SERVICE SCHEDULES

GEN ETH, INC. d/b/a CMDash

Version 1.0 · November 18, 2026

GENERAL TERMS FOR ALL SCHEDULES

G1. Application. Each Schedule below describes one professional services offering. A Schedule takes effect only when an Order identifies it. It is governed by the Master Services Agreement between the Parties or, for a purchase through AWS Marketplace, by the Standard Contract for AWS Marketplace as amended by Provider's Professional Services Amendment (in either case, the "Governing Agreement"). Capitalized terms have the meanings given in the Governing Agreement. Under the AWS Marketplace option, "Provider" means the Licensor, "Client" means the Buyer and "Client Materials" means the Buyer Materials.

G2. Scope. The exclusions listed in each Schedule are illustrative and not exhaustive. Anything a Schedule does not expressly state as in scope is out of scope. Where a Schedule states scope limits, they apply unless the Order states different ones. Within those limits, the accounts, sites, systems, frameworks and documents in scope are those stated in the Order or in the scoping record the Parties agree at Kickoff; a change to them after they are agreed is a change of scope. No Schedule includes remediation. Out-of-scope work is performed only under a Change Order accepted before the work begins, at the rate stated in the Order ($300 per hour, billed in 30-minute units, unless the Order states another rate).

G3. Governing Agreement Applies. The acknowledgements, disclaimers, reliance provisions, intellectual property provisions and limitations of liability in the Governing Agreement apply to every Schedule, including a Schedule provided at no charge. Deliverables are licensed to Client and are not assigned, and nothing produced under a Schedule is a work made for hire, except as the Governing Agreement and the Order expressly provide.

G4. Fees. The Fee shown in a Schedule is Provider's list fee for a direct purchase on the version date above. The Fee that applies is the one stated in the Order, and for an AWS Marketplace purchase, in the private offer. No Fee includes a CMDash plan, taxes, or Client's cloud infrastructure and other third-party costs.

G5. Kickoff, Timing and Delivery. Provider confirms the Kickoff date after the Order is placed, according to its availability. A delivery period stated in a Schedule runs from Kickoff and only while Client is meeting its responsibilities; where a Schedule states none, the Parties agree the dates at Kickoff. The Delivery Date is the date Provider records for the final session or final Deliverable or, for a Service that ends with a finished file or kit, the date Provider sends it.

G6. Cancellation and Refund. Client may cancel an Order in writing before Kickoff begins and receive a full refund. Kickoff is the start of work, and the Fee is not refundable once it has begun, except as the Governing Agreement provides.

G7. Access and Data. Provider works with read-only, least-privilege access and deploys no agents. Client will not send Controlled Unclassified Information, export-controlled data, classified information, protected health information or payment card data to Provider, and will not place any of it in hosted CMDash. Material of that kind is viewed only in place, inside systems Client controls.

G8. Questions After Delivery. For thirty (30) days after the Delivery Date of a Schedule with a Fee, Provider will answer Client's reasonable e-mail questions about the findings and recommendations in the Deliverables. This does not include new analysis, remediation or work outside the Schedule, and it does not apply to Schedule 1.

G9. CMDash. Where a Schedule records information in CMDash or requires a CMDash organization, Client's use of CMDash is governed by the Platform Terms, the frameworks, integrations and features available are those of Client's CMDash plan, and what Provider records there is Client's data. Unless a Schedule says otherwise, an organization on any plan, including the Free plan, is sufficient.

G10. Credit Toward an Annual CMDash Plan. If Client signs an annual CMDash plan directly with Provider after buying a Service under these Schedules and within sixty (60) days after that Service's Delivery Date, Provider will credit twenty percent (20%) of the Fee paid for that Service to that plan. Each purchase earns one credit, calculated on the Fee and not on tax. Only the first purchase of a Service earns a credit; a renewal, and any billing period after the first of a recurring Service, earns none, so for Fractional Security Leadership the credit is calculated on the first month's Fee

only. All credits on one plan together will not exceed that plan's first-year list price. No credit is earned for a monthly plan, for an annual plan signed before the Service was bought or after the sixty days, for a Service provided at no charge, or where the Fee for the Service is refunded or reversed. A Service bought through AWS Marketplace earns no credit, and no credit is applied to a plan bought through AWS Marketplace. The credit is applied to Client's CMDash account against later invoices and is never paid in cash.

