SKY SHADOW SYSTEMS

Pilot Programme Brief

A controlled pathway from site assessment to validated mission-system evaluation.

Document type	Pilot Programme Brief
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.

Purpose of the pilot programme

The Sky Shadow pilot programme is designed to convert strategic interest into a controlled, measurable evaluation. It gives ports, offshore operators, infrastructure owners and strategic partners a disciplined route to test mission fit without accepting unsupported claims or exposing sensitive site information publicly.

Five-stage pilot pathway

Stage	Workstream	Outputs	Decision gate
01 Assess	Operating environment, risk picture, existing assets, authority model and stakeholder objectives.	Mission-context brief, site constraints, data-handling assumptions.	Proceed only if the use case is legitimate, bounded and governable.
02 Configure	Select platform class, sensor layer, operator workflow and evidence outputs at high level.	Pilot architecture, integration notes, success criteria.	Approve scope, safety, legal and disclosure boundaries.
03 Pilot	Controlled evaluation in agreed zones with oversight and limited-public claims.	Event logs, operator feedback, coverage mapping and reporting samples.	Evaluate operational value and buyer workload.
04 Validate	Review reliability, evidence quality, integration fit and stakeholder outcomes.	Validation pack, KPI dashboard, risk notes and next-step options.	Go / no-go / refine decision.
05 Scale	Move to phased deployment if commercially and operationally justified.	Rollout plan, training plan, support model and governance schedule.	Commercial agreement or extended trial.

Pilot measurement framework

Coverage	Detection review
Zone coverage, observation continuity, gaps and operating-window constraints.	Number of relevant events presented for human review and confidence notes.

Operator workload Whether the system reduces raw-feed burden and improves decision readiness.	**Evidence quality** Completeness of logs, timestamps, event summaries and briefing outputs.
Integration fit Fit with existing security operations, reporting lines and data-handling expectations.	**Governance** Evidence that technical scope, legal boundaries and disclosure controls are understood.

Pilot evidence pack

The pilot should conclude with a structured evidence pack suitable for internal buyer review and investor-level traction evidence. It should not expose sensitive technical settings or site-specific vulnerabilities.

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

Commercial structure

- Use a paid discovery or pilot-fee model where possible to validate buyer seriousness.
- Separate professional services, platform rental, software access, integration and reporting deliverables.
- Avoid indefinite free trials; define time, zone, scope, data handling and review cadence.
- Use pilot outputs as investor proof only where the customer permits disclosure.
- Keep sensitive operational data under NDA and avoid public deployment claims without approval.

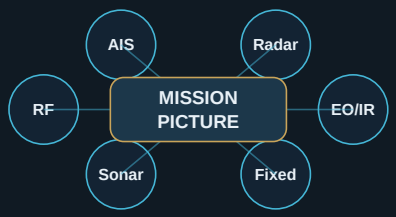
Investor value of pilot programme

A disciplined pilot programme turns a conceptual technology company into a measurable evaluation partner. Investors can understand the route from website interest to scoped pilot, then from pilot metrics to scalable commercial packages.

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

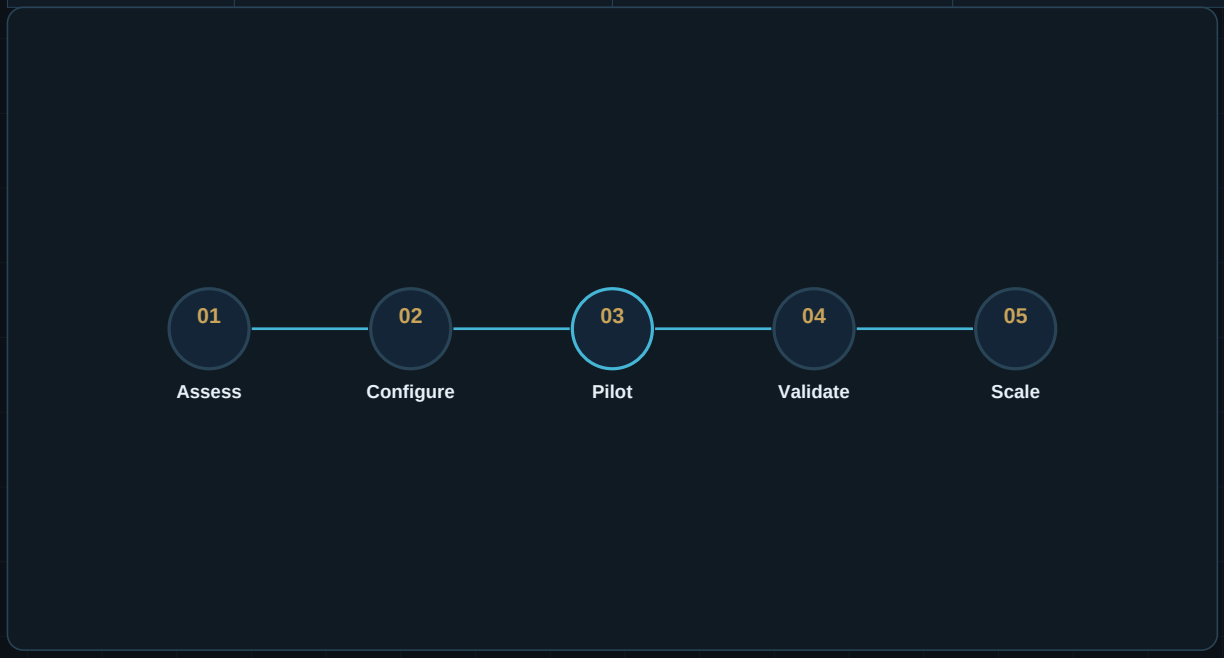
Sky Shadow should present itself as a modular mission architecture. Each layer can be explained as an interface boundary. This gives investors confidence that the company is building a repeatable system, not merely a collection of disconnected visual concepts.

