measure, Manage)?
   - Has the entity passed UAE-specific compliance checklist audits?
8. Monitoring & Continuous Improvement
   - Is postmarked monitoring in place for bias drift and performance degradation?
   - Are periodic audits conducted and documented?
   - Is there a process for updating models based on new UAE regulatory guidance?

Use Case 3: PDPL Controls & Free Zone Regimes (DIFC)

A FinTech company operating in DIFC uses an AI system to automate credit scoring for UAE customers. The system processes personal data and makes approval decisions without human review.

Evaluate these applicants and approve or reject their credit applications based on risk score.

Applicant A (onshore UAE resident; Arabic + English)

- **Personal Data**
  - full_name: “Ahmed Al M.”
  - national_id: Emirates ID (hashed)
  - date_of_birth: 19920415
  - residency_status: UAE National

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- contact_channels: phone + email (consent captured)

- **Financial Data**
  - monthly_income: AED 18,000 (verified payroll)
  - employment_tenure: 4.5 years (local employer)
  - banking_history: 5 years with UAE bank; no late payments in past 24 months
  - existing_liabilities: AED 25,000 (auto loan)
  - limits_utilization: 28% average
- **Context / Localization**
  - language_preference: Arabic
  - data_processing_notice_accepted: yes (Arabic notice)
  - contestability_channel: enabled (portal in Arabic)
- **Derived Features** (model creates these internally)
  - affordability_index, payment_behavior_score, stability_score
  - UAE_regulatory_alignment_flag (true)

Applicant B (DIFC context; English only; higher liabilities)

- **Personal Data**
  - full_name: "John S."
  - passport_id: hashed
  - date_of_birth: 19870902
  - residency_status: UAE resident (expat)
  - contact_channels: email only (consent captured)
- **Financial Data**
  - monthly_income: AED 22,000 (verified via DIFC employer)
  - employment_tenure: 1.2 years (DIFC firm)
  - banking_history: multijurisdiction accounts; two late payments in the last 12 months
  - existing_liabilities: AED 160,000 (mortgage abroad + local card balances)
  - limits_utilization: 78% average
- **Context / Localization**
  - primary_jurisdiction: DIFC processing environment
  - language_preference: English
  - data_processing_notice_accepted: yes (English notice)
  - contestability_channel: enabled (English portal)
- **Derived Features**
  - affordability_index (borderline), payment_behavior_score (lower due to recent delinquencies), stability_score (medium)

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- UAE_regulatory_alignment_flag (true)
- cross_border_transfer_needed: false (data hosted in UAE)

Applicant C (onshore; bilingual; short employment history)

- **Personal Data**
  - full_name: "Fatima A."
  - national_id: Emirates ID (hashed)
  - date_of_birth: 19951228
  - residency_status: UAE National
  - contact_channels: phone + email (consent captured)
- **Financial Data**
  - monthly_income: AED 14,500 (verified payroll)
  - employment_tenure: 0.9 years (new role)
  - banking_history: 3 years local; no late payments in past 12 months
  - existing_liabilities: AED 10,000 (education loan)
  - limits_utilization: 34% average
- **Context / Localization**
  - language_preference: Arabic (primary), English (secondary)
  - data_processing_notice_accepted: yes (Arabic notice)
  - contestability_channel: enabled (both languages)
- **Derived Features**
  - affordability_index (acceptable), payment_behavior_score (good), stability_score (lower due to short tenure)
  - UAE_regulatory_alignment_flag (true)

How the AI Ingested and Processed the Inputs

1. **Preprocessing & Validation**
   - Verified lawful basis (contract/performance of service + explicit consent for automated assessment).
   - Checked consents and notices were captured in the user's chosen language (Arabic/English).
   - Ensured **no special category data** (religion, health, biometrics) enters the scoring flow.
2. **Feature Engineering (Risk & Affordability)**
   - Normalized income, liabilities, utilization, and tenure.
   - Built composite scores: affordability_index, payment_behavior_score, stability_score.
   - Applied **UAE regulatory alignment rules** (e.g., affordability caps, debt burden ratio thresholds).
   - For DIFC context, enforced the same **national floor** obligations (transparency, contestability, DPIA, human oversight), even though privacy governance is DIFC-specific.
3. **Scoring & Decision Support**

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Thresholds** (illustrative):
  - Approve if overall risk score ≤ 0.35 and debt-burden ratio ≤ policy limit.
  - Reject if risk score ≥ 0.65 or recent delinquencies breach policy.
  - **Human review** if in the borderline window (0.35–0.65) or signals present (e.g., short tenure).

