RSM

CONFIDENTIAL

Cybersecurity & Cyber Risk Services

Empowering End to End Digital Transformation & Business Resilience | RSM UAE

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

UAE Regulatory Alert

UAE PDPL is now enforceable. DESC Information Security Regulation and Federal **Decree-Law No. 26 on Child Digital Safety are effective from January 2026.** Non-compliance carries financial, reputational, and operational consequences

Overview

This document provides an overview of RSM UAE's comprehensive Cybersecurity and Cyber Risk Services practice. It is designed for senior decision-makers and procurement stakeholders evaluating cybersecurity advisory and managed security partnerships in the UAE and wider GCC region.

Security Posture Challenges

UAE Organisations Face an Expanding Cyber Threat Landscape

The UAE's rapid digital transformation, combined with a tightening regulatory environment, creates both opportunity and exposure. Organisations that fail to align their security posture with evolving regulations face growing legal and operational risk.

Regulatory Complexity

Navigating evolving frameworks including UAE Cybercrime Law, PDPL, NESA, DESC, and ADHICS compliance requirements .

Sophisticated Threat Actors

Rising ransomware (+32% in 2024), AI-powered phishing, and state-sponsored APTs targeting critical sectors

Cloud & Digital Expansion Risks

Misconfigured cloud environments and weak access controls amid rapid digital transformation

Supply Chain Vulnerabilities

Third-party dependencies creating hidden entry points for attackers across interconnected ecosystems .

Talent & Capability Gaps:

Shortage of specialized cyber skills to design, operate, and respond to advanced threats at scale.

Data Sovereignty & Cross-Border Flows

Balancing global operations with UAE data localization and privacy obligations.

Emerging Tech Exposure

Securing AI, IoT, and OT environments where security frameworks are still maturing

Incident Response Readiness

Ensuring rapid detection, containment, and legally compliant breach notification under UAE mandates .

Regulatory Complexity

Evolving Regulatory Complexity in UAE Cybersecurity

The UAE's cybersecurity regulatory landscape is rapidly maturing, from fragmented guidelines to a sophisticated, multi-layered framework. Organizations now navigate intersecting mandates: federal laws (PDPL, Decree-Law 26/2025 on Child Digital Safety), emirate-specific regimes (DESC ISR in Dubai), free-zone standards (DIFC/ADGM), and strategic directives (National Cybersecurity Strategy 2025–2031).

UAE PDPL

Cross-border data controls & consent frameworks now enforceable

Dubai DESC

Mandatory IS audit certification for Dubai-registered entities

Decree-Law 26/2025

Child digital safety controls required on consumer platforms

UAE NCS 2025–2031

Systematic resilience mandated across all critical sectors

Our Service Framework

Multi-Layered Cyber Défense Strategy for the UAE Market

Secure your organization against sophisticated threats with a Défense-in-Depth strategy. Align with national frameworks like NESA, PDPL, and DESC to protect critical assets across hybrid environments. Explore the emerging cyber priorities essential for compliance and resilience in the UAE market.

RSM UAE delivers cybersecurity services through two integrated engagement models, our Strategic Advisory Practice and our Managed Security Services. Both are designed around UAE regulatory alignment, sector-specific risk intelligence, and executive-ready reporting.

Défense-in-Depth strategy

The 7-Layer Security Architecture

UAE Regulatory Alignment: NESA IAS, PDPL, ADHICS, DESC and Child Digital Safety Compliance (2026 frameworks.

