SPECIMEN ENGAGEMENT · COMPLEX TIER

Site Security Vulnerability Assessment

Findings pack — specimen engagement.

SITE REFERENCE	GREENMAR-MW-N (specimen)
ENGAGEMENT REFERENCE	CA-2026-SP-01
ENGAGEMENT DATE	8 April 2026 (specimen)
TIER	Complex (single-site, mixed-asset)
ASSET PROFILE	20 MW ground-mount solar PV, English Midlands
ISSUED BY	Martin — Lead analyst & remote pilot
ISSUED TO	Specimen — prospective broker, underwriter and asset-owner readers
METHODOLOGY	SANS GIAC GCTI/GOSI · Treadstone 71 CTIA · PHIA-aligned
SOURCE FRAMEWORK	NATO Admiralty Code (A1–F6)
DOCUMENT VERSION	v5.0 · external specimen issue

DOCUMENT MAP

Contents

About this document. This is a specimen Critical Asset Site Security Vulnerability Assessment (SSVA), produced to show prospective broker, underwriter and asset-owner readers the shape of a real engagement deliverable. The fictional asset profile is a 20 MW ground-mount solar PV site in the English Midlands. Findings, source detail, OSINT items and review-pathway items are illustrative — modelled on the structure of a Critical Asset SSVA and on publicly reported UK renewables risk patterns. Not drawn from any specific real client.

What stays consistent in a real engagement. Document anatomy, dual grading (risk priority × Admiralty source confidence), scope boundary, chain-of-custody log, operator-owned control-review pathway, and the standalone broker one-pager extract. The substantive findings change site-by-site.

01 · FOR SPONSOR & BROKER

Executive summary

AGGREGATE RISK

ELEVATED

Driven by one confirmed physical exposure and one high-impact credential-exposure indicator requiring operator confirmation. Pack contains 8 findings across physical and intelligence surfaces; the broker one-pager (Section 08) is structured for renewal handover.

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	Site service credential (facilities@) appears in a 2024 breach dump with cross-references in 2025 dark-web mentions; credential validity untested.	HIGH*	B2
F-02	Access-track terminus PIR lighting does not extend across the perimeter-camera coverage gap.	HIGH	A1

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

Why this pack matters at renewal.

The confirmed physical finding and the high-impact 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 07); it does not specify, price, design, install, test or certify any control. Surfacing these areas before renewal lets the broker present an evidenced review posture rather than a passive risk profile.

Two OSINT items also appear in the indicative-watch category and are tracked in the 90-day post-engagement OSINT watch-list included with this tier. Negative findings — what we looked at and did not find — are listed in Section 06 and are themselves part of the underwriter-facing evidence.

This document is a specimen. The site does not exist; findings, source references and asset details are illustrative. Real engagement deliverables carry the same anatomy, with the substantive content drawn from the on-site walkdown, 3D twin capture and OSINT sweep.

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.

• Pre-visit OSINT sweep — open-source intelligence on the asset, the operator's 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.

• 90-day post-engagement OSINT watch-list and one progress check-in call.

Explicitly out of scope.

✗ Credential testing or password validation — no attempt is 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 (referred to RICS-qualified partners) and PCN/NDT certified inspections (referred to PCN partners).

✗ 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 — for example, an on-site walkdown observation typically grades A1, while a 2024 breach-dataset entry cross-checked against a 2025 dark-web reference typically 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.

Bands are intentional. Numerical scores invite false precision; bands let the broker and underwriter read source confidence at a glance without needing prior familiarity with the framework. The plain-English summary on Section 08 is built so the pack stands on its own.

03 · THE SUBSTANCE

Findings register — 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.	CRITICAL	A1	Priority
F-02	Physical · Lighting	Access-track terminus PIR lighting does not extend across the camera gap.	HIGH	A1	Priority
F-03	Physical · Perimeter	Vegetation barrier degraded along S boundary; visibility line interrupted by mature poplar growth.	MEDIUM	A1	Structural
F-04	Physical · Inverter compound	Compound floodlighting partial — two of four fixtures inoperative.	MEDIUM	A1	Priority
O-01	OSINT · Credential	Shared service address (facilities@) in 2024 breach dump with 2025 dark-web cross-reference; credential validity untested.	HIGH*	B2	Priority — operator confirmation
O-02	OSINT · Personnel	O&M contractor staff LinkedIn surface exposes role, site and partial routing.	MEDIUM	B3	Structural
O-03	OSINT · Asset surface	Site coordinates and inverter make/model visible on cached planning portal documents.	LOW	A1	Structural
O-04	OSINT · Threat surface	Regional Telegram channel chatter referencing cable theft across adjacent solar cluster.	MEDIUM	C3	Watch · 90 d

Each finding is expanded in the full report with: location reference (where applicable cross-keyed to the 3D digital twin), supporting evidence (photograph, OSINT artefact, breach reference), risk-priority justification, Admiralty source reasoning, and an operator-owned review pathway. Two deep-dives follow on the next two pages.

