APOGEE GLOBAL RMS

TAKING PEOPLE, PROCESS AND TECHNOLOGY TO THE NEXT LEVEL

INTEGRATED ENTERPRISE RISK MANAGEMENT

Capabilities and Partnership Briefing

An external guide for media, prime contractors, and prospective partners

Risk advised as one connected system.

NOVEMBER 2026 · APPROVED FOR EXTERNAL DISTRIBUTION

CERTIFICATIONS	REGISTRATION	PRESENCE
SDVOSB · VOSB	UEI NFDUQKK8E6N3	San Jose, CA · Washington, D.C.
California DVBE · CA DGS SB	CAGE 08WU4	Nationwide and international
Maryland SBR · Maryland VSBE	SAM.gov Active, All Awards	apogeeglobalrms.io

Apogee Global RMS, LLC · 2059 Camden Avenue, Suite 242, San Jose, CA 95124
(408) 256-2198 · (415) 251-5510 · mkp@apogeeglobalrms.com · info@apogeeglobalrms.com

Contents

1 About Apogee Global RMS

2 What Apogee Sells, and What It Does Not

3 The Nexus of Risk Framework

4 Human Risk, Defined

5 How Organizations Engage: Four Services, One Ladder

6 The Phase Ladder: Ascend, Meridian, Zenith

7 Accountable Executives Behind a Vendor's Motion

8 Specialty Practices

9 Platforms, Programs, and Intellectual Property

10 Sectors Served

11 Proof Points, Practitioners, and Leadership

12 Certifications, Vehicles, and Partnership Pathways

13 For Journalists and Event Programmers · Contact

HOW TO USE THIS BRIEFING

Sections 1 through 10 describe what Apogee does and how it engages. Section 11 names the people behind the work. Section 12 carries the contracting credentials and the five partnership pathways, and is the section a prime contractor or teaming partner should read first. Section 13 is for media.

SECTION 1

About Apogee Global RMS

Apogee Global RMS is a principal-led risk management firm headquartered in San Jose, California, with a Washington, D.C. presence. Founded in 2018, Apogee advises enterprise and public sector organizations on the convergence of cyber, physical, and human risk through its proprietary Nexus of Risk framework. Apogee is a certified Service-Disabled Veteran-Owned Small Business, a Veteran-Owned Small Business, and a California Disabled Veteran Business Enterprise.

Every engagement is delivered by named senior practitioners who have held the decision, not studied it, and is calibrated for executive and board consumption from day one. Apogee 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 qualifies clients by consequence, not by industry: organizations where a failure in cyber, physical, or human systems produces regulatory, operational, or reputational damage the organization cannot absorb quietly.

Firm Fast Facts

Founded	2018
Headquarters	San Jose, California, with a Washington, D.C. presence supporting federal capture and on-site board and agency briefings
Delivery	On-site, remote, or hybrid; nationwide and international
Model	Principal-led. Senior practitioners lead every engagement start to finish, not delegated supervision of junior staff
Pricing	Fixed-fee clarity: priced to outcomes and timelines, not hours, with no ambiguity on scope, team, or deliverables
Certifications	SBA-certified SDVOSB and VOSB; California DVBE (valid through 02/28/2027); California DGS Small Business; Maryland SBR and VSBE; SAM.gov Active, All Awards
Track record	50+ engagements completed; 90%+ client retention; 30-day average to first client-facing deliverable

SECTION 2

What Apogee Sells, and What It Does Not

Apogee sells accountability for risk outcomes. It does not sell labor capacity.

An audit passed. A certification maintained. A framework implemented. A program operating. The client buys the outcome and the named practitioners behind it, not hours against a queue.

