

APOGEE GLOBAL RMS

INTEGRATED ENTERPRISE RISK MANAGEMENT · SDVOSB / DVBE / MBE CERTIFIED

Risk advised as one connected system.

SET-ASIDE ELIGIBLE

- **SDVOSB**, SBA certified
- **CA DVBE**, valid thru 02/28/2027
- CA Small Business
- **MD MBE**, Maryland
- MD CSB / VSBE

REGISTRATION

- UEI NFDUQKK8E6N3
- CAGE 08WU4
- SAM.gov Active, All Awards

CONTACT

2059 Camden Ave, STE 242
San Jose, CA 95124
(415) 251-5510
information@apogeeglobalrms.com
apogeeglobalrms.io

DELIVERY

- Nationwide + International
- On-site | Remote | Hybrid

HOW TO ENGAGE

- Direct award
- SDVOSB set-aside
- Competitive task order
- Prime / sub teaming
- GSA Schedule (pending)

INSURANCE

- Professional Liability (E&O)
- General Liability
- Cyber Insurance

STRATEGIC PARTNER

Tacilent, developer of the Rogue Risk Platform. Apogee is an investor and the platform anchors sustained engagements.

DELIVERY PARTNERS

Nortal · Satrix · PruTech · VigilAgent · First Health Advisory · Digital Mountain



Scan to visit · apogeeglobalrms.io

WHY APOGEE

Apogee Global RMS is a principal-led risk management firm. Founded in 2018 and led by M.K. Palmore, a U.S. Naval Academy graduate, Marine Corps officer, and retired FBI senior executive whose private-sector leadership includes VP and Field CISO at Palo Alto Networks and cybersecurity executive at Google Cloud. Every engagement is delivered by named senior practitioners who have held the decision, not studied it. The proprietary Nexus of Risk framework governs cyber, physical, and human risk as one consequence chain, grounded in COSO ERM and ISO 31000, so leadership receives a single unified risk picture that siloed point vendors cannot provide.

Apogee sells **accountability for risk outcomes**. It does not sell labor capacity. The firm that prepares an organization does not grade it: Apogee prepares, remediates, and governs; independent parties attest.

THE NEXUS OF RISK · THREE DOMAINS, ONE CONSEQUENCE CHAIN

CYBER RISK

Systems, data, identity, and the technology estate. Framework assessment and program design across NIST CSF 2.0, NIST 800-53, CMMC, ISO 27001, and SOC 2. Identity governance, AI governance, third-party risk, compliance readiness.

PHYSICAL RISK

Facilities, operational environments, and the physical estate. Security assessment and program design, OT exposure, distributed operations, workplace violence prevention, executive protection posture, crisis and continuity, tabletop exercises.

HUMAN RISK

The people an organization trusts. Executive due diligence, vetting program governance, insider threat, leadership and succession risk, workforce assurance, AI hiring governance. A governance and assurance discipline, not recruitment.

SERVICES

Assessment

Risk posture measured against a framework. Documented gaps, prioritized findings.

Strategy

Multi-year risk roadmap with sequencing, resourcing, and decision gates. Founder-led.

Governance Design

Structures, policies, roles, and reporting by which risk is governed going forward.

Sustained Engagement

Fractional risk and compliance leadership. Renewable six-month intervals. Execution included.

PLATFORMS AND INTELLECTUAL PROPERTY

Rogue Risk Platform, powered by Tacilent

The enterprise risk apparatus at the core of sustained engagements, establishing a full risk operating capability across the three Nexus domains.

Apogee Vanguard

Governance, risk, and compliance platform behind the advisory relationship.

Apogee Vantage

Human Risk and Strategy platform supporting leadership assessment and succession risk work.

RRAG

Intelligence research arm producing published risk advisories and geopolitical briefings.

SECTORS SERVED

State & Local Government · Law Enforcement · Federal Civilian · Financial Services · Healthcare · Critical Infrastructure · Technology · M&A. Apogee qualifies by consequence, not industry: organizations where a failure in cyber, physical, or human systems produces damage that cannot be absorbed quietly.

REPRESENTATIVE ENGAGEMENTS

State Judiciary (3,000+ employees)

NIST CSF 2.0 cybersecurity risk assessment and full remediation roadmap at enterprise scale.

Regional Health System

Ransomware and physical-access-control failure contained within 72 hours.

Law Enforcement (200+ officers)

Four-session AI leadership training program, POST certification-aligned.

Enterprise Security Buildout

Zero to audit-ready in 90 days; passed first audit.

PRINCIPAL

M.K. Palmore · Founder and Principal Advisor

CISSP · Carnegie Mellon CISO · MBA, Pepperdine · USNA · USMC Officer · Retired FBI Senior Executive

ADVISORY BOARD

LTG Omar Jones, USA (Ret.) · Defense & Government

Gail Gottehrer, Esq. · Law, AI & Data Privacy

Brian Grayek · Cybersecurity

Renee Wynn · Federal Technology, former NASA CIO

Kasia Hanson · Physical Security, Cybersecurity & AI

Mike Skurko · Technology

NAICS CODES

541611 (primary) · 541512 · 541511 · 541519 · 541513 · 541618 · 541690 · 561621 · 518210 · 541612 · 611430 · 541720 · 541990 · 541330 · 541614 · 541613