

Digital Transformation: DFR Series

Ten Steps to a Successful DFR Program

Strategy - Transparency - Accountability



Letter from the Author

Over 10 years ago I taught a Surveillance in Modern Society course at George Mason University in Fairfax, VA. I encouraged students to explore the subjects of privacy, surveillance, and safety. Through each course I watched their opinions start one way, shift, then shift back or change completely—leaving the class more informed about these topics and the idea of convenience. One of the final exam questions was for them to make a policy—or argue against it—for a drone program for their local police department. Those concerns from a decade ago, when there weren't any programs, are even louder today as our exploration of drones for local public safety and emergency services continue to shape the future.

What began as a theoretical classroom debate has become one of the most pressing policy challenges facing American communities. Since Chula Vista launched the first Drone as First Responder program in 2018, we've witnessed explosive growth to over 300 programs serving more than 1,500 agencies. The technology delivers undeniable benefits—response times measured in seconds rather than minutes, lives saved through faster emergency response, and officers equipped with critical intelligence before arriving at dangerous scenes.

Yet the civil liberties concerns my students grappled with have only intensified. We now have documented evidence of mission creep, disproportionate surveillance in communities of color, inadequate transparency, and regulatory gaps that leave constitutional protections vulnerable. The fundamental question remains: can we achieve operational efficiency without sacrificing the privacy expectations and civil liberties that define a free society?

I wrote this guide because I believe the answer is maybe—and only if we get the implementation right. Having analyzed over 200 DFR programs through policy documents, news releases, government documents, and other open sources, advising dozens of agencies, and witnessing both spectacular successes and preventable failures, I've identified the patterns that separate accountable innovation from surveillance expansion. The difference isn't whether agencies use drone technology, but how they govern its use.

This isn't a marketing document promoting drones, nor is it advocacy against them. It's a practical framework grounded in evidence from agencies that built community trust through transparency, from civil liberties organizations that shaped responsible policies, and from communities that demanded—and received—meaningful oversight. The 10 steps outlined here represent hard-won lessons from early adopters who learned, sometimes painfully, what works and what destroys public trust.

My students taught me that people's views on surveillance technology evolve when they understand both the benefits and the risks. They want safety, but not at any cost. They value innovation, but demand accountability. They recognize operational necessity while insisting on constitutional protections. This guide honors that nuanced perspective. To public safety leaders: you have an opportunity to implement transformative technology responsibly. The agencies profiled here demonstrate that transparency and effectiveness aren't opposing forces. They're complementary requirements. Your willingness to engage communities before purchasing equipment, to accept meaningful oversight, and to operate with radical transparency will determine whether your program becomes a model or a cautionary tale.

To community advocates: you have leverage. Seattle's successful opposition in 2013 proved that organized communities can shape technology deployment. The ongoing legal victories securing drone footage transparency show that persistence matters. This guide provides the policy frameworks, oversight mechanisms, and accountability measures you should demand. Don't accept promises—insist on written policies, public reporting, and independent audits before a single drone launches.

To policymakers: you hold the key. DFR programs operate in regulatory spaces and gaps at federal, state, and local levels. The approaches presented here—warrant requirements, usage restrictions, transparency mandates, community consent processes—provide legislative templates. Your constituents deserve both effective emergency response and constitutional protections. You don't have to choose between them.

The technology is here. The question is whether we'll sleepwalk into widespread aerial surveillance or deliberately construct frameworks that preserve civil liberties while advancing public safety. My students understood a decade ago that convenience often comes with hidden costs. Their generation—now making these decisions as professionals, advocates, and citizens—has the chance to prove that democratic societies can adopt powerful technologies without compromising the values that make democracy worth protecting.

This guide, and others in our Digital Transformation Series, provides the roadmap. The choices are yours.

A handwritten signature in black ink that reads "Dr. Jessica Herbert". The signature is fluid and cursive, with the first letters of each word being capitalized and prominent.

Dr. Jessica Herbert
Founder & Digital Transformation Advisor, IDEA Analytics

Suggested Citation: Herbert, J. 2025. Ten Steps to a Successful DFR Program - Digital Transformation: DFR Series. Phoenix, AZ. ISBN: 979-8-9936123-0-0

Table Of Contents

Letter from the Author	1
Executive Summary	5
How to use this document	6
Developing or Expanding your DFR Program	6
Step 1: Build the foundation through executive leadership and strategic research	7
Step 2: Conduct comprehensive needs assessment and coverage analysis	8
Step 3: Engage community stakeholders before equipment purchase	10
Step 4: Develop comprehensive policy and governance framework	12
Step 5: Navigate FAA regulatory pathways and secure operational waivers	15
Step 6: Develop budget and identify funding sources	17
Step 7: Build operational infrastructure and integration architecture	20
Step 8: Execute comprehensive community transparency and launch strategy	24
Step 9: Implement risk management and compliance framework	27
Step 10: Establish post-implementation monitoring, evaluation, and evolution framework	30
Critical Success Factors Synthesis	36
About IDEA Analytics	38
Our Services	38

Executive Summary

Drone as First Responder (DFR) programs represent a significant advancement in emergency response capabilities. These programs demonstrate measurable operational benefits including quicker response times for fire, EMS, or police, first-on-scene arrival rates assist with visual dispatching and information for officer safety, and assistance with crime interventions and/or de-escalation. Some programs have even boasted delivering 71-second response times, clearing 20-25% of calls without officer dispatch, and building community trust when implemented with transparency.

However, for many communities during initial planning or ongoing operations, these benefits exist in inherent tension with fundamental civil liberties concerns around privacy, surveillance, and constitutional protections. **This tension is not irreconcilable.** Evidence from leading programs demonstrates that robust governance frameworks, proactive transparency measures, and community-centered oversight can preserve operational effectiveness while protecting civil liberties. The critical differentiator between successful and problematic programs is not whether they use the technology, but **how they govern its use.**

This document provides ***10 Steps to a Successful DFR Program***. These steps are designed to guide your efforts in to develop and/or expand your DFR program with accountability, transparency, and responsible reporting.

How to use this document

If you have starting out your program, it is encouraged that you follow these 10 steps in order. These steps are based on lessons learned in over 200 programs that have operated -- some continuously, some having to shut down due to poor planning, some having significant operational delays for years. So, if you are new to the DFR world, you are in a great position to learn and avoid the natural mistakes of the early adopters in this space.

