White paper

AI Regulation and Governance in the Middle East

A strategic guide for compliance teams, legal counsel, and governance leaders operating across the region

March 2026 | Version 1.0

VerifyWise Thought Leadership Series

TABLE OF CONTENTS

1. Executive Summary

Across the Middle East, AI regulation is being delivered through three channels rather than a single cross-sector AI act: national AI strategies and ethical charters that set expectations but are usually nonbinding; data protection and data governance regimes that constrain training and deployment where personal data is involved; and sector regulators, especially central banks and financial free-zone authorities, issuing operational guidance for AI adoption covering governance, accountability, human oversight, transparency, and consumer protection.

This report covers 14 Middle East jurisdictions, organized into 3 tiers based on regulatory maturity and operational readiness.

Tier 1 leaders (UAE, Saudi Arabia, Qatar, Israel, Oman, Egypt) have established binding data protection regimes and published AI-specific governance instruments. They differ in regulatory posture: the UAE operates a layered multi-regulator ecosystem; Saudi Arabia centralizes governance through SDAIA; Qatar channels operational AI controls through its central bank; Israel favors soft law and public sector risk management; Oman has published unusually concrete whole-of-government AI policies; and Egypt combines strategy-led governance with a responsible AI charter and an evolving PDPL framework.

Tier 2 countries (Bahrain, Jordan, Kuwait) have credible privacy or digital regulation foundations but fewer AI-specific operational instruments. Bahrain leads with a dedicated personal data protection law and procurement-facing AI guidance developed with the World Economic Forum. Jordan has paired an AI ethics charter with a new binding personal data protection law. Kuwait is comparatively developed on cloud and data governance but its national AI strategy remains under development.

Tier 3 environments (Lebanon, Iraq, Palestine, Syria, Yemen) are characterized by partial digital frameworks, political instability, or limited accessible primary sources. Regulatory coverage varies from Lebanon's emerging institutional capacity through the Ministry of Technology and AI, to Yemen's absence of comprehensive data protection legislation.

A practical way to unify compliance across this region is to run an AI governance program that meets data protection obligations where personal data is used and remains inspection-ready under sector regulator expectations. Mapping controls to the NIST AI RMF's GOVERN, MAP, MEASURE, MANAGE functions provides a strong baseline that also aligns with the EU AI Act's risk-based structure for organizations needing cross-jurisdictional comparability.

Scope note.

This report covers 14 Middle East jurisdictions as specified. Turkey is not included in this edition.

1.1 How to use this report

This report is a compliance planning resource. It provides:

- **Country-level dossiers.** with binding laws, AI-specific instruments, enforcement posture, and compliance takeaways for each jurisdiction.
- **A maturity scoring model.** validated against external benchmarks including the Oxford Government AI Readiness Index and OECD AI Policy Observatory data.
- **Sector deep dives.** for financial services, public sector, and healthcare, with cross-country control mapping.
- **Regulatory comparison tables.** showing how overlapping authorities operate within Saudi Arabia (SDAIA vs sector regulators) and Qatar (QCB vs MCIT).
- **Framework mapping.** against the EU AI Act and NIST AI RMF for organizations operating across regions.
- **Enforcement case studies.** documenting real regulatory actions across the region.

Use it to:

1. **Scope your compliance program..** Identify which jurisdictions carry binding obligations versus soft law expectations for your specific sector and deployment type.

2. **Prioritize control implementation..** Start with data protection obligations (the binding layer) and layer sector-specific AI governance requirements on top.

3. **Build regulator-ready evidence..** Use the framework mapping tables to structure documentation that satisfies both regional regulators and international standards.

4. **Brief leadership and boards..** Use the country comparison table and maturity scores to communicate regional risk posture to decision-makers.

1.2 Quick reference: regulatory posture by tier

Tier	Countries	Regulatory posture	Primary compliance driver
Tier 1 - Advanced/Operational	UAE, Saudi Arabia, Qatar, Israel, Oman, Egypt	Binding privacy laws + AI governance instruments + sector regulator guidance	Data protection compliance + sector-specific AI controls
Tier 2 - Emerging	Bahrain, Jordan, Kuwait	Privacy law foundations + limited AI-specific instruments	Privacy compliance + procurement-driven governance

Tier 3 - Early	Lebanon, Iraq, Palestine, Syria, Yemen	Partial digital frameworks, limited AI-specific regulation	Internal governance standards + contractual controls

2. Regional overview

2.1 Three channels of AI governance

The Middle East isn't producing AI regulation through a single legislative instrument comparable to the EU AI Act. Instead, 3 distinct channels are creating the operational governance environment that compliance teams need to navigate.

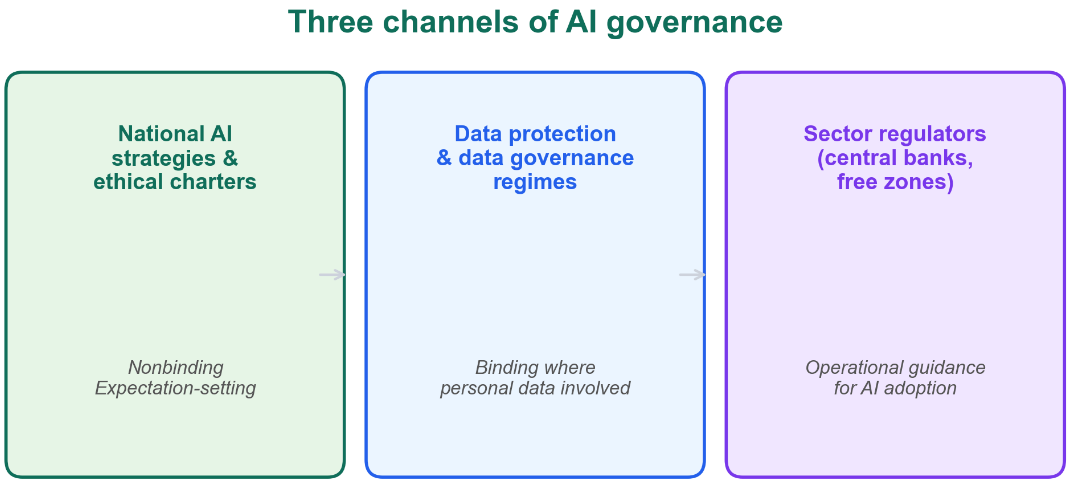

Three channels of AI governance
National AI strategies & ethical charters
Nonbinding
Expectation-setting
Data protection & data governance regimes
Binding where personal data involved
Sector regulators (central banks, free zones)
Operational guidance for AI adoption

Figure: Three channels of AI governance in the Middle East

National AI strategies and ethical charters. Every Tier 1 country and most Tier 2 countries have published national AI strategies, ethical principles, or responsible AI charters. These documents set directional expectations for transparency, fairness, human oversight, and accountability. They are typically nonbinding. But they matter because they shape public procurement requirements, inform regulator expectations, and provide the language that supervisors use during examinations.

Data protection and data governance regimes. The binding core of AI compliance across the region is personal data protection law. The UAE, Saudi Arabia, Qatar, Oman, Egypt, Bahrain, Jordan, and Kuwait all have enacted or are operationalizing personal data protection statutes. For AI systems that collect, process, store, or infer personal data, these laws impose concrete obligations: lawful processing basis, data minimization, security controls, cross-border transfer restrictions, data subject rights, and in some cases DPIAs and automated decision-making safeguards. This is where AI governance becomes enforceable.

Sector regulator AI guidance. Financial regulators are leading operational AI governance in the region. The UAE Central Bank's 2026 guidance note on responsible AI and ML use by licensed financial institutions, the Qatar Central Bank's dedicated AI guideline, and ADGM's rulebook provisions on big data analytics and AI represent the most compliance-specific instruments retrieved in this research. These instruments create supervisory expectations that go beyond what national AI charters alone require: governance frameworks, approval processes, monitoring, transparency, and consumer-facing complaint handling.

2.2 The soft law hardening effect

A pattern visible across Tier 1 countries is what we call "soft law hardening." AI charters and guidelines may be nonbinding as legislation, but they become mandatory in practice through three mechanisms:

- **Public procurement..** Government buyers increasingly reference national AI principles in RFP requirements and vendor evaluation criteria. Oman's Safe and Ethical AI Public Policy and Egypt's Responsible AI Charter both contain language that public-sector procurement teams can operationalize as vendor obligations.
- **Supervisory expectations..** Regulators can incorporate ethical AI principles into their examination frameworks without separate legislation. When a central bank issues AI guidance that references national AI ethics principles, those principles gain regulatory weight for supervised institutions.
- **Contractual flow-down..** Large enterprises and government entities embed AI governance expectations into vendor contracts, effectively making nonbinding national guidance a contractual obligation across supply chains.

For compliance planning purposes, treating soft law instruments as "aspirational only" understates the risk. Organizations operating in Tier 1 jurisdictions should assume that national AI principles will influence regulator behavior, procurement decisions, and contractual expectations.

2.3 Enforcement is arriving faster than legislation

Enforcement across the Middle East is still maturing, but early actions signal where regulators are focusing. Data protection authorities are building enforcement capability, and the first wave of actions is targeting personal data handling, breach notification failures, and cross-border transfer violations rather than AI-specific governance gaps.

Several enforcement patterns are now visible across the region:

- **Free zone data protection enforcement..** The DIFC Commissioner of Data Protection has issued enforcement decisions and guidance notes addressing data handling obligations. ADGM's Office of Data Protection has published compliance guidance and conducted supervisory reviews. These free-zone regulators represent the most structured enforcement capability for data-related AI obligations in the region.

- **Central bank supervisory action..** Financial regulators across the GCC have the strongest operational enforcement levers for AI governance because they can incorporate AI expectations into standard supervisory examination cycles. The UAE Central Bank's 2026 guidance note explicitly creates consumer protection and responsible AI expectations for licensed financial institutions.
- **PDPL enforcement activation..** Saudi Arabia's SDAIA has begun operationalizing PDPL enforcement, and Egypt's executive regulations (Decree 816/2025) are creating a compliance timeline that will activate enforcement pathways. Bahrain's Personal Data Protection Authority has enforcement powers under Law 30/2018.
- **Sector-specific actions..** Telecommunications regulators in Kuwait (CITRA) and broader GCC markets have enforcement authority over data handling in their sectors, creating additional compliance exposure for AI systems that process subscriber or communications data.

The practical takeaway: organizations should not wait for AI-specific enforcement actions before building governance programs. Data protection enforcement is the leading edge, and AI systems that handle personal data are already within scope of active regulators.

2.4 Summary

The Middle East is building AI governance through privacy law, sector regulation, and national strategy rather than a single horizontal AI act. This creates a fragmented but increasingly operational compliance landscape. Privacy law provides the binding baseline. Sector regulators, especially in financial services, add operational specificity. National AI strategies and charters set expectations that harden through procurement, supervision, and contracts. Enforcement is arriving through data protection channels first, with sector-specific AI oversight close behind.

Organizations that wait for "AI-specific legislation" before building governance programs will find themselves behind. The regulation is already here; it's distributed across multiple instruments rather than consolidated in one.

3. Tier 1 country dossiers

3.1 United Arab Emirates

Maturity score: 36/50 (Advanced)

Snapshot.

The UAE's AI governance operates as a multi-layer system: federal strategies and policies set national direction, federal privacy law establishes baseline constraints on personal-data-based AI, and sector regulators plus financial free zones provide the most operationally specific rules. Many AI controls in practice are being enforced as consumer protection and model risk expectations in finance, and as accountability, DPIA, and cross-border transfer constraints under data protection regimes, especially inside DIFC and ADGM.