SCHEDULE 1 · AWS CLOUD SECURITY POSTURE REVIEW

Fee: No charge. One review for each organization in any twelve (12) month period.

Timing: One remote review session of up to two (2) hours, on a date the Parties agree.

A. Scope. An automated, read-only review of the security posture of up to three (3) Amazon Web Services accounts that Client designates, in all Regions, covering identity and access, logging and monitoring, configuration and compliance, data protection, and multi-account guardrails. The review uses the read-only AWS and AWS Security Hub integrations of CMDash and an open-source configuration scanner that Provider runs through a scoped read-only role. No agents are installed and no write permission is requested. It is followed by one remote review session led by Provider's CISSP-credentialed Principal Consultant.

B. Deliverables. (1) An automated report sent before the review session, with each finding rated by severity and mapped to the security pillar of the AWS Well-Architected Framework. (2) The review session. (3) A one-page e-mail, sent on the day of the review session, listing the top five actions and next steps.

C. Exclusions. Remediation of any finding; penetration testing; review against any control framework for certification or attestation purposes; a written narrative report or summary beyond the automated report and the action e-mail; support or questions after the review session; continuing monitoring; review of more than the three designated accounts.

D. Client Responsibilities. A CMDash organization with its read-only AWS and AWS Security Hub integrations connected to the designated accounts; a scoped read-only role in each designated account, created and later removed by Client; a named technical contact; and attendance at the review session. Client starts the CMDash organization on CMDash's standard trial under the Platform Terms. A payment method is required to start the trial, and the trial converts to a paid plan at the end of the trial period unless Client cancels before then, as the sign-up page states. The review itself carries no charge, and Client is not required to keep a paid plan.

E. Acknowledgement. This Schedule is provided at no charge and “as is.” The disclaimers, reliance provisions and limitations of liability in the Governing Agreement apply in full despite the absence of a Fee. Provider deletes the Client Materials it holds for this Schedule, including the raw scanner output, within fourteen (14) days after the review session.

SCHEDULE 2 · CMMC LEVEL 2 READINESS REVIEW

Fee: $28,500, one time

Timing: Written Deliverables within six (6) weeks after Kickoff.

A. Scope. A readiness review of Client's environment and organizational practices against the one hundred ten (110) security requirements of NIST SP 800-171 that apply to CMMC Level 2 on the Order date, across the Amazon Web Services and AWS GovCloud (US) accounts within the scope boundary that Client confirms in writing. The review covers the scoping of the Controlled Unclassified Information boundary, read-only review of the in-scope AWS configuration through a scoped role, review of Client's existing policies, procedures and prior self-assessment work, and interviews with Client's personnel. Scope limits: one (1) Controlled Unclassified Information boundary, up to six (6) AWS accounts across the commercial and GovCloud partitions, up to two (2) sites, and up to six (6) interview sessions. Anything beyond these limits is a change of scope and is handled by Change Order.

B. Deliverables. (1) An environment scoping memorandum recording the Controlled Unclassified Information boundary that Client confirms. (2) A control-by-control gap analysis across all 110 requirements, scored, with evidence gaps identified. (3) A System Security Plan outline. (4) A Plan of Action and Milestones with owners, target dates and effort estimates. (5) A remediation roadmap sequenced by assessment risk. (6) An executive readout.