Where remediation is needed to reach an outcome Apogee owns, Apogee executes it. What the firm does not do is sell standalone implementation capacity, operate client infrastructure as an outsourced technology function, or run a commercial recruitment practice. These boundaries are structural, and they protect one further discipline that partners and clients should expect Apogee to state plainly:

> *The firm that prepares an organization should not be the firm that grades it.*

Apogee assesses, remediates, prepares, and governs, and sits beside the client on assessment day. It does not attest, certify, or audit a program it built. In public sector work this discipline is applied to the stricter standard of FAR Subpart 9.5 and its state analogues.

SECTION 3

The Nexus of Risk Framework

Apogee's proprietary framework governs enterprise risk as one connected system: three domains, one consequence chain. A cyber breach, a physical security failure, and an insider event are frequently the same event observed at different points in the chain. The value lives in the intersections that siloed vendors miss.

CYBER

Systems, data, identity, and the technology estate.

Framework assessment, program and control design, identity governance, AI governance, third-party risk, and compliance readiness across NIST CSF 2.0, NIST 800-53, CMMC, ISO 27001, and SOC 2.

PHYSICAL

Facilities, operational environments, and the physical estate.

Security assessment and program design, OT exposure at the physical plant, site and distributed operations risk, workplace violence prevention, executive protection posture, crisis and continuity, and tabletop exercises for executive and operational teams.

HUMAN

The people an organization trusts.

Due diligence and verification, vetting program governance, insider threat, leadership and succession risk, workforce assurance, and AI hiring governance. The domain most enterprises leave ungoverned, and the origin point of a large share of events that surface first as cyber or physical failures.

Frameworks applied across the practice include COSO ERM, ISO 31000, NIST CSF 2.0, NIST 800-53, CMMC, and ISO 27001, extended by sector-specific authorities such as HIPAA, NYDFS Part 500, NERC CIP, TSA security directives, FISMA and RMF, FedRAMP, the NIST AI RMF, and SEC Regulation S-K Item 106.

SECTION 4

Human Risk, Defined

The domain most enterprises leave ungoverned, and the one where Apogee's investigative credential is least imitable. Human Risk is a governance and assurance discipline: Apogee assesses, verifies, and governs the people function. It does not recruit and it does not staff roles.

AREA	WHAT IT COVERS
Executive and personnel due diligence	Independent pre-appointment verification of senior candidates, key personnel, and privileged hires. Credential and employment validation, public record and adverse media review, reputational assessment, and identity assurance against synthetic and AI-assisted candidate fraud. To an investigative standard, not a screening-vendor standard.
Background and vetting program governance	Assessment and design of the client's own vetting apparatus. Position risk designation, screening scope proportionate to role sensitivity, reinvestigation frameworks, adjudication standards, contractor and third-party personnel assurance, and governance of the vendors screening on their behalf.
Insider threat	Program design, assessment, and maturity evaluation. Behavioral and technical indicator frameworks, detection and referral pathways, governance across security, HR, and legal, privacy and civil liberties safeguards, case management, and response planning. This is where the three domains most visibly converge.
Leadership and succession risk	Board and executive assessment of exposure created by leadership concentration, planned or unplanned succession, and transformation mandates. Key person dependency, single points of institutional knowledge, and the risk a given transition introduces.
Workforce and personnel assurance	Continuous evaluation for privileged and trusted populations, separation and offboarding risk, access revocation discipline, and the human indicators that precede loss events.
AI hiring governance	Assessment of automated employment decision tools against emerging state regimes. Bias audit readiness, candidate notification and alternative assessment obligations, vendor governance, and documentation that survives regulatory examination.

Human Risk is a governance and assurance discipline. It is not recruitment and it is not staffing. Apogee governs the people function; it does not fill the roles.

SECTION 5

How Organizations Engage: Four Services, One Ladder

Four services, each delivered across the three Nexus domains. The first three are discrete engagements and are usually how a client meets the firm. The fourth is Apogee's principal service and the relationship every engagement builds toward.

01 Assessment

The client's risk posture measured against a framework. A documented gap analysis and prioritized findings, calibrated for board consumption.

02 Strategy

A multi-year risk roadmap with sequencing, resourcing, dependencies, and decision gates. Founder-led by design.