Institutions and governance centers. At the national level, the UAE Strategy for AI and related national initiatives reference government structures supporting AI implementation. In regulated finance, the most direct operational expectations for AI come from the Central Bank of the UAE via its February 2026 guidance note on responsible AI and ML use by licensed financial institutions. In free zones, DIFC and ADGM operate their own data protection regimes with dedicated enforcement structures.

Key binding laws.

- **Federal Decree-Law No. 45 of 2021 (PDPL):.** Baseline rules for processing personal data, including controller and processor obligations, record keeping, and governance requirements applicable to AI training, fine-tuning, and production uses involving personal data.
- **DIFC Data Protection Law No. 5 of 2020:.** GDPR-style regime applicable in DIFC with dedicated commissioner enforcement structure.
- **ADGM Data Protection Regulations 2021:.** Similarly benchmarked against GDPR, governing processing in ADGM with extensive published guidance, templates, and DPIA frameworks.

AI-specific instruments.

- **UAE Charter for the Development and Use of Artificial Intelligence:.** Policy instrument setting expectations for responsible AI development and use.
- **UAE Strategy for Artificial Intelligence:.** Positions AI as a government modernization and economic initiative.
- **Dubai AI Ethics Principles and Guidelines:.** Published by Digital Dubai Authority, provides a self-assessment oriented principles and guidelines format.
- **National Cloud Security Policy:.** Directly relevant to AI deployments using cloud infrastructure and shared compute.

Privacy and data implications for AI. Privacy compliance for AI splits into three practical tracks: federal PDPL for onshore UAE processing; DIFC data protection for DIFC entities and processing context; and ADGM DPR 2021 for ADGM entities and processing context. For AI projects, this translates to concrete duties around lawful basis, transparency, data minimization, security, DPIAs, and cross-border transfer controls. ADGM's published guidance on automated individual decision-making and profiling is especially relevant to ML decision systems in HR, lending, insurance, and public services, because it summarizes restrictions on decisions with legal or significant effects based exclusively on automated processing.

Sector rules. The Central Bank's Guidance Note on Consumer Protection and Responsible Adoption and Use of AI and ML in Financial Services (February 2026) is the most operationally detailed AI governance instrument in the region. It describes a framework for protecting consumers and structuring trustworthy AI adoption in UAE-licensed financial institutions. For firms in ADGM-regulated activity, the ADGM rulebook includes explicit language on ethics and fair treatment expectations for big data analytics and AI.

Public-sector AI. The UAE emphasizes public-sector digital transformation through national strategy and emirate-level initiatives, including the Dubai Universal Blueprint for Artificial Intelligence. From a compliance standpoint, public-sector AI tightens vendor expectations around documentation, model governance, and transparency because these initiatives tend to be procurement-driven.

Enforcement reality. The clearest enforcement levers are sectoral: the Central Bank governs licensed financial institutions and can supervise against its articulated AI expectations as part of broader compliance and consumer protection frameworks. Data protection enforcement is strongest and most structurally defined inside DIFC and ADGM, with commissioner-style enforcement in their regimes. Federal PDPL enforcement mechanics are evolving.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	5
AI guidance	4
Binding AI-specific	2
Privacy	4
Sector rules	4
Public-sector AI ops	4
Institutions	3
Enforcement	3

Cross-border governance	3
Operational tooling	4
Total	**36/50 (Advanced)**

Compliance takeaways.

Design UAE AI compliance programs as "privacy + regulated sector + procurement readiness," not "AI act compliance." Start by defining AI inventory, model lifecycle controls, human oversight and escalation, and evidence of fairness and transparency, then map controls to the data protection regime applicable to each entity (federal vs DIFC vs ADGM). If operating in financial services, align model governance, transparency, and consumer outcomes to the Central Bank guidance and treat it as supervisory expectation.

Key risks.

Fragmentation risk is real: controls that satisfy DIFC or ADGM expectations may not automatically evidence compliance under federal PDPL (and vice versa), and vendor contracts need to reflect the correct regime and transfer mechanisms. Regulated finance adds additional risk: model controllability and consumer harm management become supervisory concerns, not just internal governance matters.

12-24 month forecast.

Expect the UAE model to continue: more sector-specific AI guidance (finance first, then other regulated sectors), more procurement standardization, and clearer operational linkage between AI governance and data governance controls.

3.2 Kingdom of Saudi Arabia

Maturity score: 35/50 (Advanced)

Snapshot.

Saudi Arabia's AI governance structure is unusually centralized for the region. SDAIA leads both national AI strategy and ethics work and hosts the Personal Data Protection Law and related implementing regulations, positioning personal data governance as a core AI constraint layer. The operational center of gravity is an ecosystem of nonbinding AI ethics and GenAI use guidance, plus binding PDPL obligations that directly affect model training, personalization, profiling, and generative AI deployment patterns.

Institutions and governance centers. Saudi Data and Artificial Intelligence Authority (SDAIA) curates the national AI Ethics Principles, hosts the PDPL text and associated regulations, and acts as the single front door for AI governance, data governance, and privacy governance. This signals that the Kingdom expects organizations to treat these three areas as one integrated compliance problem.

Key binding laws.

- **Personal Data Protection Law (PDPL):.** English text published via SDAIA, with executive/implementing regulations. Constrains dataset collection and reuse, sensitive data handling, transfers, and processor arrangements.

AI-specific instruments.

- **AI Ethics Principles:.** National ethics framework defining roles and responsibilities at national and entity levels, with monitoring and update expectations.
- **Generative AI Guidelines for Government:.** Concrete governance expectations for GenAI adoption in public bodies, covering safety, transparency, privacy, and oversight.
- **AI Adoption Framework:.** Designed to guide entities through adoption practices and measurable implementation.

Privacy and data implications for AI. PDPL makes privacy compliance a first-class risk factor for AI. Practical implications include documenting lawful processing grounds, implementing security controls, structuring processor arrangements, and treating breach and incident handling as regulatory events. For AI programs, this typically means: data provenance and consent management, training data minimization, clear retention policies, and vendor controls for model hosting and inference services.

Sector rules. SDAIA primary sources were prioritized in this research. Sector regulators such as the Saudi Central Bank (SAMA) are referenced inside the PDPL implementing materials. SAMA operates a fintech sandbox and has regulatory oversight of AI applications in banking and financial services. The

Communications, Space & Technology Commission (CST) has authority over telecom and data-related regulations. The National Cybersecurity Authority (NCA) publishes security standards relevant to AI system deployments. A full sector-by-sector extraction is provided in Section 8.1.

Public-sector AI. Saudi's GenAI guidance for government changes the minimum bar for ministries and government entities: it pushes AI adoption toward formal governance, risk management, and documented use cases rather than ad hoc experimentation.

Enforcement reality. SDAIA's central role in publishing PDPL materials indicates regulatory ownership of the privacy regime and the ability to use PDPL enforcement as the main lever affecting AI programs. The AI Ethics Principles are framed as principles and roles rather than an enforcement code, so practical enforcement risk is typically mediated through PDPL violations, sector regulator expectations, or public-sector procurement conditions.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	4
AI guidance	4
Binding AI-specific	2
Privacy	4
Sector rules	3
Public-sector AI ops	3
Institutions	4
Enforcement	3
Cross-border governance	3
Operational tooling	4
Total	**35/50 (Advanced)**

Compliance takeaways.

Treat PDPL compliance as the gating function for AI. Build an AI register tied to data inventories, document model use cases and risks, and ensure GenAI deployment has clear outputs classification (public vs internal vs confidential), human oversight, and incident response procedures that map to PDPL expectations.

Key risks.

Soft law hardening: even if AI ethics documents are not statutes, they can become procurement requirements, supervisory expectations, or evidence benchmarks during investigations. Data handling and transfer constraints are a major practical risk for organizations using cross-border cloud and foundation model services.

12-24 month forecast.

Expect incremental tightening via implementable guidance, procurement rules, and sector regulator integration, with PDPL as the backbone and GenAI guidance as a rapidly iterated layer.

3.3 State of Qatar

Maturity score: 30/50 (Operational)

Snapshot.

Qatar's AI governance is balanced between national strategy, statutory privacy law, and strong sector regulator intervention in finance. The single most compliance-important AI document is the Qatar Central Bank AI guideline, which reads like a supervisory framework for how regulated entities should design, approve, monitor, and explain AI systems. For non-financial sectors, governance is more strategy and principles led, anchored by the National AI Strategy (2019) and national-level AI guidance materials.

Institutions and governance centers. Qatar's AI strategy work is tied to the Ministry of Communications and Information Technology (MCIT), including an AI Committee tasked with overseeing strategy execution and AI initiatives across ministries. In regulated finance, the Qatar Central Bank (QCB) is the operational rule center through its AI guideline and related fintech governance materials.

Key binding laws.

- **Law No. 13 of 2016 on Protecting Personal Data Privacy:.** Hosted on Al Meezan (Qatar legal portal). Shapes AI programs where personal data is processed, particularly around lawful processing, security, and permissions for sensitive categories.

AI-specific instruments.

- **National Artificial Intelligence Strategy for Qatar (2019):.** Sets national direction with AI vision and pillars for adoption.
- **AI principles and guidelines:.** Explicitly described as legally nonbinding and intended for periodic updating, signaling an ethical governance approach.
- **QCB Artificial Intelligence Guideline:.** Targets QCB-licensed entities with governance, controls, and accountability requirements. The most operational AI governance instrument in the country.

Privacy and data implications for AI. Organizations building AI in Qatar should assume that privacy compliance is the main cross-sector constraint, and in finance, privacy is paired with supervisory AI governance. For GenAI and advanced analytics, the highest-risk patterns are: training on customer data, automated profiling and decisioning, and cross-border model hosting that complicates legal control and breach response.

Sector rules. Finance is the most mature sector. The QCB AI guideline and related fintech materials indicate that QCB expects governance frameworks (approval, oversight), technical controls (security, monitoring), and customer-facing transparency and complaint handling. QCB also publishes related data-handling and protection regulation materials, reinforcing that AI programs must be built on disciplined data governance.

Enforcement reality. The highest enforcement likelihood is inside regulated finance because the central bank can incorporate AI governance expectations into standard supervisory activity. Outside finance, enforcement routes are more likely to come through privacy law and sector regulators where applicable.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	4
AI guidance	3
Binding AI-specific	1
Privacy	3
Sector rules	4
Public-sector AI ops	3
Institutions	3
Enforcement	3
Cross-border governance	3
Operational tooling	3

Total	**30/50 (Operational)**

Compliance takeaways.

For multi-country AI programs, treat Qatar as "finance-led." If QCB-regulated, implement AI governance comparable to model risk management: documented approvals, traceable datasets, monitoring, and customer explainability pathways. For non-financial sectors, anchor the program around privacy compliance and publishable AI principles aligned with national guidance.

Key risks.

Regulated entities face the risk of supervisory findings for weak governance, poor transparency, or inadequate human oversight in AI decisions.

12-24 month forecast.

Expect further deepening of finance-sector controls and broader adoption of voluntary principles in public service programs, with privacy law continuing as the baseline.

3.4 State of Israel

Maturity score: 31/50 (Operational)

Snapshot.

Israel's regulatory posture is "responsible innovation via policy and guidance" rather than immediate cross-sector AI legislation. The government has published a formal AI regulation and ethics policy document and practical public-sector guidance for managing AI risk and implementing AI responsibly. The privacy regulator has issued a dedicated guide on privacy-enhancing technologies for AI, bringing privacy engineering into the AI compliance conversation.

