SPECIMEN ENGAGEMENT REPORT · 8 APRIL 2026 · COMPLEX TIER

Site Security Vulnerability Assessment

GREENMAR-MW-N · 20 MW solar PV · English Midlands.

SITE REFERENCE	GREENMAR-MW-N (specimen)
ENGAGEMENT REFERENCE	CA-2026-SP-01
ILLUSTRATIVE VISIT DATE	8 April 2026
TIER	Complex (single-site, mixed-asset)
ASSET PROFILE	20 MW ground-mount PV solar, English Midlands
OPERATOR	Operator-A Ltd (specimen)
SITE REP ON THE DAY	Site representative (controlled annex in live report)
ISSUED BY	M. McLean · lead analyst & remote pilot
METHODOLOGY	SANS GIAC GCTI / GOSI · Treadstone 71 CTIA · PHIA-aligned
SOURCE FRAMEWORK	NATO Admiralty Code (A1–F6)
CAPTURE WINDOW	09:25 BST → 14:18 BST · 127 min flight time
SPECIMEN REVISION DATE	v16.0 · issued 21 May 2026

CLASSIFICATION — Specimen · illustrative only · not a real engagement deliverable.
In live engagement, this report is advisory security-risk evidence for operator, broker and insurer discussion. It is not a legal opinion, regulatory determination, insurance-coverage decision or guarantee against loss.
Content is faithful to the SSVA-Field-Checklist-FILLED-EXAMPLE capture — 4 graded findings, real-format kit serials, the on-day tractor incident, the operator interview, and 90-day OSINT watch programme.
Distribution: operator · broker partner with operator consent. No third-party reliance absent separate reliance letter.

DOCUMENT MAP

Contents

About this document.

This is the engagement report for the GREENMAR-MW-N specimen visit of 8 April 2026, derived directly from the field checklist captured on the day. Four findings were graded; additional OSINT signals are held on the 90-day watch-list (Section 06) rather than presented as findings. An operator-interview section is included because Q5 in particular materially supports the renewal-evidence picture and is reproduced in the operator's own words.

This is a specimen. Asset profile, operator, role references (site representative, site manager), kit serials, interview content and findings are illustrative placeholders — modelled on the structure of a Critical Asset SSVA and on publicly reported UK renewables risk patterns. Not drawn from any specific real client. Live engagement copies follow the role-only convention described in the workflow note at Appendix A1.

01 · FOR SPONSOR & BROKER

Executive summary

AGGREGATE RISK

ELEVATED

Driven by one confirmed physical exposure (F-01 NE camera coverage gap, A1) and one high-impact credential-exposure indicator requiring operator confirmation (O-01, B2). Pack contains 4 graded findings; additional OSINT signals are held on the 90-day watch-list. A site-representative field comment indicates the NE blind spot was known locally; reproduced for operational context, not as a legal admission or corporate acknowledgement.

Aggregate-risk bands. Critical Asset uses a four-band scale — LOW · ELEVATED · HIGH · SEVERE. ELEVATED denotes one or more graded findings consistent with a recognised loss archetype where an operator-owned control-review pathway exists inside the operator's normal control cycle. Bands are banded judgements, not numerical scores.

Headline findings.

ID	Finding	Risk priority	Admiralty
F-01	NE perimeter camera coverage gap — 40 m undocumented zone overlapping the access-track terminus.	CRITICAL	A1
O-01	Shared service mailbox facilities@ observed in 2024 breach dump · 2025 dark-web cross-reference · mailbox in active operational use on site; credential validity untested.	HIGH*	B2
F-02	Access-track terminus PIR lighting (L-02) intermittent — does not reliably extend across the F-01 camera gap.	HIGH	A1
F-03	Inverter compound floodlighting partial — 2 of 4 fixtures (L-05, L-06) inoperative; compound interior under-lit at night.	MEDIUM	A1

HIGH — potentially Critical pending operator confirmation; see deep-dive O-01.*

OPERATOR'S OWN VIEW · Q5

"The NE corner — I know there's a blind spot but never had time to fix it."

— site representative, recorded in operator interview, 8 April 2026

Why this pack matters at renewal.

The confirmed physical finding and the credential indicator sit within the operator's renewal-window review horizon, in the geometric and intelligence-surface categories consistent with the UK renewables loss patterns described in the April 2026 cable-theft briefing. The report provides evidence of identified control areas and a referral pathway for qualified operator review (see Section 08); it does not specify, price, design, install, test or certify any control. The operator's Q5 response (Section 07) is recorded as a site-representative field comment for operational context, not a legal admission or corporate acknowledgement. The pre-visit OSINT pack required minor correction during the engagement — 6 cameras in service rather than 8 (operator: 2 not yet installed); the findings register reflects the as-found state.

