SKY SHADOW SYSTEMS

Capability Statement

Mission architecture for persistent maritime awareness, infrastructure protection and evidence-ready operations.

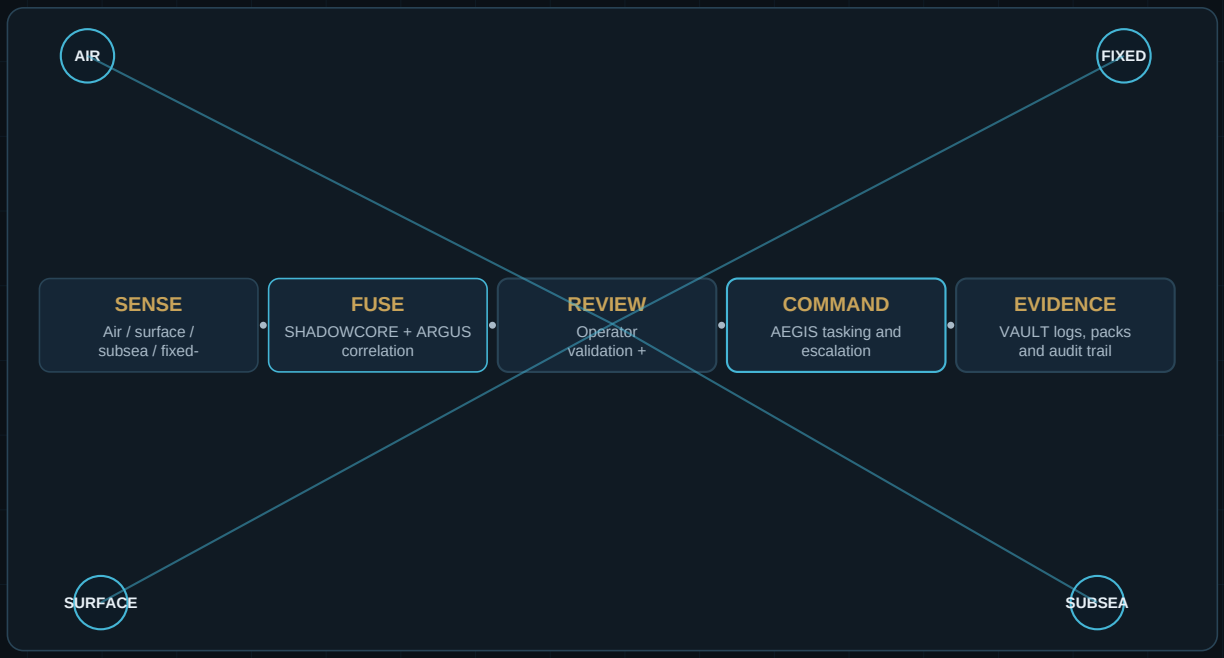
Document type	Capability Statement
Audience	Investors, ports, offshore operators, infrastructure owners, integrators and approved public-sector stakeholders
Disclosure level	Public-level strategic material. Detailed specifications and deployment-sensitive information reserved for approved private review.
Version	Draft v1.0 - 29 May 2026

Disclosure boundary

This document is intentionally written at public strategic and procurement level. It avoids controlled technical details, exact performance values, deployment-sensitive parameters, offensive capabilities, bypass methods, targeting instructions, and site-specific configuration data. The aim is to support investor and stakeholder understanding of system architecture, governance, pilot design and commercial positioning.

Executive summary

Sky Shadow Systems is positioned as a UK mission-systems company connecting air, surface, subsea and fixed-site sensing into operator-reviewed mission architectures for ports, offshore assets, coastlines, fleets and protected infrastructure. The core investor thesis is not a single platform: it is a modular architecture that can be piloted, validated and scaled across multiple maritime and infrastructure environments.



Capability envelope

Mission focus Persistent maritime awareness, infrastructure protection and operator-reviewed autonomous surveillance.	**Operating domains** Air ISR, surface systems, subsea layer and fixed-site sensing as one mission stack.
Software layers SHADOWCORE prioritisation, ARGUS correlation, AEGIS command workflow and VAULT evidence preservation.	**Pilot pathway** Assess, configure, pilot, validate and scale using evidence-led adoption.
Stakeholder fit Ports, harbours, offshore operators, critical infrastructure owners, integrators and strategic partners.	**Governance posture** Public-level disclosure, controlled technical review, NDA pathways and responsible communications.

