DRONESHIELD

Airspace Under Pressure

A Global Assessment of Counter-UAS Readiness Across Airports and Critical Infrastructure

Survey data sourced directly from operators across:
20+ organizations · 6 continents · Airports, ports, corrections and critical infrastructure

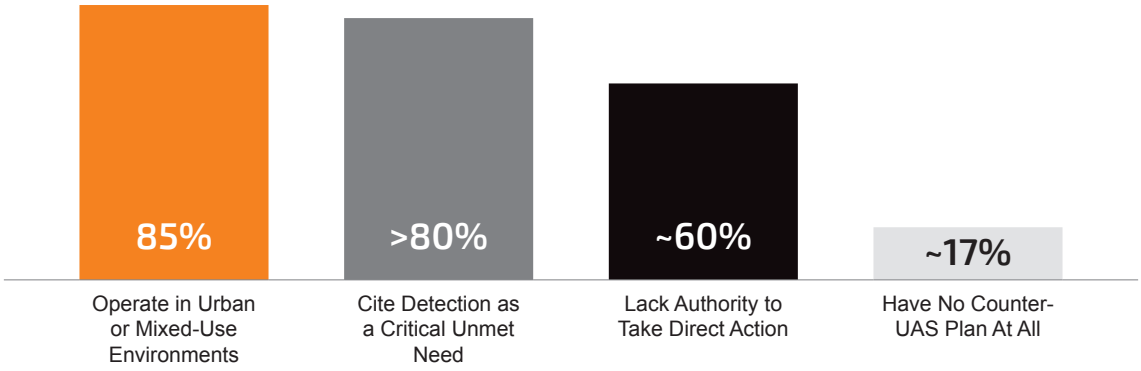
2026

Executive Summary

Drone proliferation has crossed a threshold. For the security decision-makers who responded to this global survey, managing international airports, correctional facilities, seaports, and critical infrastructure across five regions, unauthorized unmanned aircraft systems are no longer an emerging concern. They are a daily operational reality.

What this research reveals is not that operators are unaware of the threat, they are acutely aware. The crisis is that awareness has not translated into capability. The industry knows exactly what is needed and is largely unable to deliver it, constrained by detection gaps, regulatory barriers, fragmented systems, and an absence of the standardized frameworks that effective response requires.

That gap is the central finding of this report. And it is the defining challenge facing airport and infrastructure security leaders today.



This report is structured to:

1. Diagnose the current state of readiness across the industry
2. Show where organizations likely sit within that picture
3. Define what a credible path forward requires

The data is sourced directly from real-world operators in the field – not modeled nor projected. These are the conditions as they exist today.

Core Findings

The primary counter-UAS challenge in 2025 is not awareness of the threat – it is the capacity to convert awareness into authorized, coordinated, real-time action. Technology investment alone will not close this gap. Regulatory reform and operational integration must advance simultaneously.

Introduction: The Data Behind This Report

The findings presented here are drawn from DroneShield's proprietary structured survey responses collected directly from more than twenty operators actively managing drone-related risks. Respondents represent airports and aerodromes, aviation authorities, port facilities, correctional institutions, and other critical infrastructure organizations spanning North America, Europe, Africa, Asia-Pacific, and the Middle East.

The survey captured both qualitative operational insight and structured assessments across five key dimensions: operating environment, counter-UAS objectives, current capability maturity, regulatory constraints, and identified challenges. All responses were anonymized, normalized, and categorized to enable consistent comparative analysis across the dataset.

This is not a theoretical study. Every finding reflects the lived operational reality of the people responsible for keeping these environments secure. The consistency of responses across sectors and geographies is itself a significant finding: the challenges are not organization specific. They are structural.