03 Governance Design

The structures, policies, roles, and reporting by which the client governs risk going forward.

04 Sustained Engagement

Fractional security, risk, and compliance leadership. Apogee holds accountability for a defined outcome over time. The principal service.

The sustained engagement model

Accountability, not capacity. Apogee is accountable for a stated outcome. The client buys the outcome and the practitioners behind it, not hours.

Renewable six-month intervals. Each interval has objectives, deliverables, and a gate review in month five where the client renews, rescopes, scales, or concludes. The client is never committed beyond one interval.

Named practitioners. An Engagement Principal directs delivery. Specialists are named at SOW. A Principal Advisor serves as Executive Sponsor, holding the escalation path and the accountability at each gate.

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

Stepped allocation. Fees step down as the program matures. Clients pay build-phase rates during the build.

Knowledge transfer as an objective. Runbooks, trained staff, systems the client owns. If the relationship concludes, the apparatus stays.

Independence preserved. Apogee prepares, remediates, and governs. It does not attest, certify, or audit a program it built.

Two buyer conditions

WHERE THE RISK OWNER EXISTS

Apogee advises the executive

The buyer is the CISO, CRO, CSO, or public sector equivalent. That executive owns risk; Apogee brings judgment, method, and outside perspective.

WHERE THE RISK OWNER IS ABSENT

Apogee becomes the owner

The buyer is the President, CEO, or senior operating leader who sees the exposure. Apogee supplies the accountable owner through the fractional model. At a high-consequence organization, the absence of a risk executive is the buying signal, not a disqualifier.

SECTION 6

The Phase Ladder: Ascend, Meridian, Zenith

Three engagement structures, one integrated practice. Each stands on its own; together they form a ladder as an organization's needs evolve across the three Nexus domains.

	APOGEE ASCEND	APOGEE MERIDIAN	APOGEE ZENITH
Scope	Executive-grade cyber risk posture assessment, with adjacent-domain exposure reported as standard practice	Integrated assessment and governance design across all three Nexus domains	Sustained enterprise risk partnership across the full Nexus, anchored by the Rogue Risk Platform
Service	Assessment	Assessment and governance design	Sustained engagement

Structure	Fixed-fee, defined scope	Fixed-fee, scoped to client needs	Renewable six-month intervals; gate review in month five
Timeline	6 to 10 weeks	4 to 6 months	Ongoing, one interval at a time
Typical buyer	CISO, CIO, CFO, CEO	Expanded executive committee	CEO, board chair, audit committee chair
What it proves	Apogee delivers practitioner-grade work that stands on its own	Apogee operates as an integrated risk practice, not a cyber-only consultancy	Apogee is the partner the organization governs alongside

Apogee Ascend · Phase 1

Ascend establishes a defensible cyber risk picture a board, insurer, regulator, or counterparty will accept, fast. Clients retain six board-consumable deliverables: a Cyber Risk Posture Assessment Report against NIST CSF 2.0; a Cyber Risk Register the client team retains and operates after engagement close; a third-party risk posture review of supply-chain exposure; a prioritized roadmap with effort, ownership, and dependency mapping; an Executive Briefing Deck; and a Board Briefing Deck with director-audience governance framing. Where the engagement is scoped to one domain, the assessment still reports the adjacent cyber, physical, or human exposure the client is not looking at. Optional modules: penetration testing, AI Governance baseline, Cyber Insurance Readiness, and SBOM plus EO 14028 / SSDF.

Apogee Meridian · Phase 2

Meridian operationalizes the Nexus of Risk across all three domains and analyzes the intersection zones that siloed reviews miss. It is the move when the board is asking about cyber, physical, and human exposure as connected risks rather than three separate vendor reports leadership must reconcile. Deliverables include the Integrated Nexus Risk Assessment Report with intersection-zone analysis, an updated multi-domain risk register, an AI Governance framework and roadmap, a Human Risk assessment, a crisis and continuity assessment, an integrated cross-domain roadmap, a board reporting framework including SEC Regulation S-K Item 106 readiness, and executive and board briefing decks. Three named senior practitioners lead the engagement. Optional modules: TPRM program build, Cyber-Physical Convergence, Cyber Insurance Readiness, SBOM plus EO 14028 / SSDF, and a facilitated tabletop exercise.