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.

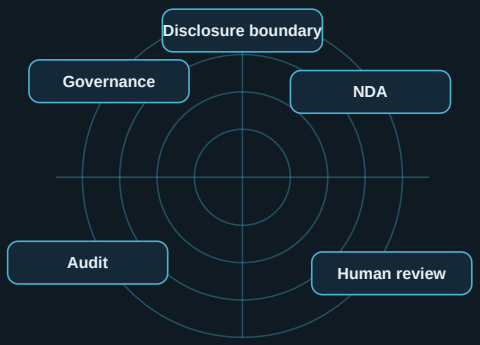
Criterion	Measurement method	Evidence artifact	Investor signal
Coverage fit	Compare planned zones with reviewed observation windows.	Coverage map and gap note.	Shows practical utility.
Signal relevance	Measure useful events versus irrelevant raw inputs.	Event relevance dashboard.	Shows operator-value, 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.

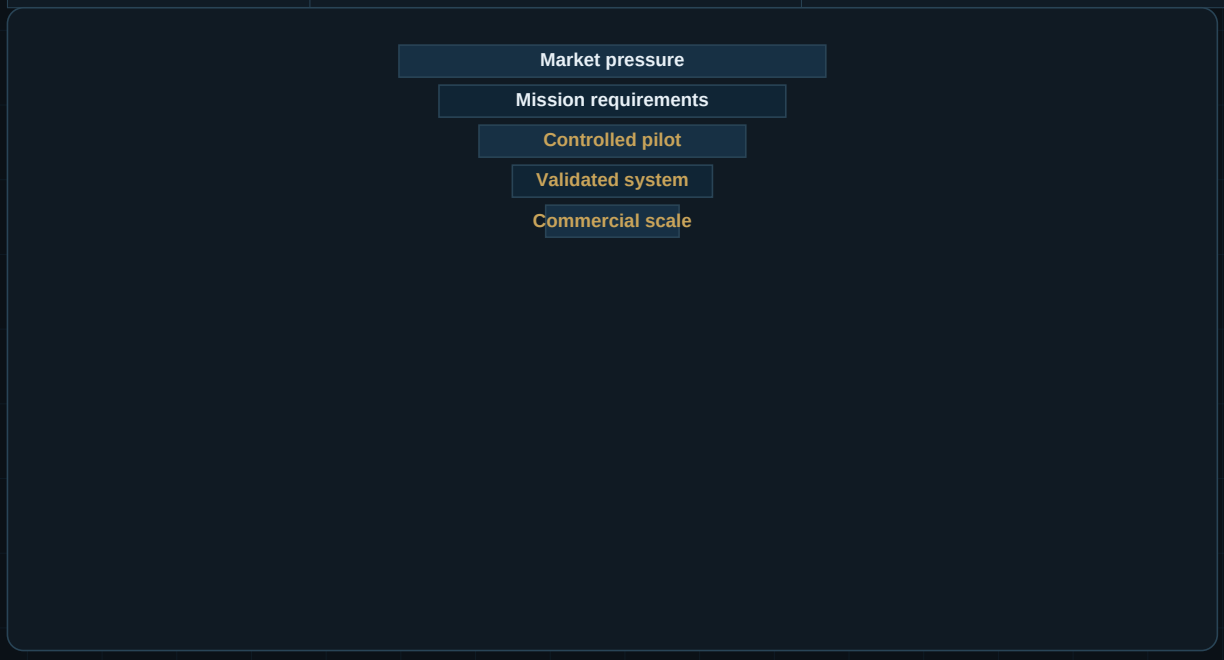
Public-safe architecture Describe system layers, buyer value and governance without exact technical settings.	**NDA technical review** Route deeper technical discussions through private briefing and controlled diligence.
Human authority Present autonomy as operator-supporting and human-commanded for 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.