However, based on the patterns of technology adoption and policy changes in public safety, there is a high likelihood that the 10 steps defined here isn't the way you started off your program.

Chances are, you may not have approached your program in this order of operations within this document. That's okay! You can use this framework to evaluate your program effectiveness, identify the gaps, and determine how to build your capacity and sustain your program moving forward. You may find that the steps or supporting actions detailed within this document are reasons your program isn't operating with efficiency or effectiveness you first desired. Digital transformation projects like DFR are not always linear, and many things can happen in the process of implementation that changes decision making.

Developing or Expanding your DFR Program

While the technology purchases and training for pilots may be at the forefront of your program plans, the true investments need to be in the systematic processes to ensure proper governance frameworks, reporting, and public transparency does not crush your program. In evaluating lessons learned from over 200 DFR programs, the following 10 Steps are designed to assist your agency in replicating what works and ensure the program serves your community within regulatory frameworks.

Step 1: Build the foundation through executive leadership and strategic research

Executive buy-in is the essential condition of DFR success—no program has survived without unwavering support from the chief executive, city manager, and at least three council members identified before formal proposal. Secure this foundation by conducting site visits to operational programs within 200 miles (Chula



Vista, Montgomery County, and Scottsdale maintain open-door policies), assembling a cross-functional implementation team with legal counsel, IT, community relations, and operations representatives, and developing a preliminary concept of operations defining specific use cases restricted to emergency 911 calls.

Form an implementation team with clear roles: Designate a program manager (typically lieutenant or captain level) with 25%-time allocation, assign a policy lead for FAA coordination and waiver applications, identify IT liaison for CAD integration planning, and recruit community engagement officer for stakeholder management. This team should complete a **60–90-day research phase** visiting minimum three operational programs, interviewing their communities about concerns, and documenting both successes and mistakes to avoid.

Critical early decision: Determine whether to pursue **Part 107 + waivers or Certificate of Authorization (COA) pathway**. Most agencies now pursue both in parallel—Part 107 for immediate training and simple operations while the **new 91.113 waiver** (streamlined in 2025) processes for beyond visual line of sight (BVLOS) capability. The 2025 regulatory changes reduced approval times from 11+ months to 24 hours-2 weeks with 4-year validity, making this the fastest path to operational status for qualifying Public Safety Organizations.

Deliverables for this step: Executive sponsor commitment letter, implementation team charter with meeting schedule, completed site visit reports from 3+ programs, preliminary use case matrix (emergency calls only vs expanded operations), and draft timeline for council presentation. Budget 3-6 months for this foundation phase—rushing produces programs that collapse under community opposition.

Step 2: Conduct comprehensive needs assessment and coverage analysis

Data-driven site selection multiplies program effectiveness—Montgomery County's crime analysts studied statistics across six patrol districts before selecting locations, resulting in 71% first-on-scene rates. Begin with jurisdictional analysis: total square miles, population density, annual call volume by type and location, current average response times by district, and officer staffing levels by shift. DFR platforms typically cover 3–6-mile radius per site; calculate how many dock locations would provide adequate coverage balancing cost against response time goals.

Develop use case priority matrix based on actual call data: highest frequency emergency calls (structure fires, medical emergencies, active violence), highest officer safety risk calls (domestic violence, mental health crises, barricaded subjects), calls benefiting most from aerial perspective (pursuits, missing persons, accident reconstruction), and calls currently requiring helicopter support. The **critical constraint:** DFR responds only to active emergencies, not "occurred earlier" calls, to address civil liberties concerns and focus on time-sensitive situations.

Technology selection driven by mission requirements: All successful programs emphasize mission over platform. Essential capabilities include dual visual/thermal cameras (minimum 12MP), 20–30-minute flight time, weather tolerance (wind, rain, darkness), autonomous waypoint navigation for BVLOS operations, 360-degree obstacle avoidance, and remote ID compliance. Blue UAS Framework compliance increasingly standard with 37+ approved platforms including Skydio X10D (industry leader), BRINC Responder (purpose-built USA), Freefly Astro, Anduril Ghost, and Parrot ANAFI variants.



Cost modeling for realistic budgeting: Calculate *cost per square mile* using formula:
(Hardware + Software + Infrastructure + 1st Year Staffing) / Total Coverage Area. Typical range: *\$4,285-\$8,771 per square mile* depending on altitude operations and staffing model. For 50 square mile jurisdiction, expect

\$215,000-\$440,000 startup investment. Single dock installation with equipment: \$250,000-\$308,000.

Annual staffing (largest expense): \$300,000-\$500,000 for 24/7 rooftop pilot coverage, or \$60/hour for contracted remote pilot services offering substantial savings.

Deliverables: Needs assessment report with call volume analysis, coverage area map with proposed dock locations and response radius circles, technology comparison matrix weighted by mission requirements, and preliminary 5-year budget showing startup (\$300K-\$500K) and annual operating costs (\$300K-\$500K). Include ROI framework projecting officer hours saved (20-25% call clearance rate), response time improvements (75%+ reduction typical), and cost avoidance vs helicopter operations (\$200-\$400/hour flight time).

Step 3: Engage community stakeholders before equipment purchase

One year of community engagement before purchasing equipment is the universal success pattern—Chula Vista, Montgomery County, and Scottsdale all invested 6-12 months in stakeholder consultation, while Seattle's 2013 program collapsed when they purchased drones first and consulted later. This step is non-negotiable and cannot be shortened without risking program failure. Begin by mapping stakeholders: political leaders (council members, mayor, city manager), civil liberties organizations (ACLU, EFF, local advocacy groups), community organizations (neighborhood associations, faith communities, business districts), and internal stakeholders (police/fire unions, rank-and-file, command staff, sister agencies).

ACLU engagement as early as policy concept phase prevents later opposition. Schedule meetings presenting five core commitments: usage limited to warrant, specific articulable grounds, or emergencies (not routine patrol); data retention restricted to reasonable suspicion of crime with 7-14 day auto-deletion otherwise; democratic policy control by elected officials not police alone; abuse prevention through audits and oversight; and absolute prohibition on weaponization. Montgomery County's proactive civil liberties engagement resulted in ACLU partnership rather than opposition—a pattern replicable through genuine responsiveness to concerns.



