APOGEE GLOBAL RMS

WHO WE ARE · AUGUST 2026

Integrated Enterprise Risk Management

Where cyber, physical, and human risk converge.

SAN JOSE, CA · WASHINGTON, D.C. · FOUNDED 2018

SDVOSB · DVBE · MBE CERTIFIED · SAM.gov Active, All Awards

information@apogeeglobalrms.com · (415) 251-5510 · apogeeglobalrms.io

THE PROBLEM

Risk is integrated. Vendors are not.

Organizations face enterprise-grade threats across the cyber, physical, and human domains simultaneously. The market's response is fragmented: one vendor for cybersecurity, another for physical security, another for governance, another for the people function, each delivering findings never designed to inform each other.

> The client is left to connect the dots. Most never do. The gaps between vendors are where incidents happen.

The cost of fragmentation

A typical mid-market organization spends $400K to $1.2M annually across siloed vendors, with the integration gap still unsolved. The compounding cost of failure is far greater.

RANSOMWARE RECOVERY

Average mid-market ransomware recovery exceeds $1.8M: downtime, remediation, reputational damage, and regulatory response combined.

FAILED EXECUTIVE APPOINTMENT

A single failed executive hire costs two to three times first-year compensation, including severance, search fees, and organizational disruption. Independent pre-appointment due diligence is cheaper than the failure.

GOVERNANCE FAILURE

A board-level governance failure can trigger regulatory action, D&O exposure, and shareholder litigation, simultaneously.

Apogee is not an additional cost. It replaces a more expensive failure mode.

OUR APPROACH

A principal-led risk management firm

Apogee is a principal-led risk management firm. Every engagement is delivered by senior practitioners who have held the decision, not studied it, calibrated for executive and board consumption from day one. Apogee governs cyber, physical, and human risk as one connected system, grounded in COSO ERM and ISO 31000, giving leadership a unified risk picture that siloed point vendors cannot provide.

> Apogee sells accountability for risk outcomes. It does not sell labor capacity.
>
> An audit passed. A certification maintained. A framework implemented. A program operating. And the firm that prepares an organization does not grade it: Apogee prepares, remediates, and governs; independent parties attest.

The Nexus of Risk: our governing thesis

Every risk, cyber, physical, operational, or reputational, originates in or is mitigated by human decisions. The three domains are causally interconnected: a single consequence chain observed at different points.

A cybersecurity incident is a leadership crisis

It exposes governance gaps, stress-tests board oversight, and reveals whether human risk decisions created the vulnerability.

A physical security failure is an information-security exposure

Unauthorized physical access and data exfiltration are the same event. Organizations that treat them separately respond to them separately, and slowly.

An ungoverned human layer is a security vulnerability

Unvetted appointments, insider risk, and succession gaps in critical roles are not HR problems. They are exploitable weaknesses adversaries identify before you do.

CYBER | PHYSICAL | HUMAN

DIFFERENTIATION

What makes Apogee different

SENIOR PRACTITIONER WORK

Experienced leaders and executives lead every engagement from start to finish. Not delegated supervision of junior staff.

INTEGRATED RISK PRACTICE

Cyber, physical, and human risk under one lens. Not a single-domain consultancy chasing adjacencies.

FIXED-FEE CLARITY

Priced to outcomes and timelines, not hours. No ambiguity on scope, team, or deliverables.

EXECUTION INCLUDED

Where remediation is needed to reach an outcome Apogee owns, Apogee does it. Findings are closed, not handed over as a backlog.

INDEPENDENCE PRESERVED

Apogee prepares, remediates, and governs. It does not attest, certify, or audit a program it built: the same governance discipline it sells, demonstrated on itself.

KNOWLEDGE TRANSFER

Runbooks, trained staff, systems the client owns. If the relationship concludes, the apparatus stays.

The platforms behind the practice

- **Rogue Risk Platform, powered by Tacilent.** The enterprise risk apparatus at the core of sustained engagements. Apogee is an investor in Tacilent, its deepest partner relationship, reflecting the conviction that the Risk Platform is the future of enterprise risk management.
- **Apogee Vanguard.** Governance, risk, and compliance platform: the operating tooling behind the advisory relationship.
- **Apogee Vantage.** Human Risk and Strategy platform supporting executive assessment, succession risk, and workforce assurance.
- **RRAG.** Intelligence research arm producing published risk advisories and geopolitical briefings.

LEADERSHIP

M.K. Palmore, Founder and Principal Advisor

- U.S. Naval Academy graduate and Marine Corps officer
- Retired FBI senior executive: directed cybersecurity investigations at the highest levels of federal law enforcement
- VP and Field CISO, Palo Alto Networks; Cybersecurity Executive Advisor, Google Cloud
- CISSP · Carnegie Mellon CISO · MBA, Pepperdine
- Host, The Risk Apogee podcast · Keynotes at RSA and ISSA · 200+ C-level leaders convened through the Executive Dinner Series

> "Risk judgment forged across national security, Fortune 500 enterprise architecture, and operational leadership. Not theory borrowed from textbooks."

