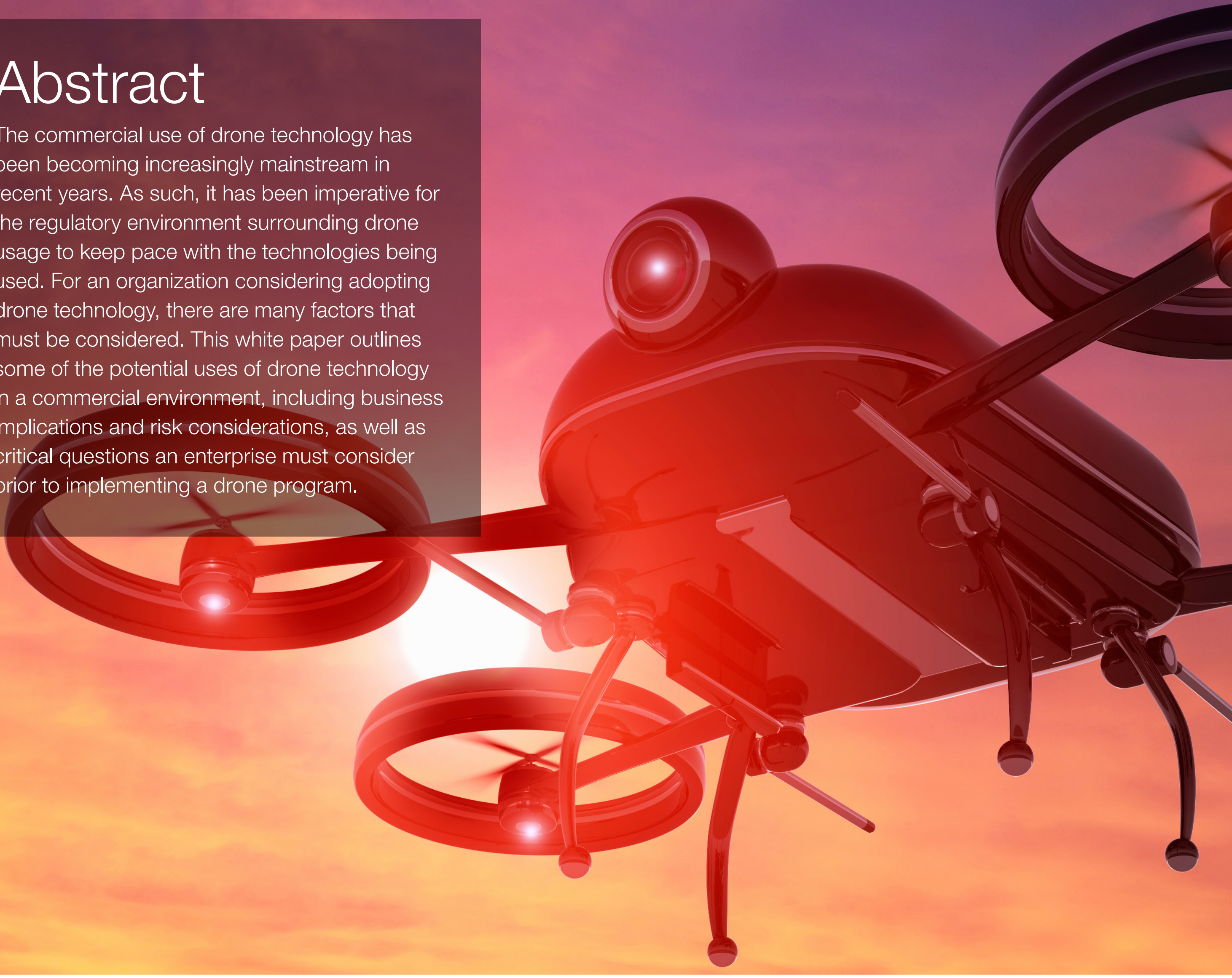
ISACA EMERGING TECH REPORT

Rise of the Drones

IS YOUR ENTERPRISE PREPARED?

Abstract

The commercial use of drone technology has been becoming increasingly mainstream in recent years. As such, it has been imperative for the regulatory environment surrounding drone usage to keep pace with the technologies being used. For an organization considering adopting drone technology, there are many factors that must be considered. This white paper outlines some of the potential uses of drone technology in a commercial environment, including business implications and risk considerations, as well as critical questions an enterprise must consider prior to implementing a drone program.



ISACA®

Trust in, and value from, information systems

Introduction

Raven, Sentinel, Reaper, Predator, Global Hawk, Gray Eagle. These are not the flying machines of an earlier era; instead, they are at the forefront of today's military aviation technology. Phantom 4, Typhoon H, Parrot Bebop 2, Automatic Dependent Surveillance Broadcast (ADS-B), Yuneec Typhoon 4K, autonomous flight, 360-degree stitching, geofencing, swarm robotics. This is the world of the rapidly expanding and very competitive commercial drone industry.

Whether used by military services, nation-states, online megastores or the neighborhood grocer, drones are quickly becoming a go-to technology for organizations seeking to eke out every possible strategic advantage in an increasingly competitive global marketplace.

Organizations of every type (public, private, governmental) are investigating or already investing in and embracing the technological and competitive advantages afforded through the use of remotely piloted aircraft, unmanned aircraft system(s) (UAS) or, simply, drones.