Apogee Zenith · Phase 3 · The Flagship

Zenith is the sustained engagement: the team that builds the integrated picture continues to operate it alongside the client, holding accountability for a defined outcome across all three Nexus domains, one renewable six-month interval at a time.

At the core of every Zenith engagement is the Rogue Risk Platform, powered by Tacilent, which establishes a full risk apparatus covering the cyber, physical, and human domains. Apogee is an investor in Tacilent, its deepest partner relationship, reflecting the firm's conviction that the Risk Platform is the future of enterprise risk management: governance the client can see, operate, and keep.

Initial Integration · Months 1 through 6

- Full Nexus of Risk application across the cyber, physical, and human domains, with the strategy overlay delivered through the Apogee Vanguard GRC platform
- Rogue Risk Platform deployment: the risk apparatus stood up, populated, and operating across the three domains
- AI Governance integrated operating model, and Cyber-Physical Convergence as a core component
- A built Third-Party Risk Management program delivered as core scope
- Board and director services integration, including SEC Regulation S-K Item 106 readiness
- Human Risk assessment through the Apogee Vantage platform, including leadership and succession risk
- Governance architecture and operating-cadence design; Integrated Nexus Baseline and Roadmap

Sustained partnership · Month 7 forward

- Named senior team continuity, with an Engagement Principal directing delivery and a Principal Advisor as Executive Sponsor
- Quarterly Integrated Risk Reviews and monthly operating-cadence sessions
- Board and audit-committee engagement on a defined cadence
- On-call advisory access and an annual Strategic Refresh
- Gate review in month five of every interval: renew, rescope, scale, or conclude
- Rogue Risk Platform, Apogee Vanguard, and Apogee Vantage licensing included throughout the partnership

Right for the organization if

- The CEO, board chair, or audit committee chair is the decision authority, and the regulatory environment warrants a sustained advisory presence
- An inflection event has produced an enterprise-wide risk reassessment, or a portfolio of point vendors is producing fragmented governance
- The organization wants the risk apparatus built inside its own walls: if the relationship ever concludes, the platform, the runbooks, and the trained staff stay

SECTION 7

Accountable Executives Behind a Vendor's Motion

Two engagements place a named senior executive inside a technology vendor's go-to-market motion and hold a defined outcome. One carries the enterprise motion. The other carries the government motion. They are sold separately and can run together.

THE ENTERPRISE MOTION

Fractional Field CxO: CISO, CTO, and CIO Capability

For technology vendors scaling into the enterprise, Apogee places a seasoned Field executive, a former CISO, CTO, or CIO, into an accountability position: a named executive who holds a defined outcome for the client's enterprise motion, backed by an Apogee team delivering the governance, compliance, and build work behind it. The Field CxO speaks executive-to-executive as evangelist, technical authority, and peer to the buyer's C-suite; the team behind the seat closes the gaps that stall enterprise deals: attestation readiness, AI governance posture, security documentation, and trust-center substance. Every engagement pairs the Field CxO with a dedicated Risk Program Manager who owns cadence, deliverables, and follow-through.

ENGAGEMENT	COMPARED WITH	BUILT FOR
from $15K / month Scoped by the pursuit, the quarter, or the program	$385K to $850K+ Full-time Field CxO annual carry, before recruiting and ramp	Growth-stage vendors · Scale-ups moving upmarket · PE-backed portfolio companies · Teams between hires

THE GOVERNMENT MOTION

Market Entry Advisory: U.S. Public Sector

For technology vendors selling into government, Apogee places a senior practitioner who has sat on both sides of the government technology transaction inside the vendor's public sector motion, for long enough to build the pipeline and the evidence, and not one day longer. Federal and state relationship cycles run a year or longer, so the first twelve months produce the same leading indicators under a fractional structure as under a full-time hire, at a fraction of the loaded cost and with thirty days of termination exposure rather than a nine to twelve month mis-hire.