02 · FOR THE FILE

Engagement scope & methodology

In scope.

- On-site walkdown of perimeter, access tracks, inverter and substation compounds, and camera coverage zones.
- Aerial drone capture under CAA Operational Authorisation (PDRA01-28445) — full-site orthomosaic and 3D digital twin. Primary platform M3E-SPECIMEN-01; secondary M2P-SPECIMEN-02.
- Pre-visit OSINT sweep — open-source intelligence on Operator-A, its stated O&M chain, and the surrounding cluster.
- Credential-exposure check using lawfully sourced breach datasets and dark-web reference cross-checking.
- Findings register, dual-graded for risk priority and evidence confidence (Admiralty A1–F6).
- Operator-owned control-review pathway (referral matrix) and standalone broker one-pager.
- Five-question operator interview, recorded in Section 07.
- 90-day post-engagement OSINT watch-list and one progress check-in call.

Explicitly out of scope.

- ✗ Credential testing or password validation — no attempt was made to authenticate with any exposed credential found.
- ✗ Penetration testing of OT/SCADA systems or any live operational technology.
- ✗ Hardware vulnerability assessment, panel performance or thermal-efficiency work.
- ✗ Chartered structural surveying and PCN/NDT certified inspections.
- ✗ Security-systems design, electrical installation and CCTV/perimeter specification.
- ✗ Insurance loss adjustment, claim determination or suspect identification.

How findings are graded.

Every finding carries two independent grades. **Risk priority** is a banded judgement of severity × likelihood (CRITICAL / HIGH / MEDIUM / LOW / INFORMATIONAL). **Admiralty grade** (A–F × 1–6) records the source reliability and information credibility behind the finding — e.g. on-site walkdown observations grade A1; a 2024 breach-dataset entry cross-checked against a 2025 dark-web reference grades B2.

Where a finding carries the modifier **HIGH***, the asterisk denotes a "potentially-Critical pending operator confirmation" envelope — the exposure could escalate to CRITICAL if the operator confirms an active or re-used credential, but Critical Asset does not test credentials directly. O-01 carries this modifier.

Risk-band definitions.

Band	Meaning
CRITICAL	Direct exposure overlapping high-value access, asset or recognised loss route; operator-owned control-review pathway applies inside the immediate horizon.
HIGH	Material exposure with a plausible exploitation path or degraded control.

MEDIUM	Control weakness that increases loss likelihood but does not directly expose a high-value route.
LOW	Minor weakness or hygiene issue.
INFORMATIONAL	Contextual observation, not a finding.

Methodology references — in plain English.

SANS GIAC GCTI / GOSI	Global Information Assurance Certifications in Cyber Threat Intelligence and Open-Source Intelligence — industry-recognised certifications for analytical tradecraft.
Treadstone 71 CTIA	Certified Threat Intelligence Analyst — practitioner certification covering structured analytical techniques and adversary research.
PHIA-aligned	Aligned to the UK Professional Head of Intelligence Assessment community's standards for analytical rigour and source handling.
NATO Admiralty Code	Source-grading framework: reliability A (completely reliable) → F (cannot be judged) × credibility 1 (confirmed) → 6 (cannot be judged).

03 · THE SUBSTANCE

Findings register — 4 findings, dual-graded

ID	Category	Finding (short)	Risk	Admiralty	Review category
F-01	Physical · CCTV	40 m perimeter camera coverage gap at NE corner; overlaps access-track terminus. L-02 PIR intermittent. S-boundary vegetation observed separately (not graded as part of F-01).	CRITICAL	A1	Priority
F-02	Physical · Lighting	Access-track terminus PIR lighting (L-02) intermittent — does not reliably extend across the F-01 camera gap at night.	HIGH	A1	Priority
F-03	Physical · Inverter compound	Inverter compound floodlighting partial — 2 of 4 fixtures (L-05, L-06) inoperative. Compound interior under-lit at night.	MEDIUM	A1	Priority
O-01	OSINT · Mailbox + credential	Shared service mailbox facilities@ observed in 2024 breach dump (S-04) with associated plaintext password. 2025 dark-web cross-reference (S-05). Mailbox in active operational use on site (A1); credential validity at this site untested (CMA 1990).	HIGH*	B2	Priority — operator confirmation

OBSERVED — NOT GRADED AS A FINDING

Mature poplar line along the S boundary interrupts perimeter sightlines for ~80 m. Captured in the walkdown notes; not graded as a finding because it doesn't overlap a high-value access or compound zone. Surfaced under the structural review row in Section 08 (vegetation management).