Community consultation methods proven effective:

Town hall series (minimum three sessions, varied locations/times), demonstrations at community events (county fairs, National Night Out, community festivals), school

presentations building youth awareness, targeted presentations to neighborhood associations and business groups, social media campaign with educational videos, and community survey collecting concerns and suggestions. Document all feedback received and demonstrate responsiveness by incorporating appropriate recommendations into draft policies.

Council member individual briefings 3-6 months before formal presentation—secure commitments from at least five of seven members (adjust ratio to your council size) through one-on-one meetings presenting program benefits, addressing specific concerns, offering site visits to operational programs, and gauging support level. Identify potential opponents early and understand their concerns: privacy advocates need transparency commitments, fiscal conservatives need ROI data, civil libertarians need use restrictions, and progressive members need equity analysis showing all neighborhoods benefit equally.

Deliverables: Stakeholder engagement log documenting all meetings and feedback received, community survey results with concerns and support levels, ACLU meeting summary with agreed-upon policy commitments, council member assessment matrix showing support/opposition/undecided status, and draft policies incorporating community feedback. Timeline: *6-12 months concurrent with Step 2*. This investment prevents the program-killing opposition that destroyed early implementations.

Step 4: Develop comprehensive policy and governance framework

Policy before platforms is the iron law of successful programs—clear written restrictions on use, data retention, and oversight mechanisms must exist before operational launch. The IACP Model Policy (April 2019) provides proven framework covering administration, training, operations, privacy, and maintenance. Essential policy components include explicit use authorization (emergency 911 calls, missing persons, accident reconstruction, tactical support, disaster assessment, training/demonstrations) and absolute prohibitions (no random surveillance, no general patrol absent explicit community approval, no First Amendment activity monitoring except immediate safety threats, no warrantless evidence collection intruding on reasonable privacy expectations, no weaponization of platforms).



Data governance framework addressing civil liberties concerns: Adopt your states public records retention and data governance procedures. Need something more? Establish five-tier classification system with retention schedules such as:

- Criminal Investigation Evidence (retain per criminal justice standards, typically 7+ years)
- Preliminary Investigation (30-90 days pending investigation outcome)
- Emergency/Non-Criminal (7-14 days with auto-deletion if not elevated)
- Training Footage (retain with privacy redactions)
- Public Disclosure (comply with state records laws).

Access controls mirror body-worn camera policies with official use only, comprehensive audit trails for all access, and strict prohibition on personal use or unauthorized disclosure.

Oversight architecture with multiple accountability layers: Real-time supervisor approval for each launch documenting mission purpose and authorization; regular audits by executive officer (monthly or quarterly) reviewing all flights for policy compliance; annual public reports with comprehensive statistics (calls responded, response times, calls cleared, policy exceptions); community advisory board with quarterly meetings reviewing program operations; and legal compliance reviews by city attorney. Montgomery County's model includes Lieutenant conducting periodic audits with violations published publicly—transparency that builds trust.

Privacy protections operationalized in procedures: Camera pointed forward/horizon during transit (not downward); recording begins only at call location; no intentional recording where reasonable expectation of privacy exists; flight altitude standards (typically 200-400 feet AGL); gimbal pointed upward during return flights (Chula Vista policy adjustment responsive to community concern); technology restrictions including absolute prohibition on facial recognition, no audio recording capability, no persistent wide-area surveillance, and no data sharing without legal process.

Deliverables: Complete written policy manual (50-100 pages) covering all operations, training, privacy, data governance, and oversight; Standard Operating Procedures for pilots with pre-flight/mission/post-flight checklists; data retention policy with classification system and deletion schedules; community advisory board charter with membership selection process and meeting schedule; and memoranda of understanding with external stakeholders (hospitals for rooftop sites, FAA district office, mutual aid partners). Engage city attorney for legal review ensuring constitutional compliance and state law alignment.

Need help with policies?

IDEA Analytics provides editable templates for these documents based on industry standards for public safety policies and accreditation standards.

Step 5: Navigate FAA regulatory pathways and secure operational waivers

The 2025 regulatory breakthrough makes DFR dramatically more accessible—FAA's new **91.113 Public Safety Waiver** consolidates previous Tactical BVLOS, First Responder BVLOS, and Blanket COAs into streamlined 4-year approval with processing times of 24 hours to 2 weeks (Noblesville PD: 23 hours 47 minutes). This replaces the previous CAPS system causing months-long delays. Qualifying Public Safety Organizations meeting both PSO (49 USC 44806(e)—primarily engaging in public safety activities) and PAO (49 USC 40102(a)(41)—aircraft used only for government purposes) criteria should pursue this pathway as primary regulatory vehicle.



Dual-track regulatory approach for maximum flexibility: Immediate pilot training for Part 107 Remote Pilot Certificates (\$150 per test, 15-20 hours study time, 24-month validity requiring recurrent training) enables operations within days while 91.113 waiver application processes. Submit waiver request to 9-AVS-AFS-750-91.113Waivers@faa.gov with required documents: FAA Form 7711-2 (waiver application), Public Declaration Letter signed by senior official (Sheriff/Chief), Concept of Operations (ConOps), PAO-PSO 91 BVLOS Waiver Checklist (200ft or 400ft version depending on shielded vs DAA operations), and if using Detect and Avoid technology, the CMD-DAA worksheet.

Choose between shielded operations (200ft AGL) or non-shielded with DAA (400ft AGL)—shielded operations require no visual observers and leverage natural obstacles (buildings, trees) limiting range to 200ft above ground level or 100ft above obstacles within 100ft radius (max 400ft AGL absolute). This fastest-approval pathway suits urban DFR perfectly. Non-shielded operations require Detect and Avoid systems (electronic, acoustic, or visual observers + ADS-B In) enabling full 400ft AGL operations but demand more complex applications. Most DFR programs pursue shielded pathway first, expanding to 400ft later as needed.

Equipment compliance requirements for waiver approval: Total UA weight under 55 lbs.; ADS-B In receiver (mandatory for manned aircraft detection); anti-collision lighting visible 3 statute miles for night operations; Standard Remote ID compliance; maximum speed 87 knots (100 mph); pre-programmed Return-to-Home capability; and for routine (non-emergency) operations over people, Part 107 Category



compliance OR prop guards (under 0.88 lbs.) OR parachute recovery systems (over 0.88 lbs.). Emergency operations over people allowed with "due care" under PAO status.