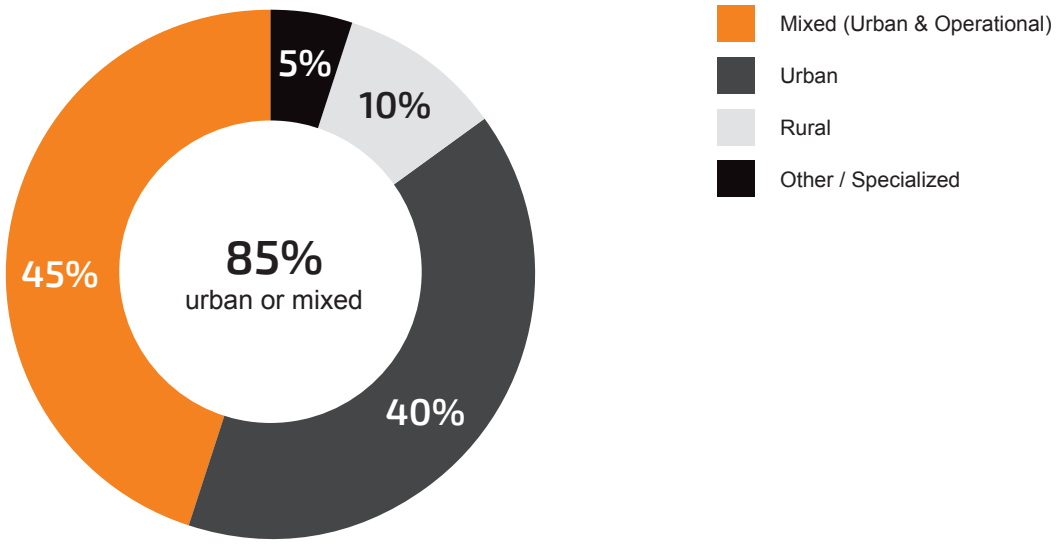
Who Responded

Respondents include senior security managers, operations directors, and aviation authority officials at major international airports, a major port of entry, a multi-airport national authority, correctional system operators, and critical infrastructure oversight organizations. All responses are anonymized in accordance with survey commitments.

Section 1: The Environments Operators Are Managing

Understanding where operators work is essential context for understanding the nature of the threat they face. Approximately 85 percent of survey respondents operate in urban or mixed-use environments, settings where aviation operations intersect continuously with residential neighborhoods, commercial activity, and open airspace accessible to any drone operator within range.

Figure 1: Operational Environment Distribution



Most respondents manage airspace that is shared with legitimate commercial and recreational drone activity — making threat classification a constant operational challenge, not a periodic one.

In shared airspace, the challenge is not simply detecting a drone. It is determining, rapidly and reliably, whether that drone is authorized to be there, what it is doing, and whether it warrants escalation. Without integrated detection tools, that determination defaults to visual observation by ground personnel: a method that is slow, range-limited, and entirely reactive.

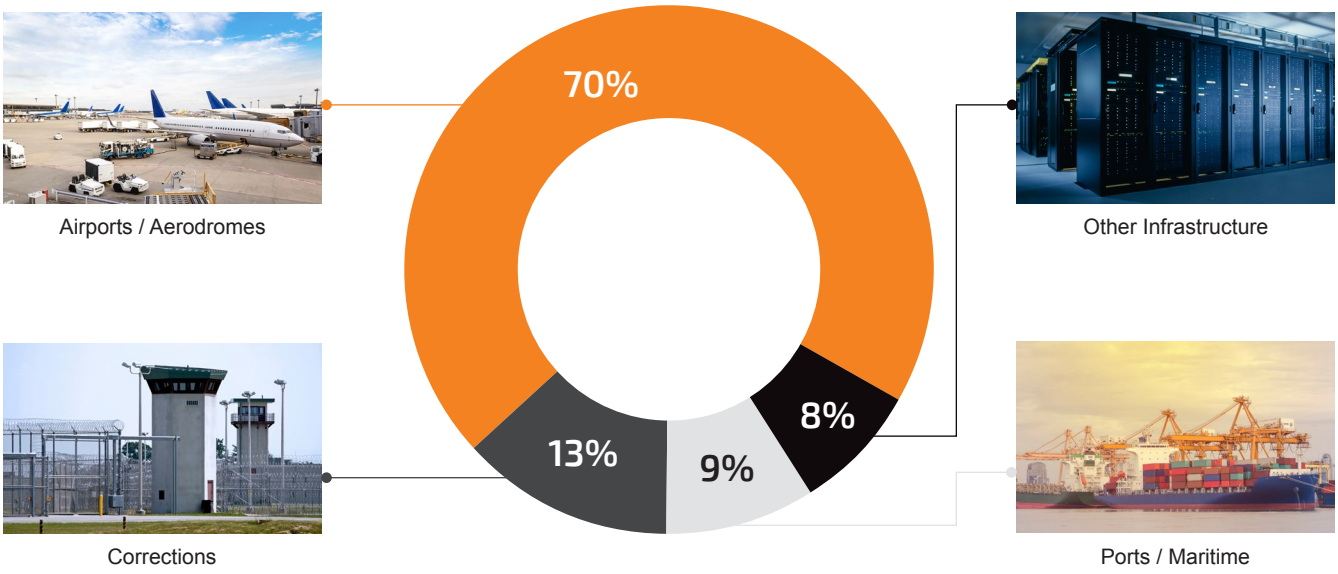
Rural respondents, a smaller share of the dataset, reported that open terrain creates its own exposure. Limited personnel resources, absence of natural barriers, and geographic isolation combine to make early detection difficult and the consequence of a missed incursion significant.

The operational environment data establishes a baseline: the facilities represented in this dataset are not operating in controlled, low-traffic conditions. They are managing complex, high-exposure environments where drone activity is persistent and classification is continuous.

