Management statement on the information security management system

Management assertion, not a certificate and not a certification body finding

Entity: Dephiant Consulting Inc.
Registered address: 5510 Cherokee Ave, Suite 300, Alexandria, Virginia 22312, United States
Signed by: Cleandra LeSane, Chief Executive Officer, Dephiant Consulting Inc.
Issued: 2026-11-22
Management system artifacts complete: 50 percent
Certificate held: None. No stage one audit has been booked.

Purpose and limitations of this statement

This document is a statement by the management of Dephiant Consulting Inc. about its information security management system. It is not a certificate, it is not an accredited certification body's finding, and it is not a stage one or stage two audit report. Dephiant Consulting Inc. does not hold an ISO 27001 certificate, a SOC 2 Type 1 or Type 2 report, a CMMC certification, or a FedRAMP authorization. Any party relying on this document should read it as management's own assertion, supported by dated evidence that is available for inspection, and nothing more than that.

Scope of the management system

The information security management system covers the advisory, assessment, and managed advisory services we deliver to clients, the people who deliver them, and the systems that hold client material. It is a single location and a single legal entity, which keeps the management system proportionate to the size of the firm.

Risk assessment and treatment method

Risk is assessed against confidentiality, integrity, and availability for each information asset, using the same register and the same scoring method we run for clients. Treatment decisions are recorded with an owner and a review date, and accepted risk is signed by the CEO rather than absorbed quietly.

Statement of applicability

The statement of applicability lists every Annex A control, whether it applies, the justification either way, and the control reference in our own register. A control marked not applicable carries a written reason, because an auditor will test that reason before accepting it.

Management assertion

Management asserts that the controls described in the attached extract are documented, assigned to a named owner, and operating as described, except for those recorded with a status of in progress or planned, which are listed separately with the window in which they are scheduled. Management further asserts that the management system artifacts listed in this statement are at the state recorded against each one, currently 50 percent complete by artifact, and that We operate a documented control set aligned to SOC 2 trust services criteria, ISO 27001 Annex A, and the NIST SP 800-171 practices that CMMC Level 2 assesses. We hold no SOC 2 report and no CMMC certification, because those come from an independent auditor or an authorized assessor. What we do hold is a register of controls, named owners, and dated evidence, which we review every quarter and will walk a client or their auditor through on request.

How the register and the management system are maintained

The register is reviewed on this cadence: Every quarter, with three controls tested in depth each cycle so every control is tested at least once a year. Client security questionnaires and vendor diligence requests are answered from this register only. Nobody answers a diligence question from memory. Where the register and any public statement disagree, the public statement is corrected, not the register.

Relationship to our SOC 2 work

The control build serves both frameworks. The SOC 2 examination tests control design and operation over a period. ISO tests whether a management system governs those controls and improves them. Running them together saves roughly a third of the effort compared with running them apart.

Artifacts not yet complete

Management system artifacts recorded as in progress or not started are listed in the attached extract with their clause and the proof that will close them. They are disclosed here rather than omitted, because a client discovering them later is worse for both parties.

Client information handling

Client material is held in approved stores only, separated by client, retained only as long as the engagement and the agreed retention period require, and returned or destroyed on request with a record of the destruction. Subcontractors are assessed and bound to the same obligations before they touch client material.

Certification path

Certification requires a stage one audit of the documented management system, then a stage two audit of it operating, both performed by an accredited certification body. A surveillance audit follows annually, and recertification every three years. We treat the annual surveillance cost as part of the decision, not a surprise after it.

What we will do on request

We will provide the statement of applicability extract relevant to your engagement, the written risk method, a walkthrough of the evidence behind any clause or control you name, and a completed diligence questionnaire answered from the record. Where we do not hold something you require, we say so in writing.

Signature

Signed for and on behalf of Dephiant Consulting Inc. by Cleandra LeSane, Chief Executive Officer, Dephiant Consulting Inc.. This statement is reissued every quarter with the register review, and on request where a procurement needs a letter dated inside a stated window.