04 · PHYSICAL SURFACE

Specimen finding deep-dive · F-01

F-01 · NE perimeter camera coverage gap

CRITICAL

LOCATION · NE-1 ↔ NE-2 coverage cones · Twin reference pin 04-NE

Observation.

40-metre gap between camera coverage cones NE-1 and NE-2. The access-track terminus is unmonitored. Perimeter visibility is further interrupted by a poplar line along the southern boundary; night-time PIR lighting does not extend across the gap. The geometric blind spot overlaps the only access point for the substation compound.

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. 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 access point and a recognised loss archetype). Likelihood LIKELY (regional cluster activity per O-04; physical geometry is observable to anyone reconnoitring the site).

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

OPERATOR-OWNED REVIEW PATHWAY

The operator may wish to refer F-01 (and the adjacent F-02 lighting deficit) 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 07 for the full referral matrix.

04 · INTELLIGENCE SURFACE

Specimen finding deep-dive · O-01

O-01 · Exposed service credential (facilities@)

HIGH*

REFERENCES · Lawfully sourced 2024 breach dataset · 2025 dark-web cross-reference · Source list item S-04

Observation.

Shared service address `facilities@[operator-domain]` appears in a 2024 credential dump with an associated plaintext password. The same address is referenced — separately — in a 2025 dark-web mention, with credential validity remaining untested. Potential re-use across site authentication systems and supplier portals.

Plaintext passwords are not reproduced in this report. We did not test, validate or attempt to authenticate with the credential. The exposure indicator is reported with source confidence; the operator is the only party in a position to confirm whether the credential is still in use and where.

Why it matters.

Supplier and shared-service credentials are an intelligence surface most physical-security vendors do not look at, and most cyber-security vendors do not connect to physical risk. The intersection is where unmanned-site loss events disproportionately concentrate. Even where the credential is no longer active, the appearance pattern (shared mailbox, supplier-adjacent, recent cross-reference) is informative to an underwriter assessing the operator's broader operational discipline.

Grading.

Risk priority: HIGH — Potentially Critical pending operator confirmation. Severity HIGH (shared service account with possible supplier-portal re-use; could escalate to CRITICAL if confirmed active). Likelihood POSSIBLE — the credential could be inactive, partially rotated, or unused at this site. The operator is the only party in a position to confirm whether the credential is still in use and where.

Evidence: B2. Source reliability B (usually reliable — established breach dataset with documented provenance). Information credibility 2 (probably true — corroborated by independent 2025 dark-web reference). Not graded A1 because we have not tested whether the credential is active; doing so would be out of scope and outside the Computer Misuse Act 1990 envelope.