Institutions and governance centers. Israel's AI policy was developed by the Ministry of Innovation, Science and Technology and the Ministry of Justice's economic law function. Privacy enforcement and guidance are led by the Privacy Protection Authority, responsible for protecting personal information held in digital databases.

Key binding laws.

- **Protection of Privacy Law, 5741-1981:.** Governs databases and privacy infringements, meaning AI systems that store, enrich, or infer personal data fall into database compliance and security expectations.

AI-specific instruments.

- **AI Policy on regulation and ethics (December 2023):.** Frames AI risks (bias, transparency, human oversight, privacy, vulnerability, safety, accountability) and recommends steps to foster responsibility while supporting innovation.
- **Responsible AI Guide (public consultation draft):.** Sets out best practices and a structured risk management process for government entities deploying AI.
- **PETs for AI guide:.** Explains how privacy-enhancing technologies can mitigate privacy risks across the AI lifecycle.

Privacy and data implications for AI. AI compliance is assessed via privacy and database obligations plus sector-specific requirements rather than a single AI statute. The PETs guidance is a strong indicator that regulators expect technical privacy controls (not only policies) to be deployed where feasible, especially for high-impact AI uses.

Sector rules. The AI policy endorses a sector-based regulatory approach rather than one cross-sector AI regulator. Organizations should track regulator guidance in their domain and treat government AI policy as a harmonizing layer.

Public-sector AI. Israel's public-sector Responsible AI guide is unusually concrete for the region: it targets government bodies, outlines a structured process, and specifies roles and responsibilities in risk management. For companies selling AI to government, procurement evaluation is likely to demand documentation, explainability, risk testing, and ongoing monitoring commitments.

Enforcement reality. Privacy enforcement exists through the Privacy Protection Authority's powers and ongoing regulatory activity. For AI governance, enforcement pressure will come through privacy violations, consumer harms, and sector regulator interventions, with public-sector buyers demanding responsible AI evidence packs.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	4
AI guidance	4

Binding AI-specific	1
Privacy	3
Sector rules	3
Public-sector AI ops	4
Institutions	3
Enforcement	3
Cross-border governance	3
Operational tooling	3
Total	**31/50 (Operational)**

Compliance takeaways.

Build an Israel posture around three artifacts: an AI risk management process (aligned to the public-sector guide's logic), a privacy and database compliance program, and PETs feasibility assessments for high-risk uses.

Key risks.

The main risk is treating Israel as "unregulated." AI risk is being governed through privacy, public-sector procurement expectations, and regulator guidance on technical privacy measures.

12-24 month forecast.

Expect increasing specificity in regulator guidance (especially privacy and public sector) rather than an immediate, EU-style AI Act approach.

3.5 Sultanate of Oman

Maturity score: 28/50 (Operational)

Snapshot.

Oman has published a notably structured set of governmental AI governance documents: a National AI Policy (August 2024) and a Public Policy for Safe and Ethical Use of AI Systems (2025). It also has a binding privacy regime via Royal Decree 6/2022 and detailed national data governance policies for government entities. Oman's AI policy footprint is strong, but sector-by-sector AI regulation is still limited.

Institutions and governance centers. AI policy is issued under the Ministry of Transport, Communications and Information Technology (MTCIT), which also leads data governance frameworks and hosts policy libraries.

Key binding laws.

- **Personal Data Protection Law (Royal Decree No. 6/2022):.** Prohibits processing certain sensitive personal data categories (including biometric and health data) without a permit and sets the Ministry's responsibilities for implementation.

AI-specific instruments.

- **National Artificial Intelligence Policy (2024):.** Establishes general rules and ethical practices for AI systems and mitigating risks and negative impacts.
- **Public Policy for Safe and Ethical Use of AI Systems (2025):.** Framework and ethical guideline for safe adoption, explicitly motivated by rapid AI advances including generative AI.
- **Executive Program for AI and Advanced Technologies:.** Structured implementation roadmap.

Privacy and data implications for AI. The PDPL creates compliance requirements around consent and permitted processing, and for sensitive categories uses a permit-based approach. National Data Governance and Management Policies apply to government units and set requirements for how public-sector entities organize data governance.

Sector rules. Sector-specific AI regulation beyond public-sector policies was not strongly evidenced in primary sources. The highest immediate compliance load for AI comes from PDPL constraints (especially sensitive data) and government data governance requirements where the customer is a government unit.

Enforcement reality. The PDPL assigns implementation responsibilities to the Ministry and references permit-based control for sensitive data processing. Where AI policies are nonbinding, enforcement will more often be contractual (public procurement), reputational, or channeled through privacy law.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	4
AI guidance	4
Binding AI-specific	1
Privacy	4
Sector rules	2
Public-sector AI ops	3
Institutions	3
Enforcement	2
Cross-border governance	2
Operational tooling	3
Total	**28/50 (Operational)**

Compliance takeaways.

Build an AI policy alignment pack for public-sector deployments: explain model governance, human oversight, testing, and data handling choices in the language of the Safe and Ethical AI policy, and ensure PDPL-sensitive categories are addressed explicitly (including permits if required).

Key risks.

Sensitive data and public sector analytics are high exposure. Biometric or health AI systems that skip permits, consent management, or security controls are likely to create hard compliance failures.

12-24 month forecast.

Expect gradual sectorization, especially where public services and critical infrastructure adopt AI and require standardization, while PDPL enforcement capability and implementing instruments mature.

3.6 Arab Republic of Egypt

Maturity score: 27/50 (Operational)

Snapshot.

Egypt's AI governance stance combines strategy, public-sector enablement, and a responsible AI charter with a privacy law backbone that is now being operationalized via executive regulations. The primary AI governance artifacts are hosted on Egypt's official AI portal, and the National Council for AI is positioned as the coordinating body for strategy implementation.

Institutions and governance centers. The National Council for AI is chaired by the Minister of Communications and Information Technology and is responsible for outlining and governing implementation. For data protection, the PDPL framework establishes the Personal Data Protection Center as the supervisory authority.

Key binding laws.

- **Law No. 151 of 2020 (Personal Data Protection Law):.** Includes a licensing and permit architecture and supervisory functions that affect how AI systems collect, store, share, and process personal data.
- **Executive Regulations (Ministerial Decree No. 816/2025):.** Reported issued November 2025 with compliance runway. Specifies procedures, documentation, and compliance timelines.

AI-specific instruments.

- **National AI Strategy (Second Edition 2025-2030):.** Hosted on Egypt's official AI portal.
- **Egyptian Charter for Responsible AI:.** Localizes responsible AI principles and includes concrete public-sector expectations, including that government AI projects should be preceded by thorough impact assessment.

Privacy and data implications for AI. The PDPL and its implementation architecture require licensing and permits for certain personal data processing activities and impose GDPR-style governance obligations (DPO functions, breach and security expectations, cross-border transfer constraints). Training and inference involving personal data will need strong documentation, security evidence, and contract controls.

Sector rules. The most important sector follow-ups are the Central Bank of Egypt perimeter (often excluded or treated differently in data laws) and health data governance in public-sector deployments.

Enforcement reality. The PDPL creates an enforcement pathway through the supervisory Center's powers and the licensing/permit structure. Executive regulations, if fully operationalized, increase enforceability by specifying procedures, documentation, and compliance timelines.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	4
AI guidance	4
Binding AI-specific	1
Privacy	3
Sector rules	2
Public-sector AI ops	3
Institutions	3
Enforcement	2
Cross-border governance	2
Operational tooling	3
Total	**27/50 (Operational)**

Compliance takeaways.

Treat Egypt as "strategy + responsible AI charter + PDPL." Build and be ready to show impact assessments for public-sector deployments, and separate AI data flows into personal vs non-personal, because personal-data-based AI will be subject to PDPL licensing, security, and cross-border constraints.

Key risks.

Uncertainty risk is meaningful: if executive regulations are available but not consistently published through a single official portal, organizations may face uneven interpretations and documentation expectations.

12-24 month forecast.

Expect increased operational enforcement as executive regulations become standardized in market practice and as public-sector AI programs mature and demand stronger evidence packs.

4. Tier 2 country dossiers

4.1 Kingdom of Bahrain

Maturity score: 26/50 (Operational)

Snapshot.

Bahrain's strongest AI-relevant legal layer is its dedicated statutory privacy regime. The Personal Data Protection Authority hosts Law No. 30 of 2018 with Respect to Personal Data Protection, providing a mature baseline for handling personal data used in AI training, personalization, and profiling. For AI-specific governance, Bahrain has pursued a procurement-driven approach, developing AI guidance in collaboration with the World Economic Forum's Centre for the Fourth Industrial Revolution.

Institutions and governance centers. The Personal Data Protection Authority (PDPA) enforces data protection obligations and has been operational since Law 30/2018 took effect. The Information & eGovernment Authority (iGA) leads digital government transformation. The Bahrain Economic Development Board (EDB) promotes technology investment and has positioned Bahrain as a regional fintech and AI hub. Bahrain's Cloud First policy encourages government entities to adopt cloud services, which has implications for how AI systems are deployed and data is governed in the public sector.

Key binding laws.

- **Personal Data Protection Law (Law No. 30 of 2018):.** Comprehensive data protection statute with controller and processor obligations, consent requirements, cross-border transfer controls, and enforcement powers vested in the PDPA.

AI-specific instruments.

- **AI procurement guidance for government (2020):.** Developed in collaboration with the World Economic Forum's Centre for the Fourth Industrial Revolution. While not domestic statute, it influences how government buyers structure requirements for AI vendors and how AI projects are evaluated for sustainability and responsibility.
- **National Policy for the Use of Artificial Intelligence (July 2025):.** Launched by the Information & eGovernment Authority (iGA), with compliance mandatory for all government entities from May 2025. Covers legal compliance, AI use and adoption, public education and awareness, and international cooperation.
- **Draft AI Regulation Law (April 2024):.** The Shura Council unanimously approved a draft standalone AI law with 38 articles, the first in the GCC to define licensing, civil liability, and administrative fines for AI. Penalties include up to 3 years imprisonment or BD 2,000 fines.

Includes provisions for an AI oversight unit, biometric tampering prohibitions, and anti-discrimination rules. Awaiting further legislative action.

- **Cloud First Policy (2017):.** Bahrain was the first Middle East and Africa country to mandate cloud adoption for the public sector, attracting AWS to establish its first regional data center in Bahrain.
- Bahrain adopted the GCC Guiding Manual on the Ethics of Artificial Intelligence Use, coordinated with UNESCO.
- The iGA launched an AI Talent Program (June-December 2025), and the Labour Fund Tamkeen announced training of 50,000 Bahrainis in AI by 2030.
- Bahrain has participated in regional AI initiatives through the GCC and Arab League cooperation frameworks, and the EDB has promoted AI adoption through investment incentives and innovation programs.

Privacy and data implications for AI. Bahrain operates as "privacy-law first" for AI compliance. Organizations building or deploying AI systems that use personal data should align data lifecycle controls to PDPL principles and anticipate oversight from the PDPA, especially around lawful processing, transfer governance, and security. The Cloud First policy adds a layer of cloud governance requirements relevant to AI system deployment.

Sector rules. The Central Bank of Bahrain (CBB) regulates financial services and operates a fintech sandbox that has implications for AI-based financial products. CBB's regulatory framework includes provisions on technology risk management relevant to AI deployments in banking and insurance.

