

RISK GCC 2025 WAS A LANDMARK CONVERGENCE IN THE GULF



The third annual #RISK GCC 2025 conference concluded on the ninth of December at the gleaming DIFC Conference Centre and the DIFC Academy in Dubai's Gate Village, drawing together a remarkable constellation of governance, risk and compliance professionals from across the Gulf and from financial centres beyond the GCC. What unfolded over two days was more than an industry gathering. It felt like a living chronicle of how the region is redefining risk, building new governance vocabularies and embracing an era where artificial intelligence, digitisation, geopolitics and sustainability intersect in unexpected yet profoundly consequential ways.

The event's organisers, GRC World Forums, working in strategic partnership with the Dubai International Financial Centre, managed to create an atmosphere that blended intellectual rigour with the warmth and fluidity of a global community that understands the speed at which the GCC's economic and technological landscape is changing.

From the very start, there was palpable anticipation among over a thousand delegates who had made their way from more than twenty countries, packing conference halls with bankers, compliance chiefs, cybersecurity architects, regulators, risk consultants, sustainability managers, legal advisers and emerging founders from fintech and energy innovation ecosystems.

A SHIFT TOWARD DEEPER EXPERTISE

What set this edition apart was its unmistakable shift toward mid-to-senior level depth. Gone were introductory overviews or superficial talk around the edges of AI. These were sessions crafted for professionals actively shaping policy, steering digital transformation and designing the internal frameworks through which risk is governed in a region that has placed innovation at the heart of its economic destiny. Attendees flowed between parallel tracks that catered to very different decision-making needs.

Some were exploring the role of AI in anti-money laundering. Others were examining data protection maturity, energy cybersecurity, sanctions volatility or the contours of a proposed GCC-wide regime for harmonised AI oversight. Throughout both days there were conversation pockets forming naturally in lounge corners and coffee clusters, where executives compared notes on algorithmic bias, operational resilience or the long tail of geopolitical tensions in a world shaped by renewed American assertiveness after the presidential transition in Washington.

The conference venues in Gate Village elevated the experience. With their glass-lined architecture, abundant natural light and impeccable technical infrastructure, they conveyed a sense of modernity that matched Dubai's ambitions. Screens streamed crisp visuals, audio never faltered and the Wi-Fi held steady even as attendees moved rapidly between halls.

Sustainable catering added a thoughtful touch, as did the decision to operate with digital agenda booklets that minimised paper waste. Live captioning screens supported accessibility, and though the hybrid format was not fully active this year, the organisers teased an expanded streaming offering for 2026, ensuring that the global audience could engage with the region's fast-accelerating GRC community.

Conversations across the two days consistently reflected an urgency that could only have emerged from the GCC's rapidly evolving digital economy. Whether one looked at Saudi Arabia's monumental investments in AI research, the UAE's bold experimentation with fintech regulation, Qatar's commitment to data localisation, Bahrain's agile financial supervision or Oman's interest in cybersecurity resilience, it was clear that the region was no longer testing the waters but diving into the deep end of innovation.

This was particularly evident in how speakers framed artificial intelligence: not as a separate component of digital transformation, but as the nucleus around which economic growth, risk frameworks, compliance controls, and public policy are being constructed. Delegates repeatedly referred to AI as the defining force of the next decade, used in everything from sanction screening to predictive auditing and real-time cyber threat intelligence.

THE OPENING KEYNOTE: AI AS CATALYST AND CAUTION

The opening keynote on the first day, led by senior DIFC leadership, laid down the foundational tone. The speaker described AI as both a transformative catalyst and a potential existential risk when deployed without guardrails. He reminded the audience that the UAE Central Bank's regulatory sandbox for AI models was not an experiment but a signal of direction, pointing toward a financial future where algorithmic tools will be responsible for fraud detection, dynamic credit scoring, behavioural analysis, customer identity authentication and personalised advisory services.

The presentation drew nods across the hall, partly because of the GCC's ambitious digital transformation agendas and partly because executives in the audience recognised the delicate balance between innovation and responsibility. The address underscored that this era demands more than just compliance. It requires a philosophical rethinking of how organisations conceptualise risk, how they distribute accountability across human and automated layers and how they prevent unintended harms that may arise from unchecked machine autonomy.

Panels that followed pushed the conversation further. The much-anticipated session on AI risks in financial services generated lively exchanges as experts from leading banks like Mashreq and Emirates NBD shared how they were confronting the challenges of algorithmic bias in credit underwriting. The discussion moved fluidly from technical design considerations to ethical implications.

