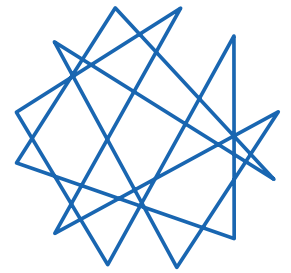


gisf



Drone guidance: 'Operating safely' principles

GISF Research Paper



Contents

1. Re-think Your Risk Assessments	03
2. Implement good governance	03
3. Improve situational awareness	04
4. Reassess movement logic	04
5. Ensure coordination and deconfliction	05
6. Manage visibility, markings & messaging	06
7. Implement operational discipline & training	06
8. Consider contingency & medical preparedness	07
9. Manage digital and data security	07
10. Implement low-cost detection & physical measures	08



How do we plan, move, and operate when drones are part of the threat environment?

Purpose

This guidance sets out core principles to support decision-making in environments where drones shape risk, visibility, and access. It is not prescriptive or tactical; rather, it provides a framework to help NGOs interpret risk and adapt operations in a context where surveillance, ambiguity, and rapid escalation are persistent features.

It focuses on the high-level planning and operational measures intended to reduce exposure, improve decision-making and situational awareness, strengthen coordination and deconfliction, manage visibility and markings in context, improve operational discipline and training, and ensure contingency and medical preparedness. More detailed operational measures and context-specific mitigation options are provided separately in annexes and should be applied based on local risk assessments.

Audience

NGO staff managing and mitigating drone-related risks (including those planning movements, managing sites, overseeing staff safety arrangements, and coordinating with relevant actors)

Introduction

Once organisations understand the types of drones present, the tactics used, and the logic of targeting, they can more accurately anticipate how, when and why drones may threaten their staff, assets or communities. Clear situational awareness enables stronger decision-making, from route planning and site layout to communication with armed actors and communities. The following risk management principles can help organisations to reduce exposure, respond faster to threats, and maintain access in environments where drones shape the operational landscape. (Specific tools, such as risk assessment templates, can be found in the annexes, which will enable translation of the principles into operational measures).



Note: this framework is intended to support judgment, not replace it. Drone-affected environments are fluid, and no single approach will apply across contexts.

1. Re-think Your Risk Assessments



Principle: risk is continuous, perception-driven, and multi-actor

- Move beyond event-based risk models (e.g. checkpoints, incidents) toward continuous risk assessment.
- Consider not only what you are doing, but how it may be observed and interpreted.
- Map:
 - Who has drone capability (state, non-state, unknown actors)
 - What types of drone use are present (surveillance, strike, testing, opportunistic)
- Assess exposure across:
 - Locations (fixed sites)
 - Movements (routes, timings)
 - Patterns (routine behaviours)
- Identify vulnerabilities: single-point dependencies (one bridge, one road), predictable schedules, clustering of assets, and critical cargo/loads.
- Plan for uncertainty and misinterpretation, not just known threats.

2. Implement good governance



Principle: Decision-making should be clear, consistent, and anchored in humanitarian principles under conditions of uncertainty.

- Define authority and scope: Identify who at HQ, regional, and country level is responsible for approving drone-related SOPs, operational decisions, and any deviations from standard procedures.
- Clarify decision-making lines: Ensure roles and responsibilities are clearly understood across field and management levels, particularly in time-sensitive or high-risk situations.
- Risk appetite: Establish organisational thresholds for:
 - Continuing operations
 - Suspending activities
 - Relocating or evacuating staff in response to elevated or changing drone threats
- Principle-based decision-making: Reaffirm that humanitarian principles (neutrality, impartiality, and independence) and the commitment to “do no harm” remain the primary criteria guiding decisions related to movement, visibility, and any use of drone technology.
- Consistency vs flexibility: Balance the need for standardised approaches with the ability to adapt to rapidly changing local conditions.
- Documentation and accountability: Ensure that key decisions, especially those involving elevated risk, are documented and can be reviewed, supporting organisational learning and accountability.



Tool: Security Decision-making matrix for national NGOs

3. Improve situational awareness



Principle: Situational awareness is built through layered human insight, not just technical inputs.

- Maintain an up-to-date operational picture: Draw on a combination of sources.
 - No single source should be treated as definitive; value lies in triangulation
- Prioritise interpretation, not just collection: Focus on how information is understood and contextualised:
 - What patterns are emerging?
 - What has changed recently?
 - What remains unclear or contested?
 - Ensure teams are not only receiving information, but actively assessing its implications.
- Establish simple, reliable reporting flows: Use consistent check-ins and basic reporting protocols (e.g. for convoy status, movement milestones, or delays) to:
 - Maintain a shared understanding across field and coordination levels
 - Enable timely decision-making when conditions change.
 - Systems should be simple enough to function under stress or disruption.
 - Ensure that situational awareness is shared across field teams, coordination staff and senior decision-makers.
 - Avoid siloed information that leads to inconsistent risk perceptions
- Synchronise air and ground awareness where relevant: If using aerial assets for mapping or assessment, ensure alignment with ground activities to:
 - Avoid confusion or misinterpretation
 - Prevent overlapping signals that could increase exposure
 - Awareness should include not only “what we are doing” but “how it may appear”
- Acknowledge uncertainty and gaps: Recognise that:
 - Drone activity may not always be visible or attributable
 - Information may be delayed, partial, or inaccurate
 - Decision-making should explicitly account for these limitations

4. Reassess movement logic



Principle: Movement is exposure, not just transit.

- Treat movement as a high-visibility activity, not a neutral one. Consider:
 - Why movement is necessary
 - What it signals when observed
 - How it may be interpreted (logistics, coordination, targeting relevance)
- Reassess assumptions that:
 - Movement reduces risk compared to fixed locations
 - Convoys inherently increase safety
- Balance:
 - Efficiency vs exposure
 - Scale vs discretion
- Introduce variability where feasible, while balancing operational needs.