F-01 and O-01 are expanded in deep-dive form on the next two pages and illustrate the deep-dive anatomy. F-02 and F-03 are summarised in the findings register above and in the broker one-pager (Section 09); in a real engagement they would receive the same deep-dive treatment, omitted here for length.

04 · PHYSICAL SURFACE

Specimen finding deep-dive · F-01

F-01 · NE perimeter camera coverage gap

CRITICAL

LOCATION · NE-1 ↔ NE-2 coverage cones · pin 1 on the site schematic · Twin reference 04-NE

Observation.

40-metre gap between camera coverage cones NE-1 and NE-2. The access-track terminus is unmonitored. Lamp L-02 (PIR) night-time coverage on the internal access route supporting this exposure is intermittent (see F-02). The geometric blind spot overlaps an internal access-track terminus and high-value routing corridor serving the inverter compound area; the site's only external access is the SW gate (see Section 05 schematic). Perimeter visibility along the S boundary is also interrupted by a mature poplar line — that observation is recorded separately as observed-not-graded in Section 03 (contextual to F-01, not part of its grade) and surfaced for operator review in Section 08.

Operator dialogue.

Asked Q5 in the operator interview — *if you could fix one thing on this site today, what would it be?* — the site rep answered (in his own words): "The NE corner — I know there's a blind spot but never had time to fix it." That answer was recorded before the on-site walkdown reached the NE corner. F-01 is therefore evidenced both by analyst observation and by an operator field comment. The Q5 quote is reproduced for operational context, not as a legal admission or corporate acknowledgement.

Why it matters.

Camera coverage gaps that overlap access routes are consistent with the geometric weaknesses repeatedly observed in unmanned renewables-site theft reporting and described in the April 2026 cable-theft briefing. Q1 of the operator interview confirms the adjacent solar farm 12 km E was hit in April 2024 (~£18k loss); the OSINT watch-list (Section 06) records the same regional cluster activity. The underwriting issue is not that loss is predicted; it is that the exposure is observable, material, and has a defined operator-owned control-review pathway.

Grading.

Risk priority: CRITICAL. Severity HIGH (direct overlap with a high-value internal routing corridor and a recognised loss archetype). Likelihood LIKELY (regional cluster activity per OSINT watch-list; physical geometry is observable to anyone reconnoitring the site).

Evidence: A1. Direct on-site walkdown observation, cross-confirmed against drone-derived 3D twin (captured 8 April 2026, 10:42 BST, conditions Beaufort 2). Source reliability A (direct observation). Information credibility 1 (confirmed by independent twin geometry).

Operator-owned review pathway.

The operator may wish to refer F-01 and F-02 to a qualified CCTV/security and electrical contractor to verify the observed gap against live camera views, lighting coverage and operational requirements. Critical Asset has not specified the appropriate design response or assessed control adequacy. Review or implementation of any control may reduce identified exposure but cannot eliminate theft, intrusion or reconnaissance risk; treat any selected control as one layer in a defence-in-depth posture, not a standalone control. See Section 08 for the full referral matrix.

04 · INTELLIGENCE SURFACE

Specimen finding deep-dive · O-01

O-01 · Shared service mailbox — breach exposure + active operational use

HIGH*

REFERENCES · 2024 breach dataset (S-04) · 2025 dark-web cross-reference (S-05) · on-site corroboration by site rep

Observation — two independent points.

(1) Breach exposure. The shared service mailbox `facilities@[operator-domain]` appears in a lawfully sourced 2024 credential dump with an associated plaintext password (S-04). The same mailbox address — separately — is referenced in a 2025 dark-web mention (S-05), showing the mailbox continues to appear in relevant exposure sources after the original 2024 breach dataset. Credential validity at this site remains untested and is not asserted by this report.

(2) Active operational use. The mailbox itself was observed in active operational use during the engagement — the site representative referred to it as the address for site comms during the interview (Q3-adjacent observation, not a direct answer to Q3).