Advisory Services

- UAE Cybersecurity Regulatory Compliance Assessment (NESA, PDPL, DESC, ADHICS)
- Cyber Risk Governance & Board Advisory
- Information Security Policy Development & Review
- Cyber Risk Appetite & Strategy Alignment

Managed Services

- Virtual CISO (vCISO) Services
- Compliance Monitoring & Reporting
- Policy Management & Maintenance
- Regulatory Change Management

Défense-in-Depth strategy

The 7-Layer Security Architecture

Layer 2: Identity & Access Management (IAM)

Advisory Services

- Zero Trust Architecture Design & Roadmap
- IAM Strategy & Implementation Planning
- Privileged Access Management (PAM) Assessment
- UAE Pass Integration Advisory
- Identity Governance & Administration (IGA) Design

Managed Services

- IAM Operations & Support
- Access Review & Certification Management
- PAM Administration & Monitoring
- Identity Lifecycle Management

Layer 3: Identity & Access Management (IAM)

Advisory Services

- Network Security Architecture Review
- Cloud Network Security Design (AWS/Azure/Oracle UAE)
- DDoS Resilience Assessment
- Network Segmentation Strategy
- SASE/Zero Trust Network Access (ZTNA) Design

Managed Services

- Managed Firewall Services
- Network Security Monitoring
- DDoS Mitigation Management
- Secure Web Gateway Operations
- VPN & Remote Access Management

Layer 4: Endpoint & Workload Protection

Advisory Services

- Endpoint Security Strategy & Tool Selection
- Cloud Security Posture Management (CSPM) Assessment
- Mobile Security & BYOD Policy Design
- OT/ICS Security Assessment
- EDR/XDR Implementation Advisory

Managed Services

- Managed EDR/XDR Services
- Endpoint Patch Management
- Mobile Device Management (MDM) Operations
- Cloud Workload Protection Monitoring
- Vulnerability Management as a Service

Layer 5: Data Security & Privacy

Advisory Services

- UAE PDPL Compliance & Data Privacy
- Advisory
- Data Classification & Handling Framework
- Data Loss Prevention (DLP) Strategy
- Encryption & Key Management Design
- Data Sovereignty & Cross-Border Transfer Assessment
- Privacy Impact Assessments (PIA)

Managed Services

- DLP Operations & Tuning
- Data Discovery & Classification Services
- Encryption Key Management
- Privacy Program Management
- Data Subject Request (DSR) Fulfillment Support

Défense-in-Depth strategy

The 7-Layer Security Architecture

Layer 6: Application Security

Advisory Services

- Application Security Program Development
- Secure SDLC & DevSecOps Integration
- API Security Assessment & Design
- Web Application Penetration Testing
- Code Review & Security Testing Advisory
- Container & Kubernetes Security Assessment

Managed Services

- Managed WAF Services
- Application Security Testing
- (SAST/DAST/SCA)
- Vulnerability Scanning & Remediation Tracking
- API Security Monitoring
- Penetration Testing as a Service

Layer 7: Monitoring, Detection & Response

Advisory Services

- SOC Maturity Assessment & Design
- Incident Response Plan Development
- Cyber Threat Intelligence Strategy
- Digital Forensics Readiness Assessment
- Tabletop Exercise & Simulation Design
- UAE CERT Integration Advisory

Managed Services

- 24/7 Managed Security Operations Center (SOC)
- Managed Detection & Response (MDR)
- Managed SIEM & Log Management
- Incident Response Retainer Services
- Digital Forensics & Incident Investigation
- Threat Hunting Services
- Breach Notification & Crisis Management Support

Strategic Cyber Risk Integrated -Service Packages

RSM UAE Cyber Risk Integrated Service Packages

Our advisory methodology is structured across multiple pages and can be customized to clients' requirements . Ensuring your organization builds lasting security capability, not just point-in-time compliance.

01	**Cyber Essentials Package**	For organizations beginning their cyber journey Layer 1-3 Advisory + Basic Managed Monitoring
02	**Cyber Essentials Package**	For mature organizations seeking comprehensive protection. Full 7-Layer Assessment + SOC + Incident Response Retainer

Strategic Cyber Risk Integrated –Service Packages

03 — **Cyber Essentials Package**

For regulated entities requiring UAE-specific compliance
NESA/PDPL/DESC Compliance + vCISO + Audit Support

04 — **Cyber Essentials Package**

For organizations undergoing digital transformation
Cloud Security + Zero Trust + DevSecOps Integration Retainer

Strategic Cyber Risk Integrated –Service Packages

RSM UAE Cyber Risk Integrated Service Packages

Our advisory methodology is structured across four progressive phases, ensuring your organisation builds lasting security capability, not just point-in-time compliance.