WORKSTREAM	WHAT THE ENGAGEMENT OWNS
Coverage model and account strategy	Segment the addressable market, size the opportunity by segment, and produce a ranked account plan naming the mission problem and the buying center for each target.
Senior engagement and pipeline	Executive-level conversations that connect capability to mission outcome, conversion of existing inbound interest into qualified opportunity, and management of the advisory and partner relationships already in place.
Acquisition pathway and channel	Validate where the vendor can transact today and where a vehicle gap blocks revenue, across schedules, governmentwide acquisition contracts, other transaction authority, cooperative vehicles, and reseller or integrator routes, then qualify the partners that close the gap.
Hire enablement and transition	Define the role the evidence supports, build the scorecard, source a candidate bench, and hand over a documented territory, pipeline, and partner map at close.

Engagements run against a published scorecard of leading and lagging measures, reviewed monthly, with a formal decision gate at month six. Apogee reports against the vendor's own system of record, not a parallel tracker.

STANDING CONDITIONS OF EVERY MARKET ENTRY ENGAGEMENT

- Apogee carries no quota, no direct reports, and no signatory authority.

- Apogee performs no activity meeting the Lobbying Disclosure Act definition and holds no registration.
- No contingent fee is accepted on any federal procurement. Performance components are tied to engagement measures, never to award value.
- An organizational conflict of interest screen runs before signature against Apogee's own active pursuits, and a conflicts register is available to the client.
- Where a Founder or practitioner holds a board seat at the client, its treatment during a paid engagement is addressed in the agreement.
- Where Apogee is itself a candidate teaming partner to the vendor, that is disclosed at engagement start in writing.

Market entry advisory operates on a different axis from assessment and attestation, so it does not engage the firm's independence boundary. Apogee advises a vendor on reaching a government buyer; it does not grade the vendor's program and then certify it.

SECTION 8

Specialty Practices

Six productized practices. Each is scoped as a standalone assessment, as a program build, or as a module inside an Ascend, Meridian, or Zenith engagement.

AI Governance

Policy, inventory, impact tiering, vendor AI review, and board reporting against the NIST AI RMF and emerging state regimes.

Cyber-Physical Convergence

The seams where systems meet facilities: OT exposure, access control, and converged governance across the cyber and physical estates.

K-12 and Higher Education Cyber

Districtwide and campus assessment, student data governance, and the preparedness that survives an audit or an incident.

Cyber Insurance Readiness

Posture evidence a carrier and broker will accept at renewal, and remediation of the controls that drive premium and coverage terms.

Board & Director Services

Director-audience briefings, board reporting frameworks, SEC Regulation S-K Item 106 readiness, and risk oversight design.

Supply-Chain and Third-Party Risk

TPRM program design and build, vendor tiering, concentration exposure, and continuous assurance over critical third parties.

SECTION 9

Platforms, Programs, and Intellectual Property

Nexus of Risk	Proprietary framework governing enterprise risk as one connected system: three domains, cyber, physical, and human, on one consequence chain.
Rogue Risk Platform, powered by Tacilent	The enterprise risk apparatus at the core of Zenith engagements, establishing full risk operating capability across the three Nexus domains. Delivered through Apogee's deepest partner relationship: Apogee is an investor in Tacilent and holds 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 human capital governance. [CONFIRM current instrument licensing before publication.]
Rogue Risk Analysis Group	Apogee's intelligence and risk analytics arm. A portfolio of Risk Analysts producing published Rogue Risk Advisories, geopolitical briefings, and sector risk intelligence, foundationally supported by the Rogue Risk Platform, so published analysis draws on the same risk apparatus that anchors client engagements.
AI leadership training	Multi-session AI leadership programs for public safety and enterprise audiences, POST certification-aligned for law enforcement.
The Risk Apogee	Podcast hosted by the Founder featuring peer-level conversations with senior risk and security leaders; keynote presence includes RSA and ISSA.