C. Exclusions. A certification assessment or any assessment result, which only an authorized CMMC Third-Party Assessment Organization (C3PAO) or the Government decides; any service reserved to a C3PAO or other authorized body; remediation of any finding; authoring of complete policies, procedures or a complete System Security Plan;

penetration testing; calculating, entering or submitting any score or affirmation in the Supplier Performance Risk System or any other government system; preparation, support or review of any affirmation submitted to a government body; receipt, storage or handling of Controlled Unclassified Information by Provider outside Client's environment.

D. Client Responsibilities. Definition and written confirmation of the scope boundary; read-only access to in-scope systems, configured so that it does not permit reading stored data; availability of subject-matter experts for interviews; and timely provision of existing policies, diagrams, procedures and evidence. Client decides whether any Deliverable is itself Controlled Unclassified Information; if it is, the Deliverable is produced and kept inside Client's environment and Provider keeps no copy.

E. Acknowledgement. THIS IS A READINESS REVIEW. IT IS NOT A CMMC ASSESSMENT, CERTIFICATION OR AFFIRMATION. Provider is not a C3PAO and does not act as a CMMC assessor. The scores in the gap analysis are Provider's advisory estimates and are not Supplier Performance Risk System scores. The Plan of Action and Milestones is a planning document; it is not a statement that any requirement may lawfully remain open at the time of a certification assessment. Provider makes no representation that Client will achieve any CMMC level or status, any score, or any contractual or regulatory outcome. Having provided this readiness review, neither Provider nor its Principal Consultant will act as, or for, the C3PAO that assesses Client, and Provider does not recommend or select a C3PAO.

SCHEDULE 3 · AI GOVERNANCE READINESS: ISO/IEC 42001 AND NIST AI RMF

Fee: $18,500, one time

Timing: Deliverables within four (4) weeks after Kickoff.

A. Scope. A readiness review of Client's artificial intelligence workloads on Amazon Bedrock and Amazon SageMaker, and of the related AWS configuration that governs them (including, where in use, Amazon Q, AWS CloudTrail, Amazon Macie, AWS Key Management Service and AWS Identity and Access Management), against the Annex A controls of ISO/IEC 42001 and the Govern, Map, Measure and Manage functions of the NIST AI Risk Management Framework, within the scope boundary agreed in writing with Client. The review consists of discovery workshops with Client's stakeholders, a read-only review of the in-scope configuration through a scoped role, and a gap analysis. Scope limits: up to twelve (12) AI systems, up to four (4) AWS accounts, and up to three (3) discovery workshops. Anything beyond these limits is a change of scope and is handled by Change Order.

B. Deliverables. (1) An inventory of the in-scope AI systems, with owners, data flows and risk classification, based on the information Client provides. (2) An ISO/IEC 42001 gap analysis against the Annex A controls, scored, with evidence gaps identified. (3) A NIST AI RMF mapping across Govern, Map, Measure and Manage. (4) A draft AI governance policy set covering acceptable use, model approval, data handling, human oversight and AI incident handling, for Client's review and adoption. (5) A control set formatted for import into Client's governance, risk and compliance platform. (6) A board-ready briefing on Client's AI risk posture.

C. Exclusions. Certification against ISO/IEC 42001, which only an accredited certification body performs; model evaluation, red-teaming, bias testing or safety testing; a legal or regulatory opinion on any law or regulation governing artificial intelligence; adoption, implementation or enforcement of the draft policies; remediation of any finding; review of workloads outside the agreed boundary.

D. Client Responsibilities. Read-only access to in-scope workloads and model configurations; documentation of intended use, data sources and human oversight arrangements; attendance of AI, security and legal stakeholders at the workshops; and availability of the personnel accountable for the workloads.

E. Acknowledgement. Provider does not certify conformity with ISO/IEC 42001 and gives no opinion on whether any workload complies with any law or regulation governing artificial intelligence. The policy set is a draft: Client is responsible for reviewing, adapting, approving and enforcing it.