5. Ensure coordination and deconfliction



Principle: Information about you may be shared and acted upon by others.

- Recognise that drones may be operated by:
 - States
 - Non-state armed actors
 - Unknown or overlapping actors
- Where possible:
 - Maintain dialogue with relevant authorities and stakeholders
 - Clarify humanitarian presence and intent
- Understand that coordination:
 - May reduce risk with some actors
 - May increase visibility to others
- Clarify internally:
 - What information is shared
 - With whom
 - For what purpose
- Avoid assumptions that:
 - Deconfliction guarantees protection
 - All actors respect humanitarian status
- Ensure consistency of engagement:
 - Avoid fragmented or contradictory messaging
- Understand limitations:
 - Not all actors can be engaged
 - Deconfliction does not guarantee protection
 - Information shared for coordination may circulate beyond intended actors
- Avoid over-reliance on coordination as a sole risk mitigation strategy

6. Manage visibility, markings & messaging



Principle: Visibility is contextual, not inherently protective

- Reassess the assumption that visibility equals safety. Marking a vehicle can reduce the risk of a drone strike, but only in some contexts, and in others it may offer no protection or even increase risk. The impact depends entirely on who the actors are, their capabilities, and whether they respect humanitarian distinction.
- Visibility can:
 - Signal neutrality and legitimacy
 - OR create exposure and targeting relevance
- Decisions on marking (logos, vehicles, compounds) should be:
 - Context-specific
 - Regularly reviewed
- Balance:
 - Being recognised vs being detectable and trackable
 - Recognise that visibility without understanding does not generate trust



Tool: Visibility decision-making

7. Implement operational discipline & training



Principle: Information is part of the risk environment

- Treat operational data as potentially sensitive:
 - Locations
 - Movements
 - Schedules
 - Program details
- Limit unnecessary sharing of:
 - Real-time movement information
 - Detailed operational patterns
- Ensure internal discipline on:
 - Communications
 - Digital storage and transmission
- Recognise that data can be:
 - Intercepted
 - Reinterpreted
 - Used by unintended actors

8. Consider contingency & medical preparedness



Principle: Reduced warning time requires increased readiness.

- Plan for compressed timelines: Assume limited warning before incidents and reduced time to react or coordinate responses.
- Account for unpredictability: Recognise that incidents may be difficult to anticipate, including indirect or incidental exposure rather than deliberate targeting.
- Ensure immediate response capacity at field level: Field teams should be able to act without reliance on remote decision-making. Critical first-response capabilities should be locally available.
- Develop clear and adaptable contingency plans: Cover both movement-related and site-based scenarios, and avoid overly rigid plans that depend on specific assumptions.
- Prepare for access constraints: Anticipate delays in medical evacuation or external support. Avoid reliance on one evacuation route, facility, or coordination channel
- Strengthen communication continuity: Ensure teams can maintain basic communication during disruption.
- Regularly review and test preparedness:
 - Reassess readiness as the operating environment evolves
 - Incorporate lessons from incidents, near-misses, or changes in drone activity
- Consider cumulative and secondary impacts: Repeated exposure to drone activity may affect team performance and stress levels.

9. Manage digital and data security



Principle: how information is collected, stored, and shared can create or reduce exposure, as data may be accessed, aggregated, or reinterpreted by unintended actors.

- Treat data as a potential source of exposure: Assume that operational information (locations, movements, schedules, contacts) could be accessed, combined with other data, or used out of context.
- Limit collection to what is necessary: Avoid gathering or retaining detailed information that does not directly support operational needs. Balance information sharing with protection, so that efforts to coordinate, report, or demonstrate transparency do not unintentionally increase risk to staff, operations, or communities.
- Control access and sharing: Ensure that sensitive information is shared only with those who require it, and that internal distribution is proportionate to risk
- Be aware of aggregation risks: Recognise that small, seemingly harmless data points can be combined over time to reveal patterns of activity.
- Know which of your devices are passive, and which emit frequencies. For example, clusters of mobile phones, particularly of foreign origin, can initiate targeting.
- Align digital and operational practices: Ensure consistency between what is done on the ground and what is communicated or stored digitally, recognising the interplay between physical and digital security risks.

- Account for secondary use and reinterpretation:
 - Consider how data may be understood differently by external actors, including being misinterpreted as intelligence or operational coordination.
- Regularly review data practices: Adapt data handling approaches as the risk environment changes, particularly in contexts with increased surveillance or monitoring.

10. Implement low-cost detection & physical measures



Principle: Detection improves awareness, not control; and low-cost measures offer partial mitigation, not protection.

- Position detection as “awareness,” not control: emphasise limits of detection being often partial, delayed, or uncertain.
- Focus on: recognising indicators (sound, behaviour, patterns) and building shared awareness, not technical tracking.
- Adopt a layered awareness approach, combining human observation (staff, communities) with situational reporting (networks, coordination)
- Reinforce that no single detection method is reliable.
- Acknowledge time and reaction constraints: warning times may be minimal, so responses need to be simple, and pre-planned.
- Recognise trade-offs and limitations: Avoid implying that detection equates to safety. Highlight any false confidence risks.
- Frame any physical environment measures as risk reduction, not “hardening.” Consider:
 - Exposure of points (vehicles, queues, compounds)
 - Use of space (open vs covered areas)
 - Focus on reducing concentration and visibility of people/assets

gisf



Global Interagency Security Forum

GISF Research and Programmes

T: +44 (0)20 7274 5032

E: research@gisf.ngo

www.gisf.ngo