Who Is At Risk: Cross-Sector Exposure

Aviation environments carry the highest-consequence exposure. An unauthorized drone near an active runway is an immediate flight safety risk. The regulatory and reputational implications of an incursion-linked incident are severe. Operators in this environment have both the strongest motivation to act and, in many jurisdictions, the most constrained legal authority to do so.

Figure 2: Facility Type Breakdown



Aviation and transportation dominate the dataset, but the presence of corrections, ports, and other critical infrastructure confirms that drone threats are systemic — not sector-specific.

Correctional facilities present a different but equally acute risk profile. Drone-assisted contraband delivery, including narcotics, mobile devices, and weapons, is an established and growing tactic. Visual detection of low-altitude, slow-moving drones in facility airspace is unreliable. The consequences of successful deliveries are significant for institutional security and public safety.

Port and maritime operators describe surveillance, espionage, and potential sabotage as their primary drone-related concerns, targeting fuel storage, cranes, communication infrastructure, and vessels at berth. The geographic scale of port environments makes perimeter-based approaches inadequate.

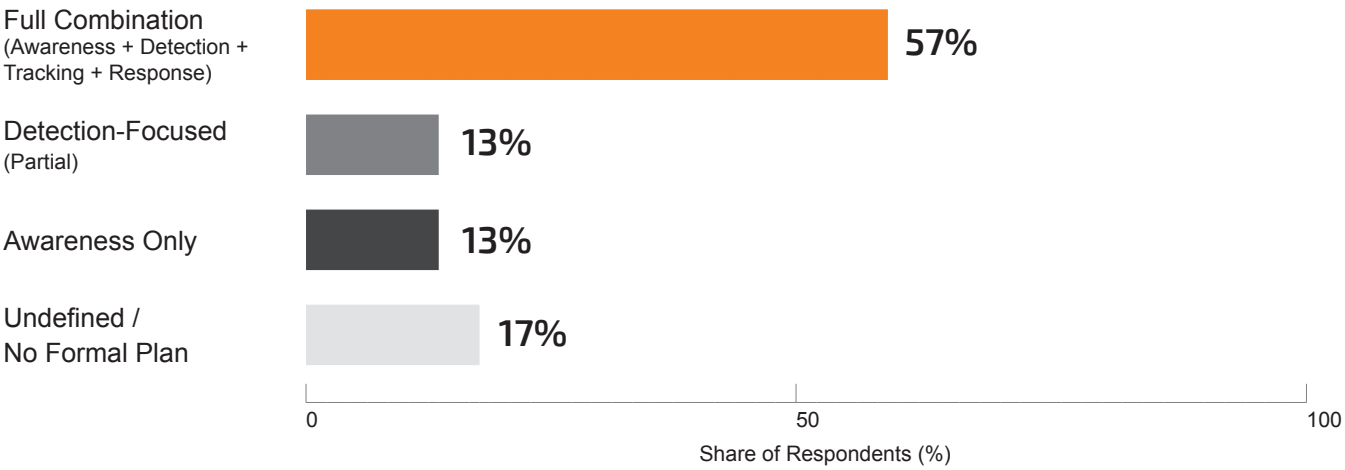
What unifies these contexts is a shared set of underlying failures:

- inadequate detection
- absent legal authority
- fragmented procedures
- dependency on external agencies that cannot always respond in time.

Section 2:
What Operators Want and What They Have

Survey respondents were asked to describe their counter-UAS operational objectives. The distribution of responses reveals a critical structural problem: the gap between what organizations intend and what they have built.

Figure 3: Stated Counter-UAS Operational Objectives



While a majority have defined comprehensive objectives, 17 percent of respondents operate without a full counter-UAS plan — and many with defined objectives acknowledge significant gaps in implementation.

Operator Voices

"The objective is not clearly defined. Drone issues are dealt with as and when they arise."

Another respondent noted: "Most counter-UAS activities are done as part of general facility contingency planning and may not have enough detail to deal with this emerging threat effectively."

Approximately 57 percent of respondents described a comprehensive counter-UAS objective encompassing awareness, detection, tracking, and coordinated response. This indicates genuine operational sophistication in the majority of the surveyed population. But it also sets up the most important finding in the dataset: having defined objectives does not mean having the capability to execute them.

Several respondents who described the most comprehensive objectives also acknowledged that their current implementation falls substantially short. Objectives exist in policy documents and contingency plans. The systems, authority, and trained personnel to deliver on them do not yet exist in practice.