Enforcement reality. The PDPA has enforcement powers under Law 30/2018 and has been building operational enforcement capability. Financial sector enforcement through CBB's supervisory framework provides an additional channel for AI governance compliance in banking and financial services.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	4
AI guidance	3
Binding AI-specific	1
Privacy	4
Sector rules	2
Public-sector AI ops	3
Institutions	3
Enforcement	2
Cross-border governance	2
Operational tooling	2

Total	**26/50 (Operational)**

Compliance takeaways.

Treat Bahrain as privacy-law driven. Align AI data lifecycle controls to PDPL principles. If selling AI to government entities, treat procurement ethics guidance as a de facto standard and produce a vendor-facing documentation pack covering model governance summary, testing evidence, bias and transparency notes, and incident response.

Key risks.

Limited AI-specific regulatory instruments mean compliance requirements may shift as Bahrain develops more concrete AI governance frameworks. Organizations should monitor EDB and iGA publications for emerging guidance.

12-24 month forecast.

Expect further development of procurement-driven AI governance standards and potential alignment with GCC-wide AI cooperation initiatives.

4.2 Hashemite Kingdom of Jordan

Maturity score: 22/50 (Emerging)

Snapshot.

Jordan has made a clear shift into AI governance readiness by combining an AI ethics charter with a binding personal data protection law. The National AI Ethics Charter is available as a bilingual (Arabic/English) PDF hosted by the Ministry of Digital Economy and Entrepreneurship (MODEE), and it includes practical commitments such as integrating AI ethics principles into education and conducting awareness and capacity-building. On the binding side, the Personal Data Protection Law No. 24 of 2023 provides a concrete statutory baseline.

Institutions and governance centers. MODEE leads digital transformation policy and hosts the AI Ethics Charter. The ministry has been active in promoting digital economy initiatives and building institutional capacity for AI governance. Jordan has also established partnerships with international organizations including the World Bank and ITU to support digital transformation and AI readiness programs.

Key binding laws.

- **Personal Data Protection Law No. 24 of 2023:.** Official English translation hosted on a government domain. Provides statutory baseline for lawful processing, controller obligations, and data subject rights applicable to AI systems handling personal data.

AI-specific instruments.

- **National AI Ethics Charter:.** Bilingual PDF with practical commitments including ethics integration in education and capacity-building programs. Approved in 2022 and published through MODEE.
- **National AI Strategy and Implementation Plan (2023-2027):.** Launched November 2022 with 68 targeted projects. Goals include 30% increase in AI researchers, 50 new AI startups, training 15,000 individuals, and deploying AI in 25 government projects by 2027.
- A dedicated AI division was established within MODEE in 2020.
- Jordan has additional AI policy references including an AI policy framework referenced in government communications, though the two most directly actionable instruments are the ethics charter and the PDPL.

Privacy and data implications for AI. Jordan should be treated as "new privacy baseline with ethical AI overlay." Practical near-term work for AI product teams includes classifying data (personal vs sensitive), defining lawful processing basis, implementing notices and consent where required, and operationalizing data subject rights workflows.

Sector rules. The Central Bank of Jordan has issued a regulatory framework for AI in banking, covering fraud detection, customer service, and digital transformation applications. Jordan's telecommunications regulatory commission also has authority extending to AI applications.

Enforcement reality. PDPL Law 24/2023 is still in early enforcement stages. The primary enforcement pathway is through the data protection provisions, with the ethics charter serving as a benchmark for procurement and institutional expectations rather than direct enforcement.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	4
AI guidance	3
Binding AI-specific	1

Privacy	3
Sector rules	1
Public-sector AI ops	2
Institutions	2
Enforcement	2
Cross-border governance	2
Operational tooling	2
Total	**22/50 (Emerging)**

Compliance takeaways.

Classify data (personal vs sensitive), define lawful processing basis, implement notices and consent where required, and operationalize data subject rights workflows. Use the ethics charter to structure internal principles, vendor requirements, and public-sector procurement readiness, but treat it as complementary to statutory compliance.

Key risks.

The PDPL is new and enforcement practices are still forming. Organizations should build conservatively and monitor regulatory guidance for interpretation clarity.

12-24 month forecast.

Expect PDPL enforcement to become operational and ethics charter principles to gain weight through procurement and institutional adoption.

4.3 State of Kuwait

Maturity score: 18/50 (Emerging)

Snapshot.

Kuwait's AI governance is early-stage when looking for dedicated AI law, but comparatively developed on the data and cloud governance layers that AI systems depend on. The Communication and Information Technology Regulatory Authority (CITRA) publishes a Data Privacy Protection Regulation and a Cloud Computing Regulatory Framework that become AI governance instruments in practice because many AI systems are deployed on cloud platforms and rely on large-scale data processing.

Institutions and governance centers. CITRA regulates communications and IT services, including data privacy and cloud governance. The Central Agency for Information Technology (CAIT) has publicly stated it worked on preparing a draft national AI strategy through workshops (including with Microsoft), but a final adopted government PDF for a national AI strategy was not located on an official Kuwait government portal in this research. Kuwait's New Kuwait Vision 2035 includes digital transformation and technology development as strategic pillars.

Key binding laws.

- **CITRA Data Privacy Protection Regulation:.** Applicable across public and private sectors within CITRA's scope.
- **Cloud Computing Regulatory Framework:.** Governs licensed cloud providers and data center requirements, including rules about data storage locations, classification, and cloud provider obligations relevant to AI architectures.

AI-specific instruments.

- **Draft National AI Strategy (2025-2028):.** Prepared by CAIT and published as a strategy document. Goals include establishing an AI Centre of Excellence, centralized data repository, and pilot projects in critical sectors in year 1. By 2028, aims to embed AI across government, healthcare, energy, education, and infrastructure.
- **Microsoft-Kuwait AI Partnership (March 2025):.** Intent to establish first AI-powered Azure Region (in-country cloud). Government deployed Microsoft Copilot across public-sector workforce with a Copilot Center of Excellence. National "Kuwait Skills" training program launched with CAIT.
- AI is positioned as central to Kuwait Vision 2035, emphasizing economic diversification and digital infrastructure.

Privacy and data implications for AI. Design Kuwait deployments around CITRA requirements, especially cloud licensing and data governance. If using hyperscaler LLM APIs or cross-border model hosting, assume modifications may be needed to data flows, storage locations, and contractual terms to align with CITRA's cloud and privacy expectations.

Sector rules. The Central Bank of Kuwait (CBK) regulates financial services and has authority over technology risk management in banking. CITRA's regulatory authority extends to telecommunications providers deploying AI-based services.

Enforcement reality. CITRA has enforcement authority over data and cloud governance within its regulatory perimeter. CBK has supervisory enforcement over financial institutions. AI-specific enforcement is limited by the absence of dedicated AI regulation, but data governance enforcement through CITRA creates indirect compliance exposure.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	3
AI guidance	1
Binding AI-specific	0
Privacy	3
Sector rules	2
Public-sector AI ops	2
Institutions	2
Enforcement	2
Cross-border governance	2
Operational tooling	1
Total	**18/50 (Emerging)**

Compliance takeaways.

Anchor deployments around CITRA data and cloud requirements. Monitor CAIT for the finalization of the national AI strategy. Treat cloud licensing and data governance as the primary compliance layer for AI systems.

Key risks.

Regulatory uncertainty: without a finalized AI strategy or dedicated AI governance instruments, compliance requirements may shift significantly as Kuwait develops its regulatory framework.

12-24 month forecast.

Expect finalization of the national AI strategy and potential development of sector-specific AI guidance, particularly in financial services and government services.

5. Tier 3 country profiles

5.1 Republic of Lebanon

Maturity score: 12/50 (Early)

Snapshot.

Lebanon is building institutional capacity for AI governance faster than its regulatory framework would suggest. The Council of Ministers approved a draft law to establish MITAI (Ministry of Technology and AI), Lebanon's first new ministry since 1993, though it still awaits parliamentary approval. A National Digital Transformation and AI Strategy 2025-2030 was launched at the LTAI Summit, targeting AI and digital initiatives to reach 10% of GDP by 2030 (approximately $3.5 billion, up from $1.3 billion in 2025). The strategy includes a Digi-Tech Foundation, Special Technology Economic Zones, and regulatory sandboxes.

Key instruments.

- **Law No. 81 of 2018:.** Covers electronic transactions and includes personal data protection provisions. Requires DPOs and mandatory impact assessments for high-risk processing including profiling and automated decision-making. Fines range from 1 million to 30 million Lebanese Pounds.
- **MITAI:.** The Council of Ministers approved the draft law to establish MITAI as Lebanon's institutional home for digital transformation and AI. Awaits parliamentary approval.
- **National Digital Transformation and AI Strategy 2025-2030:.** Launched at the LTAI Summit with targets for economic contribution, digital infrastructure, and regulatory sandboxes.

International partnerships and investment. In June 2025, MITAI and Sofrecom Group signed an MoU at VivaTech 2025 for National Digital Infrastructure Transformation. In February 2026, the World Bank approved a $200 million project for digital public services and cybersecurity, signaling international confidence in Lebanon's digital development path.

Compliance posture.

Compliance risk for AI in Lebanon is driven by personal data handling risks under Law 81/2018, which includes specific obligations for automated decision-making and profiling. International organizations (World Bank, UNDP) operating in Lebanon impose additional governance requirements on AI projects they fund or support.

Practical considerations. Lebanon faces structural challenges: brain drain (talent outflows 3-4x higher than inflows), limited broadband speeds (9.21 Mbps fixed, 30.83 Mbps mobile), and under 1% 5G coverage. The Oxford AI Readiness 2025 score places Lebanon 113th globally with a score of 34.38/100. Organizations deploying AI should apply conservative internal controls (privacy-by-design, security controls, documented oversight) and monitor MITAI's development for emerging regulatory requirements.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	2
AI guidance	2
Binding AI-specific	0
Privacy	2
Sector rules	1
Public-sector AI ops	1
Institutions	2
Enforcement	1
Cross-border governance	1
Operational tooling	0
Total	**12/50 (Early)**

5.2 Republic of Iraq

Maturity score: 7/50 (Early)

Snapshot.

Iraq has moved beyond a purely aspirational AI posture. A Supreme Committee for AI was established in August 2024 under PM Al-Sudani, and a National Strategy for Artificial Intelligence (INSAIN) was drafted in 2024, focusing on healthcare, agriculture, tourism, education, and environmental protection. The Ministry of Communications launched Iraq's first national AI platform with a National Data Centre, featuring an open data library and Arabic language models. However, this research didn't surface a standalone personal data protection law comparable to PDPL-style regimes in Tier 1 GCC peers.

Key instruments.

- **Supreme Committee for AI (August 2024):.** Established under PM Al-Sudani to coordinate national AI initiatives.
- **National Strategy for Artificial Intelligence (INSAIN, 2024 draft):.** Focuses on healthcare, agriculture, tourism, education, and environmental protection.
- **AI portal (ai.gov.iq):.** PM advisory office initiative with training platforms and AI program materials.
- **National AI Platform and Data Centre:.** Ministry of Communications launched Iraq's first national AI platform with open data library and Arabic language models.
- **National Development Plan 2024-2028:.** Published with UNDP support, includes technology and digital development as strategic priorities.
- No comprehensive data protection statute comparable to GCC peers was located in accessible primary sources.

Education and talent development. AI was introduced into school curricula in July 2024. A 100 digital leaders training program was announced in November 2024. University programs are expanding: College of AI at University of Baghdad (planned 2025-2026), AI department at University of Mosul (2024-2025), AI Engineering at University of Zakho (September 2024), and American University of Baghdad received $2.1 million in AI grants.