These two observations are independent. The mailbox-active observation says nothing about whether the breach-exposed credential is still valid for authentication. Critical Asset did **not** test whether the password from the breach dump can be used to access the mailbox or any other operator system; doing so would be out of scope and outside the Computer Misuse Act 1990 envelope. Plaintext passwords are not reproduced in this report. The operator is the only party in a position to confirm whether the credential has been rotated, retired, or remains active in supplier-portal authentication.

Grading.

Risk priority: HIGH — Potentially Critical pending operator confirmation. Severity HIGH (shared service mailbox with possible credential re-use across authentication systems; could escalate to CRITICAL if the operator confirms the exposed credential remains active). Likelihood POSSIBLE — the mailbox is in active operational use at this site (observed), but whether the breach-exposed credential is still valid for authentication is untested and is the operator's to confirm.

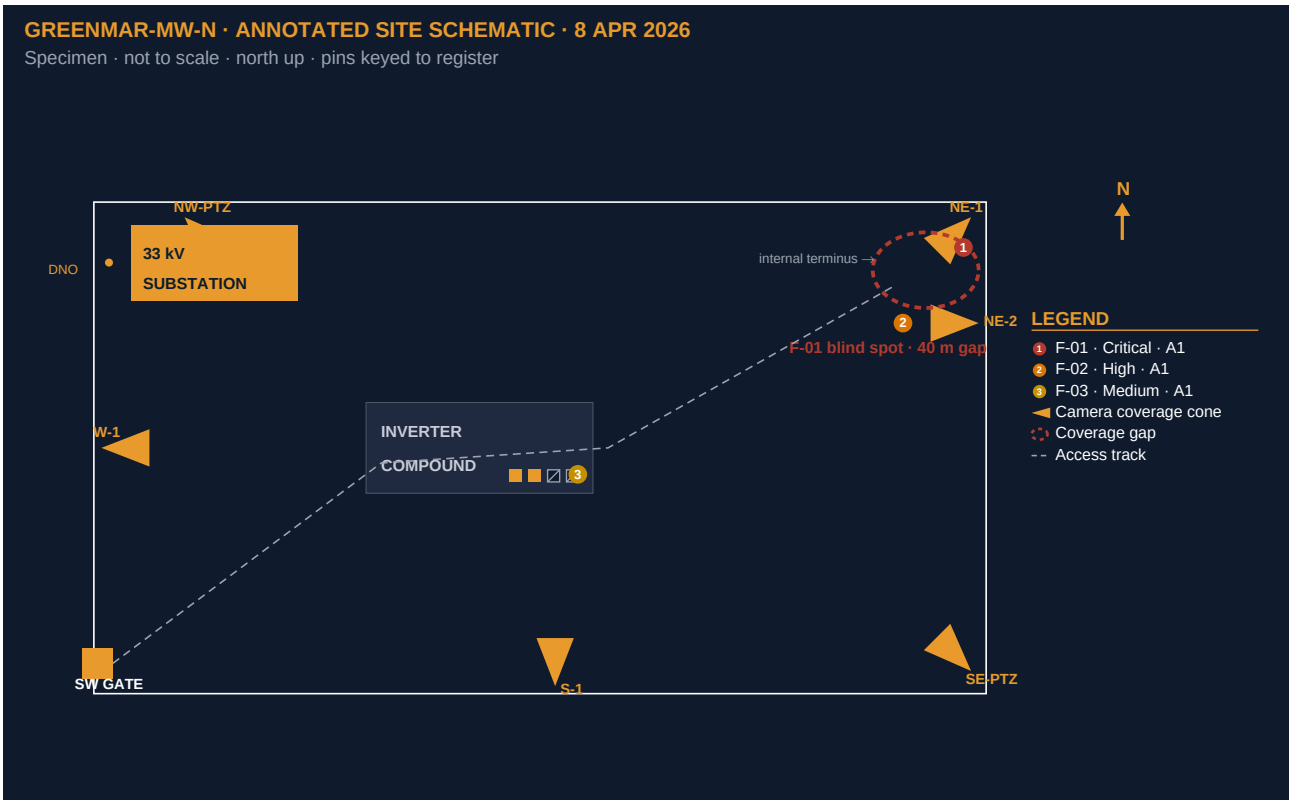
Evidence: B2. Source reliability B (usually reliable — established breach dataset with documented provenance). Information credibility 2 (probably true — corroborated by an independent 2025 dark-web reference for the same mailbox). The on-site observation of the mailbox in active operational use is itself A1, but that observation concerns the mailbox, not the credential; it does not promote the credential indicator above B2.

Operator-owned review pathway.

