Kiteworks

MIDDLE EAST EXECUTIVE SUMMARY

Data Security and Compliance Risk: 2026 Forecast Report

56% See the Risk, 19% Control It: Why Middle East AI Vendor Governance Is All Awareness, No Action

Five Gap-Driven Predictions for UAE and Saudi Arabia

Middle Eastern enterprises have moved decisively on data sovereignty. Organisations across the UAE and Saudi Arabia have invested heavily in sovereign cloud infrastructure, regional data residency, and localised compliance frameworks. These investments position the region as a leader in controlling where data lives. But controlling where data lives is not the same as controlling how data is used, who accesses it, or what happens when something goes wrong.

The survey data reveals a troubling pattern: sovereignty progress masks governance gaps. AI workloads operate without dedicated incident response coverage. Third-party AI vendors process sensitive data without kill-switch mechanisms or jointly tested playbooks. Software supply chain controls vary dramatically by country and sector. Compliance automation remains incomplete, leaving organisations unable to demonstrate—in real time—that their sovereign infrastructure meets regulatory expectations. Sovereignty without governance is a foundation without walls.

This regional analysis draws from a survey of 225 security, IT, compliance, and risk leaders globally, with specific breakouts for the UAE and Saudi Arabia. The findings reveal that despite strong infrastructure investments, critical governance gaps persist in AI incident response, vendor controls, supply chain security, compliance automation, and AI risk awareness. Five predictions emerge—not as criticisms of sovereignty progress, but as warnings about the gaps that sovereignty alone cannot close.

Five Predictions for the Middle East in 2026

1. AI-specific incident response will remain uneven across UAE and Saudi Arabia
2. Third-party AI vendor risk will be recognised but under-controlled
3. Software supply chain maturity will be sector- and country-skewed
4. Compliance automation and evidentiary readiness will stay incomplete
5. Key AI risks will be under-weighted in critical environments

Middle East Governance Gaps: Where Sovereignty Doesn’t Reach

Governance Capability	Global	UAE	Saudi Arabia
AI anomaly detection	40%	54%	32%
AI training-data recovery	47%	58%	36%
Joint AI vendor IR playbooks	13%	19%	12%
AI vendor kill-switch capability	~20%	24%	16%
SBOM management	28%	38%	22%
Automated compliance (policy-as-code)	43%	52%	38%

***Green** = above global average. **Yellow** = at or below global average, indicating governance gap.*

Five Gap-Driven Predictions for the Middle East in 2026

Prediction #1: AI-Specific Incident Response Will Remain Uneven Across UAE and Saudi Arabia

By 2026, AI incident response capabilities will vary dramatically across the Middle East, with UAE organisations advancing while Saudi Arabia trails global benchmarks—creating a fragmented regional posture.

AI Incident Response Capability	Global	UAE	Saudi Arabia
AI anomaly detection	40%	54%	32%
AI training-data recovery	47%	58%	36%
AI-specific IR processes	~35%	46%	28%

The data reveals a 22-point gap in AI anomaly detection between UAE (54%) and Saudi Arabia (32%). For training-data recovery, the gap is equally stark: 58% vs. 36%. These aren’t minor variations—they represent fundamentally different levels of preparedness for AI incidents. When AI systems behave unexpectedly or training data is compromised, UAE organisations will detect and recover while Saudi organisations struggle to understand what happened.

This country-level disparity creates regional risk. Multinational organisations operating across both countries will face inconsistent AI governance. Regulators assessing regional compliance will see uneven capabilities. Partners evaluating Middle East operations will find different levels of AI incident maturity depending on which country hosts the workload. Sovereignty investments have unified where data lives; AI governance gaps fragment how it’s protected.

The Gap

In the UAE, **46%** of organisations lack AI anomaly detection—meaning AI workloads operate without dedicated incident response coverage. In Saudi Arabia, **68%** lack this capability.

Opportunity

Establish AI-specific incident response as a prerequisite for AI deployment, not an afterthought. Close the UAE-Saudi gap through shared regional standards and cross-border capability building.

Prediction #2: Third-Party AI Vendor Risk Will Be Recognised But Under-Controlled

By 2026, Middle Eastern enterprises will identify third-party AI vendor handling as a top data security concern, but most will still lack the controls—kill switches, joint playbooks, continuous monitoring—to manage that risk.