Kurdistan Region. The KRG has its own Digital Transformation Strategy, opened the country's first Tier-3 data center (September 2022), issued 2+ million digital IDs, and Salahaddin University launched Kurdistan's first AI department. This creates a separate regulatory context within Iraq.

Cybersecurity concerns. A 2023 cybersecurity incident resulted in personal data from multiple ministries being leaked. In April 2025, the National Security Service arrested individuals for cyberattacks leaking 1,500 GB of data. These incidents highlight the gap between digital ambition and security infrastructure.

International engagement. UNESCO has trained Iraqi trainers on ethics of AI. The Oxford AI Readiness 2024 score places Iraq 107th globally with a score of 40.91/100.

Compliance posture.

Treat Iraq as "programmatic AI adoption with legal uncertainty." For deployments, apply conservative internal controls (privacy-by-design, security controls, documented oversight) and stronger contractual governance to compensate for uncertainty in statutory AI and privacy layers.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	2
AI guidance	1
Binding AI-specific	0
Privacy	0
Sector rules	0
Public-sector AI ops	2
Institutions	2
Enforcement	0
Cross-border governance	0
Operational tooling	0
Total	**7/50 (Early)**

5.3 State of Palestine

Maturity score: 5/50 (Early)

Snapshot.

Palestine's most directly relevant binding instrument is the Cybercrime Decree-Law No. 10 of 2018, available as a government-hosted translation. This law affects AI deployments indirectly through online content, surveillance, investigation powers, and restrictions relevant to digital services. A personal data protection law appears to still be in draft form, with the most accessible materials being civil society analyses rather than an official draft on a legislative portal.

Key instruments.

- **Cybercrime Decree-Law No. 10 of 2018:.** Government-hosted translation available. Affects digital services and AI deployments indirectly.
- **Draft data protection law:.** Civil society organizations, notably 7amleh (The Arab Center for the Advancement of Social Media), have published analyses of the draft personal data protection legislation, but an official government draft was not located on a legislative portal.

Compliance posture.

Treat Palestine as "cybercrime law present, privacy law incomplete." For AI products, emphasize content moderation, security logging, and careful handling of personal data, and avoid assuming a stable, GDPR-style privacy rights framework exists.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	0
AI guidance	0
Binding AI-specific	0
Privacy	1
Sector rules	0
Public-sector AI ops	0
Institutions	1
Enforcement	1
Cross-border governance	1
Operational tooling	1
Total	**5/50 (Early)**

5.4 Syrian Arab Republic

Maturity score: 4/50 (Early)

Snapshot.

Syria's searchable, accessible legal layer most relevant to AI regulation is cybercrime and online control. Civil society and rights organizations describe Cybercrime Law No. 20 of 2022 as expanding state control over online content and imposing broad obligations and sanctions, which has indirect implications for AI systems that generate or moderate content and for data-access demands.

Key instruments.

- **Cybercrime Law No. 20 of 2022:.** Described in civil society analysis as expanding state control. An official gazette-hosted full text was not retrieved in this research.

Post-regime change developments (late 2024 onward). Syria's new government has made digital reconstruction a central priority. Minister of Communications Abdul Salam Haykal (returned from Silicon Valley exile) aims to position Syria as a digital hub. In February 2025, the SYNC conference in Damascus (the largest Syrian tech conference to date) was organized by Silicon Valley-based Syrian entrepreneurs. Trial launch of 5G services began in Damascus, and installation of the first submarine cable (Medusa system) in Tartus is connecting Syria to the Mediterranean network. Saudi telecom companies signed investment agreements totaling nearly $1 billion for digital infrastructure and cybersecurity. In July 2025, a strategic cooperation agreement was signed with Saudi firm Cypher to rebuild Syria's cyber architecture.

Compliance posture.

Syria presents unique challenges due to political transition and limited institutional capacity. Cybercrime Law 20/2022 is part of the inherited legal infrastructure requiring reform under the new government. AI deployments should apply maximum internal governance standards regardless of local regulatory expectations. International organizations operating in Syria typically impose their own data governance and technology use requirements. The Oxford AI Readiness 2025 score places Syria 163rd globally with a score of 21.53/100.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	1
AI guidance	0
Binding AI-specific	0
Privacy	1
Sector rules	0
Public-sector AI ops	0
Institutions	0
Enforcement	1
Cross-border governance	0
Operational tooling	1
Total	**4/50 (Early)**

5.5 Republic of Yemen

Maturity score: 1/50 (Early)

Snapshot.

We didn't locate a Yemen personal data protection law in accessible primary sources. Yemen has a Law No. 13 of 2012 on the Right of Access to Information, but that is not a privacy or AI governance regime. Civil society analysis explicitly notes the absence of a Yemeni law protecting digital data as a contributing factor to cybercrime.

Key instruments.

- **Law No. 13 of 2012 (Right of Access to Information):.** Not a privacy or AI governance regime.
- No comprehensive data protection law located in accessible primary sources.

Recent developments. The World Bank (June 2025) approved $30 million in grants: $20 million for the Yemen Financial Market Infrastructure and Inclusion Project (digital payments, Fast Payment System, Real Time Gross Settlement System), and $10 million for education. Mobile money is the primary vector for digital financial services; internet connectivity remains severely limited. The Oxford AI Readiness 2025 score places Yemen 191st globally (near bottom) with a score of 13.74/100.

Compliance posture.

Yemen represents a legislative vacuum for AI governance planning. Organizations deploying any AI-based services should apply international best-practice governance standards regardless of local regulatory requirements. The ongoing conflict and political division between internationally recognized government and Houthi-controlled areas create additional governance complexity.

Maturity scoring (0-5 per dimension):

Dimension	Score
Strategy	0
AI guidance	0
Binding AI-specific	0
Privacy	0
Sector rules	0
Public-sector AI ops	0
Institutions	0
Enforcement	0
Cross-border governance	0
Operational tooling	1
Total	**1/50 (Early)**

6. Country comparison and maturity scoring

6.1 Scoring methodology

Each country is assessed across 10 dimensions on a 0-5 scale (maximum 50 points). The dimensions are:

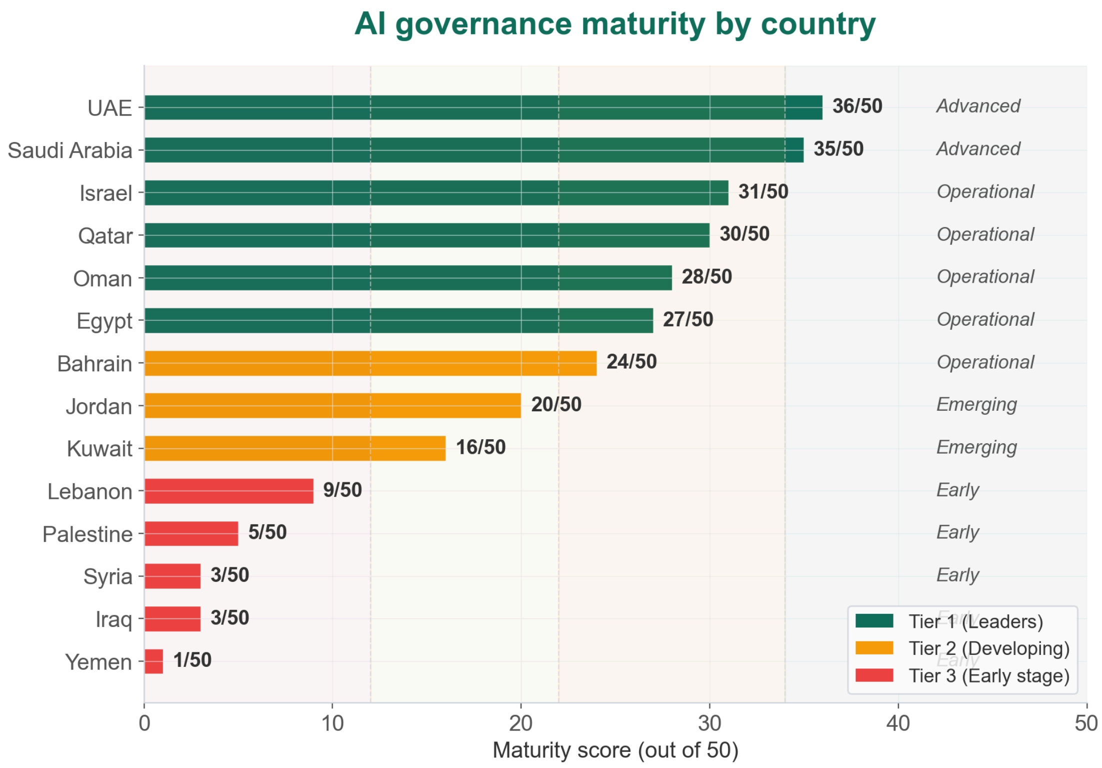


Figure: AI governance maturity scores across 14 Middle East jurisdictions

1. **Strategy:.** Presence and specificity of national AI strategy documents.
2. **AI guidance:.** Published AI-specific guidelines, principles, or ethical frameworks.
3. **Binding AI-specific:.** Existence of legally binding AI-specific regulations or statutes.
4. **Privacy:.** Maturity and enforceability of personal data protection regime.
5. **Sector rules:.** AI-related regulatory guidance from sector regulators (finance, telecom, health).
6. **Public-sector AI ops:.** Government AI procurement standards, responsible AI guides, and operational programs.
7. **Institutions:.** Dedicated bodies, committees, or authorities with AI governance mandates.
8. **Enforcement:.** Demonstrated enforcement capability and activity relevant to AI and data.
9. **Cross-border governance:.** Rules on data transfer, cloud hosting, and cross-border AI operations.
10. **Operational tooling:.** Availability of templates, self-assessment tools, implementation guidance.

Maturity bands:

- **Advanced (35-50):.** Multiple binding and operational instruments, active enforcement, sector-specific guidance.
- **Operational (23-34):.** Binding privacy regime, published AI guidance, emerging enforcement.
- **Emerging (13-22):.** Privacy foundations, limited AI-specific instruments, early-stage enforcement.
- **Early (0-12):.** Partial digital frameworks, no AI-specific regulation, limited enforcement.