The operator may wish to refer O-01 to its IT/security function or qualified cyber provider to confirm credential status and determine any appropriate account, MFA, supplier-portal or incident-response steps. Critical Asset did not test credential validity and does not certify the status of any account. Review or implementation of any control may reduce the identified credential-exposure surface but cannot eliminate it; broader supplier-chain credential hygiene, monitoring and incident-response capability remain operator matters. See Section 08 for the full referral matrix.

05 · GEOMETRIC REFERENCE

Site overview & schematic



Annotated site schematic. Pins keyed to the findings register. Pin 1 (F-01, Critical) marks the NE perimeter camera coverage gap between cones NE-1 and NE-2; pin 2 (F-02, High) the L-02 PIR lighting deficit at the access-track terminus, which co-locates with the F-01 blind spot at the NE corner; pin 3 (F-03, Medium) the inverter-compound floodlighting (2 of 4 fixtures inoperative, shown as outlined boxes with diagonal slashes). The dashed access-track path enters the site at the SW gate, passes through the inverter compound, and terminates at the NE F-01/F-02 zone — making the internal high-value routing corridor visually explicit. The mature poplar line along the S boundary (walkdown observation, not graded) is not pinned on this view. In a real engagement this page also carries the orthomosaic and 3D digital twin still.

Site geometry summary.

Footprint	20 MW ground-mount solar PV · ~32 ha enclosed (specimen)
Perimeter	~1.8 km · galvanised palisade · single gate at SW
Camera estate	6 cones in service · 4 fixed perimeter · 2 PTZ access-control · (pre-visit pack noted 8 — operator: 2 not yet installed)
Lighting	PIR perimeter (L-01, L-02) · static inverter-compound flood (L-03–L-06)
Access	Single tracked access from SW gate · O&M; visits 2× weekly
Substation	33 kV step-up · DNO connection at NW corner
Lock pattern	Compound padlock + hasp + secondary keypad · last rotated Dec 2025

06 · INTELLIGENCE SURFACE

OSINT findings summary

What was reviewed.

- Public planning portal — 2022 design & access statement, supplier supplements.
- Operator and O&M contractor public surface — corporate sites, LinkedIn personnel (4 staff mapped).
- Breach datasets — lawfully sourced, indexed credential exposure for operator and supplier-chain domains.
- Dark-web reference search — current marketplace and forum mentions of operator domain and regional keywords.
- Passively observed closed-channel reference — Telegram channels associated with regional copper/cable activity (no active infiltration or privileged access).
- Cluster context — adjacent solar sites within 25 km, recent incident history per published news and police releases.

What was found at finding grade.

One finding only at graded level — **O-01**, the shared service mailbox / credential-exposure indicator (deep-dive Section 04). Additional OSINT signals identified during the engagement are held on the 90-day watch-list rather than presented as findings.

Corroborations — pre-visit OSINT confirmed on site.

- Inverter make/model on the 2022 planning portal (S-03) matches the kit observed on site — confirmed not replaced since 2022.
- Shared mailbox `facilities@[operator-domain]` confirmed in active use by the site representative for site comms.
- LinkedIn O&M personnel surface (S-06) maps to badged staff observed on site — 4 mapped, 4 confirmed.

Contradictions — what the pre-visit pack got wrong.

- Pre-visit pack listed 8 cameras on site. As-found is 6 in service; operator confirms 2 not yet installed. Pack will be refreshed for the next engagement.

90-day watch leads.

- Telegram channel `@[specimen-channel-handle]` — regional chatter, identified during the engagement, added to the watch list.
- Two domains observed on O&M van signage during the visit — queued for credential-exposure check across the watch window.
- Adjacent solar farm 12 km E was hit in April 2024 (per operator Q1 — see Section 07, ~£18k loss); the regional cluster remains active per published police releases. Flagged for repeat-targeting monitoring across the 90-day window.

06 · INTELLIGENCE SURFACE — UNDERWRITER FILE NOTE

What was not found — negative findings

Negative findings are part of the underwriter-facing evidence. They record the boundary of what an open-source review at this date and scope could surface, and are deliberately presented on a dedicated page so a careful reader can verify that absence has been considered alongside the graded findings on the preceding page.

Negative findings — for the underwriter file.

No direct marketplace listings of GREENMAR-MW-N or Operator-A during the review window. **No evidence** the 2024 credential has been actively used to authenticate against operator systems (we did not test). **No evidence** the site appears on any reviewed targeting list. **No public planning-portal artefacts** beyond the standard residual exposure already captured at S-03 (inverter make/model on a 2022 design statement).