Speakers explained how explainable AI systems could help demonstrate fairness during regulatory audits, reducing the likelihood of hidden discrimination while empowering institutions to defend their automated decision-making with clarity and confidence. This session resonated with participants from jurisdictions that lacked strong AI governance frameworks, prompting several after-panel conversations around the need to embed explainability into the region's forthcoming rules.

Another highly attended session explored data sovereignty and cross-border data governance. With national strategies being drafted across the GCC, including Qatar's firm requirement that critical financial data be fully localised by 2026, organisations were grappling with new complexities. Panelists highlighted the dilemma between embracing global cloud services and respecting national sovereignty imperatives. The conversation took a particularly interesting turn when experts compared data localisation to federated learning models, which allow AI systems to learn from decentralised data without transferring raw information across borders.

The debate reflected broader global tensions between the United States and China, whose technological decoupling had ripple effects on cloud vendors, semiconductor supply chains, cyber dependencies and even blocked foreign acquisitions. Delegates from multinational corporations listened intently, taking notes on how future GCC regulations might affect vendor selection, cloud deployment strategies and cross-border compliance operations.

Operational resilience sessions on the first day also attracted practitioners from telecommunications, logistics, energy infrastructure and ports. The conversation centred around lessons drawn from disruptions reminiscent of the globally impactful CrowdStrike outage. Risk leaders emphasised the significance of AI-enhanced continuity frameworks that can anticipate, detect and respond to cascading failures in essential services.

The speakers explained that AI does not eliminate risk but transforms its nature by opening new threat vectors. Telco executives discussed how predictive analytics could keep their critical systems functioning even when unexpected service dependencies collapse, while port administrators highlighted the need for adaptive responses to cyber incidents in heavily automated logistics chains.

Cybersecurity tracks were especially charged. Experts warned of ransomware attackers who now target energy giants in the GCC, seeking to infiltrate operational technology environments that interact with pipelines, drilling machinery and high-value industrial assets. Speakers urged the region's firms to align with zero-trust architecture principles and to adopt AI-driven behavioural analytics that detect anomalies long before human teams could. These conversations felt urgent and often deeply technical.

Yet, they remained accessible enough to draw participants from non-technical backgrounds who wanted to understand what cyber maturity should look like in the coming years. Many attendees commented that this year's cybersecurity coverage felt more grounded in operational detail than in previous editions, marking a turning point toward real-world focus.

ESG, CLIMATE INTELLIGENCE AND GEOPOLITICAL FLUX

Environmental, social and governance themes also held a prominent place throughout the first day. AI-powered climate risk modelling occupied an entire set of discussions, with analysts demonstrating how generative simulations could visualise the long-term impact of rising sea levels, extreme heat or storm surges on GCC infrastructure. These tools, speakers explained, have become crucial to Saudi Arabia's Vision 2030 commitments and to emerging regulatory frameworks across the Gulf.

Delegates from ESG departments found themselves moving quickly between climate sessions and those discussing geopolitical risk. The latter examined how shifting United States foreign policy under the second Trump administration had affected sanctions on entities connected to Iran, putting new pressures on banks that operate in the Middle East. Experts recommended using AI-driven horizon scanning to detect future policy shifts and to enhance third-party due diligence for counterparties operating near geopolitical fault lines.

The final highlight of the first day was an intimate fireside conversation between a chief risk officer at Saudi Aramco and a leading DIFC regulator. Their discussion focused on the concept of GRC-by-design, a methodology that embeds governance, risk and compliance thinking directly into the development cycles of AI startups. They shared examples of how Dubai's AI Lab was assisting innovators in constructing systems that could demonstrate auditability, accountability and reliability from the very first line of code. As the audience absorbed the significance of this exchange, it became evident that the future of the GCC's digital economy rests on collaborative frameworks that bridge cutting-edge enterprise with regulatory foresight.

DAY TWO: ETHICS, FINTECH, QUANTUM FUTURES

The transition to the second day of #RISK GCC 2025 was seamless but marked by a shift toward deeper thematic exploration. The morning began with an absorbing examination of AI ethics in workplaces, contrasting Bahrain's permissive stance on employee monitoring with Kuwait's more structured, data-protection-oriented safeguards. Speakers referred to PwC's regional breach statistics, noting that the average cost of cyber incidents in the Middle East had climbed steeply. This ascribed greater urgency to the ongoing adaptation of NIST frameworks to local contexts, especially with the introduction of new AI-specific controls.

Fintech experts filled the next round of sessions, focusing on the UAE's Virtual Asset Testing Framework and demonstrations from ADGM innovators who showcased AI tools that identify anomalous wallet activity. These pilots had already delivered measurable reductions in fraud, prompting investors and compliance teams to pay close attention. Participants from digital asset exchanges and regulatory sandboxes found the use cases particularly relevant, given how rapidly virtual asset ecosystems are growing across the Gulf.