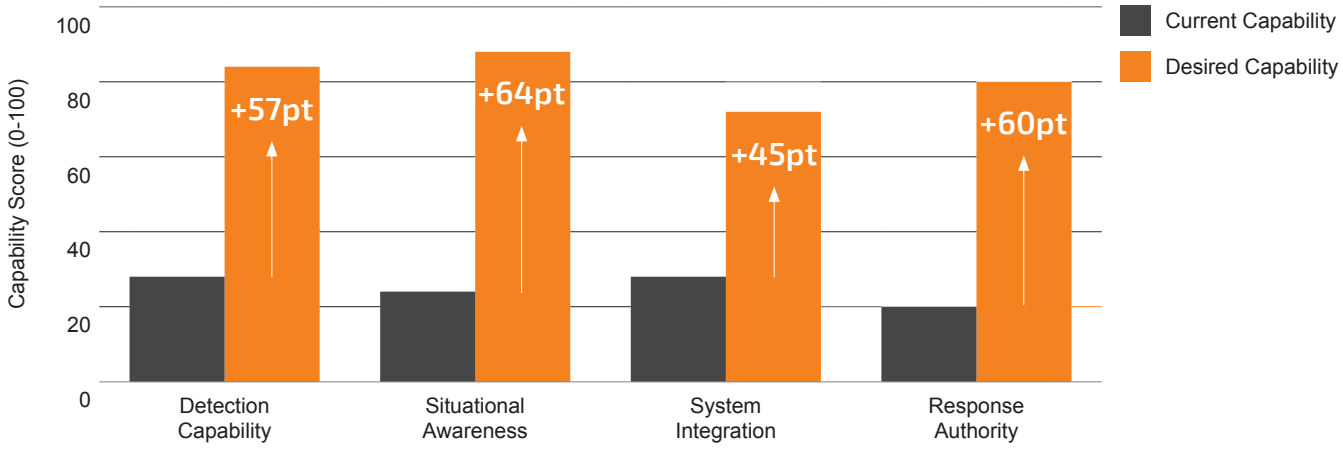
The 17 percent of respondents with no formalized counter-UAS plan represent a specific and acute risk: organizations that will be managing a drone incident for the first time during the incident itself, with no established procedures, no clear escalation pathway, and no baseline situational awareness from which to act.

Section 3: The Detection Gap — Highest Priority, Lowest Capability

Detection and situational awareness are the most consistently cited capability requirements across the entire dataset. More than 80 percent of respondents identified real-time detection as essential. It is the highest-priority need, expressed across every sector, every geography, and every facility type in this study.

It is also the area of greatest failure. The gap between what operators need and what they currently have is larger here than in any other dimension assessed.

Figure 4: Current vs Desired Capability Across Key Dimensions



Across all four critical capability dimensions, current operator capability falls sharply below what they themselves define as adequate. The detection and situational awareness gaps are the most severe.

The inadequacy of visual detection as a primary method is not simply a technology preference issue. It creates an operational asymmetry with serious security consequences: operators cannot know what they cannot see. Threats that are not detected are not logged, not assessed, and not escalated. Incident patterns that should inform security planning leave no record. Decisions about response are made in the dark.

The RF-Silent Problem

Multiple respondents specifically identified RF-silent drones, autonomous UAS that operate without radio frequency emissions, as a category that current detection approaches cannot address. As the cost of autonomous systems falls and their operational capability increases, the population of drones that existing RF-monitoring tools simply cannot detect is growing.

Respondents who have evaluated detection technologies describe integration as a significant secondary barrier. Even where systems are technically available, connecting them to existing security infrastructure (command centers, surveillance systems, communication platforms), requires resources and planning that many facilities cannot currently commit.

