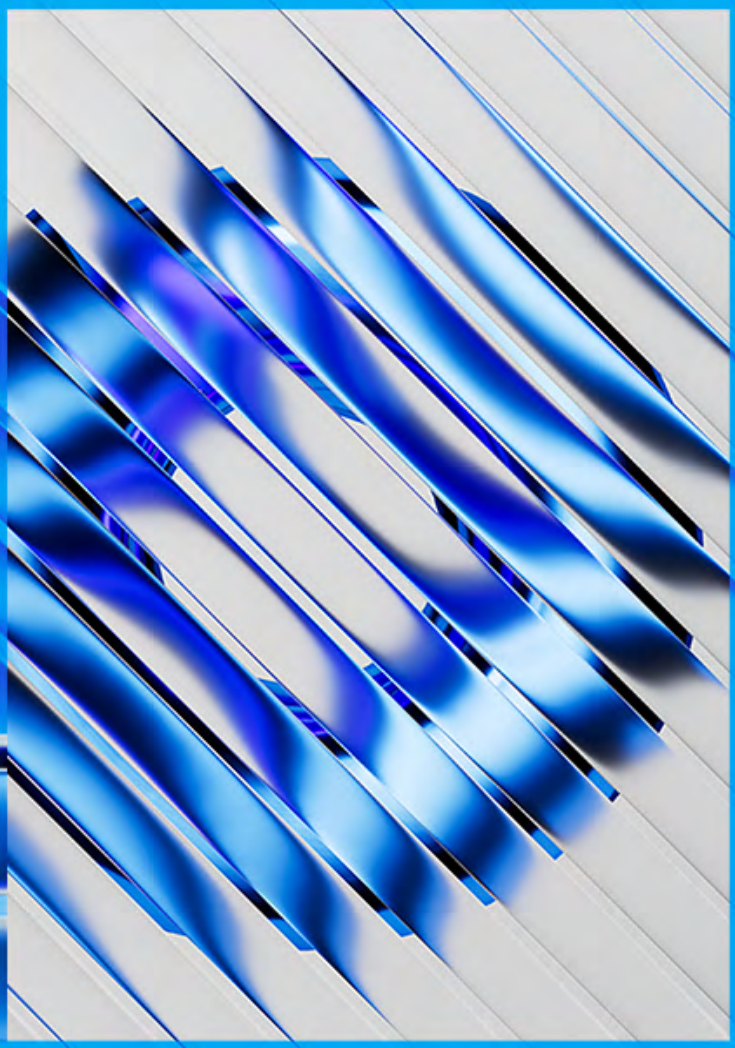
KPMG

A bold step towards cyber resilience

Advancing readiness in today's complex threat landscape



KPMG. Make the Difference.

April 2026

Foreword

The UAE has taken a decisive step forward in its national cyber maturity journey with the release of the UAE Information Assurance (IA) Standard v2.1 in November 2025, replacing the earlier UAE IA Regulation v1.1 (2020). This evolution reflects a clear national intent to strengthen cyber resilience, enhance governance, and align with leading international best practices in response to an increasingly complex and evolving threat landscape.

The current geopolitical environment across the Middle East has further intensified the cyber threat landscape, with a marked increase in state-sponsored activities, hacktivism, and targeted campaigns against government entities and critical infrastructure. Regional tensions have amplified the likelihood of disruptive and destructive cyber operations, while also increasing the sophistication, frequency, and coordination of these attacks. In this context, cyber resilience is no longer solely a technical priority but a national security imperative, requiring organizations to strengthen their defensive posture, enhance situational awareness, and adopt proactive, intelligence-driven security measures.

The UAE IA supports this through alignment with the national cyber mandates aimed at standardized practices and a cohesive response to cyber threats across the ecosystem. As government entities, critical infrastructure operators, and regulated organizations prepare to meet the new requirements, it is essential for leadership teams to understand not only what has changed, but why it matters. This paper outlines the key shifts introduced by UAE IA v2.1, their strategic implications, and how organizations can respond pragmatically and effectively.