Free FAA support resources: Monthly webinars via DRONERESPONDERS (second Wednesday, 4pm EST) with FAA officials answering questions; downloadable toolkit at

[faa.gov/uas/public_safety_gov/public_safety_toolkit](https://www.faa.gov/uas/public_safety_gov/public_safety_toolkit) including "Drones in Public Safety: A Guide to Starting Operations," sample Public Declaration Letter template, waiver checklists, and flow charts for pathway determination. Brandon Karr's step-by-step COA application guide through DRONERESPONDERS has supported 466+ departments achieving 100% BVLOS waiver success rate using provided templates.

Timeline expectations: Part 107 certification achievable in days-to-weeks once pilots' complete study; 91.113 waiver processing now 24 hours-2 weeks (down from previous several months); emergency COA available in 3 hours for qualifying life-safety situations; airspace authorizations via LAANC near-real-time to minutes in controlled airspace. **Budget 3-6 months for this regulatory phase** allowing time for pilot training, comprehensive ConOps development, equipment procurement and compliance verification, and waiver submission with complete documentation.

Deliverables: All pilots Part 107 certified with certificates on file; 91.113 waiver approved and filed; Concept of Operations document meeting FAA requirements; equipment compliance verification documentation (ADS-B In, Remote ID, anti-collision lights); waiver renewal tracking system (4-year cycle); and internal SOPs incorporating FAA operational requirements. Partner with consultants if internal capacity limited—their expertise accelerates approvals.

Step 6: Develop budget and identify funding sources

Realistic budget modeling prevents program collapse—Clovis PD suspended operations due to insufficient staffing budget despite equipment acquisition. Total cost of ownership includes startup investment (\$300,000-\$500,000 for single-site program) and annual operations (\$300,000-\$500,000 with staffing as largest variable). Break startup into components:

- **hardware** (complete dock system \$250,000-\$308,000, or drones without dock \$30,000-\$50,000 each),
- **software** (\$8,970-\$10,000 annually for flight operations platform with CAD integration, evidence management, cloud storage),
- **infrastructure** (high-speed internet/cellular connectivity, RF infrastructure for low-latency video),
- **training** (\$5,000-\$15,000 per pilot for comprehensive programs beyond Part 107 certification), and
- **consulting** (\$50,000-\$200,000 optional for turnkey implementation support).

Annual operating costs dominated by staffing decisions: Full-time dedicated DFR pilot at 24/7 coverage requires \$300,000-\$500,000 (largest expense line), while contracted remote pilot services at \$60/hour offer substantial savings. Alternative staffing models include distributed approach with trunk-deployed drones launched by patrol officers (Skydio X10/R10), hybrid model with strategic docks supplemented by mobile units, or part-time coverage (8–12-hour shifts targeting peak call periods). Additional annual costs: maintenance and battery replacement (every 2-3 years), software subscriptions and licenses, insurance premiums (\$500-\$5,000 annually for liability coverage \$1M-\$5M), spare equipment inventory, and ongoing training (10+ hours monthly per pilot).



If you are including your program with your communication center or real-time crime operations, consider the salary of other staff, not just drone pilots, such as analysts, camera operators, supervisors, and administrative staffing. Most small-medium sized cities operating DFR with real time crime operations estimate a \$2-3M annual

budget. Larger agencies can require \$4-5M a year.

Federal grant sources substantially offset local investment: Department of Justice Edward Byrne Memorial **JAG grants** (\$306+ million annually) previously prohibited UAS purchases (Category C) but 2025 executive order directs reclassification to Category B with **bipartisan DRONE Act of 2025** explicitly authorizing JAG and COPS funds for drone purchases and operations. Application via SF-424 and SF-LLL through [Grants.gov](https://www.justgrants.gov) then JustGrants. **DHS Homeland Security Grant Program** (\$1+ billion annually) includes State Homeland Security Program (\$415 million) and Urban Area Security Initiative targeting high-threat urban areas—apply through State Administering Agency.

State and local funding supplements federal sources: State homeland security programs, highway safety grants, emergency management funds, asset forfeiture (where legally permissible and politically acceptable), general fund budget allocation, and foundation/corporate grants. DARTdrones Public Safety Grant awarded \$500,000+ to 237+ departments for training. Community partnerships can provide rooftop sites (hospitals, tall buildings) reducing infrastructure costs. Phased implementation approach—pilot program first 6-12 months with limited coverage, then full deployment if evaluation positive—reduces initial investment and demonstrates value before major budget commitment.

ROI demonstration strengthens funding requests: Present quantitative metrics including 75%+ response time reduction (traditional 6-12 minutes vs DFR 45-90 seconds), 20-25% calls cleared without patrol dispatch (Chula Vista: 1000+ calls, freeing hundreds of officer hours), helicopter cost avoidance (\$200-\$400/hour flight time vs fraction for DFR), and 92% of programs see ROI within first year. Qualitative benefits include officer safety improvements (better threat assessment before arrival), de-escalation tool for mental health crises, enhanced investigation quality with aerial documentation, and community trust through transparency. Calculate cost per call and cost per resident showing value proposition.

Developing your impact and performance metrics requires baseline information. Be sure to have your analyst - or your data analytics consultant - develop and document repeatable data models to measure response times, capture enrichment data for population, weather, and other factors that influence flight, and have procedures for consolidating data sources for analysis. Need a model? Contact IDEA Analytics.