SCHEDULE 4 · FRACTIONAL SECURITY LEADERSHIP

Fee: $9,500 per month, recurring

Timing: Minimum term of three (3) monthly billing periods, during which neither Party may cancel for convenience. After the minimum term the Service continues month to month, and either Party may cancel by written notice given before the next monthly renewal; the cancellation takes effect at the end of the month then paid for. This is the cancellation rule for this Schedule.

A. Scope. Director-level security leadership for an organization that runs on Amazon Web Services, at approximately twenty (20) hours per calendar month. Provider leads the security program on Client's behalf, under the direction of Client's executive sponsor: it produces and maintains the program's documents and reporting and coordinates the program's work, using read-only access to Client's AWS security services and telemetry. Client retains accountability for the program and makes every decision.

B. Deliverables. (1) Within the first thirty (30) days, a baseline review, an initial risk register and a security program roadmap. (2) The roadmap, maintained and sequenced against Client's compliance obligations and business priorities. (3) A policy and standards set, as agreed in the roadmap, authored and kept current. (4) A maintained risk register with owners, treatment decisions and status. (5) Vendor and third-party risk reviews for the suppliers Client refers. (6) A monthly report of key performance indicators drawn from Client's AWS security telemetry. (7) A quarterly board or executive readout, prepared and presented.

C. Exclusions. Hours beyond the monthly commitment, which require a Change Order; availability outside Provider's business hours (Monday to Friday, 9:00 a.m. to 6:00 p.m. U.S. Eastern Time); an incident response retainer or on-call coverage; hands-on administration of, or write access to, Client's systems; certification or any assessment result; remediation. Unused hours do not carry forward from one month to the next.

D. Client Responsibilities. A named executive sponsor with decision-making authority; read-only access to systems, personnel and documentation; timely decisions on the matters Provider raises; and adoption and approval of each policy before it takes effect. If Client stops the Service or its payments during the minimum term, the Fees for the rest of the minimum term remain payable.

E. Acknowledgement. PROVIDER IS AN INDEPENDENT CONTRACTOR AND IS NOT AN OFFICER, DIRECTOR, EMPLOYEE, FIDUCIARY OR AGENT OF CLIENT. Provider does not assume, and Client will not hold Provider or its Principal Consultant out as holding, any statutory, regulatory or fiduciary office of Client, including any role as Chief Information Security Officer of record, senior accountable official, affirming official, or signatory for any regulatory filing, attestation or affirmation, unless the Parties agree otherwise in a separate writing signed by an officer of Provider. All decisions, approvals and risk acceptances remain Client's.

SCHEDULE 5 · CMDASH LAUNCH

Fee: $4,500, one time

Timing: Delivered within five (5) business days after Kickoff. The period runs from the date Client has provided everything listed in Section D.

A. Scope. Set-up of the CMDash Program Builder for Client's organization, worked through with Client: users and roles, dashboards and alert rules; up to three (3) control frameworks enabled, with Client's existing controls mapped to them; up to three (3) integrations from CMDash's live catalog connected; Client's existing risk register, Plan of Action and Milestones and policy list imported from Client's spreadsheets; and one (1) administrator session of up to ninety (90) minutes.

B. Deliverables. Client's CMDash organization configured as described in Section A; a one-page administrator guide; and a next-steps checklist.

C. Exclusions. Any review, assessment or gap analysis; authoring of policies or a System Security Plan; remediation of any finding; development of custom connectors, or integrations beyond three from the live catalog; data cleansing or reconstruction of incomplete Client records; frameworks, integrations or features that Client's CMDash plan does not include.

D. Client Responsibilities. A CMDash organization (any plan); Client's existing controls, risk register, Plan of Action and Milestones and policy list in a readable spreadsheet format at Kickoff; administrative credentials for the integrations to be connected; and attendance at the administrator session.

E. Acknowledgement. This is a configuration service. Provider maps and imports Client's records as Client supplies them and does not verify their accuracy or completeness. The Service is not a review of Client's controls or compliance.