© 2026 KPMG Middle East LLP, a Jersey limited liability partnership, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

Establishing guardrails against disruption

Recent developments in the Middle East have highlighted the increasing convergence of cyber and physical risks. For UAE entities, strengthening cyber security is essential to ensuring resilience in the face of increasingly complex and interconnected threats.

Cyber as a core business risk

Organizations should treat cyber risk as a business-critical function rather than a purely technical domain. Cyber security must be embedded into enterprise risk management, with leadership oversight on how disruptions could impact operations, safety, and service delivery. Continuous monitoring of emerging threats and alignment with national directives are essential.

Threat intelligence and situational awareness

Organizations should leverage real-time threat intelligence and actively monitor their environments for anomalies. Integrating insights from security operations, incident response, and external threat feeds enables early detection and faster response to evolving threats.

Managing external threat actors

Entities must be prepared for attacks from hacktivist groups or opportunistic threat actors, particularly during periods of regional instability. Strengthening application security, DDoS protection, and monitoring external-facing assets is critical, along with having clear response strategies for ambiguous or unattributed threats.

Enhancing cyber readiness across the organization

Cyber security should be consistently enforced across business units and third parties. Regular audits, vulnerability assessments, and simulation exercises (e.g. red teaming) help validate controls and improve readiness. Collaboration with partners and sector peers strengthens collective defense.

Managing third-party and supply chain risks

Organizations should continuously assess risks arising from vendors, cloud providers, and technology dependencies. Clear security requirements, monitoring mechanisms, and contingency planning are essential to mitigate cascading impacts from third-party incidents.

Addressing misinformation and social engineering risks

Organizations should actively monitor for misinformation or impersonation attempts targeting their brand or employees. Internal awareness programs should emphasize verification of communications, particularly during crisis situations, to reduce the risk of phishing, fraud, or reputational damage.

Incident response and operational resilience

Entities must maintain well-defined incident response and escalation procedures, ensuring clarity of roles and rapid decision-making. Regular testing of business continuity and disaster recovery plans is critical to ensure the organization can recover quickly from both cyber and physically induced disruptions.

Protection of critical systems and operations

Entities must identify and secure critical systems, particularly those supporting essential services and operational technologies. They should implement strong network segmentation, restrict privileged access, and ensure the availability of offline backups and manual fallback processes to maintain continuity during disruption.

© 2026 KPMG Middle East LLP, a Jersey limited liability partnership, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

Why UAE IA v2.1 matters now

The refresh of the UAE Information Assurance Standard is not a routine regulatory update. It has direct implications for leadership accountability, operational resilience, and organizational risk management.

Cybersecurity underpins operational resilience

UAE IA v2.1 promotes mature cyber practices enabling organizations to anticipate and respond to physical events that affect digital operations and critical services.

Cyber risk is a leadership issue

UAE IA v2.1 reinforces executive ownership of cyber risk, requiring informed risk acceptance, sustained oversight, and continuous assurance.

Digital transformation increases exposure

As cloud, shared platforms, and emerging technologies are rapidly adopted, UAE IA v2.1 provides a structured framework to enable secure innovation without impeding agility.

Non-compliance has tangible consequences

Weak information assurance can result in service disruption, regulatory scrutiny, and erosion of public trust—particularly for entities delivering critical or citizen-facing services.

Early action reduces cost and complexity

Proactive gap assessments and phased implementation are significantly more cost-effective than reactive remediation following audits or incidents.

A governance shift

UAE IA v1.1 (2020) was issued by the Telecommunications Regulatory Authority (TRA), primarily focused on establishing a foundational information assurance baseline.

UAE IA v2.1 (2025) is issued by the UAE Cyber Security Council (CSC), signaling a more centralized, coordinated, and strategic national cyber governance model.