Phase 1 (0-6 months)

Governance foundation + Layer 1-3 alignment and deployment

- Cyber governance maturity assessment (NIST CSF 2.0 'Govern' function)
- Regulatory gap analysis — DESC, DIFC, ADHICS compliance roadmap
- Cross-border data flow mapping — UAE PDPL & transfer impact assessments
- Child digital safety compliance — age-assurance architecture (Decree-Law 26)

Phase 2 (6-12 months)

Risk-Based Strategy Development + Layer 4-5 implementation & compliance validation

- Threat landscape assessment — ISO 27001:2022 Annex A; prioritised risk register
- Climate resilience integration — ISO 27001:2024 Amend.1 & ISMS continuity
- Supply chain risk framework — NIST CSF SCRM; third-party vendor risk scoring
- AI security governance — NIST AI RMF; SDAIA AI safety; AI procurement policy

Phase 3 (12-18 months)

Risk-Based Strategy Development + Layer 4-5 implementation & compliance validation

- Threat landscape assessment — ISO 27001:2022 Annex A; prioritised risk register
- Climate resilience integration — ISO 27001:2024 Amend.1 & ISMS continuity
- Supply chain risk framework — NIST CSF SCRM; third-party vendor risk scoring
- AI security governance — NIST AI RMF; SDAIA AI safety; AI procurement policy

Phase 4 (Ongoing)

Continuous improvement, threat hunting, resilience testing

- Control effectiveness testing — independent validation & exception reporting
- Vendor management oversight — MSSP SLA/KPI framework & performance scorecard
- Board-level reporting — cyber risk heat map & regulatory compliance dashboard
- Continuous improvement — annual posture review & NIST CSF 2.0 tier benchmarking

Why RSM UAE

The Advantages of Working with RSM UAE

RSM is not the largest firm , we are the most client-centred. In cybersecurity, that distinction drives better outcomes: deeper engagement, senior continuity, and advice genuinely aligned to your interests.

Global Network, Local Depth

Part of RSM International's 120-country network — our UAE team combines global methodology with deep knowledge of UAE DESC, DIFC, and ADHICS regulatory frameworks.

Advisory Independence

Unlike technology vendors or MSSPs, our advisory practice is vendor-neutral — ensuring your architecture decisions and service selections are in your interest, not ours.

Integrated Risk Practice

Cyber risk does not exist in isolation. RSM integrates cybersecurity with financial risk, internal audit, regulatory compliance, and ESG for a unified board-level view.

Board-Ready Reporting

We translate technical risk into business language. Every engagement produces executive dashboards, heat maps, and compliance status reports for board and C-suite decision-making.

Mid-Market Specialist

RSM's global reputation is built on the middle market — organisations that need senior expertise, genuine engagement, and responsiveness — not junior-team delivery.

Future-Ready Frameworks

From AI security governance (NIST AI RMF, SDAIA) to climate resilience (ISO 27001:2024 Amend.1) and quantum readiness — we build for tomorrow's threats today

Standards & Frameworks

RSM UAE aligns all advisory and managed services to internationally recognised standards, customised for GCC regulatory requirements.

NIST CSF 2.0	ISO/IEC 27001:2022	DESC Regulation
DIFC Requirements	ADHICS Standard	NIST AI RMF
SDAIA AI Safety	UAE PDPL	ISO 27001:2024 Amend.1
NIST SCRM Framework		

Sectors We Serve

Financial Services

CBUAE · DIFC · ADGM

Healthcare

ADHICS · DHA · MOH

Energy & Utilities

OT/ICS Security · SCADA

Real Estate & Construction

Smart Buildings · BIM

Government & Public Sector

UAE Strategy 2025–2031

Aviation & Transport

GCAA · RTA Compliance

Retail & E-Commerce

PCI DSS · UAE PDPL

Education & Technology

Child Safety · Data Privacy

Complimentary Offer

Complimentary Cyber Health Check

Before committing to any engagement, understand where your organisation stands. RSM UAE's Cyber Health Check gives your leadership team an objective view of your security posture at no cost.