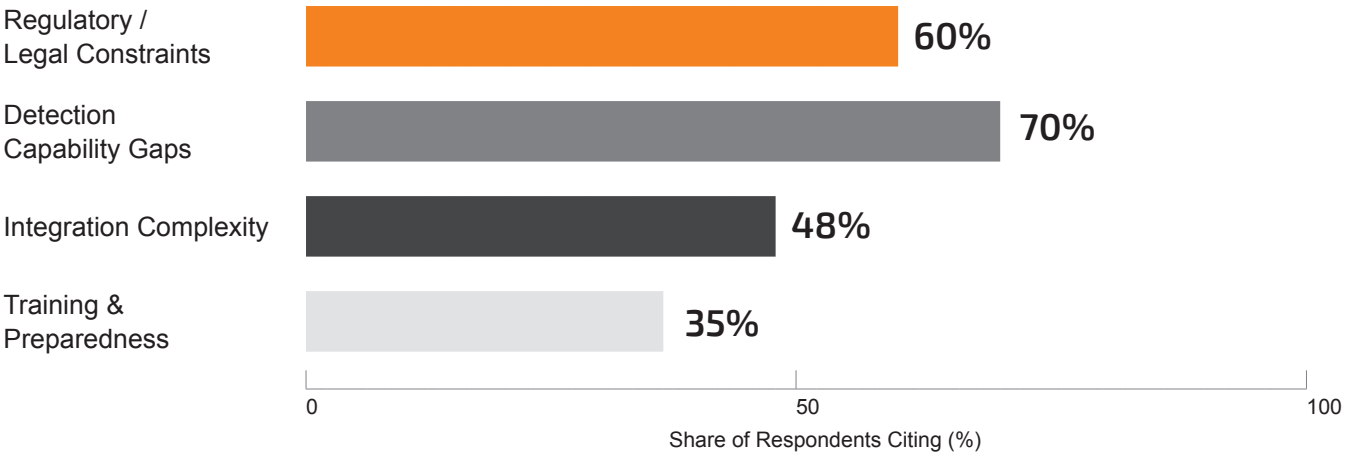
Operator Voices

"Detecting RF-silent drones and managing swarm-based threats remains a key challenge." And separately: "One of the key challenges is maintaining continuous situational awareness of unauthorized UAS activity within and around the airport environment. Airports typically rely on visual reporting or ad-hoc detection, which may limit early identification of drone incursions."

Section 4:
The Authority Gap — When Detection is Not Enough

Of all the barriers identified in this survey, regulatory constraints represent the most structurally persistent. Approximately 60 percent of respondents, across aviation, corrections, ports, and other critical infrastructure, indicated that they lack the legal authority to take direct mitigation action against unauthorized drones, even when the threat to safety is clear and immediate.

Figure 5: Primary Barriers to Effective Counter-UAS Operations



Regulatory and legal constraints are cited more frequently than any technical limitation — a finding that underscores the structural nature of the readiness gap and the limits of technology-only solutions.

This is not a technology problem. It is a policy problem. And it defines the ceiling on counter-UAS readiness in the current environment: operators can detect a threat; they can classify it, and then they must wait for external authorization to act.

The Dependency Chain

The data reveals a critical dependency structure. Effective counter-UAS response requires detection, authority, and response capability to function as a system. Weakness in any element degrades the effectiveness of the entire chain.

Detection without authority produces situational awareness, but not security outcomes. Operators know the threat is there. They cannot act on that knowledge.

Authority without detection cannot be exercised. If a threat is not identified, the legal authority to respond, even where it exists, is irrelevant.

Both without integration produce inconsistent, slow, and unpredictable responses, degrading the operational value of both investments.

The regulatory landscape varies significantly by jurisdiction. But the common finding across responses is reliance on external agencies, aviation authorities, law enforcement, national security bodies, to authorize and execute any response beyond detection and reporting. That reliance introduces delays. In scenarios involving aircraft safety, active contraband delivery, or infrastructure surveillance, those delays have direct operational consequences.

The data strongly suggests that technology investment alone will not close the counter-UAS readiness gap. For that investment to achieve its intended security outcomes, regulatory frameworks must evolve to give operators proportionate, defined, and legally clear authority to act.

Operator Voices

“There is currently no authority to interdict UAS due to federal law. We would like to have the ability to proceed with mitigation but cannot.” Another respondent noted the need for: “Delegation of power to apply UAS neutralization — to airport managers, state authorities...”