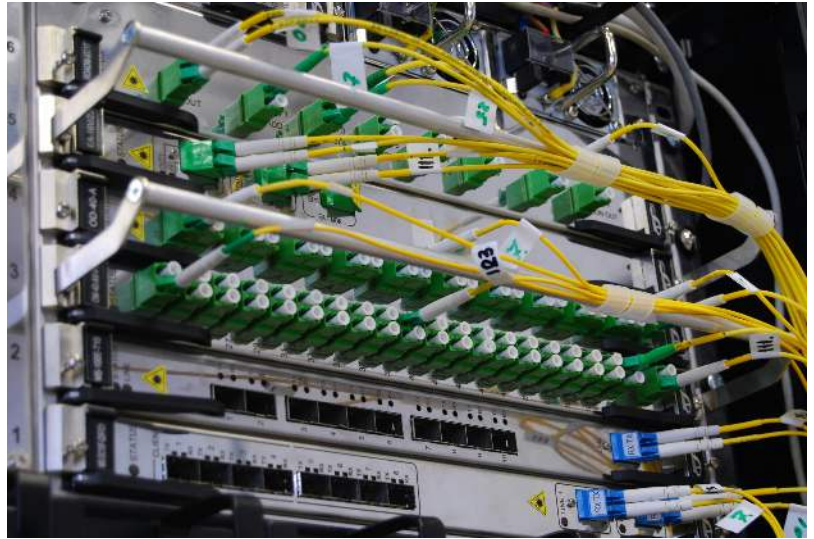
Procurement pathways for Blue UAS compliance: Defense Logistics Agency TLS, GSA schedules, direct from manufacturers (Skydio, BRINC, Freefly, Anduril, Parrot), and approved distributors. *Buy vs lease decision* based on risk tolerance—purchase provides ownership but requires spare equipment and maintenance budget, while leasing offers "insurance policy" with replacements and maintenance included spreading costs predictably. Many vendors now offer leasing to mitigate agency financial risk.

Deliverables: Comprehensive 5-year budget with startup and annual operating costs by category; grant application calendar with deadlines and requirements; completed grant narratives with operational need justification, community benefit description, and cybersecurity/privacy mitigation plans; letters of support from community stakeholders; ROI analysis with quantitative projections and qualitative benefits; and procurement plan specifying Blue UAS compliance pathway and buy/lease recommendation. Pre-draft grant narratives before application windows open—competitive programs have tight submission deadlines.

Step 7: Build operational infrastructure and integration architecture

Seamless CAD integration is non-negotiable—every successful DFR program emphasizes that drones must launch automatically upon call entry to CAD, not through manual dispatcher notification adding critical seconds. Partner with CAD vendor (Motorola, Tyler, Hexagon, Central Square) early in planning to ensure API connections enabling automatic drone tasking. Integration requirements include real-time call data push to flight operations platform (DroneSense, CAPE, Skydio DFR Command, Aerodome), automatic mission creation with GPS coordinates and call type, live video streaming to multiple endpoints (dispatch console, patrol MDCs, command post), and automatic evidence upload to management system (Axon Evidence most common).

Live911 integration described as "game-changer" by all users—this platform provides real-time access to 911 calls as they occur, allowing drone pilots to hear caller's voice describing situation while en route. Chula Vista and Montgomery County attribute significant success to this capability enabling better tactical decisions. Additional integration points: Real-Time Crime Center feeds (if existing), license plate reader systems, gunshot detection (ShotSpotter), crash detection systems, body-worn camera ecosystems, and Records Management Systems for comprehensive documentation.



Infrastructure requirements for reliable operations: High-speed internet connectivity (fiber preferred, minimum 100 Mbps upload) at dock locations, 5G/LTE cellular backup for redundancy, RF infrastructure preventing video latency (Cradlepoint or equivalent), uninterrupted power supply (UPS) for dock operations, environmental monitoring (weather stations, wind sensors), and physical security for equipment (roof access control, surveillance cameras, alarm systems). Scottsdale's integration with 5,000+ camera feeds and Flock Safety license plate readers demonstrates how DFR becomes aerial component of comprehensive public safety ecosystem.

Launch site selection balancing coverage and feasibility: Identify locations providing 3–6-mile radius covering high-call-volume areas. Ideal sites include municipal buildings (police/fire stations, city hall), hospital rooftops (Fremont's partnership with Washington Hospital Healthcare System), tall commercial buildings (Beverly Hills Business Triangle coverage), parking structures, and communication towers. Site requirements: structural capacity for dock installation (typically 200-500 lbs.), roof access for maintenance, clear airspace (minimal obstacles), electrical service (120V minimum), internet connectivity, and landlord/property owner agreements. Chula Vista operates from 5 launch sites achieving 98% coverage of 52 square miles.

Technology deployment following "crawl-walk-run" methodology: **Crawl Phase (Months 1-6)** operates Visual Line of Sight only, limited call types (high-priority emergencies), single launch location, intensive training and documentation, and weekly community updates. **Walk Phase (Months 7-12)** implements BVLOS waiver operations, expands call types based on data, adds additional launch sites, enhances technology capabilities, and provides monthly transparency reports. **Run Phase (Year 2+)** achieves full autonomous operations, 24/7 capability (if approved), multiple dock locations, advanced integrations, and regional partnerships.

Pilot training beyond Part 107 minimum: Comprehensive programs include:

- **Tier 1 Foundation** (40 hours—Part 107 prep, UAS basics, regulations, weather, airspace),
- **Tier 2 Operational** (80 hours—SOPs, flight proficiency minimum 20 hours, scenario training, emergency procedures),
- **Tier 3 Advanced** (120+ hours—BVLOS operations, night operations, tactical support, multi-drone coordination, instructor qualifications), and
- **Ongoing monthly training** (5-10 hours monthly flight time plus quarterly regulatory updates), like other specialty teams in public safety.

DRONERESPONDERS Position Task Books provide standardized training documentation. Los Angeles Regional Training Center and partnerships with Pilot Institute, Flying Lion, Regional Training Center offer comprehensive public safety-specific curricula.

See IDEA's DFR Program for Public Safety Resource Document for more information and training sources.

Deliverables: CAD integration technical specifications and API documentation; launch site agreements and memoranda of understanding; infrastructure installation plan with timeline and contractors; pilot training curriculum with completion requirements; Standard Operating Procedures covering pre-flight inspections (weather, airspace, equipment), mission operations (launch, flight, landing, emergency procedures), and post-flight documentation (flight logs, evidence upload, maintenance checks); and integration testing results demonstrating end-to-end functionality from 911 call through drone launch to evidence storage. Budget *6-12 months for implementation phase* including infrastructure installation, pilot training, and integration testing.



Step 8: Execute comprehensive community transparency and launch strategy

Transparency portal operational before first flight—Montgomery County and Scottsdale launched with public flight tracking from day one, preventing suspicion that undermines programs lacking immediate transparency. Minimum portal features: interactive map showing all flight paths, date/time of each flight, call for service event number, brief mission description (respect operational security—general category not specific address for active calls), filtering by date range and call type, and statistics dashboard (total flights, response times, calls cleared, policy compliance). DroneSense offers turnkey public dashboards; custom development using flight log APIs alternative approach.