Negative findings are not the same as proof of absence. They record the boundary of what an open-source review could surface at the engagement date. The 90-day watch-list captures emerging signals after delivery.

07 · RECORDED ON SITE

Operator interview

Five structured questions, asked of the site representative during the walkdown phase on 8 April 2026. Captured directly on iPad; reproduced here in the operator's own words where quoted.

Q1. Has the site been hit before? When, what, how was it documented?

No prior incident at this site. Adjacent solar farm 12 km E was hit April 2024 — cable theft, ~£18k loss, insurance paid with warranty added at renewal.

Q2. What changed at the 2025 renewal?

Premium up 12%; underwriter asked for evidence of perimeter inspection and access control review. Cover otherwise unchanged.

Q3. Who has keys / access? When was the lock pattern last changed?

Three site staff, two O&M, one landowner. Last rotation Dec 2025. Compound keypad code rotated quarterly.

Q4. What does the monitoring / alarm setup actually do at night?

Recording only — no live monitoring. Footage reviewed weekly. Alarm triggers go to operator-rep mobile — no Alarm Receiving Centre (ARC).

Q5. If you could fix one thing on this site today, what would it be?

"The NE corner — I know there's a blind spot but never had time to fix it."

What the interview adds to the underwriting picture. Q1 confirms the regional cluster context (adjacent-site loss). Q2 explains the renewal-evidence ask that this report directly addresses. Q3 anchors the lock-pattern hygiene picture for the substation and inverter compound. Q4 sits behind the existing monitoring posture — recording-only, no ARC — which is the operational context for the F-01 / F-02 finding pair. Q5 records F-01 as evidenced both by analyst observation and by an operator field comment.

Site-representative field comments are reproduced for operational context. They are not legal admissions or corporate acknowledgements; in live engagements they are reproduced only with operator consent.

08 · OPERATOR-OWNED CONTROL-REVIEW PATHWAY

Operator-owned control-review pathway

The items below identify **control areas for operator review**. They are not remediation instructions, technical specifications, designs, scopes of work, quotations, adequacy opinions, cost estimates or fix-by-date commitments.

Critical Asset's role is limited to evidence capture, site-geometry analysis, OSINT surface review, source grading and risk-priority reporting. Specification, design, contractor selection, procurement, implementation, testing, certification and ongoing maintenance remain with the operator and its qualified advisers.

Timing of any review or action is determined by the operator and is not specified by Critical Asset. The *Review category* column below reflects analytical priority only — it is not a deadline, sequencing instruction or fix-by-date commitment.

Review category	Finding / control area	Appropriate owner	Review question	Evidence the operator may retain
Priority	F-01 / F-02 — NE camera gap and PIR lighting deficit	CCTV/security contractor and/or electrical contractor	Does the as-found camera and lighting arrangement provide adequate coverage for the internal access-track terminus and relevant high-value routing corridor?	Contractor survey note, live-view screenshots, marked-up coverage plan, work order or maintenance record.
Priority	F-03 — inverter compound floodlighting partial	Maintenance or electrical contractor	Are the inoperative floodlights defective, isolated, awaiting replacement, or intentionally out of service?	Maintenance ticket, inspection note, repair record, contractor confirmation.
Priority	O-01 — shared mailbox / credential exposure indicator	Operator IT/security function or qualified cyber provider	Is the exposed credential active, rotated, retired, reused, or present in supplier-portal authentication?	IT confirmation note, rotation record, MFA status, supplier-portal review record.
Structural	S-boundary vegetation / sightline issue	Site maintenance owner	Does vegetation materially affect visibility, patrol, maintenance or future CCTV geometry?	Maintenance plan, seasonal cutting schedule, updated site photographs.
Structural	Supplier and personnel surface	Operator security / O&M contract manager	Are supplier-domain, personnel and shared-mailbox exposures being managed through contract and access-control process?	Supplier review note, access-control procedure, agreed personnel-publicity guidance.
Strategic	Future estate refresh	Operator asset / security governance	Should future camera, lighting and credential-policy changes include security-geometry and OSINT-surface review?	Capital-plan note, policy update, future SSVA schedule.

Residual risk.

Review or implementation of any item above may reduce identified exposure but cannot eliminate theft, intrusion, credential misuse, reconnaissance or other loss risk. Critical Asset does not certify the adequacy of any selected control.

Limitations of this assessment.