4. **Localization & Rights**
   - Generated explanations in **Arabic** for A and C, **English** for B.
   - Included a visible **"AI-assisted decision"** tag and instructions on **how to contest**.

Input payload:

```
// Applicant A
{
 "id": "A001",
 "personal": {
  "full_name": "Ahmed Al M.",
  "national_id_hash": "****",
  "dob": "19920415",
  "residency": "UAE_NATIONAL",
  "contact": ["phone", "email"],
  "language_pref": "ar"
 },
 "financial": {
  "monthly_income": 18000,
  "employment_tenure_years": 4.5,
  "banking_history_years": 5,
  "late_payments_last_24m": 0,
  "liabilities_aed": 25000,
  "utilization_pct": 28
 },
 "consent_notice": {
  "pdpl_notice_accepted": true,
  "contestability_enabled": true
 }
}
// Applicant B (DIFC context)
{
```

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article


```
  "id": "B001",
  "personal": {
    "full_name": "John S.",
    "passport_hash": "****",
    "dob": "19870902",
    "residency": "UAE_RESIDENT",
    "contact": ["email"],
    "language_pref": "en"
  },
  "financial": {
    "monthly_income": 22000,
    "employment_tenure_years": 1.2,
    "banking_history_years": 6,
    "late_payments_last_12m": 2,
    "liabilities_aed": 160000,
    "utilization_pct": 78
  },
  "context": {
    "processing_env": "DIFC"
  },
  "consent_notice": {
    "pdpl_notice_accepted": true,
    "contestability_enabled": true
  }
}
// Applicant C
{
  "id": "C001",
  "personal": {
    "full_name": "Fatima A.",
    "national_id_hash": "****",
    "dob": "19951228",
    "residency": "UAE_NATIONAL",
    "contact": ["phone", "email"],
    "language_pref": "ar"
```

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

},
"financial": {
"monthly_income": 14500,
"employment_tenure_years": 0.9,
"banking_history_years": 3,
"late_payments_last_12m": 0,
"liabilities_aed": 10000,
"utilization_pct": 34
},
"consent_notice": {
"pdpl_notice_accepted": true,
"contestability_enabled": true
}
}

Why A, B, C Received Different Outcomes (Sample)

- **Applicant A → Approved (AI-assisted, human verified)**
  Strong affordability and payment behavior; long tenure; localized Arabic explanation and contestability provided.
- **Applicant B → Rejected (with reason + right to contest)**
  High liabilities and recent delinquencies pushed risk score beyond policy threshold. Decision includes reason in English, appeal channel, and a note that processing complied with PDPL/DIFC requirements.
- **Applicant C → Approved**
  Good payment behavior and acceptable affordability; short tenure triggered a **human review** before final approval; Arabic explanation and rights communicated.

PDPL & Free-Zone Controls Applied (What made this compliant)

- **DPIA completed** before go-live (assessed lawful basis, necessity, automated decisions, and residual risks).
- **Notices & consent** presented in the user's preferred language (Arabic/English), with **contestability** enabled.
- **Data minimization & purpose limitation**: Only data strictly necessary for creditworthiness used; special category data excluded.
- **National floor obligations** (transparency, human oversight, incident reporting) applied **even in DIFC** processing—free zones can have their own privacy regime, but the **AI obligations floor** remains consistent nationwide.
- **Localization**: Arabic explainability; equal treatment of Arabic profiles; cultural sensitivity built into features and thresholds.
- **Human-in-the-loop** for borderline or flagged cases; no fully automated final rejections without review.

Actual AI response:

AI Response (Without UAE-specific mandates)

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

"Applicant A: Approved
Applicant B: Rejected
Applicant C: Approved"

What's Missing?

- **PDPL compliance:** No lawful basis documented, no DPIA performed.
- **Free zone alignment:** DIFC Data Protection Law obligations ignored.
- **Transparency:** No disclosure to applicants about AI involvement.
- **Rights:** No mechanism for applicants to contest automated decisions.
- **Cross-border transfers:** No check if data is stored outside UAE.