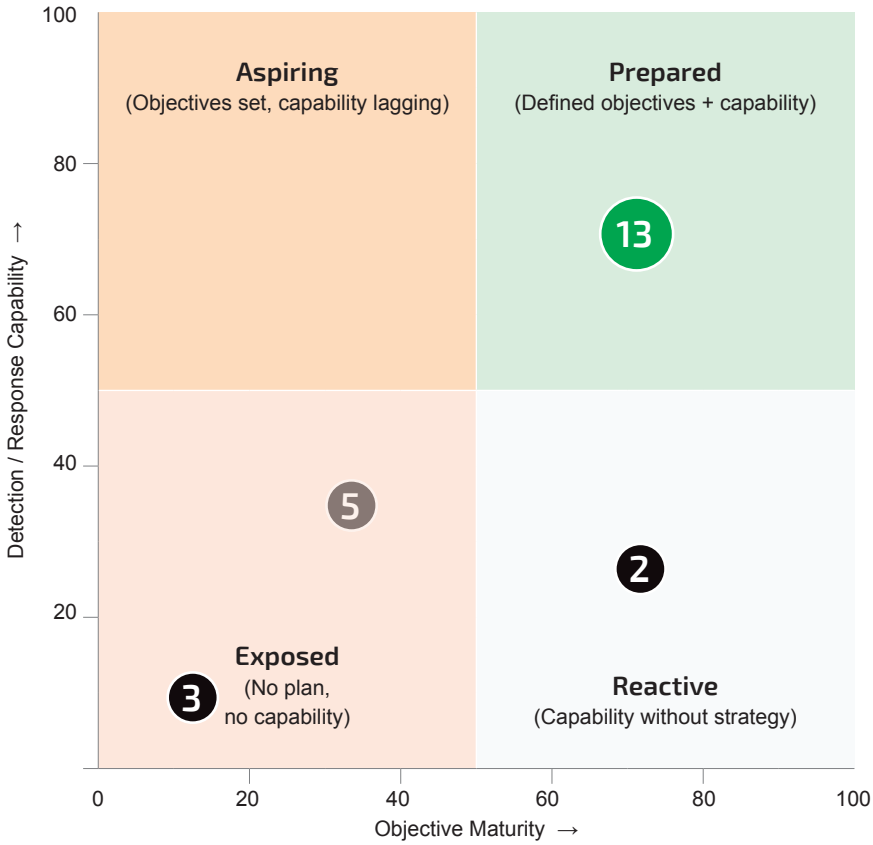
Section 5: Where Organizations Stand

Mapping respondents across two dimensions, objective maturity and operational capability, reveals a readiness landscape that is highly skewed toward the left: most organizations have stronger aspirations than they have built systems to support.

Figure 6: Counter-UAS Readiness Maturity – Respondent Distribution

The largest cluster (13 respondents) sits in the **Prepared** quadrant: organizations with defined counter-UAS objectives and moderate operational capability. These are typically larger airports and critical infrastructure operators who have invested in the problem and have structured frameworks in place. But even within this group, capability gaps remain. The Prepared quadrant describes a relative position, not an adequate one.

Five respondents fall into the **Partial** or **Limited** category, organizations where objectives exist but capability has not kept pace. These operators face a specific risk: they have plans that they cannot execute with their current tools and authority. Their frameworks create expectations for response that their systems cannot deliver.



The majority of respondents cluster in the 'Prepared' or 'Aspiring' quadrants. A significant minority remain 'Exposed' — with neither formalized objectives nor meaningful capability. Bubble size reflects number of respondents; number inside reflects count.

Three respondents, nearly 13 percent of the sample, sit in the **Exposed** quadrant: undefined objectives, minimal capability, and no formalized framework. These organizations are at the greatest risk of managing a serious drone incident reactively, without established procedures, and with outcomes that are difficult to predict or control.

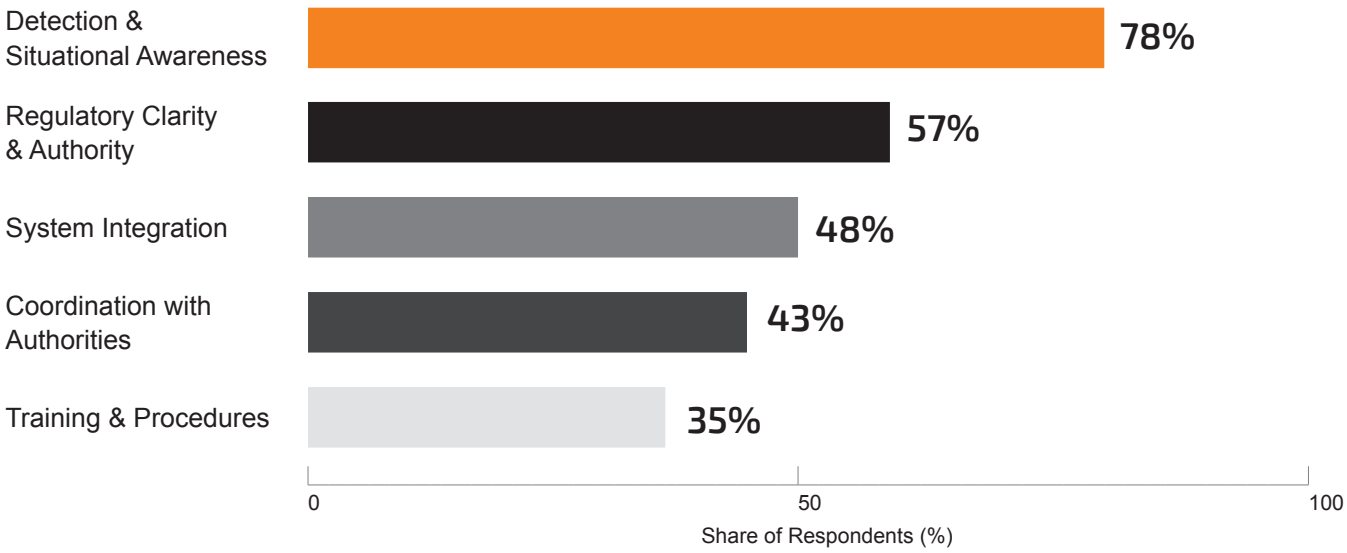
The Self-Assessment Question

The maturity map is designed to prompt a specific question: where does your organization sit in this landscape? The data suggests that most security decision-makers have a reasonable sense of their gap, they know detection is inadequate, they know the regulatory constraints they operate under, and they know their procedures need development. What many lack is a structured framework for assessing that gap systematically and a credible path for closing it.