SCHEDULE 6 · SIGNER'S FILE REVIEW

Fee: $2,500 per year, renewing each year until cancelled. Client may cancel at any time before the renewal date.

Timing: One review in each annual period, at a time the Parties agree on reasonable notice before Client's affirming official intends to sign.

A. Scope. A review of each statement in Client's Signer's File against the supporting records and evidence that Client furnishes, identifying statements that are contradicted, unsupported or imprecise on the face of that evidence. Includes one (1) review session with Client's affirming official.

B. Deliverables. A written review note to be kept with the file, and a list of the contradictions identified, each with a suggested route to fix, disclose or narrow it.

C. Exclusions. Legal advice of any kind; preparation, review, endorsement or submission of any affirmation, attestation or certification, which Client's affirming official alone makes; remediation of any finding; any assessment, audit or certification, which only an authorized assessor or accredited body performs; independent verification of the authenticity or completeness of the records furnished.

D. Client Responsibilities. The complete Signer's File and all supporting records and evidence; identification of the officer or officers responsible for any affirmation; timely response to requests for clarification; and independent legal advice on whether and how to affirm.

E. Acknowledgement. PROVIDER DOES NOT MAKE, SIGN, ENDORSE, ADOPT OR RECOMMEND ANY AFFIRMATION, ATTESTATION, CERTIFICATION OR REPRESENTATION SUBMITTED BY CLIENT TO ANY GOVERNMENT BODY, REGULATOR, CERTIFYING AUTHORITY, CUSTOMER OR COUNTERPARTY. Client and its officers remain solely responsible for determining whether any statement they affirm is accurate and complete, and for obtaining independent legal advice on that question. This review does not constitute, and may not be relied upon as, a reasonable basis, a due-diligence defense or other support for any affirmation. Provider reviews only the records Client furnishes and does not independently verify them.

SCHEDULE 7 · IACS UR E26 AND UR E27 READINESS REVIEW

Fee: $9,500 per vessel class, one time

Timing: Dates agreed at Kickoff.

A. Scope. A readiness review of one (1) vessel class against IACS Unified Requirement E26 (Cyber resilience of ships), and of the in-scope on-board systems against the maker documentation that IACS Unified Requirement E27 calls for, based on the documentation that Client or its suppliers furnish. Scope limits: one (1) vessel class and up to twelve (12) on-board systems. Anything beyond these limits is a change of scope and is handled by Change Order.

B. Deliverables. Gaps recorded against each requirement in Client's CMDash organization, with owners; a prioritized remediation list; and one (1) readout session.

C. Exclusions. Class approval, class survey, plan approval or any service reserved to a classification society; penetration testing or on-board technical testing; remediation of any finding; review of vessel classes or systems beyond those identified in the Order; verification of maker documentation against as-installed equipment.

D. Client Responsibilities. A CMDash organization; the vessel class documentation, system inventories and maker documentation; identification of the in-scope systems; and availability of technical and operational personnel.

E. Acknowledgement. Provider is not a classification society and does not grant, recommend or influence class approval. This review does not guarantee that any vessel or system will satisfy a classification society, flag administration or survey.

SCHEDULE 8 · M&A CYBER DILIGENCE

Fee: $7,500 per target company, one time

Timing: Dates agreed at Kickoff.

A. Scope. Issue of a cyber diligence questionnaire to one (1) target company that Client designates; review of the documents that target returns; and review of that target's publicly observable security posture. Scope limits: one (1) target company, up to forty (40) documents returned by the target, and one (1) round of clarification questions. Anything beyond these limits is a change of scope and is handled by Change Order.

B. Deliverables. A written memorandum of the risks identified and of first-hundred-day items; one (1) readout to Client's deal team; and the findings recorded in the mergers and acquisitions diligence module of Client's CMDash organization.

C. Exclusions. Penetration testing or any active testing of the target's systems; legal, regulatory, accounting, tax or valuation opinions; remediation of any finding, at the target or elsewhere; verification of the target's responses; review of any target beyond the one designated; any opinion on the merits, pricing or structure of a transaction.