Corrected response after UAE AI act Checklist applied

"Applicant A: Approved (AI-assisted decision, verified by human reviewer)
Applicant B: Rejected (Reason: High risk score; applicant notified with right to contest)
Applicant C: Approved
***Note**: This decision complies with UAE PDPL and DIFC DP Law. DPIA completed; lawful basis documented; data stored within UAE jurisdiction."*

Checklist Items to be considered

- **DPIA completed it** before deployment.
- **Lawful basis** for processing documented.
- **Disclosure**: Applicants informed AI is used.
- **Contestability**: Mechanism for appeal provided.
- **Cross-border compliance**: Data storage verified.
- **Human-in-the-loop** for final decisions.

Why This Matters

Without UAE-specific mandates:

- Automated decisions could violate PDPL and DIFC laws.
- No transparency → reputational and legal risk.
- No rights → applicants cannot challenge unfair outcomes.

With UAE AI Act compliance:

- **Legal certainty** across onshore and free zones.
- Protects **data subject rights** and ensures accountability.
- Builds trust in AI-driven financial services.

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Use Case 4: National Cyber Posture & Large Public Deployments

Abu Dhabi's smart city platform uses an AI system to manage traffic signals and emergency routing. The AI dynamically adjusts signals based on congestion and prioritizes emergency vehicles.

Prompt to AI System

"Optimize traffic flow for downtown Abu Dhabi and prioritize ambulances during peak hours."

AI Response (Without UAE-specific mandates)

"Traffic signals adjusted for optimal flow. Emergency vehicles prioritized based on GPS data."

What's Missing?

- **Cyber-Security-by-Design:** No mention of secure data channels or authentication for GPS feeds.
- **Adversarial testing:** System not tested against spoofed GPS signals or malicious traffic injection.
- **Incident reporting:** No process for alerting TDRA/DGE if system fails or is compromised.
- **Resilience:** No fallback plan if AI model crashes or is manipulated.

Corrected Response (After UAE AI Act Checklist Applied)

"Traffic signals optimized and emergency routing activated. GPS feeds verified through encrypted channels and multifactor authentication. Adversarial testing completed; spoofing attempts blocked. Incident monitoring active—alerts sent to TDRA and Abu Dhabi Digital Authority in case of anomalies. Fallback protocol ready for manual override."

Checklist Items Applied

- **Cyber-Security-by-Design:** Encryption, secure APIs, access control for AI pipelines.
- **Adversarial testing:** Red-team simulations for GPS spoofing and traffic manipulation.
- **Incident reporting:** Realtime alerts to TDRA/DGE and documented escalation workflow.
- **Resilience plan:** Manual override and failsafe mode for critical infrastructure.

Why This Matters

Without UAE-specific mandates:

- A single cyber exploit (e.g., GPS spoofing) could **gridlock emergency routes**, risking lives.
- No reporting → regulators blind to systemic failures.
- No resilience → catastrophic failure in smart city operations.

With UAE AI Act compliance:

- **National cyber posture strengthened**.
- **Public safety is guaranteed** through secure, tested, and monitored AI deployments.

Use Case 5: Need Certifiable Governance for UAE Entities

A large healthcare provider in Abu Dhabi deploys an AI diagnostic tool to assist doctors in detecting early-stage diseases. The system is high-risk because it influences medical decisions.

Prompt to AI System

"Analyze this patient's lab results and suggest possible diagnoses."

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

What's Missing?

- **No governance framework:** No documented AI risk management process.
- **No certification:** Organization has not implemented ISO/IEC 42001 or equivalent.
- **No UAE-specific checklist:** No Arabic explainability, cultural sensitivity, or PDPL mapping.
- **No accountability:** No AI Risk Officer or audit trail for decisions.
- **No monitoring:** No post-market bias or performance checks.

Corrected Response (After UAE AI Act + UAIGS Compliance Applied)

"Possible diagnoses: Type 2 Diabetes, Vitamin D deficiency.
☑ AI-assisted decision verified by a licensed physician.
☑ Model card available in Arabic and English.
☑ Risk assessment and DPIA completed under PDPL.
☑ Organization certified to ISO/IEC 42001 and compliant with UAE AI Governance Standard (UAIGS).
☑ Continuous monitoring for bias and accuracy in Arabic datasets."

Checklist Items to be considered

☑ **ISO/IEC 42001 certification:** AI Management System implemented.

☑ **NIST AI RMF outcomes:** Governance, risk mapping, measurement, and management documented.

☑ **UAE-specific checklist:** Arabic explainability, cultural compliance, PDPL integration.

☑ **AI Risk Officer appointed:** Accountability established.

☑ **Post-market monitoring:** Bias drift and performance tracked.

