

keypoint

AI Flash

October 2026

GCC

Kingdom of Saudi Arabia (KSA)

SDAIA highlights role of standards in operationalising

On **14 October 2026**, the Saudi Data and AI Authority (SDAIA) participated in Saudi Arabia's 10th Standards Forum, held under the theme "Standards and Artificial Intelligence: Empowering Applications and Building Trust". Saudi Arabia has issued more than 10 AI regulatory frameworks and tools and adopted 23 national AI-related standards covering areas including governance, management systems, training-data quality, safety, robustness, security and privacy. SDAIA emphasised that while policies and regulatory frameworks establish what AI systems should achieve, standards provide measurable requirements for implementation and verification.

Saudi Arabia is increasingly connecting AI policy with technical standards and measurable assurance. Organisations should therefore look beyond high-level responsible-AI principles and assess whether their governance, management systems, training data, safety, security and privacy controls can be evidenced against applicable national and international standards.

Kingdom of Bahrain

iGA highlights AI governance in digital public services

On **2 October 2026**, Bahrain's Information & eGovernment Authority (iGA) participated in a panel discussion on governing social housing in the digital era, with a focus on leveraging digital transformation and AI. iGA highlighted the role of advanced technologies in improving government performance and service outcomes, alongside the importance of governance as AI and digital technologies become more integrated into public-service delivery.

While this does not introduce a new AI-specific regulation, it reflects Bahrain's continued implementation-led approach to AI governance. Organisations embedding AI into public-facing or regulated services should ensure that technology adoption is accompanied by governance, accountability, data protection and appropriate human oversight.

The United Arab Emirates

FedAI rollout and regulatory intelligence progress reviewed

On **13 October 2026**, the UAE's Ministerial Council for Artificial Intelligence and Development reviewed progress on **FedAI**, the national technical ecosystem for agentic AI. The council considered plans to connect federal ministries and entities to the ecosystem, train government employees on agentic AI tools and models and progressively roll out AI agents. It also reviewed agentic AI projects under development in areas including regulatory intelligence and strategic government work.

The UAE is moving towards a common technical ecosystem for agentic AI across government rather than deploying individual AI agents in isolation. Organisations pursuing similar models should consider enterprise-wide controls around agent identity, permissions, system access, human approval points, monitoring, auditability and accountability for AI-performed actions.

Qatar

Digital sovereignty and AI legislation focus

On **19 October 2026**, Qatar's Amir ratified Cabinet Decision No. 34 of 2026 reorganising selected administrative units within the Ministry of Communications and Information Technology (MCIT). The new structure establishes a **National Centre for AI** to support AI projects and applications across Qatar, alongside a training and digital capacity development department. MCIT stated that the changes are intended to strengthen institutional efficiency and the governance model for Qatar's digital sector.

The creation of a dedicated national AI centre marks an important institutional development in Qatar's AI governance landscape. Organisations should monitor the centre's future mandates, programmes and guidance, particularly where these may influence national AI adoption, standards, government use cases and governance expectations.

Kuwait

CITRA emphasises responsible adoption of agentic AI

On **7 October 2026**, Kuwait's Communications and Information Technology Regulatory Authority (CITRA) highlighted the importance of the responsible adoption of agentic AI during the launch of the Agentic AI Experience 2026. CITRA described agentic AI as systems capable of carrying out multi-step activities using tools and permissions to achieve defined objectives, while emphasising that their results should remain subject to human oversight.

Kuwait's regulator is beginning to distinguish agentic AI from conventional AI applications and explicitly link autonomy with human oversight. Organisations experimenting with AI agents should define what tools and data agents can access, establish approval and intervention points and maintain accountability for outputs and actions before deploying them into critical workflows.

Sultanate of Oman

Second phase of national digital economy programme expands AI adoption

On **22 October 2026**, Oman's Ministry of Transport, Communications and Information Technology (MTCIT) launched the second phase of the National Digital Economy Programme. AI is one of eight executive programmes and the new phase seeks to expand AI adoption across strategic economic sectors. MTCIT also highlighted plans for dedicated AI data centres with capacity of up to 500 MW and launched a strategic intelligence platform with the World Economic Forum to support data- and knowledge-driven policymaking.

Oman is linking AI adoption, infrastructure, national capability and policymaking within a wider economic programme. Organisations should therefore consider AI governance alongside infrastructure resilience, data requirements, sustainability, workforce capability and the controls required to move AI from experimentation into scaled operational deployment.

International

European Union

First harmonised standard supporting the EU AI Act published

On **19 October 2026**, the European Commission published in the Official Journal the reference to EN 18286:2026 – Artificial intelligence – Quality management system for EU AI Act regulatory purposes, the first harmonised standard supporting implementation of the AI Act. Providers implementing the standard benefit from a presumption of conformity with the Article 17 quality-management-system requirements covered by the standard. EN 18286 is lifecycle-based and has been designed so it can be layered onto existing management systems such as ISO/IEC 42001, ISO 9001 and applicable sector-specific quality systems.

This is an important transition from legal requirements taken from the AI Act towards practical compliance standards. Organisations developing high-risk AI systems for the EU market should start mapping existing quality-management arrangements against EN 18286 and determine whether it can be incorporated into established ISO or sectoral management systems rather than creating a separate AI compliance structure.

United States

NIST, NSA and CISA publish AI incident-readiness practices

On **16 October 2026**, NIST, the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) published ten (non-mandatory) key practices for incident readiness and response during the training and evaluation of highly-capable AI systems. The practices cover five stages – preparation, detection, response, recovery and reporting – and specifically address situations where AI agents take significant uninstructed actions that compromise task boundaries, technical controls or human oversight.