Section 6:
What the Industry Needs — And What It Looks Like

Despite the wide variation in current capability across respondents, the data reveals striking alignment in what operators believe is needed. The industry is fragmented in execution. It is unified in direction.

Figure 7: Top Capability Needs Identified by Operators



Detection and situational awareness dominate operator demand — cited by 78% of respondents. The next-highest needs (regulatory clarity and system integration) define the structural conditions that make detection investment viable.

The priority ranking from the data is instructive. Detection and situational awareness lead by a significant margin — not because the other needs are unimportant, but because they are the foundational requirement from which everything else follows. An operator cannot coordinate with authorities around a threat they have not detected. They cannot escalate through a regulatory framework against an incident they are unaware of.

But the data also makes clear that detection alone is not sufficient. The second and third priorities: regulatory clarity and system integration, are not downstream refinements. They are preconditions for detection investment to produce security outcomes. An integrated detection system that feeds into a regulatory void generates logs, not safety.

What Operators Describe as Their Ideal Solution

Qualitative responses from across the dataset consistently described the characteristics of an effective counter-UAS capability:

- **Real-time detection** — continuous visibility into airspace activity, not incident-triggered reporting.
- **Multi-layered sensing** — capability against both RF-emitting and RF-silent drone types, reducing exploitable blind spots.
- **Integration with existing infrastructure** — connection to security operations centers, existing surveillance systems, and communication platforms, not standalone tools.
- **Defined escalation pathways** — clear, pre-established protocols for coordinating with aviation authorities, law enforcement, and national security agencies.
- **Scalable and cost-effective** — deployable across facilities of different sizes and complexity levels without prohibitive cost or operational disruption.
- **Regulatory compliance** — solutions that operate within current legal frameworks while positioning operators to act decisively as authority frameworks evolve.

Operator Voice

“A system that can provide real-time visibility of drone activity, such as passive radio frequency monitoring, radar-based detection, or integrated airspace awareness platforms, would significantly enhance our ability to understand what is occurring in the surrounding airspace and respond appropriately through established reporting and coordination procedures.”

Conclusion: The Gap Is Known — Closing It Requires More Than Technology

The findings of this global assessment are consistent across sectors, geographies, and facility types. Unauthorized drone activity is a persistent operational reality for the organizations that responded to this survey. The threat is well understood. The response capability is not yet adequate to address it.

The industry has moved beyond awareness. What it has not yet achieved is operational maturity, the alignment of detection technology, regulatory authority, operational procedures, and cross-agency coordination that converts awareness into effective, timely response.

Three conclusions are clear from the data:

Technology investment without policy reform is insufficient.	Detection systems that feed into a regulatory framework where operators cannot act produce awareness without security outcomes. The authority gap must be addressed, through regulatory reform, delegated authority frameworks, and defined escalation structures, for technology investment to achieve its intended purpose.

Fragmented approaches produce fragmented results.	Counter-UAS is a system-of-systems challenge. Detection, authority, procedures, coordination, and training must function as an integrated capability. Investment in any single element, without equivalent investment in the others, leaves the system as weak as its weakest component.

The organizations that will lead are those that act before an incident forces the issue.	The maturity data is clear: organizations in the Exposed and Aspiring quadrants face not a question of whether they will encounter a serious drone incident, but of whether they will be prepared when they do. Building that preparedness systematically, not reactively, is the defining differentiator.

The path forward requires simultaneous progress across technology, policy, and operations. The organizations and policymakers that recognize this and act on it, will determine the shape of counter-UAS readiness in the years ahead.

Appendix A:
Anonymized Survey Dataset

A.1 Dataset Overview

This dataset represents anonymized responses collected from more than twenty operators across airports, aviation authorities, correctional facilities, port infrastructure, and other critical infrastructure environments. Each respondent has been assigned a unique identifier to preserve confidentiality. No identifying information related to individual respondents, organizations, or specific facilities has been included.

Responses were normalized and categorized across six dimensions: Sector, Operating Environment, Primary Function, Counter-UAS Objective, Current Capability Maturity, and Key Operational Challenge(s).