Annex A mapped controls operating, with evidence available

GOV-01 (SOC 2 CC1.1; ISO 27001 A.5.1; CMMC CA.L2). The CEO holds accountability for security. The compliance lane owns this register and reports it at the quarterly management review. Owner: CMP. Evidence: Quarterly management review record with the register attached.

GOV-02 (SOC 2 CC1.4; ISO 27001 A.6.3; CMMC AT.L2). Every team member completes onboarding training before client work, then annual mandatory training, recorded with evidence. A skill matrix tracks capability by role. Owner: PPL. Evidence: Training completion records and the role skill matrix.

GOV-03 (SOC 2 CC2.2; ISO 27001 A.5.10). Information handling rules cover classification, client separation, storage locations, and what never leaves the approved store. Read and confirmed at onboarding. Owner: PPL. Evidence: Signed confirmation per team member, held in the people record.

RSK-01 (SOC 2 CC3.1; ISO 27001 Clause 6.1; CMMC RA.L2). We keep our own risk register on the same standard we apply to clients, reviewed quarterly, with accepted risks signed and given a review date. Owner: ADV. Evidence: Internal risk register with dated review entries and signed acceptances.

RSK-02 (SOC 2 CC9.2; ISO 27001 A.5.19; CMMC SR). Every supplier and subcontractor is tiered, assessed at the tier their access requires, contracted with flow down terms, and reassessed on the set interval. Owner: TPR. Evidence: Vendor register with tiers, assessment dates, and signed agreements.

ACC-01 (SOC 2 CC6.1; ISO 27001 A.5.15; CMMC AC.L2). Every account, ours or in a client environment, is requested and approved on the access form, granted at the lowest level that works, and recorded with a removal date where it is time boxed. Owner: CIV. Evidence: Access register with approvals, grant dates, and removal confirmations.

ACC-02 (SOC 2 CC6.1; ISO 27001 A.8.5; CMMC IA.L2). Multi factor authentication is enforced on all company accounts and on every client system where the client permits it. Exceptions are recorded with a reason and a date. Owner: CIV. Evidence: Authentication policy enforcement report and the exception list.

ACC-03 (SOC 2 CC6.2; ISO 27001 A.5.18; CMMC AC.L2). We review access to our own systems quarterly, and we remove client access at engagement close and on the day a team member departs, with timestamps recorded. Owner: CIV. Evidence: Quarterly access review records and dated exit records.

DAT-01 (SOC 2 CC6.7; ISO 27001 A.8.12; CMMC MP.L2). Client material lives only in the approved store, in a folder restricted to assigned staff, with named expiring shares. Confidential and restricted material never travels as an email attachment. Owner: OPS. Evidence: Store configuration record, share settings, and the engagement folder access list.

DAT-02 (SOC 2 CC6.5; ISO 27001 A.8.10; CMMC MP.L2). Retention is agreed at kickoff, applied at close out, and evidenced by a destruction or return record verified by a second person. Owner: OPS. Evidence: Data return and destruction records, kept for seven years.

DAT-03 (SOC 2 P1; GDPR Article 30; ISO 27001 A.5.34). We maintain our own processing record, screen new processing activities before they go live, and run a full impact assessment when screening calls for one. Owner: CMP. Evidence: Processing record and dated screening decisions, including the not required ones.

CHG-01 (SOC 2 CC8.1; ISO 27001 A.8.32; CMMC CM.L2). Website and platform changes are reviewed before release, and client facing documents pass an independent quality review by someone other than the author. Owner: OPS. Evidence: Release records and deliverable review records naming the reviewer.

VUL-01 (SOC 2 CC7.1; ISO 27001 A.8.8; CMMC RA.L2; CMMC SI.L2). Our own platform and dependencies are scanned, findings are triaged by exposure, and closure requires a clean re-scan rather than a statement that it is fixed. Owner: CIV. Evidence: Scan records, remediation dates, and verification re-scans.

IRP-01 (SOC 2 CC7.3; ISO 27001 A.5.24; CMMC IR.L2). We run the same incident procedure internally that we run for clients: a timestamped record from the first minute, a named lead, and a lessons review within ten working days. Owner: DTR. Evidence: Incident records with timelines, and lessons reviews with owned actions.