The guidance signals that AI incident management is becoming a distinct governance discipline. Organisations developing or testing highly autonomous systems should adapt existing incident-response processes to address AI-specific scenarios, including unexpected agent activity, containment failures, evidence preservation, shutdown procedures, recovery from verified baselines and near-miss reporting.

India

IndiaAI and World Bank focus on evidence-based AI scaling

On **8 October 2026**, India's Ministry of Electronics and Information Technology and the IndiaAI Mission jointly hosted the Indian launch of the World Bank Group's World Development Report 2026: The Promise of Artificial Intelligence. The report sets out an "adoption, adaptation and advancement" framework for developing economies, while discussions in India focus on moving AI initiatives from isolated pilots towards evidence-based deployment at scale across sectors.

As public and private AI programmes in India expand, organisations should ensure that evidence of effectiveness, data quality, safety, inclusion and measurable outcomes develops alongside technical deployment.

Singapore

Government sets out risk-based approach for frontier and agentic AI

On **6 October 2026**, Singapore's Ministry of Digital Development and Information outlined its approach to increasingly capable and autonomous AI systems in response to parliamentary questions on pre-deployment access to frontier models. The government emphasised a risk-based, multi-layered approach based on the sensitivity of data and systems, AI autonomy and the severity and ability to remediate potential harms. For higher-risk applications, it identified stronger testing, independently verifiable evidence, tighter deployment controls and (potentially) tighter regulatory oversight as possible safeguards, while confirming that mandatory pre-deployment government access to frontier models is not currently required.

Singapore is developing a differentiated governance model in which safeguards increase with AI autonomy and potential impact. Organisations should similarly avoid applying one governance baseline to every AI use case and should strengthen testing, access controls, monitoring, human accountability and incident-management arrangements as risk increases.

China

State Council issues guidelines addressing AI-related employment risks

On **23 October 2026**, China issued guidelines on adapting to AI advances while promoting employment-friendly development. The guidelines contain 18 tasks across six areas, including job creation, employment-friendly AI adoption, digital skills, employment services, social-security protections and the monitoring of AI-related employment risks. They call for mechanisms to assess employment displacement risks and for stronger protection of workers' rights in human-machine collaboration.

China is bringing workforce and social impacts directly into its AI policy framework. Organisations undertaking large-scale AI-enabled automation should consider workforce impact assessments, reskilling, human-machine operating models and employment-related risks alongside conventional technical and compliance assessments.

Australia

AI Safety Institute examines "epistemic safety" in advanced AI oversight

On **8 October 2026**, Australia's AI Safety Institute published research commissioned from the Commonwealth Scientific and Industrial Research Organisation (CSIRO) on epistemic safety in scalable oversight. The research examines how highly-capable AI systems could provide technically correct answers while framing or presenting information in ways that influence the beliefs of the human or AI system overseeing it. The report argues that assurance should examine not only whether AI completed a task correctly but also whether explanations, recommendations and other outputs create unintended influence.

The research identifies an emerging limitation of conventional AI testing: accuracy alone may not establish that a system is behaving consistently with its intended purpose. Organisations using AI for advice, recommendations or autonomous decisions should consider whether assurance tests examine framing, influence, objective fidelity and human-overseer robustness in addition to correctness.

United Kingdom

Government accepts all 44 AI-in-healthcare regulatory recommendations

On **6 October 2026**, the UK government accepted all 44 recommendations made by the National Commission into the Regulation of AI in Healthcare and set out initial delivery priorities and next steps. The response supports a more proportionate, risk- and lifecycle-based framework; clearer responsibilities for the safe management of AI across the healthcare system; improved transparency and predictability; and stronger post-market monitoring. The Medicines and Healthcare products Regulatory Agency (MHRA) also opened the next phase of its AI Airlock regulatory sandbox for AI-enabled medical devices.

The UK is now moving from recommendations to implementation of a lifecycle-based AI assurance model in healthcare. Healthcare organisations and AI developers should prepare for stronger expectations around real-world evidence, post-deployment monitoring, change management, organisational accountability and safe procurement and deployment of evolving AI products.

United Nations

Co-chairs appointed for next Global Dialogue on AI governance

On **16 October 2026**, the President of the UN General Assembly appointed the Permanent Representatives of Saint Kitts and Nevis and the Republic of Korea as co-chairs of the Global Dialogue on Artificial Intelligence Governance to be held in New York in 2027, pursuant to General Assembly Resolution 79/325.

The Global Dialogue is becoming an ongoing element of international AI-governance architecture rather than a one-off event. Organisations operating internationally should continue monitoring these multilateral processes as global expectations around AI safety, accountability and cross-border governance develop.

Want to understand your organisation's exposure to AI-related risks?

Take Keypoint's AI Risk Exposure Assessment to evaluate your current AI risk profile and identify areas that may require greater governance, oversight and control.

AI Risk Exposure Assessment

Contact Keypoint's technology consulting team

Srikant Ranganathan
Executive Director
srikant.ranganathan@keypoint.com

Darrshan Manukulasooriya
Executive Manager
d.manukulasooriya@keypoint.com

Sagar Rao
Executive Manager
sagar.rao@keypoint.com

Mahesh Girish
Assistant Manager
mahesh.girish@keypoint.com

Talal Alqahtani
Consultant
talal.alqahtani@keypoint.com