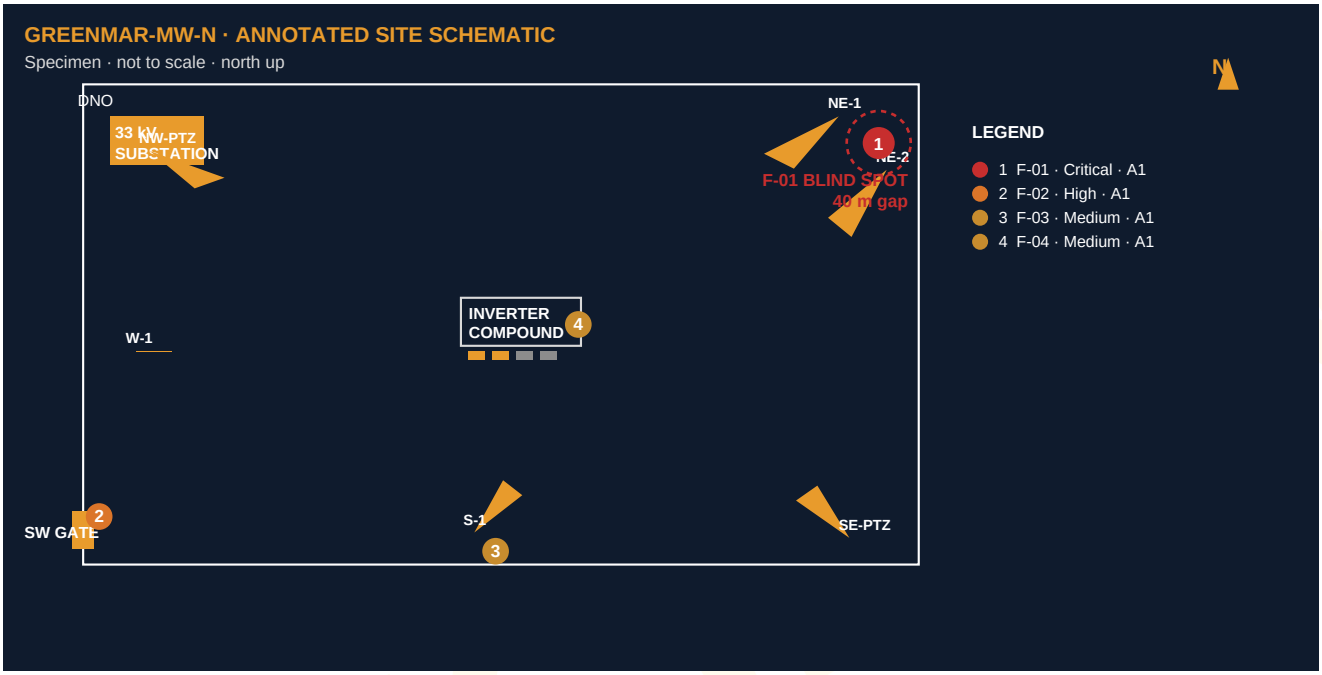
OPERATOR-OWNED REVIEW PATHWAY

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 07 for the full referral matrix.

05 · GEOMETRIC REFERENCE

Site overview & 3D digital twin

Annotated site schematic (specimen). In a real engagement this page also carries the orthomosaic and 3D digital twin still captured under CAA Operational Authorisation.



Annotated site schematic. *Pins keyed to the findings register. Pin 1 (F-01, Critical) marks the NE perimeter camera coverage gap; pin 2 (F-02, High) the access-track terminus lighting deficit; pin 3 (F-03, Medium) the south-boundary vegetation interruption; pin 4 (F-04, Medium) the inverter-compound floodlighting (2 of 4 fixtures inoperative — shown grey).*

Site geometry summary.

Footprint	20 MW ground-mount solar PV · ~32 ha enclosed perimeter (specimen)
Perimeter	1.8 km · galvanised palisade · gated single access point at SW
Camera estate	6 cones · 4 fixed perimeter · 2 PTZ access-control · partial coverage (see F-01)
Lighting	Solar PIR perimeter · partial inverter-compound floodlighting (see F-04)
Access	Single tracked access from B-road via SW gate · O&M visits 2× weekly
Substation	Single 33 kV step-up · DNO connection at NW corner

06 · INTELLIGENCE SURFACE

OSINT findings summary

What was reviewed.

• Public planning portal — historic application documents, design and access statements, supplier supplements.

• Operator and O&M contractor public surface — corporate sites, LinkedIn personnel surface, technical job adverts.

• Breach datasets — lawfully sourced, indexed credential-exposure references for operator and supplier-chain domains.

• Dark-web reference search — current marketplace and forum mentions of operator domain, O&M domain, regional cluster 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.

Four OSINT items recorded in the findings register (O-01 to O-04). The credential exposure (O-01) is the most actionable inside a 30-day operator-review horizon; the regional Telegram chatter (O-04) is graded C3 — possibly true, with limited corroboration — and is held on the 90-day watch-list rather than presented as a confirmed signal.

What was not found.

NEGATIVE FINDINGS — IMPORTANT FOR THE UNDERWRITER FILE

No direct mentions of GREENMAR-MW-N or its parent operator on indexed marketplace listings during the review window. **No evidence** that the 2024 exposed credential has been actively used to authenticate to operator systems (we did not test). **No evidence** the site appears on any reviewed targeting list. **No public planning portal artefacts** beyond standard residual exposure (inverter make/model on a 2022 design statement — O-03).

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

90-day watch scope.

Light passive monitoring of the operator domain, O&M contractor domain, the GREENMAR site reference, and a curated keyword list across cluster-adjacent sites within a 25 km radius. The operator receives a 30-day check-in, a 60-day signal review and a final report at 90 days. Critical or escalated signals are flagged on detection rather than at the next interval.