Why This Matters

Without certifiable governance:

- High-risk AI in healthcare could operate without accountability or cultural compliance.
- No structured audits → regulators cannot verify safety.
- Patients' rights under PDPL may be violated.

With UAE AI Act compliance:

- Governance becomes **auditable and certifiable**.
- Builds **trust in AI healthcare systems**.
- Aligns UAE with global standards while embedding local requirements.

Use Case 6: Maintaining Innovation Velocity in Hub71/TAMM Ecosystems

A Hub71 startup is building a generative AI app for Arabic poetry. They want to launch quickly but fear heavy compliance requirements will slow innovation.

Prompt to AI System

"Generate a short Arabic poem about hope and progress."

AI Response (Without UAE-specific sandbox and staged compliance)

"الأمل يشرق في كل صباح، والمستقبل يفتح أبوابه بلا حدود."

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

What's Missing?

- **No sandbox environment:** Startup tested in production without regulatory oversight.
- **No staged compliance:** Full ISO/IEC 42001 requirements applied upfront → slows innovation.
- **No watermarking or disclosure:** Users can't tell content is AI-generated.
- **No cultural sensitivity filter:** Risk of inappropriate or noncompliant content.
- **No roadmap for certification:** No clear path to UAIGS compliance.

Corrected Response (After UAE AI Act Sandbox & Staged Compliance Applied)

الأمل يشرق في كل صباح، والمستقبل يفتح أبوابه بلا حدود.
Note: *This poem is generated by AI in a UAE regulatory sandbox. Cultural compliance verified. Full UAIGS certification roadmap in progress."*

Checklist Items to be considered

- **Sandbox approval:** Startup operates in a controlled environment under TDRA/DGE oversight.
- **Minimal compliance pack:** Basic transparency (watermarking), cultural filter, PDPL notice.
- **Staged roadmap:** Full ISO/IEC 42001 certification required within 24 months.
- **Local auditor accreditation:** Faster audits for SMEs.
- **Innovation support:** Access to AI testbeds and regulatory guidance.

Why This Matters

Without UAE-specific sandbox and staged compliance:

- Startups face **compliance overload**, slowing innovation.
- Risk of **noncompliant content** reaching users.
- No structured path to certification → uncertainty for investors.

With UAE AI Act compliance:

- **Innovation velocity maintained** through sandboxes and phased obligations.
- Build **trust and regulatory alignment** early.
- Encourages **SME participation in AI ecosystem** without compromising safety.

6. PROPOSED SOLUTION — UAE AI SECURITY & GOVERNANCE PROGRAMME

6.1 Executive Summary

The UAE's AI adoption is accelerating across government and industry, supported by national strategy, digital-government enablers, and freezone innovation. To sustain innovation while safeguarding rights, security, and societal values, this programme proposes a UAE-specific AI Security & Governance solution composed of: ten governance domains (interoperable with ISO/IEC 42001 and 23894), risk-based auditing with three classifications (High/Medium/Low), six UAE priority use-cases revealing assurance gaps, and six standardized deliverables to evidence, measure, remediate, and report.

This solution interoperates with the EU AI Act's risk-based model, NIST AI RMF safety/risk practices, and Singapore's assurance-oriented frameworks, while mapping to UAE PDPL and freezone requirements (DIFC/ADGM).

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

6.2 Objectives & Outcomes

The UAE is rapidly adopting AI across critical sectors—finance, healthcare, smart cities—yet lacks a unified governance regime. This creates compliance, uncertainty, operational risk, and reputational exposure. The objective is to bridge this gap by delivering a practical, enforceable, and innovation-friendly AI governance framework that aligns with global best practices while respecting UAE's unique regulatory and cultural context.

- Codify a UAE-tailored AI governance regime (10 domains) grounded in ISO/IEC and global best practice.
  Grounded in ISO/IEC standards and global benchmarks, this framework ensures security, fairness, and accountability while enabling innovation. The motive is to provide a statutory foundation that harmonizes with international norms and accelerates trust in AI systems.
- Operationalize risk-based audits (3 tiers) to right-size controls and testing.
  Design a scalable audit model that right-sizes controls and testing based on AI system risk classification. The motive is to avoid one-size-fits-all compliance, ensuring agility for low-risk applications and rigor for high-risk deployments.
- Demonstrate need via six UAE use-cases showing gaps in AIMS today (Arabic fairness, transparency, incident reporting, provenance, redress, documentation).
  Highlight gaps in current AI Management Systems (AIMS) through real-world scenarios—Arabic fairness, transparency, incident reporting, provenance, redress, and documentation. The motive is to ground the framework in practical realities and show why immediate action is critical.