A.2 Structured Dataset

ID	Sector	Environment	Primary Function	CUAS Objective	Capability Maturity	Key Challenges
AP-01	Airport	Urban	Transportation	Defined	Moderate	SA, TRN
AP-02	Airport	Urban	Transportation	Defined	Moderate	SA, INT
AP-03	Airport	Rural	Transportation	Limited	Low	SA
CI-04	Critical Infra.	Mixed	Transport/Logistics	Defined	Moderate	SA, DET, REG, INT, TRN
AP-05	Airport	Urban	Transportation	Limited	Low	SA, DET
AP-06	Airport	Urban	Aviation	Defined	Moderate	SA, INT
AP-07	Airport	Mixed	Aviation Infra.	Defined	Moderate	SA, INT
AP-08	Airport	Mixed	Transportation	Defined	Moderate	SA
AP-09	Airport	Rural	Transportation	Partial	Low	DET
AP-10	Airport	Rural	Transportation	Partial	Low	DET
AP-11	Airport	Rural	Transportation	Limited	Low	SA
AP-12	Airport	Urban	Transportation	Defined	Moderate	SA, REG
AP-13	Airport	Urban	Transportation	Defined	Moderate	SA, INT
AP-14	Airport	Urban	Transportation	Defined	Moderate	SA
AP-15	Airport	Urban	Transportation	Defined	Moderate	SA
CI-16	Corrections	Mixed	Prison System	Partial	Low	DET
CI-17	Port	Mixed	Maritime/Port of Entry	Defined	Moderate	SA
CI-18	Manufacturing	Urban	Industrial	Partial	Low	—
AP-19	Airport	Urban	Transportation	Undefined	Low	—
AP-20	Airport	Urban	Transportation	Defined	Moderate	SA, REG
AP-21	Airport	Urban	Transportation	Defined	Moderate	SA, INT
CI-22	Critical Infra.	Mixed	Multi-Facility Oversight	Limited	Low	SA
AP-23	Airport	Urban	Transportation	Defined	Moderate	SA, INT

Key: SA = Situational Awareness · DET = Detection Capability · REG = Regulatory Constraint · INT = Integration Complexity · TRN = Training/Preparedness

A.3 Interpretation Notes

The dataset is concentrated in airport and aviation environments (~70% of respondents), with the remainder spanning correctional facilities, port infrastructure, manufacturing, and multi-facility critical infrastructure organizations.

- Operating environments are predominantly urban or mixed (~85% combined).
- Counter-UAS objectives show broad conceptual alignment, but capability maturity remains uneven.
- Key challenges concentrate around situational awareness (74%), detection capability (70%), and regulatory constraints (61%).

A.4 Limitations

This dataset reflects a targeted sample of operators and is intended to provide directional insight into current counter-UAS readiness rather than statistically representative conclusions across all global infrastructure. It is not a probability sample. The consistency of responses across sectors and geographies suggests the findings are broadly indicative of structural industry conditions.

Appendix B:
Thematic Analysis Framework

B.1 Analytical Approach

Survey data was analyzed using a structured thematic framework across six categories: operational environment, counter-UAS objectives, detection capability, regulatory constraints, integration maturity, and operational readiness. Responses were coded and grouped based on recurring themes. Categories with frequent, consistent agreement across respondents are treated as areas of strong alignment; categories with fragmented or capability-limited responses reflect structural gaps.

B.2 High-Alignment Themes

- Recognition of the drone threat as an active, ongoing operational concern, present across virtually all responses regardless of sector or geography.
- Importance of situational awareness and real-time detection, referenced by more than 80% of respondents as a core operational requirement.
- Need for coordination with external authorities, described as essential to any functional response model.
- Value of integrated solutions, consistent emphasis on systems that connect with existing infrastructure rather than operating as standalone tools.

B.3 Low-Alignment / High-Gap Themes

- **Regulatory Authority to Act:** ~60% lack legal authority for direct mitigation. The most critical and structurally persistent barrier in the dataset.
- **Detection Implementation Maturity:** Most respondents rely on visual observation or incident-based reporting rather than integrated systems.
- **Standardized Counter-UAS Frameworks:** A significant portion manage drone incidents on an ad hoc basis without dedicated protocols.
- **Technology Integration:** Uncertainty around system selection and interoperability is a persistent barrier to progress.
- **Training and Procedural Readiness:** Consistently identified as requiring structured development across the dataset.

B.4 Cross-Category Structural Insights

Three structural insights emerge from collective thematic analysis:

- **Awareness vs. Execution:** Operators understand the problem and can articulate the solution. What they lack is capability, authority, and integration to deliver it.
- **The Dependency Chain:** Detection, authority, and response form an interdependent system. Weakness in any element limits the effectiveness of the others.
- **System-of-Systems:** Counter-UAS requires alignment across technology, policy, operations, and coordination. Fragmentation in any dimension reduces overall system effectiveness.

DRONESHIELD

DroneShield works with airports and critical infrastructure operators worldwide to close the gaps this research has identified — detection capability, system integration, and coordinated response frameworks.

Contact

droneshield.com
info@droneshield.com