Why this matters

This transition elevates information assurance from a technical compliance obligation to a whole-of-nation cyber resilience agenda. It strengthens executive oversight, enables national-level situational awareness, and aligns organizational cyber programs with the UAE's broader national cyber security strategy.

Scope and applicability

UAE IA v2.1 expands and clarifies applicability across the national ecosystem, including:

Federal ministries and authorities.

Non-government critical information infrastructure (CII) operators.

Emirate-level government entities, subject to Emirate-specific governance models.

Emirate-level critical information infrastructure programs for Emirate CII operators

The standard establishes a national minimum baseline for information assurance, spanning both public and private sector entities that deliver or support critical services.

An overview of UAE IA v2.1

Control families (Domains)

The refreshed UAE IA Standard remains structured around 15 core security control families, ensuring balanced coverage across governance and technical domains:

- Management controls: 6 control families addressing governance, risk, and oversight
- Technical controls: 9 control families addressing preventive, detective, and corrective cyber security measures

Control architecture and structure

UAE IA v2.1 introduces a more modular and clearly structured control taxonomy aligned with international standards. Across the framework, there are:

15
control families (M1–M6; T1–T9)

47
sub-families providing thematic grouping

134
sub-families providing thematic grouping

449
sub-controls offering detailed implementation guidance

While individual control definitions have evolved, the overall 15-domain architecture remains the foundational structure of the standard.

Always applicable vs risk-based controls

To support a risk-adaptive compliance model, UAE IA v2.1 distinguishes between:

- Always applicable controls: Mandatory for all in-scope entities
- Risk-based controls: Applicable based on organizational risk profile and criticality

The distribution is defined as:

- 70 always applicable controls
- 64 risk-based controls

This approach enables organizations to prioritize effort based on risk, rather than adopt a uniform, one-size-fits-all implementation model.

Prioritization model

The four-tier prioritization model (P1–P4) has been retained to support phased implementation:

- P1: foundational controls addressing core IA capabilities
- P2–P4: progressive controls enabling broader and more advanced assurance

This model supports realistic multi-year cyber security roadmaps aligned with organizational capacity and risk appetite.

A single source of truth for cyber security policies

The UAE IA v2.1 has been developed to serve as the single source of truth for all national cyber security policies. The Cyber Security Council (CSC) has released multiple domain-specific policies covering areas such as cloud security, IoT, AI/ML systems, critical infrastructure protection, and data privacy, among others.