SECTION 10

Sectors Served

Apogee serves enterprises and SMBs across its core verticals. Each vertical engagement applies the same integrated lens, tuned to the regulatory authorities driving that sector's board conversation. The list is illustrative of where consequence concentrates, not a boundary.

SECTOR	WHAT IS DRIVING THE CONVERSATION	REPRESENTATIVE FRAMEWORKS
Financial Services	SEC cyber disclosure (Reg S-K Item 106), examiner pressure, third-party concentration, insurance renewal, M&A diligence	NYDFS Part 500, GLBA, FFIEC, NIST CSF 2.0, COSO ERM
Healthcare	HIPAA enforcement, ransomware and clinical downtime, medical device and IoT exposure, business-associate risk	HIPAA Security Rule, HITRUST, 405(d) HICP, NIST 800-66
State & Local Government, Law Enforcement	NIST CSF 2.0 mandates, audit and grant findings, incident readiness, AI adoption in public safety, workforce continuity	NIST CSF 2.0, POST-aligned training, tabletop programs
Federal Civilian	FISMA and RMF authorization, zero trust (OMB M-22-09), EO 14028 software supply chain, FedRAMP readiness, agency AI governance	FISMA, NIST 800-53, FedRAMP, Zero Trust (800-207), SSDF
Defense	CMMC assessment readiness, CUI handling, defense industrial base supply-chain assurance, OT and control-system exposure	CMMC, NIST 800-171, NIST 800-172, DFARS
Education, K-12 and Higher Ed	Districtwide and campus cyber posture, student data governance, grant and audit findings, incident readiness	NIST CSF 2.0, FERPA, state student data regimes
Critical Infrastructure	CISA directives and CPGs, OT / ICS exposure, CIRCIA reporting readiness, cyber-physical convergence, supply-chain dependency	NERC CIP, TSA directives, NIST 800-82, IEC 62443
Technology	Enterprise due diligence, SOC 2 / ISO 27001 attestations, AI governance under board scrutiny, selling to government, funding and M&A diligence	SOC 2, ISO 27001, NIST AI RMF, SBOM / EO 14028
M&A	Buy-side and sell-side risk substantiation and due diligence support, including human risk diligence on leadership and key personnel	NIST CSF 2.0, TPRM, COSO ERM

Beyond the core verticals, the consequence test extends the practice into maritime and logistics, regulated industries broadly, and distributed physical operations. A small maritime operator carrying CUI ahead of a CMMC assessment qualifies; a large company with nothing meaningful at stake does not.

SECTION 11

Proof Points, Practitioners, and Leadership

50+
Engagements completed across SMB, healthcare, financial services, and public sector

90%+
Client retention, 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

Representative engagements

Client identities are withheld consistent with Apogee's confidentiality practice. All references below are approved, anonymized engagements. Client references are provided on request following a briefing.

ENGAGEMENT	SCOPE
California Municipality	Virtual CISO under a five-year municipal contract. A named vCISO from the Apogee bench carries the security program, supported by a security engineer, GRC consultant, and program manager.
Cybersecurity Software Company	Cyber risk assessment spanning enterprise cybersecurity, AI implementation, and incident response review.

Graduate Business School	Four-phase, 90-day strategy engagement: competitive analysis, region-by-region assessment, and organizational structure review, culminating in a board-ready growth plan.
Professional Membership Association	Cybersecurity risk assessment for a national actuarial body.
AI SaaS Serving the Defense Industrial Base	FedRAMP Moderate equivalency: Rev 5 gap analysis, control remediation, body of evidence, and 3PAO readiness in 90 days.