This pack records observations and intelligence indicators as at the engagement date. The control areas above are identified for operator review only — they are not a specification, design, scope of works, quotation, adequacy opinion or commitment by Critical Asset Drone Inspections Ltd. Critical Asset is not a security-systems designer, security installer, cyber-security testing firm, structural surveyor, electrical contractor or insurance adjuster. The operator is responsible for the specification, design, procurement, installation, testing, certification and ongoing maintenance of any control, and for engaging appropriately qualified contractors to do so. Findings are non-exhaustive and reflect what was observable within the agreed scope at the engagement date.

Contract precedence. This document is issued subject to the engagement letter between Critical Asset Drone Inspections Ltd and the operator; nothing in this document amends or supersedes those terms, and in the event of conflict the engagement letter prevails.

09 · FOR UNDERWRITER HANDOVER

Broker one-pager · standalone

Designed to stand alone. The broker can extract this page from the pack and hand it to the underwriter without supporting context.

AGGREGATE RISK	FINDINGS	REVIEW POSTURE
ELEVATED	**4 graded** 1 critical · 1 high · 1 high* · 1 medium	**Control areas surfaced** Four operator-owned control-review areas identified for renewal-window consideration

HIGH = potentially Critical pending operator confirmation; credential validity untested.*

Headline items.

ID	Headline	Priority	Evidence
F-01	NE camera coverage gap overlapping access-track terminus — site-representative field comment recorded in Q5	CRITICAL	A1
O-01	Shared service mailbox address observed in 2024 breach dataset; 2025 dark-web cross-reference; mailbox observed in active operational use; credential validity untested.	HIGH*	B2
F-02	Access-track PIR lighting (L-02) intermittent — does not span F-01 gap at night	HIGH	A1
F-03	Inverter compound floodlighting partial — 2 of 4 fixtures inoperative	MEDIUM	A1

Control-review pathway in plain English.

Four control areas have been identified for operator review for renewal-window consideration. F-01 and F-02 are appropriate for operator referral to qualified CCTV/security and electrical advisers for assessment of coverage and lighting. F-03 is appropriate for operator referral to the maintenance contractor. O-01 is appropriate for operator referral to the operator's IT/security function or qualified cyber provider for credential-status confirmation. Critical Asset has not specified, designed, priced, installed, tested or certified any control. Critical Asset will deliver the 90-day progress check-in call included in this tier; a 12-month SSVA refresh is recommended, or included where separately agreed.

This extract is advisory risk-evidence only. It is not a specification, design, quotation, adequacy opinion or guarantee against loss. The review posture indicates that evidenced control areas have been surfaced for operator consideration; it does not evidence completed remediation, certify operator capability, or confirm the adequacy of any selected control. Broker and underwriter circulation is permitted with operator consent on a non-reliance basis unless Critical Asset issues a separate reliance letter; no advisory or contractual relationship is created with any onward recipient. See Section 08 for the full referral matrix and limitations.

Source: Critical Asset SSVA · GREENMAR-MW-N (specimen) · 8 April 2026 · CA-2026-SP-01 · Methodology: SANS GIAC GCTI/GOSI · Treadstone 71 CTIA · PHIA-aligned · NATO Admiralty Code.

APPENDIX · PROCESS

Appendix A1 · Methodology & chain-of-custody

Engagement flow.

→ Day -10 to -1 · Pre-visit OSINT and credential-exposure sweep. Sources lawfully accessed under PHIA-aligned tradecraft.

→ Day 0 (8 April 2026) · On-site engagement. CAA airspace check (NOTAMs clear), Beaufort 2 conditions confirmed, landowner permission verified.

→ Day 0 · On-site walkdown with the site representative. Perimeter, gates, access tracks, camera coverage, lighting, inverter and substation compounds.

→ Day +1 to +5 · Processing. Orthomosaic and 3D digital twin built. Finding pins keyed to twin geometry. OSINT items graded against the NATO Admiralty Code.

→ Day +6 to +10 · Report assembly and internal QA. Broker one-pager built last so it cannot drift from the body.

→ Day +10 to +14 · Delivery to operator and (with operator consent) broker partner. Progress check-in call scheduled for Day +90.

Chain-of-custody log — 8 April 2026.