Third-Party AI Control	Global	UAE	Saudi Arabia
Third-party AI vendor handling (concern)	42%	**56%**	**48%**
Joint incident response playbooks	13%	19%	12%
Kill-switch capability for AI vendors	~20%	24%	16%
Continuous vendor risk monitoring	35%	44%	32%

The gap between concern and control is striking. In the UAE, 56% of organisations cite third-party AI vendor handling as a top concern—14 points above global average. In Saudi Arabia, 48% share this concern. Yet the controls tell a different story: joint incident response playbooks sit at just 19% (UAE) and 12% (Saudi Arabia). Kill-switch capabilities—the ability to immediately terminate a vendor's data access—remain minority controls at 24% and 16%, respectively.

This disconnect has real consequences. When an AI vendor experiences a breach or behaves unexpectedly, organisations without joint playbooks scramble to coordinate response. Without kill switches, they can't immediately cut off data access. Regulators in government, financial services, and energy—the sectors most dependent on AI vendors in the Middle East—will increasingly demand evidence that these controls exist. High awareness without matching controls leaves boards exposed and regulators unconvinced.

Opportunity

Convert concern into control. Make joint incident playbooks and kill-switch capabilities standard requirements for AI vendor contracts, especially in regulated sectors. Awareness without action is just documented negligence.

Prediction #3: Software Supply Chain Maturity Will Be Sector- and Country-Skewed

By 2026, software supply chain security will vary dramatically across the Middle East—with UAE leading in some controls, Saudi Arabia lagging globally, and critical gaps persisting even among leaders.

Supply Chain Control	Global	UAE	Saudi Arabia
SBOM management	28%	38%	22%
Secure SDLC	41%	52%	34%
Third-party code scanning	44%	56%	38%
Zero-trust software deployment	~35%	42%	28%

The UAE-Saudi gap in supply chain controls mirrors the AI governance disparity. SBOM management: UAE at 38%, Saudi Arabia at 22%—a 16-point gap and 6 points below global average. Secure SDLC: UAE at 52%, Saudi Arabia at 34%—an 18-point gap with Saudi trailing global by 7 points. This creates a two-speed supply chain posture within the same region, with dramatically different capabilities depending on which country hosts the software development.

Even UAE's relative leadership masks incomplete coverage. At 38% SBOM management, 62% of UAE organisations can't fully inventory the components in their software. At 42% zero-trust deployment, 58% still deploy software based on implicit trust. Regulated sectors—financial services, government, energy—may show stronger numbers, but less regulated sectors drag down regional averages and create exploitable gaps in interconnected supply chains.

The Gap

Saudi Arabia trails global benchmarks on every supply chain metric. Even UAE's leadership leaves more than half without SBOM coverage. Regional supply chains are only as secure as their weakest links.

Opportunity

Establish regional supply chain standards that bring Saudi Arabia to global benchmarks while pushing UAE toward complete coverage. Make SBOM requirements a condition of government and critical infrastructure procurement across both countries.

Prediction #4: Compliance Automation and Evidentiary Readiness Will Stay Incomplete

By 2026, a large portion of Middle Eastern enterprises will still rely on manual or partially automated processes for compliance evidence—making it difficult to demonstrate in real time that sovereignty requirements are actually being met.

Compliance Approach	Global	UAE	Saudi Arabia
Automated/policy-as-code	43%	52%	38%
Continuous/partial automation	32%	30%	34%
Periodic manual audits	10%	8%	14%
Without full automation	**57%**	**48%**	**62%**

Middle Eastern enterprises have invested heavily in demonstrating where data lives—sovereign cloud, regional residency, local data centres. But demonstrating compliance with how data is used requires continuous, automated evidence. In the UAE, 48% of organisations lack full compliance automation. In Saudi Arabia, 62% rely on partial or manual processes. When regulators or boards ask for real-time evidence of data governance, most Middle Eastern organisations will scramble to produce it.

This gap undermines sovereignty investments. What value is sovereign infrastructure if you can't prove—in real time—that it meets regulatory expectations? Regional and sector-specific requirements around data residency, operational resilience, and AI governance increasingly demand continuous evidence, not periodic audits. Organisations relying on manual evidence gathering will find their sovereignty claims questioned by the regulators those investments were meant to satisfy.

Opportunity

Extend compliance automation to match sovereignty investments. Policy-as-code and continuous evidence generation should cover every workload on sovereign infrastructure—otherwise, the infrastructure investment is undermined by the governance gap.

Prediction #5: Key AI Risks Will Be Under-Weighted in Critical Environments

By 2026, certain Middle Eastern organisations—particularly in Saudi Arabia—will underestimate critical AI risks like training-data contamination and PII leakage, creating misalignment between risk perception and actual exposure.