Further engagements, client identities withheld under confidentiality

- State judiciary, 3,000+ employees: NIST CSF 2.0 cybersecurity risk assessment and full remediation roadmap delivered at enterprise scale.
- County government agency: risk-management course instruction and leadership-development program.
- Law enforcement agency, 200+ officers: four-session AI leadership training program, POST certification-aligned.
- 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.
- Enterprise real estate firm: cyber risk advisory spanning vulnerability assessment and governance program build.

The Practitioners

M.K. Palmore — FOUNDER & PRINCIPAL ADVISOR

A career spanning national security, federal law enforcement, and Fortune 500 enterprise security. M.K. Palmore is a U.S. Naval Academy graduate and Marine Corps officer, a retired FBI senior executive who directed cybersecurity investigations at the highest levels of federal law enforcement, and holds the CISSP, the Carnegie Mellon CISO certificate, and an MBA from Pepperdine. Private-sector cybersecurity leadership includes VP and Field CISO at Palo Alto Networks and cybersecurity executive at Google Cloud. He hosts The Risk Apogee podcast, has keynoted at RSA and ISSA, and has convened 200+ C-level leaders through the Executive Dinner Series over five-plus years.

Delivery bench

The commitment that every engagement names an Engagement Principal and an Executive Sponsor before work begins rests on a bench of Principal Advisors by domain. For a teaming partner, these are the practitioners available to be named as key personnel on a submission.

DOMAIN	PRINCIPAL ADVISOR
Strategy & Organizational Resilience	M.K. Palmore, Founder & Principal Advisor
Cyber Risk	Principal Advisor, Cyber Risk; with a second Principal Advisor carrying privacy and regulatory exposure
Physical Security	Principal Advisor, Physical Security
Public Safety	Principal Advisor, Public Safety
Human Risk	Human Risk Lead, Rogue Risk Analysis Group
Business Operations & Public Sector Capture	Principal Advisor, Business Operations. Capture role, not delivery.

[CONFIRM before publication: credential records on file for Physical Security and Human Risk, and the bid role label for the Human Risk lead. Names are withheld pending that confirmation and are inserted at layout.]

Advisory Board

LTG Omar Jones, USA (Ret.)
Defense and Government

Gail Gottehrer, Esq.
Law, AI, and Data Privacy

Brian Grayek
Cybersecurity

Renee Wynn
Federal Technology; former NASA CIO

Kasia Hanson
Physical Security, Cybersecurity, and AI

Mike Skurko
Technology

Teri Cotton Santos
Former Enterprise Risk & Compliance Officer

SECTION 12

Certifications, Vehicles, and Partnership Pathways

Apogee's certifications provide preferential access to federal and state contracting pools, a structural advantage for public sector clients and teaming partners.

- **SDVOSB (SBA-certified):** Federal set-aside eligibility with sole-source authority; the federal three percent SDVOSB contracting goal represents a substantial annual target pool.
- **VOSB (SBA-certified):** Veteran-owned small business eligibility alongside the SDVOSB certification.
- **California DVBE:** Three percent participation goal and streamlined SB/DVBE option procurement across California state agencies; certification valid through 02/28/2027.
- **California DGS Small Business:** State small business certification supporting California SB preference and bid evaluation incentives.
- **Maryland preferences:** VSBE and SBR certifications active for Maryland state and local procurement vehicles.

UEI / CAGE	HOW TO ENGAGE	INSURANCE
NFDUQKK8E6N3 / 08WU4 SAM.gov Active, All Awards	Direct award · SDVOSB set-aside · SDVOSB sole source · Competitive task order · Prime / sub teaming · GSA Schedule (pending)	Professional Liability (E&O) · General Liability · Cyber Insurance · Workers Compensation

NAICS codes: 541611 (primary), 541512, 541511, 541519, 541513, 541618, 541690, 561621, 518210, 541612, 611430, 541720, 541990, 541330, 541614, 541613.

