Risk control

Drones and Unmanned Aerial Vehicles

In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

Risk Management Partners
rmpartners.co.uk

Drones and Unmanned Aerial Vehicles

Introduction

Unmanned Aerial Vehicles (UAVs), commonly known as drones, are increasingly deployed by organisations for infrastructure monitoring, risk management, data capture, and operational support. Their affordability, flexibility, and capability for remote access have made them valuable assets across estates, compliance, logistics, and planning functions. However, UAV usage brings legal, regulatory, and reputational responsibilities. This guidance document supports policy managers, compliance officers, and insurance leads in governing UAV deployment lawfully, securely, and effectively.

Regulatory Framework

UAVs are regulated by the Civil Aviation Authority (CAA) under the Air Navigation Order 2016 and retained EU Regulation 2019/947. Guidance is formalised through the CAP 722 series, which defines operational permissions based on risk, not commercial intent[1].

Historically, organisations needed a Permission for Aerial Work (PfAW) to operate drones commercially. This requirement has now been replaced with a more risk-based approach:

- **Open Category** flights are low risk and do not require authorisation. Operations must remain within strict parameters, including visual line of sight, distance from uninvolved persons, and weight limits. These may be conducted for organisational purposes, even without CAA authorisation.
- **Specific Category** operations carry moderate risk (e.g. urban flights, near people, or beyond visual line of sight). These require an Operational Authorisation issued by the CAA. Organisations must submit a Specific Operations Risk Assessment (SORA), demonstrate pilot competency (typically through the General Visual Line of Sight Certificate – GVC), and maintain an Operations Manual describing flight procedures and controls.
- **Certified Category** applies to complex, high-risk operations involving heavy UAVs, autonomous flights, or integration with managed airspace. These require full airworthiness certification, remote pilot licensing equivalent to manned aviation standards, and compliance with international aviation protocols.

Authorisation requirements are determined by risk profile, not whether the activity is commercial or recreational.

Permissions, Governance, and Airspace Access

All remote pilots and operators must be registered with the Civil Aviation Authority through the Drone Registration Portal, where they obtain both a Flyer ID and Operator ID[2]. Where Specific or Certified Category permissions apply, authorisation must be obtained and documented in advance. Internally, policies should require estate or facilities teams to approve all take-off and landing areas. Geofencing, virtual flight boundaries, and automated return-to-home protocols should be embedded in operational controls. Clearly defined zones and permissions must be communicated across relevant teams and services to prevent unauthorised activity.

Competency and Pilot Qualifications

Pilot qualifications must be specified in policy and aligned with operational category. Open Category operations typically require an A2 Certificate of Competency[3]. Specific Category flights demand a GVC, assessed through written and practical tests. Certified operations may require licensed aviation qualifications. Organisations must maintain centralised training records, pilot certifications, and renewal logs, ensuring all personnel engaged in UAV operations remain demonstrably competent.

Operational Governance Risks

Deploying UAVs introduces strategic governance risks. Drones used near sensitive infrastructure, public events, or controlled airspace can cause safety and reputational harm. The 2018 Gatwick Airport incident demonstrated the widespread operational disruption possible from unauthorised UAV use[4]. Internally, fragmented oversight across departments may result in inconsistent practices, poor documentation, and increased exposure to legal liabilities. Organisations must embed UAV governance into risk registers, define roles and authorisation pathways, and ensure training and operational consistency across all users.

Risk Assessment Framework

UAVs qualify as work equipment under the Provision and Use of Work Equipment Regulations 1998 (PUWER), requiring that equipment is suitable, safe, and properly maintained[5]. Each flight must be preceded by a documented risk assessment. These assessments should evaluate pilot competency, flight location, environmental conditions, equipment status, and potential interaction with people or assets. Specific Category operations must follow the SORA framework, incorporating both ground and airspace risk analysis[6]. Risk mitigation plans—such as flight observers,

altitude limits, and emergency procedures—must be implemented and recorded within existing organisational safety systems.

Insurance Requirements

Organisations operating UAVs for professional or commercial purposes must comply with EC Regulation No 785/2004, which mandates aviation-grade insurance coverage. This includes third-party liability for injury or property damage, and may extend to payload, equipment, business interruption, and cyber liability depending on use case.

Although drones under 20 kg may be exempt when used recreationally, organisational use—even at small scale—requires compliance. For UAVs with a Maximum Take-Off Mass (MTOM) up to 500 kg, the minimum insurance requirement is 750,000 Special Drawing Rights (SDRs) (approximately £770,000), subject to annual review of currency exchange rates.

Example: An organisation uses a drone with a MTOM less than 1kg for inspection of roof assets. Despite its small size and low flight altitude, the activity qualifies as professional use. As such, the organisation must register the UAV and pilot, secure the appropriate pilot certification, and hold liability insurance in line with EC 785/2004[7].

Data Protection and Privacy Considerations

Where UAV operations involve image or data capture that could identify individuals, UK GDPR obligations apply. Organisations must assess lawful bases for data collection, avoid unnecessary surveillance, and apply retention, access, and security protocols. Written consent may be required, and privacy by design principles should guide flight planning. Internal policy should reference the Information Commissioner's CCTV Code of Practice, and UAV surveillance activities must be integrated into broader information governance frameworks[8].