Operating-domain map

Domain	Primary stakeholder question	Public capability response	Success evidence
Air ISR	Can the system improve coverage and verification?	Persistent airborne watch, rapid cueing, visual review and event prioritisation.	Coverage map, operator review log, event confidence summary.
Surface systems	Can waterside context be maintained?	Surface observation, harbour approach context and vessel-activity correlation.	Track continuity, evidence pack, operator workload metric.

Subsea layer	Can routes and assets be baselined?	Route baselining, anomaly review and protected-asset monitoring.	Baseline report, anomaly register, review summary.
Fixed site	Can protected locations be monitored without feed overload?	Perimeter, critical infrastructure and remote-site watch functions.	Watch-board outputs, escalation record, audit trail.

Mission-system architecture

The architecture deliberately separates sensing, correlation, human review, command workflow and evidence preservation. This separation supports modular procurement, pilot evaluation and governance review. It also allows different platforms and sensors to be evaluated without forcing the buyer into a single rigid hardware proposition.

Stakeholder	Need	Sky Shadow Layer	Investor Value
Ports	Entrance / berth awarene	PHAROS + AEGIS	Short pilot cycles
Offshore	Asset perimeter review	ARGUS + VAULT	Recurring monitoring
Infrastructure	Baseline anomalies	SENSE + VAULT	Evidence value
Investors	Scalable thesis	Architecture stack	Platform optionality

Investor relevance

- The platform catalogue creates product optionality while the architecture creates defensible system value.
- The pilot pathway reduces adoption friction for operational buyers and creates measurable proof points.
- Evidence-ready reporting supports regulated, accountable and security-sensitive users.
- The same operating model can be applied across ports, offshore energy, critical infrastructure, fleets and protected sites.
- Controlled disclosure protects the company from over-publishing sensitive information while still communicating credibility.

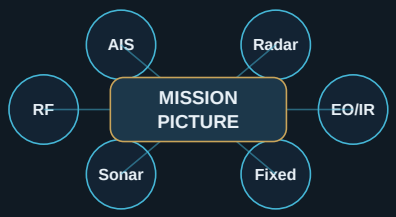
Capability maturity roadmap

Phase	Commercial objective	Technical output	Investor signal
Foundation	Website, briefing assets, capability narrative	Architecture map, public doctrine, PDF pack	Credibility and positioning
Pilot design	Convert stakeholders into scoped evaluations	Site assessment template, success criteria, report format	Buyer validation
Controlled pilot	Prove workflow value under supervision	Coverage / event / evidence metrics	Operational traction
Repeatability	Standardise packages and pricing	Reusable mission templates and training material	Scalability
Partner expansion	Integrator and channel strategy	Interoperability model and support procedure	Distribution leverage

Technical appendix A - mission data model

This technical appendix defines the public-safe information architecture used throughout the resource pack. It is suitable for investor and buyer understanding, but excludes implementation details, exact sensor settings, deployment parameters and controlled configuration data.

Data class	Examples	Treatment	Business value
Observation metadata	Time, zone, source class, event identifier	Normalised into a reviewable event record.	Enables audit, search and comparison.
Sensor context	EO/IR, radar, AIS, RF, acoustic or fixed-site context	Stored as source context, not as a definitive conclusion.	Improves confidence and reduces false interpretation.
Operator review	Human assessment, confidence note, escalation decision	Preserved in VAULT as part of event history.	Supports accountability and stakeholder trust.
Mission output	Briefing pack, event log, anomaly register, summary report	Exported to approved users and governance channels.	Creates board-level and investor-visible evidence.
Disclosure control	NDA status, public/private classification, site sensitivity	Controls what can be reused publicly or commercially.	Protects customers and company IP.