07 · 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 access-track terminus and the high-value routing corridor?	Contractor survey note, live-view screenshots, marked-up coverage plan, work order or maintenance record.
Priority	F-04 — 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 — operator confirmation	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	F-03 — 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	O-02 / O-03 — Supplier, personnel and asset-surface exposure	Operator security / O&M contract manager	Are supplier-domain, personnel and planning-portal exposures being managed through contract, access-control and publication process?	Supplier review note, access-control procedure, agreed personnel-publicity guidance.
Watch	O-04 — regional Telegram chatter	Critical Asset 90-day watch programme	Does emerging chatter indicate escalation in regional cluster activity affecting this asset?	90-day watch-list updates, escalated-signal notifications.
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.

08 · FOR UNDERWRITER HANDOVER

Broker one-pager · standalone

This page is designed to stand alone. The broker can extract it from the pack and hand it to the underwriter without supporting context — headline risk, finding count, evidence-trail reference and review posture sit on a single sheet.

AGGREGATE RISK	FINDINGS	REVIEW POSTURE
ELEVATED	**8 total** **1 critical · 2 high · 3 medium · 1 low · 1 watch**	**Control areas surfaced** Seven operator-owned control-review areas identified for renewal-window consideration

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

Headline items (full detail in pack body).

ID	Headline	Priority	Evidence (Admiralty)
F-01	NE camera coverage gap overlapping access-track terminus	CRITICAL	A1
O-01	Shared service credential exposed in 2024 breach; 2025 cross-reference	HIGH*	B2
F-02	Access-track PIR lighting does not extend across camera gap	HIGH	A1
F-04	Inverter compound floodlighting partial	MEDIUM	A1
O-04	Regional Telegram channel chatter — held on 90-day watch	MEDIUM	C3

Control-review pathway in plain English.

Seven 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. F-04 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. The remaining items sit on a 90-day watch and structural / strategic operator-review horizons. 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.

ADVISORY POSTURE ONLY

This extract is advisory risk-evidence only. It is not a specification, design, quotation, adequacy opinion or guarantee against loss. A 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 07 for the full referral matrix and limitations.

Source: Critical Asset Drone Inspections SSVA · GREENMAR-MW-N (specimen) · Issued 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; raw collection logged with timestamp and source identifier.

→ Day 0 · On-site engagement. Pre-flight risk assessment, CAA airspace check (NOTAMs, ATZ proximity), landowner permission verification, Beaufort and visibility check. Drone capture of full site under PDRA01-28445.

→ Day 0 · On-site walkdown with the operator's site representative. Perimeter, access, camera coverage, lighting, inverter and substation compounds. Field notes captured with geotag and timestamp.

→ Day +1 to +5 · Processing. Orthomosaic and 3D digital twin built in Pix4D/Metashape. Finding pins keyed to twin geometry. OSINT items graded against the NATO Admiralty Code. Cross-references checked.

→ Day +6 to +10 · Report assembly, internal QA, dual-grading review. Broker one-pager extract 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.

Every captured artefact carries: timestamp (ISO 8601, UTC and BST), GPS coordinates (where applicable), weather conditions, kit serial, operator identifier, and processing-pipeline version. Raw files (drone imagery, OSINT collection logs, breach-dataset references) are retained in the engagement archive for 24 months under ICO-registered controllership (ZC132184). Critical Asset may release raw materials to a nominated loss adjuster, insurer's investigator or police enquiry team on operator instruction, subject to identity verification.

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. Where intrusive cyber testing is required, Critical Asset recommends a CREST-accredited firm. Where chartered structural work is required, referral is to RICS-qualified partners; PCN/NDT-certified work is referred to PCN partners.

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.

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). The list is illustrative and reflects the categories a real engagement would surface; specific items, URLs and dataset references are abstracted.

Ref	Type	Source description	Admiralty	Used for
S-01	Direct observation	On-site walkdown notes · operator site rep present	A1	F-01 to F-04
S-02	Drone capture	Orthomosaic and 3D digital twin · captured 8 April 2026 · RTK GNSS	A1	F-01, F-03
S-03	Public record	Planning portal documents · 2022 design and access statement	A1	O-03
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 · current	B2	O-01
S-06	Personnel surface	Operator and O&M public personnel surface · LinkedIn observation	B3	O-02
S-07	Closed-channel (passive)	Telegram channel reference · regional cable-theft cluster · passively observed reference, no active infiltration	C3	O-04
S-08	Industry briefing	Critical Asset cable-theft briefing paper · April 2026 (35 sources)	B2	Context · F-01, O-04

End of specimen pack. A real engagement deliverable carries the same anatomy with site-specific content. For methodology questions, an actual engagement quote, or to discuss what an SSVA looks like for a specific asset, contact info@criticalasset.co.uk or 07907 337014.