Launch event building community support through demonstration: Press conference with live drone demonstration (Scottsdale's "overwhelmingly positive" response), elected official participation (Mayor/Council member remarks), community open house with hands-on displays, media ride-alongs during first operational shifts, social media campaign with educational videos (#OurSkyOurSafety successful hashtag), school visits explaining technology to youth, and transparency pledge prominently featured. Chula Vista's parachute safety demonstration addressed community concerns about crashes—visible responsiveness to feedback.



Ongoing transparency mechanisms sustaining trust: Quarterly reports to governing body (council, board of supervisors) with comprehensive statistics, annual public report available on website, community advisory board quarterly meetings open to public, complaint procedure clearly published and investigations documented, policy compliance audits with results published (including violations and corrective actions), social media updates highlighting successful deployments (protecting privacy), and media access policy enabling journalists to observe operations. Montgomery County's 2024 National Association of Counties Achievement Award recognized exemplary transparency approach.

Managing opposition constructively: Acknowledge concerns as valid and reasonable, never dismiss privacy advocates as obstructionist; point to specific policy language addressing each concern; demonstrate responsiveness by accepting reasonable modifications; offer adversaries seats on community advisory board (convert critics to oversight participants); publish data addressing factual inaccuracies; and maintain respectful dialogue even with persistent opponents. *Leaders of Beautiful Struggle v. Baltimore Police* (4th Cir 2021) demonstrates courts will scrutinize programs lacking transparency and oversight—proactive community engagement prevents legal challenges.

Handling critical incidents transparently: When crashes occur (inevitable over thousands of flights), immediate public disclosure with incident report, investigation findings, and corrective actions taken. When privacy complaints arise, investigate promptly, publish findings (protecting complainant identity if requested), and implement policy adjustments if warranted. When policy violations occur, discipline transparently (general description, not personnel details), document corrective training, and update procedures preventing recurrence. This transparency builds trust that opaque responses destroy.

Operational launch following phased approach: Consider weekly phases with key metrics for each, such as:

- Week 1 soft launch with limited operations (8am-8pm, high-priority calls only), media embedded documenting first responses.
- Week 2-4 expand hours, or adjusting on demand of high priority calls, gradually based on staffing and training readiness.

Share your weekly statistics, impacts, successes with the media. As your program continues, expand call types based on pilot proficiency and community acceptance. Be sure to measure impacts and ensure the expansion of calls continues to show returns to your program goals. All going well, your months 5+ should reach full operational capability defined in policies. Be sure to collect community feedback continuously through surveys, advisory board, public comment mechanisms, and direct outreach to initial skeptics documenting concerns and how addressed.

Deliverables: Public transparency portal operational and tested; launch event plan with media contact list and logistics; social media content calendar (first 90 days); community advisory board inaugural meeting scheduled; complaints procedure published on website; quarterly reporting template aligned with metrics collection; media policy and spokesperson training; and incident response protocols for crashes, privacy complaints, and policy violations. Launch represents beginning of community relationship, not conclusion of engagement process.

Step 9: Implement risk management and compliance framework

Privacy Impact Assessment

(PIA) before operations begin—

federal framework based on Fair

Information Practice Principles

(FIPPs) requires program

description and legal authority;

information collected and

sources; uses of information;

retention and disposal; access

controls; security safeguards;

privacy risks and mitigation; oversight and accountability; and public notice and transparency. EASA's

Privacy by Design framework emphasizes proactive not reactive measures, privacy as default setting,

privacy embedded in design (not add-on), full functionality (no zero-sum tradeoffs), end-to-end security,

visibility and transparency, and respect for user privacy.



Data governance protecting constitutional rights: Fourth Amendment compliance ensuring warrant

requirement when UA will intrude on reasonable privacy expectations and collect evidence; **First**

Amendment protection prohibiting surveillance of protests, religious gatherings, political events absent

immediate safety threat with advance notice to organizers; **Equal Protection** preventing discriminatory

deployment patterns (monitor calls responded by neighborhood, publish equity analysis showing all

communities served); state constitutional provisions often providing stronger protections than federal

(California, Hawaii, Vermont, Alaska particularly strong).

State-level regulatory compliance varying significantly: 24 states enacted privacy-specific UAS legislation.

Warrant requirement states include Florida (§934.50), Texas (Ch. 423), Illinois (725 ILCS 167), North Dakota, Minnesota, Missouri, Virginia, Nevada, and Maine with emergency exceptions (imminent danger to



life, terrorism, missing persons, disaster response, crime scene documentation within 48 hours). **Critical infrastructure restrictions** in 22 states prohibiting operations near prisons, 10 states restricting near critical facilities. Research state-specific requirements using NCSL UAS Legislation Database before finalizing policies.

Cybersecurity protocols preventing compromise: CISA best practices framework includes secure-by-design procurement (Blue UAS Framework compliance), zero trust architecture (verify every connection), network isolation (separate UAS systems from general IT), data protection (encryption at rest and in transit, US-based servers not manufacturer cloud storage), supply chain security (avoiding covered country components under NDAA), vulnerability management (regular updates, security audits), and incident response plans (breach notification procedures, evidence preservation). Chinese UAS risks include backdoor access, data exfiltration, remote shutdown capabilities, and location tracking—Blue UAS compliance mitigates these threats.

Safety protocols minimizing operational risks: Pre-flight checks include weather briefing (wind, precipitation, visibility, temperature), airspace clearance (NOTAM review, TFR verification, LAANC authorization if controlled airspace), equipment inspection (battery charge, propeller condition, camera function, anti-collision lights, obstacle sensors), mission brief (call type, coordinates, hazards, special considerations), and backup plan (alternate landing sites, lost link procedures). **Emergency procedures** for lost link (immediate Return-to-Home activation, ATC notification if in controlled airspace, ground unit coordination), flyaway (alert FAA, activate tracking, recovery procedures), crashes (treat as suspicious package, secure perimeter, investigation, FAA notification within 10 days of \$500+ damage), and battery fires (Class D fire extinguisher, evacuation protocols).