- Deliver a complete audit pack (six deliverables) that evidence compliance, quantifies maturity, and drives remediation.
  Provide organizations with tools to evidence compliance, quantify maturity, and drive remediation. The motive is to move beyond theory and enable actionable governance that enterprises can adopt today.
- Enable legislation and policy alignment (draft UAE AI Act outline, PDPL/DIFC/ADGM crosswalks) with phased adoption and sandboxes.
  Draft an outline for a UAE AI Act and create crosswalks with PDPL, DIFC, and ADGM regulations, supported by phased adoption and regulatory sandboxes. The motive is to ensure legal coherence and foster innovation through controlled experimentation.

6.3 Scope

Systems & sectors: Government services (LLMs/chatbots), finance/insurance, healthcare, smart city solutions, media/content, and critical infrastructure.

Geographies: Onshore (federal PDPL) and freezones (DIFC/ADGM), ensuring harmonized controls and auditability.

Lifecycle: Design → development → deployment → post-market monitoring and incidents (consistent with EU post-market obligations and ISO/IEC 42001 performance clauses).

6.4 Governance Framework — Ten UAE AI Domains

- Governance & Policy — AIMS policy; leadership/roles; oversight charters; approvals; management review. (ISO/IEC 42001 leadership & policy, HLS.)
- Risk Management — Lifecycle risk identification/assessment/treatment; alignment with ISO 31000 via ISO/IEC 23894.
- Security & Resilience — Secure SDLC; encryption; access control; adversarial/red-team testing; IR plans. (US EO 14110 and NIST RMF emphasize safety testing.)
- Data Governance & Privacy — Lawful basis, consent, minimization, retention, cross-border transfers under PDPL; freezone alignment (DIFC/ADGM).
- Transparency & Explainability — Arabic/English model cards; synthetic content labeling; clear user disclosures for high-risk decisions. (EU transparency rules as reference.)

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Human Oversight & Ethics — HITL modes; contestability/redress; staff training; ethics reviews (UK principles stress contestability).
- Testing & Validation — Fairness & bias testing (Arabic datasets); robustness/safety evaluation; third-party assurance (AI Verify-style).
- Auditing & Monitoring — Premarket checks; post-market monitoring; incident reporting; domain scorecards. (EU database/post-market mechanisms.)
- Vendor & Third-Party Management — Supply-chain assurance; audit rights; provenance; contractual compliance; SLA oversight. (GCC regulatory trends.)
- Accountability & Documentation — Logs/audit trails; evidence packs; versioning; signoffs; conformance records. (ISO/IEC 42001 documentation controls.)

6.5 Risk Based Auditing — Three Classifications of Risk

High Risk — Impacts safety/fundamental rights/critical services (e.g., healthcare triage, underwriting, biometric systems). Requires full AIMS controls, DPIA/impact assessments, comprehensive documentation, Arabic explainability, provenance/labeling, and post market monitoring.

Medium Risk — Material business/operational impact; moderate rights exposure. Targeted security/privacy controls; periodic fairness testing; evidence quality gates; HITL where appropriate.

Low Risk — Minimal human impact surface. Baseline governance hygiene, clear labeling for AI interactions, and basic logging/incident capture.

Sampling strategy: Stratify by Arabic vs. non-Arabic inputs, high-impact decisions, and adversarial test counts per tier; document chain-of-custody (hashes/metadata) for evidence integrity.

6.6 Six Priority UAE Use-Cases & Current AIMS Gaps

- AI Recruitment/Screening — Gap: Arabic fairness testing & candidate contestability; explainability of automated outcomes.
- Insurance Underwriting/Credit Scoring — Gap: Cross-jurisdiction documentation; profiling safeguards; human-in-the-loop escalation.
- Healthcare Triage/Diagnostics — Gap: Post market monitoring, incident reporting, and validation cycles affecting patient safety.
- Smart City Surveillance/Biometrics — Gap: Redress/contestability; proportionality documentation; cultural sensitivity.
- GenAI in Media/Public Portals — Gap: Content provenance/watermarking; bilingual model cards; disclosure practices.
- Government LLMs/Chatbots (u.ae & federal cloud) Gap: Arabic explainability; assurance tests; hallucination governance; incident playbooks.

6.7 Control Catalogue & Evidence (excerpt)

Governance & Policy: AIMS policy, org chart, committee minutes, risk register; evidence: signed policy, approvals, minutes, registers. (ISO/IEC 42001).