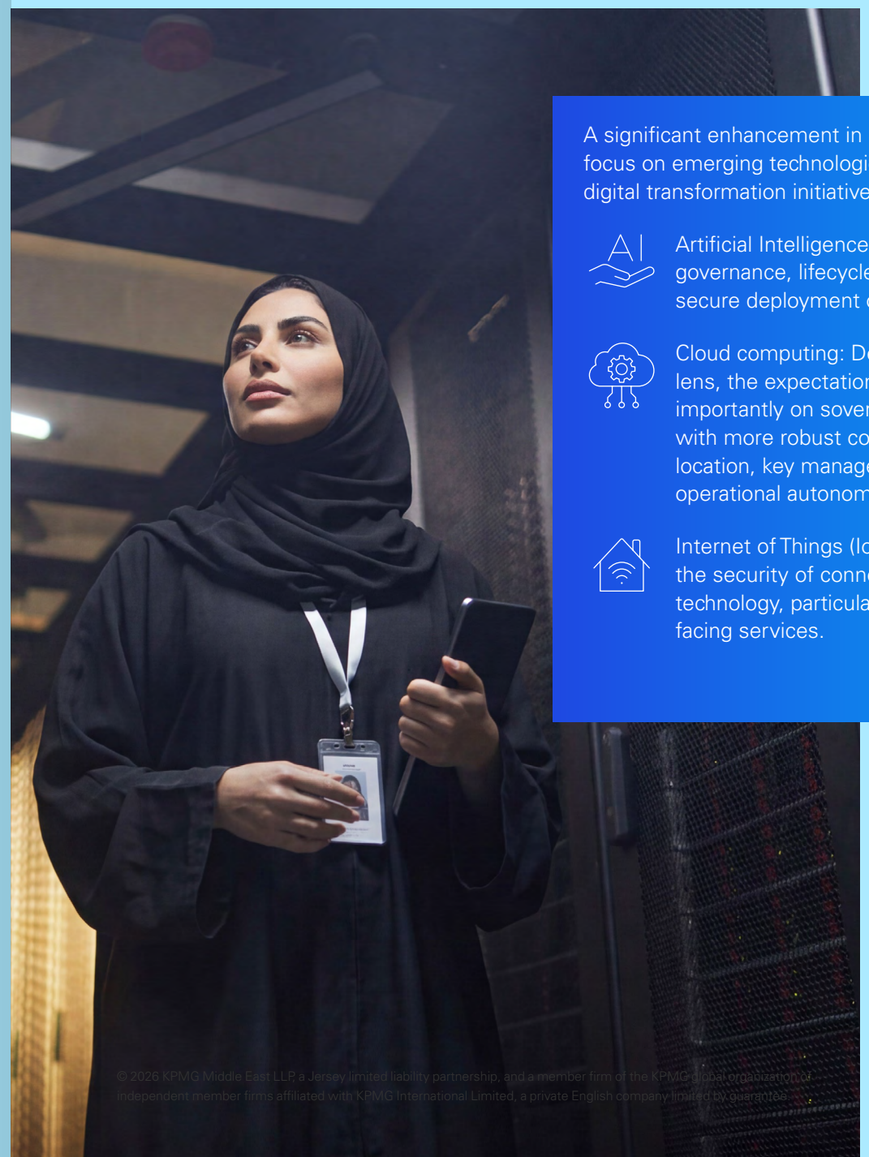
National Cyber Security Policies that are integrated into the UAE IA Standard v2.1 include:

- Critical Information Infrastructure Protection Policy
- National IoT Security Policy
- Cyber Incident response Framework
- Cyber Incident Response Plan
- Cyber Security Information Sharing Framework
- National Cloud Security Policy
- National Cyber Security Governance Framework
- SOC Baseline Capabilities
- National Cyber Security Policy for Artificial Intelligence
- National Data Exchange Security Policy
- National Encryption Policy
- National Secure Remote Work Policy
- National Third Party Security Policy
- National Vulnerability Disclosure Policy

By integrating all controls from these individual policies into a consolidated framework, the UAE IA Standard v2.1 ensures consistency, reduces overlap, and provides a clear compliance pathway. For organizations, this means that demonstrating compliance with the UAE IA Standard v2.1 automatically reflects compliance with all underlying CSC policies.

This unified approach not only simplifies governance and compliance efforts but also enables organizations to implement a holistic cyber security posture aligned with national requirements, while ensuring agility to adapt to emerging technologies and threats.

A focus on emerging technologies: AI, Cloud, and IoT



A significant enhancement in UAE IA v2.1 is its explicit focus on emerging technologies that underpin national digital transformation initiatives:

- Artificial Intelligence (AI): New controls emphasize governance, lifecycle risk management, and secure deployment of AI-driven systems.
- Cloud computing: Deploying a data aware lens, the expectations on security and more importantly on sovereignty are heightened, with more robust controls required around data location, key management, legal control, and operational autonomy.
- Internet of Things (IoT): Expanded controls address the security of connected devices and operational technology, particularly in critical and citizen-facing services.

How KPMG can support your organization

At KPMG, we support organizations with adopting the UAE Information Assurance (IA) Standard v2.1 through a simple, structured, and risk-driven approach:

- **UAE IA implementation support:** We assess your alignment with the requirements of the standard and support you as you navigate the governance, process and technical controls imperative to drive compliance and maturity.
- **Cyber resilience roadmap:** Leveraging a compliance lens, we develop, customize and embed cyber resilience journeys towards operational and digital resilience.
- **Emerging technology security advisory:** We support organizations with implementing regulatory mandates within their AI and cloud journeys, allowing entities to innovate with confidence.