Partnership Pathways

Apogee partners in five principal modes. Each pathway begins with a scoping conversation routed through the contact on the final page.

Strategic platform partnership, Tacilent. The deepest partner relationship Apogee holds. Apogee is an investor in Tacilent, developer of the Rogue Risk Platform, reflecting a shared conviction that the Risk Platform is the future of enterprise risk management. The platform anchors every Zenith engagement and establishes the client's full risk apparatus across the three Nexus domains.

Prime contractors and GovCon teaming. Apogee carries real, senior-practitioner delivery capability behind its certifications: assessment, governance, resilience, and leadership workstreams that slot into larger federal, state, and local pursuits as a certified SDVOSB and DVBE subcontractor or teaming partner.

Technology and delivery partners. Established relationships across cleared federal cyber, large-scale IT modernization, healthcare delivery, forensics and eDiscovery, investigations, and security tooling demonstrate the model: partners bring adjacent technical depth; Apogee brings the integrated governance layer and executive access.

Vendor go-to-market partnerships. Two engagements place an accountable executive and a delivery team behind a vendor's motion: the Fractional Field CxO program for the enterprise motion, and Market Entry Advisory for the U.S. public sector motion. Both are described in Section 7.

Media, analyst, and event partnerships. Practitioner spokespeople are available for interviews, contributed bylines, podcast guesting, and keynotes on enterprise risk convergence, AI governance, cyber-physical convergence, human risk governance, and public sector risk leadership.

What a teaming partner should expect from Apogee

Workshare and scope	Apogee requires a stated workshare percentage, a defined scope split, and named key personnel in the teaming agreement before a submission. Scope dilution on a large prime's bid is the failure mode Apogee guards against.
Evidence supplied	SAM registration, UEI and CAGE, certification letters with expiration dates, insurance certificates, W-9, rate card, notice period, and references with reachable points of contact.
Evidence required	The same, in return, plus written confirmation that the partner is not on a competing team for the same pursuit.

Independence	Apogee does not attest, certify, or audit a program it built. On a teamed pursuit this is confirmed in writing where the scope touches assessment and remediation together.
Process	Mutual NDA, then a pursuit-specific teaming agreement. Apogee does not name a partner on a submission before both are executed, and expects the same discipline in return.

SECTION 13

For Journalists and Event Programmers

Apogee's editorial posture is calm, structural, governance-grade analysis rather than threat hype. Spokespeople speak to frameworks and decisions, not fear.

Story angles Apogee can substantiate

- Risk convergence as a governance question: why cyber, physical, and human exposure now land on the same board agenda
- Human risk as the ungoverned domain: insider threat, executive due diligence, and AI-assisted candidate fraud
- SEC Regulation S-K Item 106 and what boards are actually being asked to disclose
- AI governance in the enterprise and in public safety, including POST-aligned law enforcement leadership training
- Cyber-physical convergence in critical infrastructure and healthcare
- What it actually takes for a technology vendor to sell into government, and why most get the sequence wrong
- The small-firm, senior-practitioner alternative to Big Four advisory models

Ground rules

- Client identities and engagement details are not disclosed without written client approval; scenarios used publicly are labeled illustrative unless client-approved
- Apogee does not attribute cyber incidents to specific threat actors and does not comment on active procurements or firm commercials
- Approved biographies, headshots, the firm fact sheet, and the public Nexus of Risk explainer are available in the standard media kit on request

Media inquiries: info@apogeeglobalrms.com, attention Communications.

Contact

Email	mkp@apogeeglobalrms.com · info@apogeeglobalrms.com
Phone	(408) 256-2198 · (415) 251-5510
Web	apogeeglobalrms.io
Mail	2059 Camden Avenue, Suite 242, San Jose, CA 95124
Next step	Schedule a scoping conversation via the contact above



APOGEE GLOBAL RMS, LLC · SDVOSB / VOSB / DVBE

Risk advised as one connected system.