6.2 Country comparison table

Country	Score	Band	Posture	Primary anchors
United Arab Emirates	36/50	Advanced	Layered, policy + privacy + finance-led operationalization	AI Charter; federal PDPL; Central Bank AI guidance; DIFC DP law; ADGM DPR 2021
Kingdom of Saudi Arabia	35/50	Advanced	Centralized, SDAIA-led ethics + privacy backbone	SDAIA AI Ethics Principles; PDPL and executive regs; GenAI guidelines for government
State of Israel	31/50	Operational	Soft-law, public sector responsible AI, privacy regulator guidance	AI policy; responsible AI guide (public sector); PETs for AI guide; privacy law
State of Qatar	30/50	Operational	Strategy-led, finance regulator drives practical AI controls	QCB AI guideline; national AI strategy; personal data privacy law
Sultanate of Oman	28/50	Operational	Policy-forward, binding PDPL + national data governance	National AI policy; safe AI public policy; PDPL (RD 6/2022); National Data Governance policies
Arab Republic of Egypt	27/50	Operational	Strategy-led, charter-based responsible AI, PDPL becoming operational	National AI Strategy (2nd ed.); Responsible AI Charter; PDPL law; executive regs 816/2025

Kingdom of Bahrain	26/50	Operational	Privacy-law led, procurement-driven AI governance	Bahrain PDPL; WEF AI procurement guidance; Cloud First policy; National AI Policy; Draft AI Law
Hashemite Kingdom of Jordan	22/50	Emerging	New privacy baseline + AI ethics charter + national AI strategy	AI Ethics Charter (bilingual); PDPL Law 24/2023; National AI Strategy 2023-2027
State of Kuwait	18/50	Emerging	Telecom and cloud regulator sets data rules, AI strategy published	CITRA data privacy regulation; cloud framework; Draft National AI Strategy 2025-2028
Republic of Lebanon	12/50	Early	Digital law includes data provisions, AI institutions emerging, national strategy launched	Law 81/2018; MITAI; National Digital Transformation and AI Strategy 2025-2030
State of Palestine	5/50	Early	Cybercrime law present, data protection still draft	Cybercrime Decree-Law; draft data protection analysis
Republic of Iraq	7/50	Early	Supreme AI Committee, national AI strategy drafted, university programs expanding	AI.gov.iq; INSAIN strategy draft; Supreme Committee for AI; National AI Platform
Syrian Arab Republic	4/50	Early	Post-regime digital reconstruction priority, inherited cybercrime law	Cybercrime Law 20/2022; digital infrastructure investment agreements
Republic of Yemen	1/50	Early	No comprehensive data protection law, limited digital rights baseline	Right of access to information law

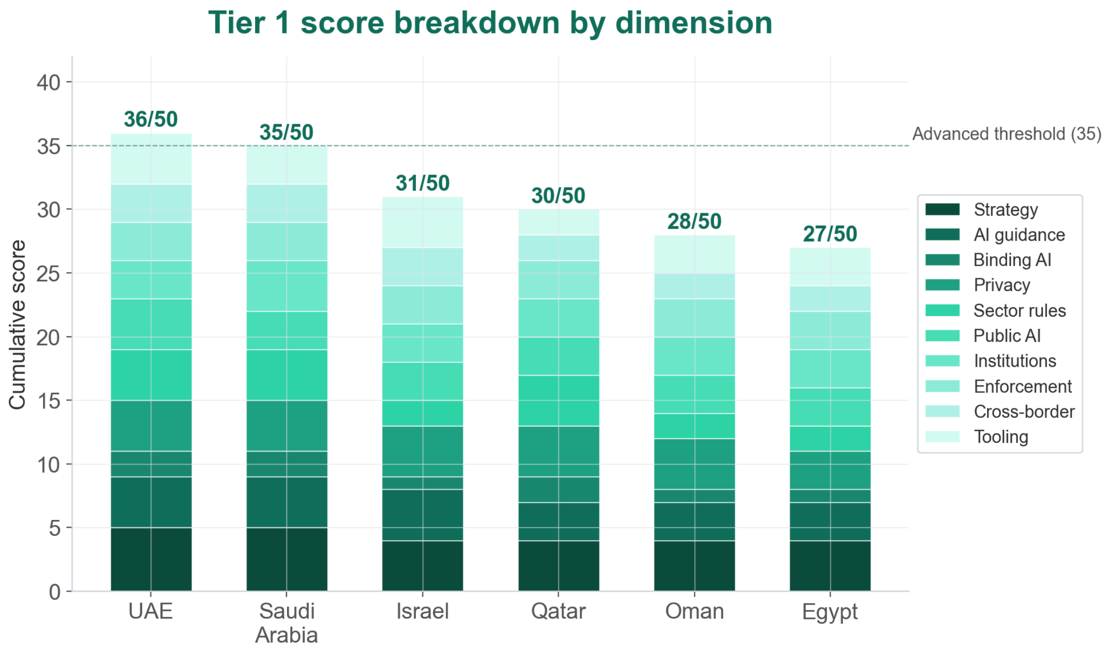


Figure: Tier 1 country score breakdown by governance dimension

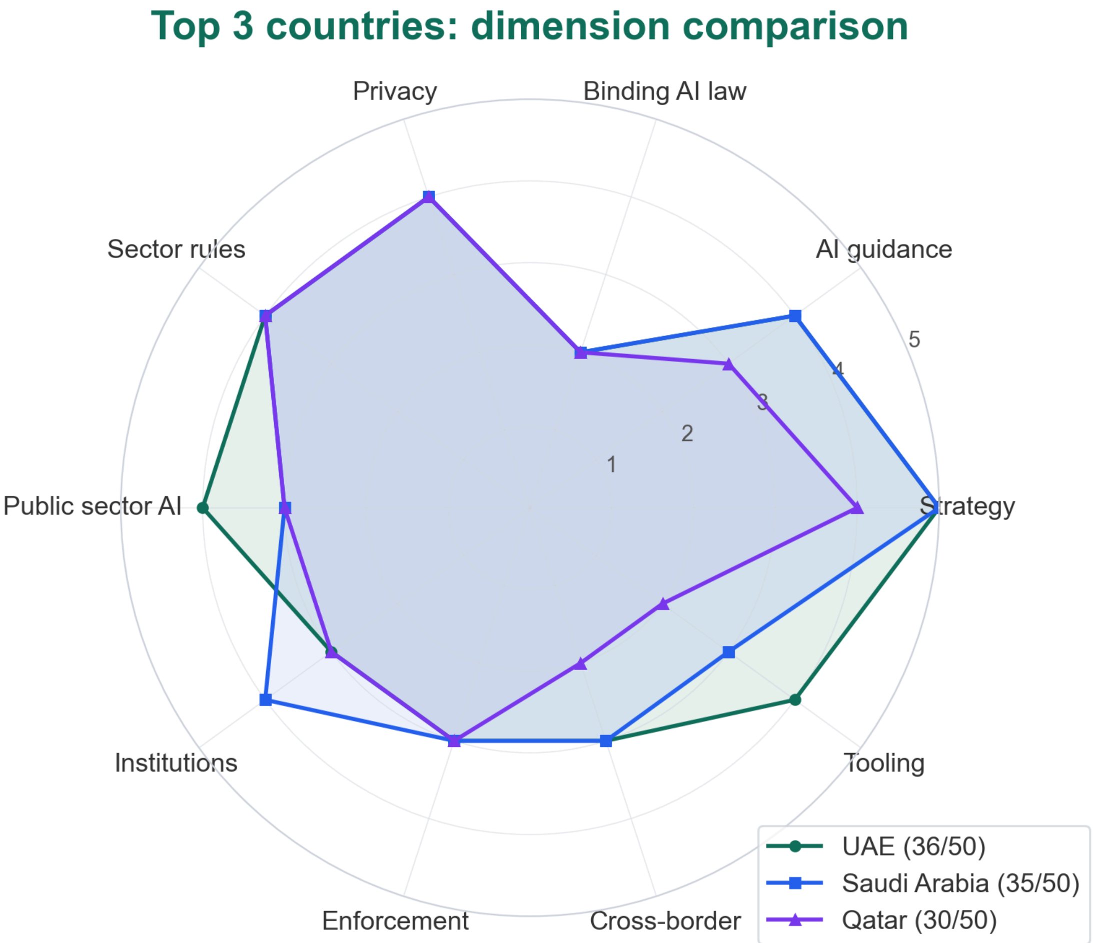
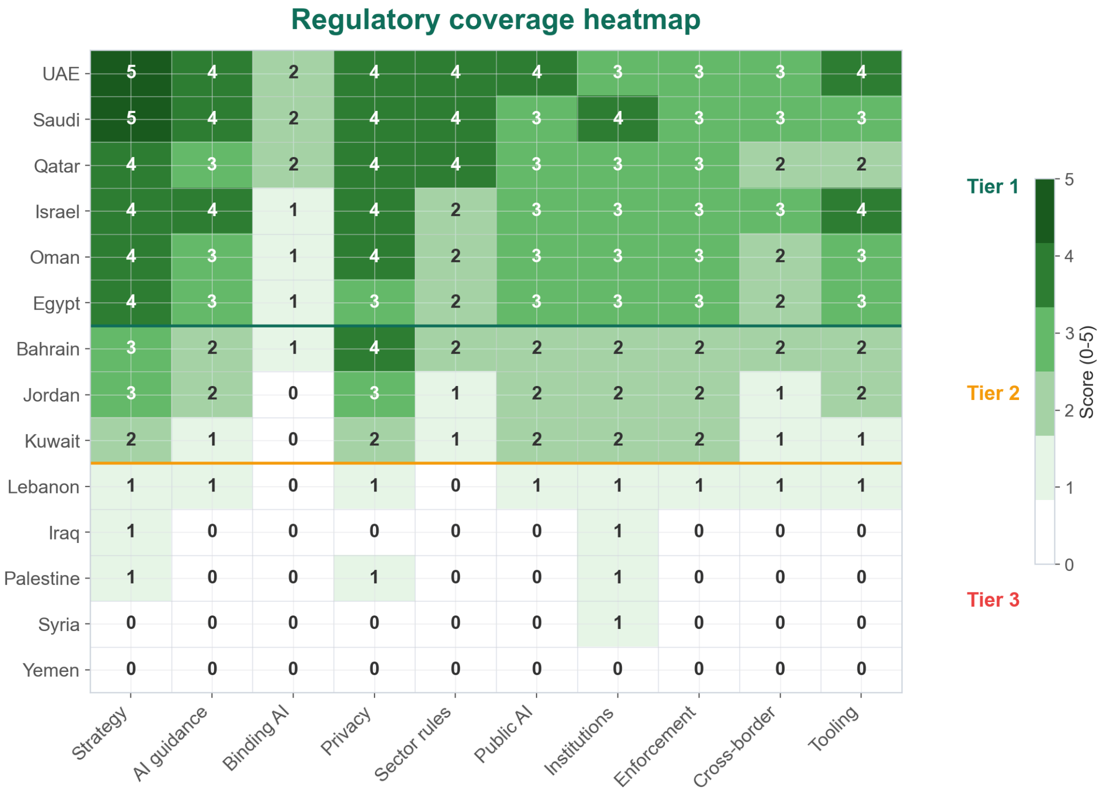


Figure: Radar comparison of top 3 countries across governance dimensions

6.3 Maturity score validation

To validate the scoring methodology, we benchmarked our results against the Oxford Government AI Readiness Index (2024/2025 editions) with actual scores:



	Strategy	AI guidance	Binding AI	Privacy	Sector rules	Public AI	Institutions	Enforcement	Cross-border	Tooling
UAE	5	4	2	4	4	4	3	3	3	4
Saudi	5	4	2	4	4	3	4	3	3	3
Qatar	4	3	2	4	4	3	3	3	2	2
Israel	4	4	1	4	2	3	3	3	3	4
Oman	4	3	1	4	2	3	3	3	2	3
Egypt	4	3	1	3	2	3	3	3	2	3
Bahrain	3	2	1	4	2	2	2	2	2	2
Jordan	3	2	0	3	1	2	2	2	1	2
Kuwait	2	1	0	2	1	2	2	2	1	1
Lebanon	1	1	0	1	0	1	1	1	1	1
Iraq	1	0	0	0	0	0	1	0	0	0
Palestine	1	0	0	1	0	0	1	0	0	0
Syria	0	0	0	0	0	0	1	0	0	0
Yemen	0	0	0	0	0	0	0	0	0	0

Figure: Regulatory coverage heatmap across 14 jurisdictions

Country	Oxford 2024 Global Rank	Oxford 2025 Global Rank	Our Score
UAE	18th (75.66)	19th	36/50
Saudi Arabia	22nd (72.36)	15th	35/50
Israel	~18th (74.52)	--	31/50
Qatar	~32nd (~64)	--	30/50
Oman	45th	61st	28/50
Egypt	--	--	27/50
Bahrain	~57th (~54)	58th	26/50
Jordan	49th (~61)	61st	22/50

Kuwait	~65th (~51)	90th	18/50
Lebanon	~85th (~46)	113th (34.38)	12/50
Iraq	107th (40.91)	~110th	7/50
Palestine	Not listed	--	5/50
Syria	~160th	163rd (21.53)	4/50
Yemen	~185th	191st (13.74)	1/50

The Tortoise Global AI Index 2024 provides additional validation: Saudi Arabia ranked 1st globally for Government AI Strategy, confirming its position as a regional leader. The BCG GCC AI Pulse classifies UAE and Saudi Arabia as "AI Contenders" and Qatar, Kuwait, Oman, and Bahrain as "AI Practitioners."