Insurance and liability coverage protecting agency: Required coverage types include liability (\$1M-\$5M limits typical, Minnesota only state mandating insurance), hull coverage (8-12% of value for damage/loss), payload coverage (cameras/sensors), cyber liability (data breach protection), and workers compensation enhancement (pilot injuries). Typical costs: \$500-\$5,000 annually for liability depending on limits and program size; \$7-\$15/hour for on-demand coverage. [SkyWatch.ai](https://www.skywatch.ai) and aviation insurance providers offer public safety-specific policies. Indemnification in vendor contracts and interagency mutual aid agreements clarifying liability allocation.

Legal risk mitigation strategies: Voluntary warrant adoption even when not legally required (builds trust, establishes pattern of constitutional compliance); privacy by design implementation (technical and policy measures restricting data collection to mission-essential); detailed documentation of all flights (justification, authorization, outcome); regular constitutional compliance reviews by city attorney; insurance coverage adequate for worst-case scenarios; qualified immunity protection through clearly established policies and training; and partnership with civil liberties organizations preventing adversarial legal challenges.

Deliverables: Completed Privacy Impact Assessment document; cybersecurity protocols and technical architecture diagram; safety management system with all emergency procedures documented; insurance certificates with adequate coverage verified; data governance policy template with classification and retention schedules; constitutional compliance review memo from legal counsel; and incident response plan covering crashes, data breaches, privacy complaints, and legal challenges. Annual compliance audit reviews all areas identifying gaps and corrective actions.

Step 10: Establish post-implementation monitoring, evaluation, and evolution framework



Performance metrics collection
from **flight one**—robust
evaluation framework enables
continuous improvement and
justifies program expansion.

Operational effectiveness metrics include number of calls responded by type, average response time (drone vs ground units), percentage arriving

before ground units (targeting 70-75% benchmark), calls cleared without officer dispatch (targeting 20-25%), arrest/conviction support from drone footage, search and rescue successes, de-escalation incidents (force avoided due to aerial intelligence), tactical support effectiveness (SWAT, barricaded subjects), and disaster response deployments.

Resource efficiency metrics demonstrating ROI: Officer hours saved (cleared calls × average on-scene time), patrol unit reallocation to higher priorities, cost per flight vs manned aviation (helicopter \$200-\$400/hour comparison), overtime reduction from efficient deployment, and equipment utilization rate (flights per day, coverage hours). Chula Vista data showing 1000+ calls cleared without patrol dispatch translates to thousands of officer hours saved for community policing, investigations, training—quantifiable value beyond response time improvements.

Community impact and trust metrics: Public records requests (volume and type indicating community scrutiny level), community complaints investigated and findings, survey results measuring satisfaction/concerns (conduct annually), media coverage sentiment analysis, advisory board recommendations and implementation rate, transparency portal engagement statistics (visits, searches, geographic distribution), and demographic analysis ensuring equitable service (all neighborhoods benefit proportionally to need). Montgomery County's systematic publication of violation investigations (disciplinary actions, corrective training) demonstrates accountability maintaining trust.



Policy compliance and safety metrics: Flights by call type verifying adherence to use restrictions, policy exceptions/violations documented with corrective actions, audit findings and remediation, training completion rates and proficiency testing, incidents (crashes, near-misses, equipment failures), maintenance records and downtime, and FAA compliance (waiver conditions, altitude violations, airspace infractions). Zero-tolerance approach to policy violations signals seriousness preventing mission creep that destroys community trust.

Quarterly reporting to governing body required—brief presentations (15 minutes) to council/board covering key metrics, significant incidents and how handled, policy adjustments and rationale, budget status and variance explanations, community feedback themes, and upcoming plans (expansion, technology upgrades, training enhancements). This regular cadence maintains political support, demonstrates accountability, enables mid-course corrections, and builds institutional knowledge as elected officials turn over.

Annual comprehensive program evaluation: Detailed report (20-30 pages) publicly available covering



program overview and objectives, complete metrics analysis vs targets, cost-benefit analysis with ROI calculation, community engagement summary and feedback themes, policy compliance and violations, significant incidents and lessons learned, comparison to peer programs (benchmarking), and recommendations for improvements.

External evaluation by academic researcher or consultant every 2-3 years provides independent assessment and credibility—Montgomery County's outside review strengthened program legitimacy.

Program evolution based on data and technology advancement: Technology refresh cycle (3-5 years) as platforms advance—current trend toward full automation eliminating rooftop pilots (largest cost reduction opportunity), detect-and-avoid systems enabling operations without visual observers, AI-powered flight path optimization, and longer endurance platforms. Geographic expansion using data showing coverage gaps and call volumes—add dock locations strategically where response times exceed targets. Capability expansion carefully with community approval—advanced sensors (higher zoom, improved thermal), indoor drones for building searches, fixed-wing platforms for extended range, but never facial recognition or weaponization absent extraordinary circumstances with full democratic debate.

Regional partnerships and mutual aid expanding value: Multi-jurisdiction programs sharing costs and resources (Murrieta exploring shared services), county-wide systems serving multiple municipalities, state/regional training centers sharing expertise, equipment sharing for disasters or major incidents, standardized policies enabling seamless mutual aid, and joint procurement reducing per-agency costs. Campbell, CA's first 24/7 BVLOS waiver without visual observer using radar detection demonstrates emerging capabilities—watch FAA regulatory evolution for opportunities.



Continuous improvement culture: Monthly pilot debriefs collecting lessons learned and improvement suggestions, technology working group evaluating vendor innovations, policy review committee meeting quarterly assessing need for updates, community advisory board as feedback mechanism, conference attendance sharing lessons with peers (AUVSI Xponential, DRONERESPONDERS Summit, IACP conference), and research participation with academic institutions advancing field knowledge. Success requires viewing



DFR as evolving capability, not static program—embrace continuous learning.

Program sustainability requires: Stable funding (multi-year budget commitments, grant diversification preventing single-source dependence), organizational resilience (succession planning for key personnel, documentation preventing knowledge loss), political support (regular council briefings, constituent service highlighting program value), community trust (sustained transparency, responsiveness to concerns), and operational excellence (training investments, equipment maintenance, safety culture). Programs surviving leadership changes and budget pressures share these characteristics.