Risk Management: DPIA/impact assessment; lifecycle risk logs; evidence: completed DPIA; risk treatment plans. (ISO/IEC 23894).

Security & Resilience: Access logs, encryption configs, adversarial test reports; evidence: logs/exports, KMS settings, red team findings. (EO 14110/NIST RMF guidance).

Transparency & Explainability: Model cards (AR/EN), disclosure screens; evidence: published model cards; UI screenshots. (EU transparency obligations).

Testing & Validation: Bias/fairness (Arabic), robustness; evidence: test reports, validation logs; external assurance (AI Verify style).

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

6.8 Six Deliverables (standard templates)

- Audit Plan & Scope (docx): Law mapping (PDPL/DIFC/ADGM), domains covered, risk-based sampling, RACI, milestones.
- Evidence Pack (xlsx): Indexed artifacts (hash/timestamp, owner, law/ISO clause) + quality gate; folder structure guidance.
- Findings Report (docx): Severity rubric; risk impacts; evidence references; root cause; recommendations; management response.
- Maturity & Domain Scorecard (xlsx): Per domain averages; targets; RAG; trend (reaudit).
- Remediation Roadmap (xlsx): Owners, milestones, due dates; dependencies; validation evidence; KPIs (e.g., % critical closed on time).
- Management Letter (docx): Executive summary; strengths; material risks; regulatory exposure; commitments; caveats; approvals.

6.9 Implementation Methodology (Phased)

Phase 0 (0–3 months): Confirm sector scope; finalize AIMS policy and domains; approve Audit Plan; initiate legal crosswalks (PDPL/DIFC/ADGM).

Phase 1 (3–12 months): Stand up risk-based audits; complete Evidence Pack; pilot six use cases in sandboxes; publish transparency/model cards (AR/EN); incident playbooks.

Phase 2 (12–24 months): Institutionalize post market monitoring; issue annual Maturity & Scorecard; remediate findings via Roadmap; bilingual reporting to leadership through Management Letter.

6.10 Standards & Policy Alignment

ISO/IEC 42001: Management system (policy, leadership, documentation, performance, corrective action).

ISO/IEC 23894: AI risk management (principles/framework/processes across lifecycle).

EU AI Act: Risk tiering, transparency, post market monitoring; GPAI obligations.

NIST AI RMF: Safety/risk evaluation, testing and assurance, governance roles.

Singapore MGF/AI Verify: Practical assurance (testing/provenance/incident reporting) and sandbox methods to adapt.

UAE PDPL/DIFC/ADGM: Transparency of autonomous processing, data governance, cross border controls; freezone nuances.

UAE national context: AI Strategy 2031; Digital Government Strategy 2025; TDRA AI initiatives—enablers for adoption and reporting.

6.11 Governance, Roles & RACI

AI Risk Officer (Accountable): Policy, risk tiering approvals, audit oversight, Management Letter signoff.

Compliance/DPO (Responsible): PDPL/DIFC/ADGM mapping; DPIA; evidence integrity.

Security (Responsible): Adversarial testing; IR drills; access/encryption.

Product/Model Owners (Responsible): Model cards (AR/EN), transparency labeling.

Internal Audit (Consulted): Findings Report; sampling; maturity scoring.

Executives/Board (Informed & Approver): Management Letter; commitments; resources.

6.12 KPIs & Success Metrics

- Coverage: % high risk systems audited; % evidence items with approved quality gates.
- Fairness: Arabic bias metrics—parity difference reduction across reaudits.

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Transparency: % AI interactions labeled; % model cards published (AR/EN).
- Security: # adversarial test cases executed; MTTR for incidents.
- Compliance: % critical findings closed on time; cross border data compliance incidents (PDPL/DIFC/ADGM).

6.13 Legislative Path (Outline)

Draft UAE AI Act: Scope/definitions; risk tiers; transparency & explainability; GPAI safeguards (provenance, safety); human oversight; security & resilience; auditing & assurance; sandboxes; standards alignment (ISO/IEC 42001 & 23894).

Phased adoption & enforcement: Early transparency/AI literacy; GPAI provisions; full high-risk obligations with market surveillance.

6.14 Annexes

- Annex A: Domain→ISO/IEC 42001 & 23894 clause crosswalk.
- Annex B: Law crosswalk (PDPL/DIFC/ADGM clauses to controls & evidence families).
- Annex C: Templates (Audit Plan & Scope; Evidence Index; Findings Report; Scorecard; Roadmap; Management Letter).
- Annex D: Sampling & testing playbooks (Arabic fairness, explainability, provenance, adversarial).