Technical appendix B - system layer interfaces

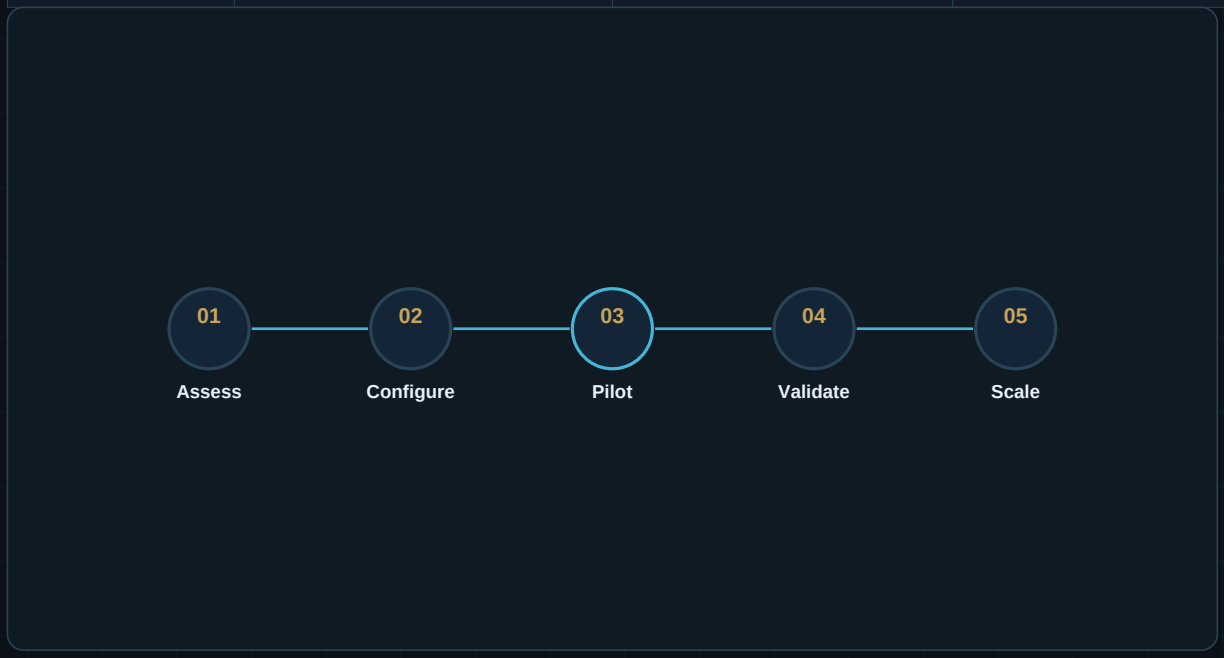
Sky Shadow should present itself as a modular mission architecture. Each layer can be explained as an interface boundary. This gives investors confidence that the company is building a repeatable system, not merely a collection of disconnected visual concepts.

Interface boundary	Input	Processing posture	Output
Sensor to SHADOWCORE	Authorised observations and metadata	Prioritisation, anomaly triage and event shaping.	Candidate events with confidence context.
SHADOWCORE to ARGUS	Candidate events and source context	Cross-source correlation and duplicate reduction.	Composite operating picture.
ARGUS to AEGIS	Correlated events and uncertainty notes	Operator tasking, review and escalation workflow.	Human decision record and task queue.
AEGIS to VAULT	Reviewed events, decisions and notes	Evidence packaging, audit trail and reporting structure.	Briefing-ready records.
VAULT to stakeholder	Approved reports and logs	Controlled distribution and disclosure review.	Buyer, investor or governance evidence.

Technical appendix C - evaluation and assurance criteria

The most investor-attractive technical story is an evidence-led adoption model. A buyer should be able to test the mission system through metrics that demonstrate reduced uncertainty, improved review quality and repeatable operational value.

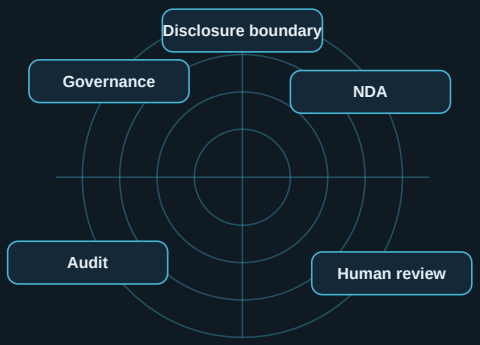
Criterion	Measurement method	Evidence artifact	Investor signal
Coverage fit	Compare planned zones with reviewed observation windows.	Coverage map and gap note.	Shows practical utility.
Signal relevance	Measure useful events versus irrelevant raw inputs.	Event relevance dashboard.	Shows operator-value, not feed volume.
Review latency	Measure time from event surfacing to human review.	Workflow timing log.	Shows process efficiency.
Evidence integrity	Check completeness of logs and event traceability.	VAULT evidence sample.	Shows governance readiness.
Integration fit	Assess fit with existing security operations.	Integration review note.	Shows procurement pathway.
Repeatability	Compare whether same template can apply to another site.	Repeatable mission template.	Shows scalability.



Technical appendix D - governance and risk controls

For a defence-adjacent and infrastructure-focused company, credibility depends on disciplined public disclosure. The documents should create confidence without disclosing parameters that could create operational risk or regulatory issues.

