

Kiteworks Survey Finds Middle East Compliance Consequence Rate Hits 76%, Highest of Any Region

Just 7% of Middle East Organizations Rank AI Regulation Their Top Compliance Concern, Lowest of Any Region

ZURICH, ZÜRICH, SWITZERLAND, July 30, 2026 /EINPresswire.com/ --

Kiteworks, which empowers organizations to effectively manage risk in every send, share, receive, and use of private data, today released Middle East findings from its [2026 Data Security and Compliance Risk: Annual Survey Report](#), based on primary

research with 459 security, compliance, risk, and IT professionals across 10 industries and three global regions, including organizations across the Middle East and Africa. The findings show a region deploying AI fast without the governance architecture, or the regulatory urgency, to match.

“

The Middle East is deploying AI at real speed, and governance covering people and agents alike hasn't caught up.”

Tim Freestone, Chief Strategy and Marketing Officer at Kiteworks

The Middle East and Africa (MEA) posts the lowest mean Data Security Maturity Score (DSMS) of any region in the survey, 35.7 out of 100, behind Europe's 40 and North America's 38, a gap that reflects controls protecting everyday human-driven data access as much as AI-specific safeguards. Its mean AI Governance Maturity Score (AIGMS), which measures governance capability for AI systems and agents, is 34, also trailing North America's 39. Read together, the two scores show controls in the region

aren't keeping pace with either people or agents. The combination produces a mean Data Security and Compliance Readiness Index (DSCRI) of 15, tied with Europe for the lowest of any region and well below North America's 19.

MEA organizations also report the highest compliance consequence rate of any region, at 76%,



compared to 69% in North America and 57% in EU/UK, alongside an AI incident rate of 78%, above Europe's 75% though below North America's 84%.

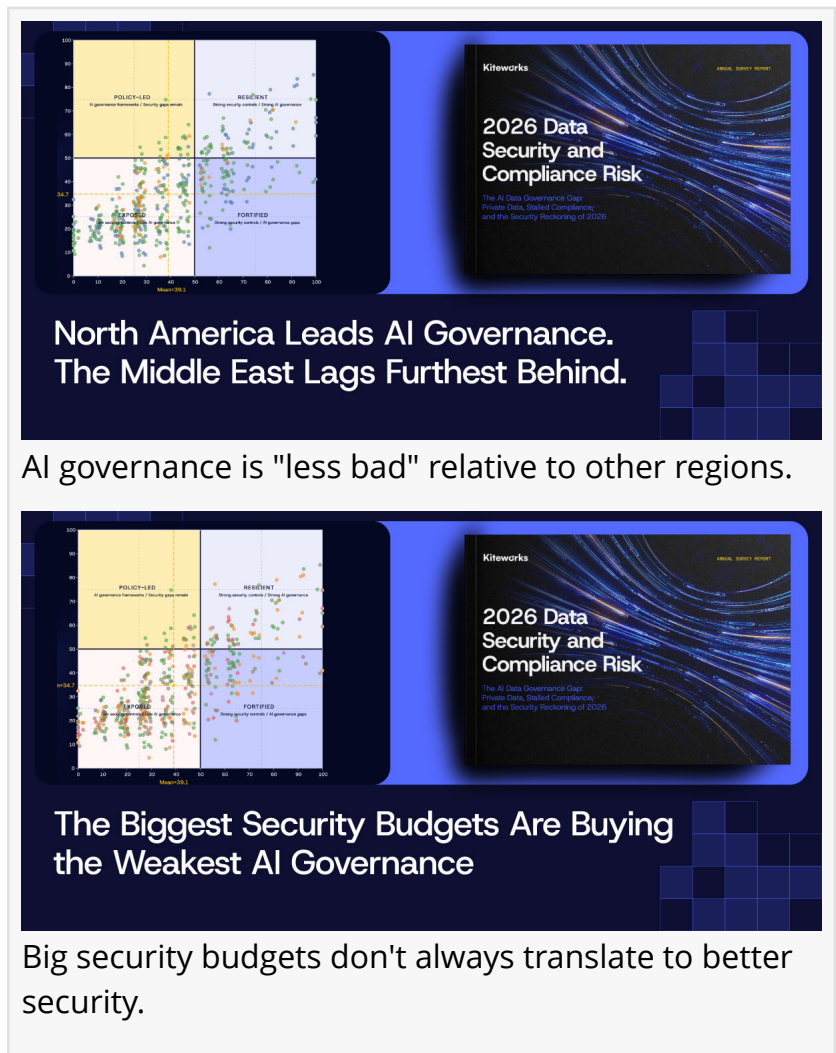
"The Middle East is deploying AI at real speed, and governance covering people and agents alike hasn't caught up," said Tim Freestone, Chief Strategy Officer at Kiteworks. "A 76% compliance consequence rate alongside the lowest security maturity score of any region isn't a knowledge problem. It's a controls problem."

The region's third-party risk data reinforces that pattern. 50% of MEA organizations have tested third-party access revocation through an actual incident response, the highest rate of any region, compared to 35% in North America. And while 29% of EU/UK respondents rank AI-specific regulation as their top compliance concern, only 7% of MEA respondents do, even though the region carries the highest incident and consequence rates surveyed.

"MEA organizations are responding to breaches and enforcement actions rather than building preventively," said Patrick Spencer, SVP of Americas Marketing and Industry Research at Kiteworks. "The controls that close this gap are the same ones the report identifies everywhere: purpose binding, SIEM integration for AI systems, and an audit trail that can be produced in a day, not a week, covering every person and every agent operating in the environment."

The governance gap behind these numbers is measurable everywhere. Seventy-four percent of organizations worldwide lack purpose binding for AI data use, and no AI containment control measured in the survey is deployed by more than 31% of organizations. Fifty percent cannot produce a complete AI data access audit record within one business day.

The gap between the top and bottom of this survey is 38 DSCRI points. The 19% of organizations in the Resilient quadrant (DSMS and AIGMS both at least 50) carry a mean DSCRI of 46. The 66% in the Exposed quadrant (both below 50) carry a mean DSCRI of 8, despite similar industry and size mixes. The difference is deployed AI governance controls. At the survey mean DSMS of 39,



raising AIGMS from 35 to 60 adds roughly 10 DSCRI points, nearly double the gain from adding four security controls while AIGMS stays fixed. The report identifies seven priorities for closing that gap:

- Classify and enforce sensitive data
- Deploy AI-specific DLP through a centralized policy engine
- Integrate MFT and AI infrastructure with a SIEM
- Implement and test an AI kill switch
- Build audit trails that meet regulatory production timelines
- Assign dedicated AI data governance ownership
- Consolidate sensitive data exchange platforms

The full 2026 Data Security and Compliance Risk: Annual Survey Report includes global, industry, regional, and organization-size breakdowns.

Download the 2026 Data Security and Compliance Risk: Annual Survey Report.

The research was conducted by Centiment on behalf of Kiteworks in Q2 2026.

About Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.

Martin Brindley

Martin Brindley PR Ltd

+44 1256 762811

martin.brindley@gmail.com

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

[TikTok](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/930034754>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.