OECD AI Policy Observatory. The OECD tracks national AI strategies and policy initiatives globally. UAE, Saudi Arabia, Qatar, and Israel are documented in the OECD AI Policy Observatory with comprehensive policy profiles, confirming their advanced governance postures. The Observatory's data on policy instruments aligns with the instrument types documented in our dossiers.

The correlation between our maturity scores and these external indices provides confidence that the scoring methodology captures meaningful differences in governance maturity across the region. Divergences, where they exist, typically reflect our methodology's heavier weighting toward operational and enforceable instruments versus aspirational strategy documents.

7. Sector deep dives

7.1 Financial services

Three regulatory patterns are visible in primary sources.

Pattern 1: Central bank as AI governance driver (UAE). The UAE Central Bank's February 2026 guidance note frames responsible AI as a consumer protection and financial stability issue, creating supervisory expectations for governance, transparency, and oversight in AI use by licensed financial institutions. This is the most operationally detailed AI governance instrument in the region.

Pattern 2: Dedicated AI guideline for regulated entities (Qatar). Qatar Central Bank's AI guideline provides an explicit AI governance architecture for regulated entities, making AI a first-class regulated operational risk topic. The guideline covers governance, approval processes, monitoring, transparency, and customer complaint handling.

Pattern 3: Data protection as AI constraint in free zones (UAE - ADGM/DIFC). Financial free zones like ADGM treat AI and big data analytics as governed activity within compliance and ethics expectations and couple it with GDPR-style data protection regimes that constrain profiling and automated decision-making.

Cross-country implementation. A bank operating across UAE and Qatar can implement one core AI governance policy and annotate it per jurisdiction: add UAE consumer protection and model governance evidence packs, plus Qatar's AI guideline-specific reporting and oversight requirements, plus the relevant data protection regime (federal vs free zone).

7.2 Public sector and procurement

Israel's public-sector Responsible AI guide is one of the region's clearest procedural documents for governments adopting AI, and it reads like a procurement-ready risk management methodology. Oman's Safe and Ethical AI policy and National Data Governance policies indicate a strong whole-of-government governance orientation. Egypt's Responsible AI Charter explicitly signals that government AI projects should use impact assessment, pushing the public sector toward documented, auditable AI adoption.

For vendors, public sector AI in the region often means compliance obligations become contractual and pre-deployment, even if the AI charter is nonbinding as law. Organizations selling AI to government should prepare:

- **Model governance summaries.** documenting purpose, data sources, risk classification, and oversight mechanisms.
- **Testing evidence.** demonstrating fairness, robustness, and accuracy evaluations.

- **Impact assessments.** aligned with the procuring country's responsible AI framework language.
- **Incident response procedures.** mapped to data protection and sector-specific notification requirements.
- **Ongoing monitoring commitments.** including drift detection, performance reporting, and escalation processes.

7.3 Healthcare and life sciences

The region's healthcare AI risk profile is privacy intensive: biometrics, health data, and large-scale profiling are either regulated as sensitive data (Oman explicitly lists biometric and health data and requires permits for certain processing) or are likely to trigger DPIA and automated decision safeguards under GDPR-style regimes (DIFC, ADGM).

A practical healthcare AI compliance approach should include:

- **Dataset provenance controls:.** Document the origin, consent basis, and processing history of all training data involving health or biometric information.
- **Explicit sensitive-data classification:.** Map all data categories to the applicable jurisdiction's definition of sensitive data and apply heightened controls.
- **DPIAs for high-risk processing:.** Conduct data protection impact assessments for AI systems that process health data at scale, make automated decisions about patients, or use biometric identification.
- **Clinical governance integration:.** Document human oversight and escalation procedures, ensuring clinical staff can override AI recommendations and that accountability chains are clear.

8. Regulatory comparison tables

8.1 Saudi Arabia: SDAIA vs sector regulators

Dimension	SDAIA	SAMA (Central Bank)	CST (Telecom)	NCA (Cybersecurity)
Primary role	National AI strategy, ethics, PDPL ownership	Financial sector supervision, fintech sandbox	Telecom and IT regulation	National cybersecurity standards
AI-specific instruments	AI Ethics Principles; GenAI Guidelines for Government; AI Adoption Framework	Technology risk management in banking; fintech sandbox rules	Data localization and telecom governance	Security standards applicable to AI systems
Privacy authority	PDPL text and implementing regulations hosted by SDAIA	Referenced in PDPL implementing materials for financial sector	Telecom data governance	Security controls for personal data
Enforcement lever	PDPL violations; procurement conditions	Supervisory examination; licensing conditions	Telecom licensing and compliance	Cybersecurity incident response
AI governance scope	Cross-sector principles and data protection	Financial institutions, banks, insurance, fintech	Telecom operators, cloud providers	Critical infrastructure, government systems
Binding force	PDPL: binding; AI Ethics: nonbinding	Supervisory expectations: effectively binding for licensed entities	Sector regulation: binding within scope	Security standards: binding for designated entities

Dimension	SFDA (Food & Drug Authority)
Primary role	AI-based medical devices, SaMD, digital health
AI-specific instruments	MDS-G010: Guidance on AI/ML-based Medical Devices (binding for marketing authorization). Requires V&V with quality datasets, transparency, explainability, risk management, lifecycle oversight. ~149 clinical trials approved by late 2024.

Key observation: SDAIA's cross-sector PDPL authority and AI ethics role can overlap with sector regulators' domain-specific authority. For organizations operating across sectors in Saudi Arabia, the practical approach is to treat PDPL as the base layer and add sector-specific requirements as overlays. The GenAI Guidelines for Government create a separate compliance track for public-sector deployments.

SDAIA achieved ISO 42001 certification in July 2024 and became the 3rd country to join the OECD AI Policy Observatory in December 2024, signaling Saudi Arabia's commitment to international AI governance standards alignment.

8.2 Qatar: QCB vs MCIT

Dimension	QCB (Central Bank)	MCIT (Ministry of Communications and IT)
Primary role	Operational AI governance for financial sector	National AI strategy and cross-sector coordination
AI-specific instruments	AI Guideline (detailed operational framework); fintech governance materials; data handling regulation	National AI Strategy (2019); AI principles and guidelines; AI Committee oversight
Governance approach	Prescriptive: governance, controls, approval, monitoring, explainability	Directional: vision, pillars, principles, periodic review
Binding force	Supervisory expectations: effectively binding for QCB-licensed entities	Strategy and principles: nonbinding, influence procurement and institutional expectations
Enforcement mechanism	Standard supervisory examination; licensing review	Institutional coordination; procurement influence
Target audience	Banks, insurance companies, payment service providers, fintech firms	Government ministries, public sector, innovation ecosystem
Data governance linkage	Data Handling and Protection Regulation (QCB); data quality requirements in AI guideline	National-level data governance strategy

National Cyber Security Agency (NCSA). The NCSA published "Guidelines for Secure Adoption and Usage of Artificial Intelligence" (February 2024, v1.0), complementing QCB's financial-sector AI guideline with a security-focused perspective. This creates a 3rd AI governance instrument for Qatar alongside QCB's operational framework and MCIT's strategic direction.

QCB operational requirements. QCB's guideline includes specific enforcement mechanisms: an AI Systems Registry must be maintained and disclosed to QCB annually; pre-approval is required for high-risk AI systems (credit scoring, fraud detection, sensitive data processing); and QCB can demand modification or decommissioning of non-compliant AI systems.

Key observation: Qatar's AI governance split between QCB (operational, sector-specific), MCIT (strategic, cross-sector), and NCSA (security-focused) creates multiple compliance pathways. Financial sector organizations face significantly more detailed and enforceable AI governance requirements than non-financial entities. For non-financial organizations, the MCIT strategy and NCSA security guidelines provide directional guidance but lack the operational specificity of QCB's instruments.

8.3 UAE: Federal vs DIFC vs ADGM

Topic	Federal UAE (onshore)	DIFC	ADGM
Data protection instrument	Federal Decree-Law 45/2021 (PDPL)	DIFC Data Protection Law 5/2020	ADGM Data Protection Regulations 2021
Regulatory style	Federal privacy baseline plus sector regulators	GDPR-style free-zone regime, dedicated enforcement structure	GDPR-style free-zone regime with extensive guidance series and templates
AI-specific governance signals	UAE AI Charter and federal AI strategy direction; finance supervisor guidance	AI governed mostly through data protection plus procurement ethics culture	AI governance intersects with data protection and financial rulebook expectations on big data and AI
Automated decision-making	Dependent on PDPL interpretation and sector rules	Addressed via GDPR-style concepts under DIFC regime (privacy rights, accountability)	Explicitly summarized in ADGM brochure on automated decision-making and profiling
DPIA expectation	PDPL governance duties apply; sector rules may require risk assessment	DPIA-style expectations across GDPR-aligned regime	Strong DPIA emphasis with published guidance

9. Framework mapping

9.1 EU AI Act alignment

The EU AI Act is a single comprehensive, risk-tiered AI regulation, while most Middle East jurisdictions are presently closer to "risk governance by sector and by data law." This matters for multi-jurisdiction programs: organizations that can comply with EU high-risk AI obligations and document them well can often reuse that evidence to satisfy Gulf central banks and government procurement expectations, while still needing to localize privacy, data transfer, and licensing requirements.