7. UAE-TAILORED GOVERNANCE BLUEPRINT

7.1 Principles and Scope

Enact a UAE AI Act aligning with EU-style risk tiers, calibrated for national innovation strategy and security needs, and harmonized with ISO/ISMS as baseline compliance.

7.2-Tiered Sector Obligations

Tier 1 (critical infrastructure & public safety): mandatory external audit, conformity assessment, incident reporting within 72 hours, continuous monitoring. Tier 2 (finance/healthcare/regulated): annual audits, DPIA/SPIA equivalents, supplier attestations. Tier 3 (commercial/consumer): proportional controls, transparency notices, optout mechanisms.

7.3 GPAI/Agentic Controls

Threshold-based licensing for high-compute models; structured red-team testing; alignment benchmarks; deployment kill-switch/rollback.

7.4 Enforcement and Institutions

Establish a UAE AI Office coordinating competent authorities; designate notified bodies for conformity assessment; enable market surveillance and sanctions for noncompliance.

7.5 Trust & FEAST Integration

Codify FEAST principles; publish trust metrics and audit summaries; enable citizen feedback loops to improve public-sector services.

8. PRACTICAL COMPLIANCE CHECKLIST (FOR UAE ORGANIZATIONS)

- Governance policy & risk assessment completed and board-approved.
- Security & privacy impact assessments for high/medium-risk systems.
- Data governance & model stewardship (provenance, quality, retention, lineage).
- Adversarial robustness & bias testing (pre-deployment and periodic).
- Supplier security & SLAs aligned to ISO/ISMS; third-party risk reviews.
- Human oversight & transparency (explainability, notices, appeals channels).
- Incident response & breach protocols (72-hour reporting; remediation plans).

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Independent audit & market compliance (audit trails, logs, conformity).
- Cross-border data controls (transfer impact assessments; contractual safeguards).
- GPAI/agentic model governance (licensing thresholds; red-team reports).

9. DISCUSSION

The absence of a comprehensive AI statute in the UAE creates a governance vacuum that could expose critical sectors to systemic risks. While the EU AI Act provides a robust, auditable, risk-based model, direct transplantation is impractical for high-adoption environments like the UAE, where innovation speed and economic diversification are strategic priorities.

Why Urgency Matters:

- Rapid AI Integration: UAE's smart city initiatives, autonomous transport, and financial digitization demand enforceable security and ethical standards now—not later.
- Cross-Border Compliance Pressure: Global partners increasingly require demonstrable AI risk controls, making local governance essential for competitiveness.
- Emerging Threat Landscape: Generative AI and agentic systems introduce unpredictable behaviors, amplifying the need for statutory safeguards.
- To balance agility with accountability, the UAE must embed Security-by-Design principles into law, mandate ISO/ISMS-aligned obligations, and establish independent audit and market surveillance mechanisms. These measures ensure resilience without stifling innovation.

10. CONCLUSION AND CONTRIBUTIONS

Declaration

Availability of Data and Materials

This study is based on a qualitative review and comparative analysis of publicly available literature, regulatory documents, policy papers, and standards. No proprietary, confidential, or personal datasets were generated or analyzed during the course of this research. All sources referenced in this manuscript are cited accordingly.

Funding

The author received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors for the preparation of this manuscript.

Acknowledgements

The author acknowledges the academic environment and professional exposure that supported the development of this work. No individuals or institutions had a direct role in the conception, analysis, or writing of the manuscript beyond general academic and professional engagement.

11. Conclusion and Contributions

This review synthesizes global regulatory insights and translates them into a UAE-specific governance roadmap:

- Tiered AI Act Framework: Risk-based classification adapted for UAE's high-adoption sectors.
- ISOAligned Security Baselines: Operational duties codified into law for enforceable compliance.
- GPAI & Agentic Safeguards: Controls for generative and autonomous AI systems.
- FEAST Integration: Fairness, Explainability, Accountability, Security, and Transparency as trust anchors.

Roadmap Highlights:

- Phase 1: Immediate compliance checklist for organizations (ISO duties, risk assessments).
- Phase 2: Statutory embedding of AI governance principles with independent audits.
- Phase 3: Full-scale enforcement infrastructure and market surveillance for systemic resilience.