Expansion decision framework: Minimum 12-18 months operational before major expansion proposals, demonstrated success in all metrics (operational, efficiency, community, compliance), community support documented through surveys and advisory board, additional funding secured (not diverting from proven program), regulatory approvals obtained for expanded operations, and clear operational need (coverage gaps, call volume growth, new use cases). Scottsdale's plan for 4-5 total sites represents methodical expansion based on first-site success—avoid premature scaling that dilutes effectiveness.

Deliverables: Performance metrics dashboard updated daily and reviewed weekly by program manager; quarterly council presentation materials; annual comprehensive evaluation report; policy review schedule with documented assessments; technology evaluation process tracking innovations; mutual aid agreements with partner agencies; succession plan for key personnel; five-year strategic plan with expansion roadmap; and continuous improvement process documented with lessons learned database. Evaluation drives decisions, preventing reactive changes based on single incidents or political pressure—data grounds program in demonstrated value.

Critical Success Factors Synthesis

The universal pattern across all successful DFR programs: Community engagement before equipment purchase (12+ months), clear written policies before operations (use restrictions, data retention, oversight), transparency from day one (public portal, flight logs, statistics), restrictive use parameters (emergency 911 calls only, no proactive patrol), strong executive leadership maintaining commitment through challenges, dedicated professional pilots (not collateral duty), seamless CAD integration (seconds matter in launch times), systematic metrics collection proving value, and continuous responsiveness to

community concerns
demonstrating trustworthiness.

Timeline expectations for concept to operational: Research and planning (3-6 months), community engagement (6-12 months concurrent), regulatory approvals (1-3 months with 2025 streamlined process),

infrastructure implementation (3-6 months), pilot program (6-12 months optional but recommended), evaluation and full deployment decision (1-2 months), totaling **18-36 months from initial concept to full operational capability**. Attempts to compress this timeline risk program failure—Seattle 2013, Clovis suspension—while methodical implementation produces sustainable programs.



Budget realism preventing collapse: Startup \$300,000-\$500,000 per site (equipment, infrastructure, training, consulting), annual operations \$300,000-\$500,000 (staffing dominates), five-year total cost of ownership \$1.8M-\$3.0M requiring *multi-year funding commitment* not single-year allocation. Federal grants offset 30-70% of startup (JAG, HSGP, state programs), but sustainable operations require local budget commitment. Programs without stable funding fail regardless of technology quality.

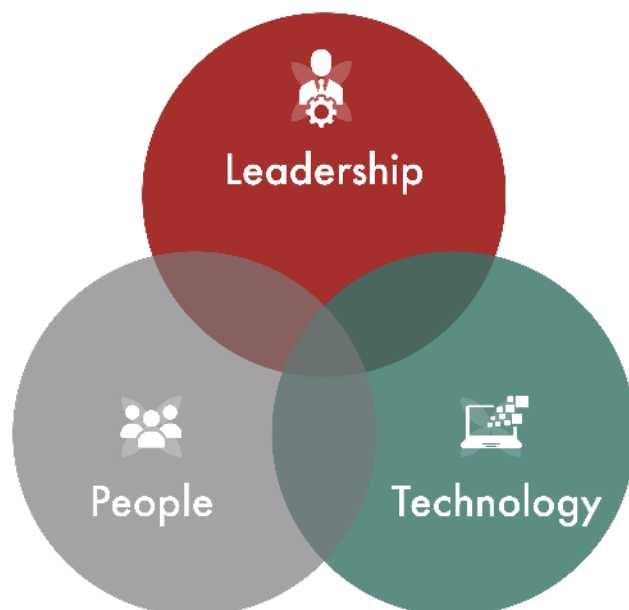
The trust equation determining survival: Even perfect technology fails without community support. Montgomery County, Chula Vista, Scottsdale are successful programs because they invested equally in community relationships as technical capabilities. Their open-door policies for peer agencies, freely shared lessons learned, and transparent acknowledgment of challenges advance the field—learn from their successes and their mistakes.

Technical Capability × Community Trust = Program Success

About IDEA Analytics

At IDEA Analytics, we've revolutionized our Digital Transformation & Analytical Capacity (DTAC)[™] program with targeted implementation solutions designed specifically for organizations facing resource constraints and data and technology bottlenecks.

Our national footprint across 36 states and over 100 projects spanning all four U.S. regions has revealed a consistent truth: technology implementation succeeds only when aligned with leadership vision and people capabilities. That's why our solutions bridge the critical gaps between your technology investments and the people who power them.



Our Services

We provide virtual and in-persons advising, workshops, and technical assistance services to support digital transformation projects for data-driven organizations. We believe that strategy and change management practices ensure success by minimizing waste (e.g., time, financial) and aligning the complexities of the workforce in evidence-based frameworks.

Join agencies across the nation who have partnered with IDEA Analytics to align their leadership vision, people resources, and technology infrastructure. When these three pillars work in harmony, organizations achieve what matters most – actionable data available to inform decision-making to serve your community and customers.

Organizational Assessment & Strategy Services

- Digital Readiness Assessment for Enterprise Organizations
- Data Governance Strategy Development

People-Centric Analytics Consulting

- Analytics Talent Acquisition Strategy
- Analytical Team Performance Optimization
- Executive Analytics Coaching

Change Management & Implementation Services

- Agile Analytics Implementation
- Data-Driven Culture Transformation

Specialized Advisory Services

- Analytical Capacity Building for Regulated Industries
- Real Time Operations Advising
- Technology Integration Strategy
- Multi-Jurisdictional Data Collaboration Design

Contact IDEA Today to learn more about how our Digital Transformation Advising can advance your program goals.

An aerial photograph of a city street, showing buildings, rooftops, and a street with a car. A semi-transparent white rectangular box is overlaid on the center of the image, containing text. The text is in a black, sans-serif font and is centered within the box. The background image shows a street with a car, buildings, and a street sign that says "MINI-BUS".

In "10-Steps to Successful DFR Program" readers will navigate the complexities of drone program implementation in public safety, balancing efficiency with civil liberties. This essential guide outlines a strategic framework for establishing transparent, community-oriented operational practices, ensuring compliance and trust from inception to execution. With practical steps and insights from successful case studies, this book empowers new adopters to avoid common pitfalls and build effective, sustainable drone initiatives.