AUT-01 (ISO 27001 A.5.31; Computer misuse and equivalent laws). No scanning, enumeration, or exploitation happens without a signed authorization letter, signed rules of engagement, and a completed go or no go checklist on the morning of testing. Owner: OFF. Evidence: Signed authorization file and completed go or no go checklists.

AUT-02 (SOC 2 CC6.7; ISO 27001 A.8.12). Findings and captured evidence live in the restricted findings store only, with the minimum data needed, personal data redacted, and no live customer records copied out. Owner: OFF. Evidence: Store access list and the evidence handling note on each finding record.

CLI-01 (SOC 2 CC2.3; ISO 27001 A.5.14). Each client has a portal holding their pack, their briefings, and the security commitments that apply to them, plus a weekly status report during active delivery. Owner: OPS. Evidence: Portal records and filed status reports.

CLI-02 (SOC 2 CC4.2; ISO 27001 Clause 9.1). Satisfaction surveys run at close out and at each quarterly review. Scores below the threshold get contact from the engagement lead within two business days and a written corrective action. Owner: OPS. Evidence: Survey records with corrective actions and closure dates.

Mapped controls not yet in place, with the scheduled window

MON-01 (in progress). Administrative activity and sign in events on our own systems are logged and alerted, with alerts routed to a named owner rather than to a shared inbox nobody reads. Scheduled: Months 2 to 4 Planned work: Central log collection for our own administrative and sign in activity, with alert rules routed to a named owner and a weekly review of what the alerts produced. Closed when a month of investigated alerts exists.

IRP-02 (in progress). We run one internal tabletop exercise each year and record the gaps as owned actions with dates. Scheduled: Months 4 to 6 Planned work: One internal tabletop exercise, facilitated against a ransomware and a client data loss scenario, with the gap list owned and dated. Repeats annually thereafter.

IRP-03 (in progress). Recovery objectives are written down for the systems we depend on, and a restore is tested annually with the measured time recorded against the objective. Scheduled: Months 4 to 6 Planned work: A recovery test that restores our working systems from backup against the stated recovery objectives, with the measured restore time recorded and compared to the objective.

Management system artifacts and their state

Clause 4.3. Management system scope statement Owner: CMP. State: done. Proof: Approved and dated scope statement naming services, people, locations, and systems.

Clause 5.2. Information security policy signed by top management Owner: CMP. State: in progress. Proof: Signed policy with a review date and evidence of communication to everyone in scope.

Clause 6.1.2. Risk assessment and treatment method Owner: ADV. State: done. Proof: Documented method plus a completed assessment showing the method applied.

Clause 6.1.3. Statement of applicability Owner: CMP. State: in progress. Proof: All Annex A controls listed with applicability, justification, and register reference.

Clause 6.1.3. Risk treatment plan with owners and dates Owner: ADV. State: in progress. Proof: Treatment plan extracted from the risk register with owners, dates, and status.

Clause 6.2. Security objectives and how they are measured Owner: CMP. State: in progress. Proof: Objectives with a measure, a target, a source, and at least one recorded measurement.

Clauses 7.2 and 7.3. Competence and awareness records Owner: PPL. State: done. Proof: Training records, the role skill matrix, and awareness campaign completion.

Clause 7.5. Documented information control Owner: CMP. State: in progress. Proof: Document register with version, owner, approval date, and review date.

Clause 8.1. Operational control evidence Owner: CMP. State: in progress. Proof: Evidence log covering at least three months for every applicable control.

Clause 9.1. Monitoring and measurement results Owner: DTR. State: in progress. Proof: Measurement records and the decisions they drove.

Clause 9.2. Internal audit program and first audit report Owner: CMP. State: not started. Proof: Audit program, audit plan, report, and nonconformity records.

Clause 9.3. Management review minutes Owner: ADV. State: not started. Proof: Minutes showing each required input, the decisions taken, and resources committed.

Clause 10.2. Nonconformity and corrective action records Owner: CMP. State: not started. Proof: Corrective action records with root cause, correction, and verified closure.