AI Risk (% citing as top concern)	Global	UAE	Saudi Arabia
Third-party AI vendor handling	42%	56%	48%
Training-data poisoning	29%	38%	22%
PII in AI outputs/embeddings	32%	40%	24%
Sensitive data in AI training	35%	44%	28%

UAE organisations show elevated awareness across AI risk categories—56% concerned about vendor handling, 38% about training-data poisoning, 40% about PII leakage. But Saudi Arabia presents a concerning pattern: Only 22% cite training-data poisoning as a top concern (7 points below global), and just 24% worry about PII in AI outputs. These aren't minor gaps—they represent fundamental under-weighting of risks that can compromise AI systems and violate privacy regulations.

The Gap

Saudi Arabia under-weights training-data contamination **(22% vs. 29% global)** and PII leakage **(24% vs. 32% global)**—the AI risks most likely to trigger regulatory action and reputational damage.

Misaligned risk perception has downstream consequences. Organisations that don't prioritise training-data risks won't invest in training-data safeguards. Those that under-weight PII leakage won't implement privacy-preserving techniques or robust governance of model life cycles. The UAE-Saudi gap in AI risk awareness will translate into a UAE-Saudi gap in AI security investment—creating uneven protection across the region at exactly the moment AI adoption is accelerating.

Opportunity

Align risk perception with actual exposure. Saudi organisations should benchmark AI risk awareness against UAE and global counterparts, then invest in training-data safeguards, privacy-preserving techniques, and model life-cycle governance proportionate to actual—not perceived—risk levels.

Strategic Recommendations for Middle Eastern Organisations

The Middle East has moved faster on data sovereignty than any other region. But sovereignty—controlling where data lives—is necessary but not sufficient. Boards and regulators will increasingly ask not just where data resides, but how it's governed, how AI uses it, and how quickly incidents are resolved. Five priorities emerge for closing the governance gaps that sovereignty alone cannot address.

1. Close the UAE-Saudi AI Governance Gap

A 22-point gap in AI anomaly detection between countries in the same region creates fragmented protection and inconsistent incident response. Establish regional AI governance standards that bring Saudi capabilities to UAE levels—and push both toward complete coverage. Multinationals operating across both countries should require consistent AI governance regardless of which hosts the workload.

2. Convert AI Vendor Concern Into AI Vendor Control

High awareness of third-party AI vendor risk (56% UAE, 48% Saudi) hasn't translated to controls. Joint playbooks at 19% and 12%, kill switches at 24% and 16%—these aren't leadership numbers. Make these controls standard requirements in AI vendor contracts, especially for government, financial services, and energy. Awareness without matching controls is documented negligence.

3. Establish Regional Supply Chain Standards

Saudi Arabia trails global benchmarks on every supply chain metric; UAE leads but with incomplete coverage. Regional supply chains are only as secure as their weakest links. Make SBOM requirements a condition of government and critical infrastructure procurement across both countries. Push UAE toward 80%+ SBOM coverage while bringing Saudi to global minimums.

4. Match Compliance Automation to Sovereignty Investment

Sovereign infrastructure without automated compliance evidence is a foundation without proof. When 48% of UAE and 62% of Saudi organisations can't demonstrate governance in real time, sovereignty claims are questioned. Extend policy-as-code to every workload on sovereign infrastructure. Make continuous evidence generation the standard, not periodic audits.

5. Align AI Risk Perception With Actual Exposure

Saudi organisations under-weight training-data contamination and PII leakage—risks that trigger regulatory action and reputational damage. Benchmark AI risk awareness against UAE and global counterparts. Invest in training-data safeguards and privacy-preserving techniques proportionate to actual risk levels, not comfortable assumptions.

The Bottom Line

The Middle East has solved the sovereignty question faster than any other region. But sovereignty alone won't satisfy regulators or boards if organisations can't prove how data is accessed, how AI uses it, and how fast they can respond when something goes wrong. The gaps in AI incident response, vendor controls, supply chain security, compliance automation, and risk awareness represent the unfinished work behind the sovereignty success story. Organisations that close these gaps will convert infrastructure investment into governance advantage. Those that assume sovereignty is sufficient will find that controlling where data lives is only the beginning of what regulators, boards, and partners demand.

Kiteworks

2026

Data Security and Compliance Risk Forecast Report

AI Adoption Is Accelerating. Governance Is Stalling. The Reckoning Is Coming.

REPORT

Kiteworks 2025. All Rights Reserved.

For the complete report with detailed methodology, industry breakdowns, and regional analysis, download it now.

Download the Report

Kiteworks