D. Client Responsibilities. A CMDash organization; designation of the target and of the transaction scope; authority for Provider to contact the target, and any confidentiality agreement the target requires, which Provider signs only as a company; and timely delivery of the target's returned documents.

E. Acknowledgement. PROVIDER'S FINDINGS DEPEND ENTIRELY ON INFORMATION THE TARGET CHOOSES TO PROVIDE AND ON PUBLICLY OBSERVABLE INFORMATION. Provider does not independently verify, audit or authenticate the target's responses, and is not responsible for risks that were not disclosed, were misrepresented or were not observable within the engagement period. The memorandum is prepared solely for Client's internal use in evaluating the transaction, and may not be furnished to or relied upon by any lender, insurer, investor, seller or other third party without Provider's prior written consent.

SCHEDULE 9 · TABLETOP EXERCISE KIT

Fee: $499, one time

Timing: Dates agreed after purchase.

A. Scope. Preparation of one (1) incident-response tabletop scenario for Client's organization, from the intake information Client supplies, with its injects, participant role descriptions and a facilitator guide.

B. Deliverables. The exercise materials loaded into the Exercises page of Client's CMDash organization, and an after-action report template.

C. Exclusions. Facilitation of, or attendance at, the exercise; more than one scenario; completion of the after-action report; remediation of anything the exercise finds.

D. Client Responsibilities. A CMDash organization on a paid Essentials plan or above (a trial does not qualify); the intake information Provider requests; and nomination of a facilitator.

E. Acknowledgement. The kit is a training aid. Provider does not warrant that running the exercise will prepare Client for any actual incident or satisfy any exercise requirement of a framework, regulator or insurer.

SCHEDULE 10 · AUDIT-PREP SPRINT

Fee: $6,500, one time

Timing: Six (6) weeks from Kickoff.

A. Scope. A readiness review of one (1) framework that Client's CMDash plan includes, in the six weeks before Client's audit or assessment: each control's recorded status in CMDash is read against the evidence behind it. Includes one (1) kickoff session of sixty (60) minutes, a check-in of thirty (30) minutes in each week after the kickoff week (five (5) check-ins), and one (1) readout of ninety (90) minutes. Scope limits: one (1) framework of up to one hundred twenty (120) controls or requirements. A larger control set is read in order of priority within the six weeks, and the closing note states what was not read; reading the remainder, or a second framework, is a change of scope and is handled by Change Order.

B. Deliverables. (1) Every gap identified, listed and recorded in Client's Plan of Action and Milestones in CMDash, with an owner and a target date. (2) An evidence request list for the audit set up in CMDash, with read-only access prepared for the auditor or assessor Client has chosen. (3) The readout. (4) A written note of what is closed and what is still open.

C. Exclusions. The audit, assessment or certification and its result, which only an independent auditor, authorized assessor or accredited body decides; choosing or recommending an audit or assessment firm; writing policies or a System Security Plan; remediation; penetration testing; a second framework; attending audit fieldwork, or answering the auditor or assessor on Client's behalf.

D. Client Responsibilities. A CMDash organization on a plan that includes the framework (an organization on the Free plan is sufficient for the framework the Free plan includes); control statuses and evidence recorded in CMDash before Kickoff; the framework, the audit or assessment date and the firm Client has chosen; named control owners who act between check-ins; and member access to the organization for Provider's Principal Consultant. Client itself gives the auditor or assessor its read-only access.

E. Acknowledgement. THIS IS A READINESS REVIEW. IT IS NOT THE AUDIT, ASSESSMENT OR CERTIFICATION, AND IT DOES NOT PREDICT THE RESULT. Provider reads the statuses and evidence Client has recorded and does not independently verify them. Provider has no working relationship with Client's auditor or assessor, does not choose or recommend one, and does not act as or for one.