Capture start	09:25 BST
Capture end	14:18 BST
Total flight time	127 minutes
Primary platform	M3E-SPECIMEN-01 (RTK GNSS)
Secondary platform	M2P-SPECIMEN-02
Multispectral payload	Not used on this engagement
Battery sets	4 sets × 2
Storage media	SC-A1 · SC-A2 · SC-B1 (SD card serials)
Files captured	~42 GB · 312 photos / videos
Weather at start	Beaufort 2 · visibility ~8 km · 11°C · light cloud · WNW
Weather at end	Beaufort 3 · visibility ~7 km · light spits
Site rep on the day	Site representative (controlled annex in live report)
Emergency contact	Site manager (controlled annex in live report)

Engagement deviations — logged.

Tractor on the access track · 09:30–09:45

Inverter-compound capture held; capture window rescheduled to 13:50 slot once the access track was clear. No safety event. Operator rep informed at the time. Affected files re-named on the day to indicate post-pause capture.

Sign-off.

Operator rep agreed engagement complete · all captured media backed up before leaving site · site gate and lock returned to original state · no equipment left on site · operator informed of delivery date (Day +14). **Analyst:** M. McLean · signed on iPad. **Off site:** 8 April 2026, 14:32 BST.

Scope discipline.

No credential testing or password validation. No penetration testing or interaction with operational technology. No security-systems design, electrical installation or CCTV specification. No structural or chartered surveying. No claim adjustment or suspect identification. Scope boundaries are maintained through referral to appropriately qualified partners where the requested work falls outside this engagement.

Document boundary & data handling.

This report is intelligence-graded advisory reporting. It is **not** a legal opinion, regulatory determination, insurance-coverage decision, or a guarantee against loss. Findings are banded judgements with stated source confidence (NATO Admiralty Code); they are not numerical risk scores. Control specification, design, contractor selection, sequencing and ongoing maintenance remain with the operator and the operator's qualified advisers. Personal data captured during the engagement is processed under UK GDPR; see the privacy notice at `criticalasset.co.uk/privacy`. Raw materials (drone imagery, OSINT collection logs, dataset references) are retained in the engagement archive for 24 months under ICO-registered controllership (ZC132184).

Distribution. Issued to the operator and (with operator consent) the operator's broker partner. Not for onward redistribution beyond that named distribution without Critical Asset's written agreement. Recipient must satisfy itself as to the relevance and current applicability of the findings before acting on them. Broker and underwriter circulation is permitted only with operator consent and on a non-reliance basis unless Critical Asset issues a separate reliance letter; no advisory or contractual relationship is created between Critical Asset and any onward recipient by virtue of such circulation.

Workflow note for live engagements. In a real engagement the cover and chain-of-custody log carry actual operator and contact details. For copies that travel to broker or underwriter audiences, role-only references (site representative / site manager / lead analyst) are used and direct mobile contacts are kept in a controlled distribution annex held by the operator. The specimen uses illustrative role references to demonstrate live-report structure.

APPENDIX · EVIDENCE

Appendix A2 · Source list & references

Every finding in the register is keyed to one or more source items below. Sources are graded under the NATO Admiralty Code for reliability (A–F) and credibility (1–6).

Ref	Type	Source description	Admiralty	Used for
S-01	Direct observation	On-site walkdown notes · the site representative present	A1	F-01, F-02, F-03
S-02	Drone capture	Orthomosaic and 3D digital twin · 8 April 2026 · RTK GNSS	A1	F-01, F-03
S-03	Public record	Planning portal · 2022 design & access statement	A1	Inverter make/model corroboration
S-04	Breach dataset	Lawfully sourced 2024 credential exposure dataset · indexed reference	B2	O-01
S-05	Dark-web reference	2025 marketplace mention cross-referencing operator domain	B2	O-01
S-06	Personnel surface	Operator and O&M; LinkedIn surface (4 staff mapped)	B3	OSINT corroboration
S-07	Closed-channel (passive)	Telegram @[specimen-channel-handle] · regional cluster · passively observed reference, no active infiltration	C3	90-day watch · context
S-08	Industry briefing	Critical Asset cable-theft briefing paper · April 2026 (35 underlying sources)	B2	Context · F-01, F-02
S-09	Operator interview	Five-question interview · the site representative · 8 April 2026	A1	Context · F-01 (Q5)
S-10	Public incident record	Published police and news releases · regional cluster activity	B2	Regional cluster context · OSINT p.10

End of report. The engagement chain — field checklist → this report — demonstrates how on-site capture flows into the broker- and underwriter-facing deliverable. Comparable structure to a real engagement; the substantive content changes site-by-site. For methodology questions or to discuss what an SSVA looks like for a specific asset, contact info@criticalasset.co.uk.