9.2 NIST AI RMF mapping

The NIST AI Risk Management Framework (AI 100-1) organizes AI governance into four functions: GOVERN, MAP, MEASURE, and MANAGE. These functions map to Middle East regulatory expectations as follows:

9.3 Practical mapping table

EU AI Act / NIST concept	Tier 1 Middle East practice	Examples
EU AI Act risk-based controls (prohibited, high-risk, transparency duties)	Risk-based governance emerges through finance regulators, public-sector responsible AI guides, and GDPR-style data regimes (DPIAs, automated decision safeguards)	QCB AI guideline; UAE Central Bank AI guidance; Israel public-sector responsible AI guide; ADGM automated decision brochure
NIST GOVERN (accountability, oversight, policies, incident response, supplier management)	Define accountability, oversight roles, policies, incident response, supplier management	UAE Central Bank guidance; Saudi AI Ethics Principles roles; Israel Responsible AI guide roles
NIST MAP (use case context, stakeholders, impacts, data flows)	Map use case context, stakeholders, impacts, and data flows, often pre-procurement	Egypt Responsible AI Charter impact assessment language; Oman safe AI policy framing
NIST MEASURE (testing, validation, bias checks, monitoring, explainability)	Testing, validation, bias checks, monitoring, explainability evidence for regulators and buyers	Israel Responsible AI guide risk management processes; finance regulators expect ongoing monitoring
NIST MANAGE (remediation, change control, decommissioning, incident reporting, consumer recourse)	Remediation, change control, decommissioning, incident reporting and consumer recourse	Central bank governance frameworks and ADGM/DIFC data regimes operationalize incident handling and accountability

10. Enforcement case studies

Enforcement activity across the Middle East is maturing, with documented cases now available across multiple jurisdictions. The following table summarizes specific enforcement actions we've identified:

Jurisdiction	Entity	Date	Fine/Penalty	Violation
ADGM (UAE)	VentureRock Global Ltd	Jun 2023	$20,000	Security breach (phishing, poor cybersecurity)
ADGM (UAE)	Okadoc Technologies Ltd	May 2024	$20,000	Failed data subject access request
DIFC (UAE)	Various entities	2023	323 admin fines ($25K-$50K each)	Non-renewal of notifications, investigation non-compliance
CBUAE (UAE)	Unnamed exchange house	May 2025	AED 200M (~$54.5M)	AML/CTF control failures
Israel	Shirbit Insurance	Nov 2021	ILS 10.7M (~$3.3M)	Cyber-attack, failure to manage cyber-risks
Israel	Data Online (BMC Lean Group)	Nov 2022	NIS 320,000	Illegal trading of personal data of millions
Israel	Tax Authority employee	Dec 2022	NIS 95,000	Misused data access, shared on Facebook
Israel	Elector App	Jan 2021	NIS 25,000	Data breach affecting 6M+ citizens
Israel	Clalit Health Services	Pre-2022	NIS 50,000	Medical data leak
Israel	HOT Telecom	2025	NIS 70,000	First fine under Amendment 13
Israel	National Insurance employee	Aug 2025	NIS 75,000	Unauthorized personal data access
Qatar (NCSA)	ICT sector company	Oct/Dec 2024	Binding Decision No. 1	Inadequate data protection measures

Qatar (NCSA)	Trade/services company	2025	Binding Decision No. 2	Violated Articles 8(3), 13, 14 of PDPPL
Qatar (NCSA)	E-commerce company	Mar 2025	Binding Decision	Consent and safeguards failures
Qatar (NCSA)	Sports sector company	Feb 2026	Binding Decision No. 3	Personal data breach

Israel: most mature enforcement. Israel has the most developed enforcement track record in the region, with 10+ named cases and published fine amounts. The Shirbit Insurance case (ILS 10.7M) remains the largest data protection fine in the Middle East. The HOT Telecom fine is notable as the first penalty under Amendment 13 to the Protection of Privacy Law. Enforcement covers a range of actors, from corporations to individual government employees who misused data access.

Qatar: most active onshore GCC enforcer. The NCSA has issued 5 binding decisions since late 2024, making Qatar the most active onshore GCC data protection enforcer. Companies aren't named in the published decisions, but the violations span sectors (ICT, trade, e-commerce, sports) and target consent failures, inadequate safeguards, and data breaches.

ADGM: named enforcement actions. ADGM has 2 named enforcement actions with published fines, both at $20,000, addressing security failures and data subject rights non-compliance. The DIFC issued 323 administrative fines in 2023 alone, though most were for procedural violations (non-renewal of notifications) rather than substantive data protection failures.

CBUAE: financial sector enforcement. The $54.5 million fine against an unnamed exchange house for AML/CTF control failures signals that UAE financial regulators will impose significant penalties for compliance failures, including those related to AI-dependent transaction monitoring and fraud detection systems.

Jurisdictions without published enforcement. Saudi Arabia, Egypt, Bahrain, Oman, and Jordan don't yet have published enforcement penalties for data protection or AI governance violations. This doesn't mean enforcement won't come. These jurisdictions are building enforcement infrastructure, and organizations should treat their obligations as enforceable.

Regional pattern. Enforcement across the region follows a predictable sequence: (1) data protection authorities build capability and publish guidance; (2) sector regulators incorporate AI expectations into supervisory frameworks; (3) named enforcement actions begin appearing. Israel and Qatar are at stage 3. The UAE free zones (ADGM, DIFC) are at stage 3 for data protection. Most GCC onshore regulators are between stages 1 and 2. Organizations shouldn't wait for enforcement actions in their jurisdiction before building governance programs.

11. Regional milestones timeline

Year	Milestone
2017	UAE AI Strategy 2031 launched (federal strategy)
2018	Bahrain PDPL (Law 30/2018) enacted
2018	Lebanon Law 81/2018 (e-transactions + personal data provisions)
2019	Dubai AI Ethics Principles and Guidelines published
2019	Qatar National AI Strategy launched
2021	UAE Federal PDPL (Decree-Law 45/2021) enacted
2021	ADGM Data Protection Regulations 2021 published
2022	Oman Personal Data Protection Law (Royal Decree 6/2022) enacted
2022	Jordan AI Ethics Charter approved and published
2022	Syria Cybercrime Law 20/2022 enacted
2023	Saudi PDPL English text updated and implementing regulations published via SDAIA
2023	Jordan Personal Data Protection Law No. 24/2023 enacted
2023	Israel AI policy on regulation and ethics published (December 2023)
2024	Oman National AI Policy published (August 2024)
2024	UAE AI Charter published (June 2024)
2024	Qatar Central Bank AI Guideline published (September 2024)
2025	Israel Responsible AI Guide for public sector (public consultation draft)
2025	Oman Safe and Ethical AI Public Policy published (April 2025)
2025	Egypt National AI Strategy (2nd ed. 2025-2030) and PDPL executive regs issued (November 2025)
2026	UAE Central Bank AI/ML consumer protection guidance note (February 2026)

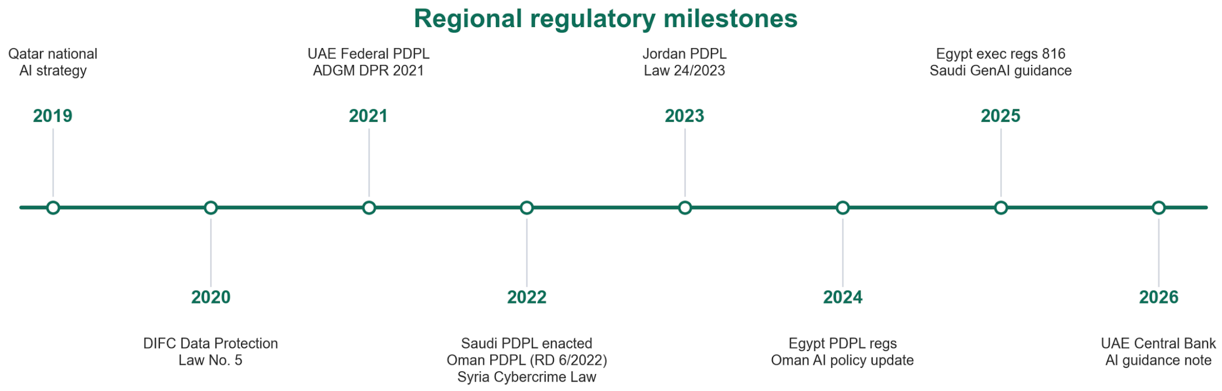

Regional regulatory milestones
Qatar national AI strategy
2019
UAE Federal PDPL ADGM DPR 2021
2021
Jordan PDPL Law 24/2023
2023
Egypt exec regs 816 Saudi GenAI guidance
2025
2020
DIFC Data Protection Law No. 5
2022
Saudi PDPL enacted Oman PDPL (RD 6/2022) Syria Cybercrime Law
2024
Egypt PDPL regs Oman AI policy update
2026
UAE Central Bank AI guidance note

Figure: Regional AI regulatory milestones (2017-2026)

12. Appendix: primary sources and methodology

12.1 Prioritized primary sources

Tier 1 UAE (federal + free zones)

- UAE Strategy for Artificial Intelligence (official UAE platform)
- UAE Charter for the Development and Use of AI (UAE legislation platform)
- Federal Decree-Law 45/2021 on Protection of Personal Data (PDF)
- Central Bank AI/ML guidance note (February 2026, PDF)
- DIFC Data Protection Law 5/2020 (PDF)
- ADGM Data Protection Regulations 2021 and guidance set

Tier 1 Saudi Arabia

- SDAIA AI Ethics Principles (PDF)
- Personal Data Protection Law, English text (PDF)
- Executive Regulations (PDF)
- Generative AI Guidelines for Government (PDF)
- AI Adoption Framework (PDF)

Tier 1 Qatar

- QCB Artificial Intelligence Guideline (PDF)
- Law No. 13 of 2016 on Protecting Personal Data Privacy (Al Meezan PDF)
- National AI Strategy for Qatar (2019, MCIT PDF)
- MCIT AI Committee page

Tier 1 Israel

- Israel AI Policy on regulation and ethics (PDF)
- Responsible AI Guide for public sector (public consultation draft PDF)
- PETs for AI guide (PDF)
- Protection of Privacy Law 5741-1981 (government PDF translation)

Tier 1 Oman

- National AI Policy (PDF)
- Public Policy for Safe and Ethical Use of AI Systems (PDF)
- Personal Data Protection Law (Royal Decree 6/2022, text)
- National Data Governance and Management Policies (PDF)

Tier 1 Egypt

- National AI Strategy, Second Edition 2025-2030 (PDF)
- Egyptian Charter for Responsible AI (PDF)
- PDPL Law 151/2020 (Arabic PDF copy)
- Executive regulations reporting (Decree 816/2025)

Tier 2 Bahrain

- Bahrain PDPL (Law 30/2018, PDF)
- Bahrain AI portal (AI procurement guidance reference)

Tier 2 Jordan

- AI Ethics Charter (bilingual PDF, MODEE)
- PDPL Law 24/2023 official English translation

Tier 2 Kuwait

- CITRA Data Privacy Protection Regulation (PDF)
- Cloud Computing Regulatory Framework (PDF)
- CAIT AI strategy workshop reference

Standards and comparative anchors

- EU AI Act (Regulation (EU) 2024/1689, EUR-Lex)
- NIST AI RMF 1.0 (NIST AI 100-1)

12.2 Source gaps and limitations

Egypt (executive regulations official publication). Strong evidence of issuance was found, but a stable government-hosted PDF of the executive regulations was not located. This should be treated as a priority retrieval task.

Syria (full text of Cybercrime Law 20/2022). An official gazette-hosted law text was not retrieved. Evidence relied on analysis sources describing the law.

Yemen (data protection statute). No comprehensive personal data protection law was located in accessible primary sources.

Palestine (personal data protection law). Civil society analysis of a draft was found, but not an official draft publication on a legislative portal.

12.3 Methodology notes

This report was compiled through systematic retrieval and analysis of primary legal sources, government-published strategy documents, regulator guidance notes, and supplementary analysis from recognized legal databases and policy organizations. Sources were prioritized in the following order: (1) official government portals and legislation databases; (2) regulator-published guidance and frameworks; (3) recognized international organization publications (OECD, World Bank, WEF); (4) established legal analysis from reputable firms and civil society organizations.

Maturity scores were developed using a consistent 10-dimension framework applied across all 14 jurisdictions and validated against external benchmarks including the Oxford Government AI Readiness Index, OECD AI Policy Observatory data, and Stanford HAI AI Index publications.

About VerifyWise

VerifyWise is an open AI governance platform built for regulated industries. It connects policy frameworks, risk workflows, testing, evidence collection and reporting across the AI lifecycle. Organizations use it to align with frameworks like the EU AI Act, ISO 42001 and sectoral standards while keeping their existing infrastructure intact.

Flexible deployment models, API-first architecture and strong evidence capabilities help teams in finance, healthcare, energy and public sectors move from fragmented governance to a unified, audit-ready environment.

Website: https://verifywise.ai

Contact: hello@verifywise.ai