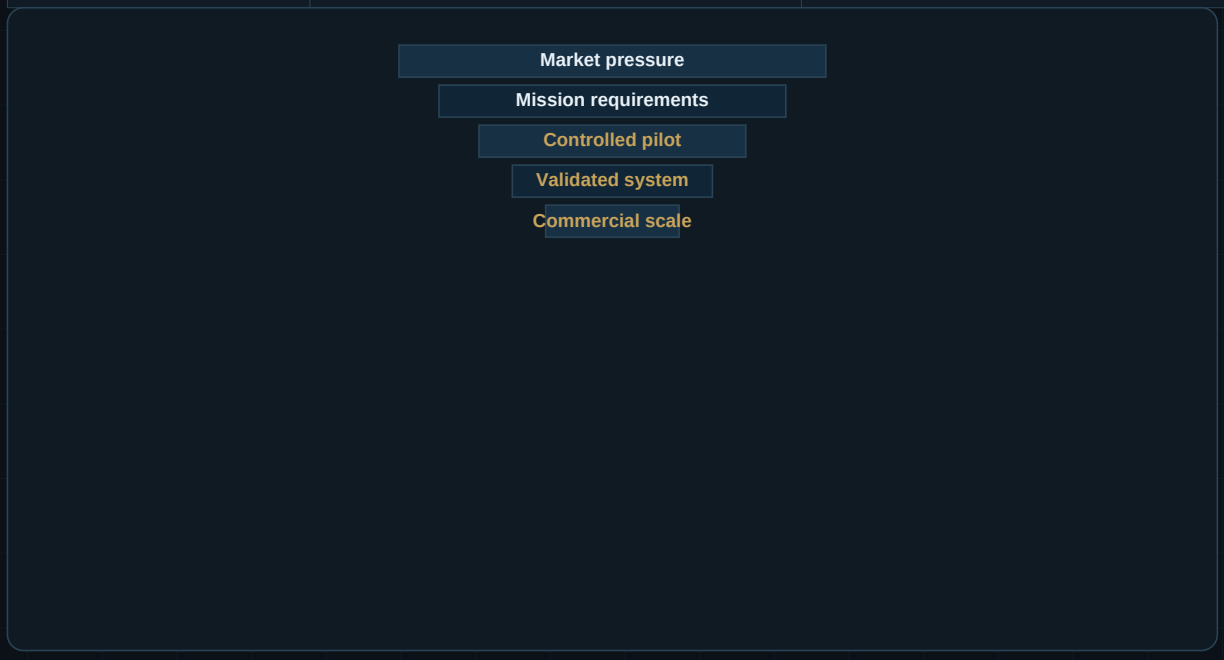
Public-safe architecture Describe system layers, buyer value and governance without exact technical settings.	**NDA technical review** Route deeper technical discussions through private briefing and controlled diligence.
Human authority Present autonomy as operator-supporting and human-commanded for sensitive contexts.	**Evidence integrity** Use audit trails, logs and review histories as a core value proposition.
Compliance posture Keep export-control, data protection and sector-specific review in the buyer process.	**Claim discipline** Avoid unverified performance, customer, funding, contract or deployment claims.



Technical appendix E - investor conversion logic

The resource library should help a serious investor quickly understand the company as an architecture-led mission-systems venture. The best conversion pathway is from public credibility to controlled private review, then from private review to pilot design, stakeholder proof and commercial scale.

Website asset	Investor purpose	What it should trigger
Capability statement	Quick credibility and scope assessment.	Private briefing request.
Whitepapers	Demonstrates doctrine, depth and market understanding.	Technical discussion under NDA.
Pilot programme brief	Shows practical route to validation.	Pilot scoping call.
Investor overview	Explains commercial thesis and roadmap.	Qualified investor diligence.
Case-style pilot report	Future proof artifact after approved trials.	Funding, partnership or customer conversion.



References and source basis

The documents use Sky Shadow public website content and public strategic references. Market figures are indicative third-party estimates and should be validated before investor use.

- Sky Shadow Systems website scan, 29 May 2026: homepage describes persistent maritime awareness, human-commanded autonomy and evidence-ready decisions.

- Sky Shadow Technology page: describes sensors, SHADOWCORE, ARGUS, AEGIS and VAULT as the public mission architecture.

- NATO Alliance Maritime Strategy, 29 Oct 2025: emphasises persistent maritime situational awareness and protection of critical maritime infrastructure.

- IMO SOLAS XI-2 / ISPS Code: mandatory port and maritime security framework for contracting governments, port authorities and shipping companies.

- UK National Protective Security Authority: provides protective security advice for critical national infrastructure owners and operators.

- Grand View Research maritime surveillance market summary: 2024 market estimate and 2025-2030 growth outlook.

- Precedence Research maritime surveillance market summary: 2025 estimate and 2035 forecast.

- ArXiv 2025 maritime AI / MDA literature used only for public-level themes: AIS/satellite fusion, adversarial AI resilience and explainable maritime autonomy.