1. Governance & Regulatory Exposure Review
2. Threat Surface & Asset Inventory
3. Third-Party & Supply Chain Risk
4. Incident Response Readiness Assessment
5. Executive Briefing & 90-Day Roadmap

Limited engagements available per quarter · UAE & GCC organisations only · Delivered within 5 business days

Terminologies

For Business functions

DESC

The **Dubai Electronic Security Center (DESC)** enforces cybersecurity regulations that apply to both government entities and private sector organizations operating in Dubai. Private sector organizations required to comply with DESC regulations include for customer data, or dealing with Dubai government entities as Vendors or service Provider.

UAE NCS 2025-2031

The United Arab Emirates National Cybersecurity Strategy 2025-2031 - a comprehensive governmental framework designed to protect the UAE's digital infrastructure, enhance cyber resilience, and position the country as a global leader in cybersecurity innovation

UAE NESA

The National Electronic Security Authority, a UAE federal authority responsible for the nation's cybersecurity and information assurance. NESA has been renamed to SIA (Signals Intelligence Agency) and serves as the UAE's intelligence agency. governs the UAE National Cyber Security Strategy (NCSS) and is responsible for implementing policies, regulations, and standards to secure the nation's digital assets and communications networks. NESA developed mandatory cybersecurity standards. (known as the NESA Standard or Information Assurance Standards) that apply to:

UAE PDPL

The UAE’s Personal Data Protection Law, formally enacted as Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data. The UAE PDPL is the UAE's first comprehensive federal data protection regulation, designed to protect the personal data of individuals residing in or having a place of business in the UAE, and to establish a unified framework for the lawful collection, processing, storage, and transfer of personal data across the Emirates

CDS-Decree Law 26/2025

Federal Decree-Law No. 26/2025On Child Digital Safety
Child Protection, General Information Technology & Telecommunications

DESC, DIFC, and ADHICS Regulatory Frameworks

DESC governs Dubai's cybersecurity through ISR standards for government and private sectors. DIFC operates an independent data protection regime within Dubai's financial free zone. ADHICS mandates healthcare-specific cybersecurity controls for Abu Dhabi health entities. These frameworks establish jurisdiction-specific compliance obligations across the UAE

RSM

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

Access RSM's Self Cyber Security Assessment tool to generate your personalized report for **FREE!**

This report serves as an ideal starting point for a deeper analysis through RSM's Cyber Security Assessment, guiding you on your journey toward stronger and more achievable Cyber Security resilience.

SCAN THIS QR CODE

OR CLICK HERE

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM UAE

Dubai

Offices 3106. 3107, 3109-10,
The Burlington Tower , Marasi Drive,
Business Bay
P.O. Box 11855
T: +971 (0)4 554 7423

Abu Dhabi

Office 711,Corniche Building,
Corniche Road, UAE
P.O. Box 73843
T: +971 (0)2 643 5623

RSM Dahman Accountants LLP
Floor 14, WeWork Hub 71, Al Khatem
Tower, ADGM Square, Al Maryah Island
P.O. Box 46617
T: +971 (0)4 554 7423

Sharjah

E-LOB, Office no. E2-115F-58 Hamriyah
Free Zone
P.O. Box 41637
T: +971 (0)4 554 7423

W: www.rsm.ae

RSM UAE is a member of the RSM Network and trades as RSM. RSM is the trading name used by the members of the RSM network. Each Member of the RSM Network is an independent assurance, tax and consulting firm each of which practices in its own right. The RSM Network is not itself a separate legal entity of any description in any jurisdiction. The RSM Network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the Network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.