This approach enables organizations to move from compliance understanding to effective and sustainable implementation of the UAE IA Standard.

KPMG brings a unique combination of local experience, regulatory insight, and digital trust expertise, making us a trusted partner for organizations navigating UAE IA v2.1 adoption:

Deep understanding of UAE cyber regulatory expectations

Our teams work extensively across UAE government entities, regulators, and critical sectors, enabling us to translate regulatory intent into practical, implementable actions.

End-to-end digital trust capabilities

We combine cyber security, risk management, data protection, cloud security, emerging technology assurance, and governance expertise, ensuring UAE IA implementation is integrated, not siloed.

Proven experience across complex environments

We support large, federated organizations with diverse technology landscapes, helping them balance compliance, operational resilience, and digital transformation.

Risk-led, leadership-focused delivery

Our approach aligns technical controls with executive oversight, risk ownership, and assurance reflecting the leadership accountability embedded in UAE IA v2.1.

KPMG enables organizations to move from understanding requirements to embedding cyber security as a core element of organizational resilience, fully aligned with the intent of the UAE Information Assurance Standard v2.1.

About KPMG Middle East LLP

KPMG Middle East LLP is a part of the KPMG global organization of independent member firms that operate in 143 countries and territories and are affiliated with KPMG International Limited. We provide audit, tax and advisory services to public and private sector clients across Saudi Arabia, United Arab Emirates, Jordan, Lebanon, Oman, and Iraq, contracting through separate legal entities. We have a strong legacy in the region, where we have been established for over 50 years. KPMG Middle East LLP is well-connected with its global member network and combines its local knowledge with international expertise.

KPMG serves the diverse needs of businesses, governments, public-sector agencies, not-for-profit organizations, and the capital markets.

Our commitment to quality and service excellence underpins everything we do. We strive to deliver to the highest standards for our stakeholders, building trust through our actions and behaviors, both professionally and personally. Our values guide our day-to-day behavior, informing how we act, the decisions we make, and how we work with each other, our clients, and all our stakeholders.

- Integrity: We do what is right
- Excellence: We never stop learning and improving
- Courage: We think and act boldly
- Together: We respect each other and draw strength from our differences
- For Better: We do what matters.

Our purpose is to inspire confidence and empower change. By inspiring confidence in our people, clients and society, we help empower the change needed to solve the toughest challenges and lead the way forward. KPMG's Impact Plan guides our commitments to serving our clients, people and communities across four categories: Planet, People, Prosperity, and Governance. These four priority areas assist us in defining and managing our environmental, social, economic and governance impacts to create a more sustainable future. We unite the best of KPMG to help our clients fulfil their purpose and deliver against the United Nations Sustainable Development Goals, so all our communities can thrive and prosper.

We are dedicated to helping our clients achieve their goals, and advancing sustainable progress to ensure that all our communities thrive. Empowered by our values, and committed to our purpose, our people are our greatest strength. Together, we are building a values-led organization of the future. For better.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

© 2026 KPMG Middle East LLP, a Jersey limited liability partnership, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

Contact us

Timothy Wood

Partner
Digital Trust- Cyber & Privacy
KPMG Middle East
timothywood@kpmg.com

Arbab Chaudhry

Partner
Cyber Strategy and Governance
KPMG Middle East
arbabchoudhary@kpmg.com

Brienish Alva

Director
Digital Trust- Cyber & Privacy
KPMG Middle East
balva@kpmg.com

www.kpmg.com/om
www.kpmg.com/ae

Follow us on:

Designed by KPMG ME Design Studio

Publication name: A bold step as strategic imperative
Publication number: 6033
Publication date: February 2026