One session that attracted considerable attention came from Oman's regulatory authorities, who described their experimental work on blockchain-based sovereign data registries designed to withstand next-generation quantum computing threats. Attendees appreciated how forward-thinking this was, given that quantum threats are usually framed as distant concerns rather than near-term policy issues. Energy analysts and defence experts seated in the hall seemed intrigued by how these innovations might scale across regional infrastructures.

Environmental discussions continued with a focus on Scope 3 supply chain transparency, where AI tools were seen as viable instruments for supporting national ESG goals in Qatar and for supporting DIFC's emerging parametric insurance solutions. The idea that AI might soon power risk-based insurance payouts for climate events seemed to capture the imagination of insurers who were exploring future business models.

TOWARD A UNIFIED GCC GRC FRAMEWORK

The GCC regulator roundtable drew perhaps the most diverse audience of the entire event. Representatives from the UAE Securities and Commodities Authority, Abu Dhabi Global Market, Qatar Financial Centre and the Saudi Arabian Monetary Authority shared their vision for a unified framework across the Gulf that would enable consistent AI audits and smoother cross-border regulatory cooperation. This proposed GRC Accord was still evolving but was clearly a top priority. Delegates whispered excitedly about what such harmonisation could enable, particularly for multinational fintech firms who currently navigate a labyrinth of varied requirements.

The final stretch of the conference immersed participants in integrated GRC platforms, with experts referencing OCEG's findings that nearly seventy percent of firms in the region were considering AI-enhanced compliance automation. However, they also acknowledged the persistent skills shortages that hindered adoption. The last keynote of the afternoon presented a resilience quotient for AI systems, a concept that leaders could use to benchmark their organisations against global best practices. As the conference reached its official close, the CEO of GRC World Forums announced that #RISK GCC 2026 would expand into quantum computing and metaverse governance, drawing loud applause. With over two hundred on-site meetings recorded, the atmosphere suggested the beginning of new collaborations rather than the end of a dialogue.

Stepping back from the dense schedule and abundant insights, the core themes of the two days stood tall in memory. AI governance emerged as the foremost priority, not merely as a compliance requirement but as a structural necessity for stability and trust. Human oversight, especially for decisions involving significant financial exposure, became a focal point. Cybersecurity stood as another pillar, urging organisations to advance toward hybrid frameworks that combine the strengths of both NIST and ISO practices. There was strong consensus that AI-powered threat hunting would become indispensable across the region's energy and financial sectors.

Data strategies were clearly evolving toward a dual model that combines localisation with federated access, and this shift was seen as both pragmatic and visionary. It was also evident that ESG considerations would now be fully entwined with digital transformation, given how intricately climate risk, data management and AI optimisation intersect.

As geopolitical conversations underscored the volatility of sanctions during the unfolding Trump era, organisations were urged to prepare for flux through predictive tools and diversified risk mapping.

The implications for GCC financial hubs were enormous. DIFC's leadership in hosting the event reinforced Dubai's trajectory toward a hundred-billion-dollar digital economy. Banks across the region were aligning their risk modelling for Basel IV with AI enhancements, while fintechs moved eagerly from regulatory sandboxes into scalable operations powered by unified risk systems. Saudi Arabia and Qatar were rapidly studying the UAE's AI governance models for replication, while Indian participants spotted parallels between GCC innovation frameworks and the Reserve Bank of India's controlled experimentation with digital payments and consumer data.

A CLOSING THAT FELT LIKE A BEGINNING

As delegates filtered out of Gate Village after the closing reception, there was a shared sense of having participated in something more consequential than a conference. #RISK GCC 2025 felt like a chapter in the GCC's transformation story, a chapter rich with complexity yet filled with optimism. The region's leaders, innovators and regulators had collectively demonstrated that resilience in an AI-defined future is neither accidental nor improvised. It is built through continuous learning, collaborative problem-solving and the courage to rethink old assumptions in the face of unprecedented technological change.

The conversations that began in Dubai will continue to reverberate through boardrooms, regulatory consultations and digital roadmaps across the Gulf and beyond. When the next edition of the conference opens, with quantum and metaverse governance likely shaping its themes, the momentum will not feel new. It will feel like a natural progression of the commitment that the region has displayed with remarkable clarity. As one chief risk officer remarked as the event concluded, AI is rewriting the contours of risk itself. Those who adapt will thrive. Those who hesitate will be left grappling with a world that has already moved on. This was the spirit that defined #RISK GCC 2025, and this is the spirit that will continue to define the GCC's bold and evolving journey into the future of governance, risk and compliance.