Every engagement is practitioner-led

The standard the Founder sets defines the firm. Every Apogee engagement is led by senior practitioners referenced by role, never by delegation to junior staff. Each of the three Nexus domains is held by a named accountable role: the Principal Advisor for Cyber Risk, the Founder and Principal Advisor for Physical Risk, and the Principal Advisor for Human Risk, with Business Operations owning delivery execution and the public sector engine end to end.

FEDERAL & LAW ENFORCEMENT

Senior executives who directed cybersecurity investigations at the highest levels of U.S. federal law enforcement.

ARMED FORCES VETERANS

U.S. military veterans with operational command experience informing every risk posture and crisis response engagement.

FORTUNE 500 ENTERPRISE

Leaders who built and led security programs inside Google Cloud and Palo Alto Networks, at scale, under pressure.

Advisory Board: LTG Omar Jones, USA (Ret.), Defense and Government · Renee Wynn, former NASA CIO · Gail Gottehrer, Esq., Law, AI, and Data Privacy · Kasia Hanson, Physical Security, Cybersecurity, and AI · Brian Grayek, Cybersecurity · Mike Skurko, Technology

HOW TO ENGAGE

The Phase Ladder

Three engagement structures. One integrated practice. Each stands on its own; together they form a ladder as your needs evolve.

Apogee Ascend · P1

Executive-grade cyber risk posture assessment. From $44,500 · 6 to 10 weeks · fixed-fee, defined scope.

Apogee Meridian · P2

Integrated assessment and governance design across cyber, physical, and human. Scoped to client needs · 4 to 6 months.

Apogee Zenith · P3 · Flagship

Sustained engagement across the full Nexus, anchored by the Rogue Risk Platform, powered by Tacilent. Scoped · renewable six-month intervals.

RESULTS

Proven results

50+

Engagements completed across SMB, healthcare, financial services, and public sector

90%+

Client retention: sustained relationships built on delivered outcomes

30 days

Average time from engagement start to first client-facing deliverable

$20M

Digital transformation delivered in 18 months against a 36-month forecast

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

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

State Judiciary · 3,000+
NIST CSF 2.0 assessment and full remediation roadmap delivered.

WHO WE SERVE

Organizations where risk carries consequence

Apogee qualifies by consequence, not by industry: organizations where a failure in cyber, physical, or human systems produces regulatory, operational, or reputational damage that cannot be absorbed quietly.

Enterprise and SMB (50–1,200 employees)

- Healthcare: HIPAA, ransomware, clinical cyber-physical risk
- Financial Services: OCC / FFIEC / GLBA, SEC Item 106
- Professional Services and Technology
- Critical Infrastructure: NERC CIP, TSA
- M&A due diligence, including executive due diligence

Public Sector and Defense

- Federal, state, county, and municipal agencies
- FedRAMP, FISMA / ATO, CMMC 2.0, CIRCIA
- Law enforcement: POST-aligned AI leadership training
- Washington, D.C. presence supports federal capture and on-site board and agency briefings

PROCUREMENT

A procurement position competitors cannot match

SDVOSB (SBA)

Federal set-aside with sole-source authority up to $4M. The federal 5% SDVOSB goal represents a $31B+ annual target pool.

CA DVBE

3% participation goal and streamlined SB/DVBE option procurement across California state agencies. Valid through 02/28/2027.

MARYLAND PREFERENCES

VSBE, MBE, and SBR certifications active for Maryland state and local procurement vehicles.

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

WHAT HAPPENS NEXT

Two ways to start

COMPLIMENTARY FOR QUALIFIED ORGANIZATIONS

REQUEST A BOARD RISK BRIEFING

A 45-minute working session with a senior practitioner. We review your posture across the cyber, physical, and human domains, surface the gaps your current vendors are unlikely to see, and leave you with a one-page prioritized action set.

FIXED-FEE · TWO WEEKS

RISK POSTURE SNAPSHOT

A fixed-fee, two-week written assessment with a 60-minute executive readout, for organizations ready to move from awareness to action.

Contact

Founder and Principal Advisor · (415) 251-5510 · information@apogeeglobalrms.com · apogeeglobalrms.io
San Jose, CA · Washington, D.C. · SDVOSB · DVBE · MBE Certified · SAM.gov Active

U.S. Small Business Administration
SERVICE-DISABLED VETERAN-OWNED CERTIFIED

Scan to visit · apogeeglobalrms.io

Risk advised as one connected system.