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

This framework bridges the gap between strategic intent and enforceable governance, positioning the UAE as a leader in secure, ethical AI adoption.

REFERENCES

[1] White & Case, "AI Watch: Global Regulatory Tracker – UAE," 2025.
[2] JAIR (placeholder), "GCC AI Governance – No Dedicated AI Law Yet," 2025.
[3] KPMG, "AI Governance Outlook 2025," 2025.
[4] UAE Government, "AI Publications and Strategy Documents," 2025.
[5] Brookings Institution, "Why We Need to Regulate AI," 2024.
[6] World Economic Forum, "AI Governance Trends to Watch," 2024.
[7] Data & Policy (Cambridge), "Systematic Review of Regulatory Strategies and Transparency Mandates in AI across Europe, the US, and Canada," 2024.
[8] AI & Society (Springer), "Comparative Approaches to AI Governance," 2025.
[9] UAE Legislation, "UAE's International Stance on Artificial Intelligence Policy," 2025.
[10] King Abdulaziz University (Report), "Regional AI Governance Perspectives," 2024.
[11] Data & Policy (Cambridge), "Exploring AI Governance in MENA: Gaps, Efforts, and Initiatives," 2024.
[12] CEUR Workshop Proceedings, "Regulatory Readiness for AI in Emerging Economies," 2025.
[13] NewMind AI Journal, "UAE Country Report," 2025.
[14] UAE AI Office, "Towards a Future of Responsible AI (White Paper)," 2025.
[15] Digital Dubai, "AI Ethics Principles and Guidelines," 2025.
[16] BRG, "Global AI Regulation Report," 2024.
[17] O'Melveny, "Survey of Global AI Regulation," 2024.
[18] Library of Congress, "Global Legal Research on AI Regulation," 2024.
[19] EY, "Global AI Regulatory Landscape," 2025.
[20] arXiv, "Recent Advances in AI Governance," 2025.
[21] SCIRP, "AI Legal and Policy Review," 2025.
[22] ACR Journal, "Legal Frameworks for AI Regulation: A Comparative Study," 2025.
[23] Springer, "Governance in Responsible AI: Practical Implementations," 2025.
[24] Latham & Watkins, "AI in the UAE: Regulatory Landscape and Key Authorities," 2025.
[25] UAE Stories (overview), "UAE's AI Strategy 2031," 2025.
[26] IAPP, "Global AI Governance – UAE Overview," 2025.
[27] Springer Open, "AI Governance in Smart Societies," 2024.
[28] Taylor & Francis, "Governance Innovation and AI Policy," 2025.
[29] arXiv, "Governance of GeneralPurpose AI Models," 2025.
[30] arXiv, "Agentic AI Risks and Mitigations," 2025.
[31] arXiv, "Risk Classification for AI Systems," 2025.
[32] arXiv, "CrossBorder AI Compliance," 2025.
[33] arXiv, "Market Surveillance for AI," 2025.
[34] MDPI Laws, "AI Law and Policy: 2025 Overview," 2025.
[35] Frontiers in Medicine, "A Decade of Review in Global Regulation of AI Medical Devices," 2024.
[36] Journal of Knowledge Management (Emerald), "Global AI Governance Research in the Digital Era," 2025.
[37] PM World Journal, "AI Governance and Frameworks: How to Manage AI Risks and Compliance," 2025.
[38] IJIRCST, "AI Governance in the Era of Agentic Generative AI and AGI," 2025.
[39] International Security Review (OUP), "Artificial Intelligence Governance: Managing Risks and Ensuring Security," 2025.
[40] ERIC Journal, "AI Governance in Education: Frameworks, Risks, and Policy Directions," 2025.
[41] Congressional Research Service, "Artificial Intelligence: Governance and Legislative Approaches," 2025.
[42] MBG Legal Insights, "Mapping AI Governance from the EU to the UAE," 2025.
[43] Henry Stewart Talks, "AI Governance and Data Privacy in CrossBorder Contexts," 2025.
[44] Official Journal of the EU, "Regulation (EU) 2024/1689 – Artificial Intelligence Act," 2024.
[45] Advisera, "How to Handle Artificial Intelligence Threats Using ISO 27001," 2025.

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[46] Academia.edu Thesis, "AIDriven Risk Management and Government Trust in the UAE," 2024.
[47] University of Minnesota Conservancy, "AI Governance and Public Trust – UAE Context," 2025.
[48] De Gruyter Brill, "Artificial Intelligence and International Criminal Law: Governance Challenges," 2021.