Disaster Recovery and Technical Faults

Drone operations are vulnerable to hardware failures, signal loss, and adverse weather. Organisational protocols must account for safe landings, data protection during device loss, and rapid recovery of assets. Devices should use geo-tagging, encryption, and remote locking to prevent misuse or unauthorised data access. Staff must know how to respond to UAV incidents, and policies should require regular simulation exercises. These protocols should complement existing business continuity and incident response plans.

Prosecutions and Enforcement Cases

Failure to comply with UAV regulations can result in enforcement by the CAA and law enforcement agencies. Breaches may lead to fines, seizure of equipment, or criminal prosecution. Past enforcement cases have involved drones flown near airports, over government facilities, and in areas with public gatherings. Organisational exposure increases if oversight and documentation are lacking. Policy managers must ensure that flight records, pilot credentials, and authorisation documents are available and internally audited[9].

UAV Classification by Size and Operational Implications

- **Small UAVs (<25 kg)**: Commonly used for visual inspection and survey work. Operate under Open or Specific Category. Professional use requires pilot certification and compliant insurance coverage[7].
- **Medium UAVs (25–150 kg)**: Typically used in logistics, corridor mapping, and advanced inspection. Require formal authorisation, advanced pilot qualifications, and tailored insurance packages[6].
- **Large UAVs (>150 kg)**: Employed in autonomous transport, tactical operations, or integration with national airspace systems. Require full certification, aviation licensing, and comprehensive insurance[10].

Procurement and operational policies must reflect UAV classification to determine authorisation, risk controls, and training standards.

Growing Use and Applications

Across sectors, UAVs are being deployed to inspect roof assets, map development sites, monitor traffic, assess coastal change, and improve access to remote or hazardous locations. Emergency services use drones for rescue operations and post-incident assessment. Logistics firms trial autonomous aerial delivery. Estates and planning teams employ drones for energy audits, drainage surveys, and asset recording. These diverse applications reflect the need for integrated governance that accounts for both innovation and operational risk[11].

Additional Considerations

UAVs present cybersecurity risks due to remote access, telemetry exposure, and GPS spoofing. Encryption, secure control protocols, and remote lockout must be policy requirements. Environmental impacts, including noise disruption and wildlife interference, should be considered in flight planning and site selection. Policies must also embed

accessibility and inclusion, ensuring training programmes are suitable for neurodivergent staff and that operating roles are clearly structured, supported, and safe.

Summary and Recommendations

Organisations adopting UAVs must establish centralised and auditable governance frameworks. This includes registration of operators and equipment, pre-flight risk assessment, authorisation tracking, compliant insurance cover, and lawful data management. Operational controls must reflect CAA categories and safety requirements. Governance teams should coordinate across departments to ensure consistency, conduct internal audits, and update policies in line with regulatory change. Through structured oversight and inclusive planning, UAV deployment can support strategic goals safely and legally.

References

1. **CAP 722A – CAA Supporting Guidance Documents:**
   Detailed guidance covering pilot responsibilities, system safety, and operational planning.
   https://www.caa.co.uk/our-work/publications/documents/content/cap-722a/
2. **CAA Drone Registration Portal:**
   Official site for registering UAV operators and obtaining Flyer and Operator IDs.
   https://register-drones.caa.co.uk/
3. **CAA Education Hub – Remote Pilot Competency Requirements:**
   Certification pathways including A2 CofC and GVC qualifications.
   https://www.caa.co.uk/drones/education
4. **BBC News – Gatwick Drone Incident Coverage:**
   “Gatwick drone arrest couple feel 'completely violated'.” BBC News, 24 December 2018.
   https://www.bbc.co.uk/news/uk-england-46675612
5. Health and Safety Executive – PUWER 1998 (Provision and Use of Work Equipment Regulations):
   https://www.hse.gov.uk/work-equipment-machinery/puwer.htm -
6. **CAP 722H**
   Methodology for assessing flight risk and operational safety under the Specific Category.
   https://www.caa.co.uk/our-work/publications/documents/content/cap-722h/
7. **Regulation (EC) No 785/2004 – Aviation Insurance Requirements:**
   Legal requirements for liability insurance applicable to UAV operations.
   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004R0785
8. **Information Commissioner's Office – CCTV Code of Practice:**
   Guidance on the responsible use of video surveillance technologies.
   https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/
9. **Air Navigation Order 2016 (SI 2016/765):**
   UK legislation governing aircraft and UAV operations.
   https://www.legislation.gov.uk/uksi/2016/765/contents/made
10. **Retained EU Regulation 2019/947:**
    Regulation outlining rules and procedures for the operation of unmanned aircraft.
    https://www.caa.co.uk/our-work/publications/documents/content/cap1789a/
11. **Civil Aviation Authority – Drones Guidance (CAP 722 Series):**
    Comprehensive operational and regulatory framework for UAVs in the UK.
    https://www.caa.co.uk/drones

Further information

For access to further RMP Resources you may find helpful in reducing your organisation's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

Get in touch

For more information, please contact your broker, RMP risk control consultant or account director.

contact@rmpartners.co.uk

Risk Management Partners

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk

FP1150-2025