Poised to be a tremendous leap forward in information collection and knowledge transfer, drones and their associated technologies—if not properly controlled, monitored and implemented—represent unchecked risk, exposing adopters and bystanders alike to significant and potentially disastrous unintended outcomes.

Today, an organization (public or private) considering employing drones as a business tool will be entering new and often uncharted territory. Just what are the regulations and policies that must be addressed prior to deploying this technology across an organization? What are the procedures (safety, maintenance and training) that must first be established and then followed, once an organization's drone program is operational?

An organization cannot simply purchase a drone, outfit it with the latest data-gathering technologies and launch it to deliver packages, survey real estate or make the next blockbuster movie—at least not without the potential for both financial and legal liability.

An organization's decision to acquire drone technology and incorporate this capability into its strategic business plan equates to a decision (conscious or not) to either establish and operate an aviation department within its business operations or to outsource this capability. Further, outsourcing this activity to a third party does not necessarily discharge the organization from the responsibility to ensure that compliance with established laws is maintained and appropriate controls are in place to mitigate the risk (to organizational operations and individuals) that may be associated with this emerging business tool and its driving technology.

Are most organizations prepared to address all the regulatory, financial, safety and operational requirements necessary to properly sustain this type of business tool? Unless the organization has previous experience managing aviation operations, the answer is most probably a resounding "no." To the contrary, rushing to implement drone technology without first being properly prepared can result in both a legal and financial disaster. An uncontrolled drone program can also cause significant damage to the organization's reputation.

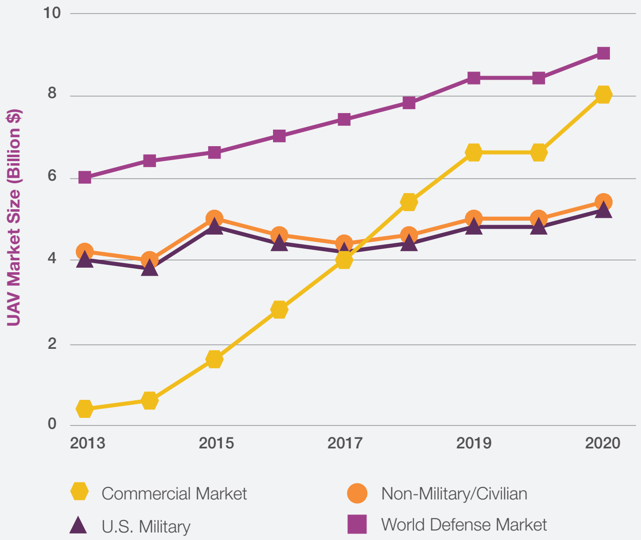
What factors must management consider prior to signing off on the acquisition and implementation of a corporate drone program? What questions must be asked and answers obtained to enable management to assess the far-ranging risk associated with the use of drones as a strategic business tool? What policies and procedures must be in place before the organization deploys its first corporate drone?

This white paper addresses these questions and more, with the intent of preparing management for the inevitable. If an organization wishes to remain competitive in today's global marketplace, it will eventually look to drones (and their related technologies) as a competitive tool and embrace all that drone technologies have to offer.

Rise of the Drones

So many people are registering drones and applying for drone pilot licenses that many government aviation officials are contemplating the possibility of millions of unmanned aircraft crowding the nation's skies in the not-too-distant future. As proof of this, in the nine months since the US Federal Aviation Administration (FAA) created a drone registration system, more than 550,000 unmanned aircraft have been registered with the agency. That agency now forecasts there will be more than 1.3 million licensed drone pilots by 2020.[1] Moreover, IGI Consulting Inc. estimates that the total US unmanned aerial vehicle (UAV) market, from large Department of Defense (DoD) UAVs to do-it-yourself (DIY) UAVs for amateurs, will grow from US $7.5 billion in 2015 to $14.8 billion in 2020 (see **figure 1**). This market will be driven by growth in the commercial and DIY markets. Major commercial applications are agriculture, real estate, filmmaking, oil and pipeline, electric utility, and specialized package delivery.[2]

FIGURE 1: UAV Market Projections



SOURCE: IGI Consulting, Inc., *UAV Market Research Study—2016 Edition*, USA, 2016, *www.igigroup.com*

Unmanned Aerial Vehicles (UAV)

A UAV, or drone, is the unmanned aircraft (UA) and all the associated support equipment, control station, data links, telemetry, communications and navigation equipment, etc., necessary to operate it. The UA is the flying portion of the system, flown by a pilot via a ground control system, or autonomously through use of an onboard computer, communication links and any additional equipment that is necessary for the UA to operate safely.[3]

While there are other terms in use such as remotely operated aircraft (ROA), remotely piloted aircraft (RPA) and others, most of the international community at this time favor the terms unmanned aircraft system(s) (UAS) and small unmanned aircraft system(s) (sUAS). Therefore, for the purposes of this paper, the UAS and sUAS acronyms will be used.

What Is a Commercial Use of sUAS?

The difference between recreational radio control aircraft and UAS is not technological, but instead a matter of intent. If the UA is flown simply for enjoyment or fun, it is recreational use. However, if the flight is purposeful and intended to perform a task (e.g., aerial competition/races, selling photos or videos taken from an sUAS, or contract services such as industrial equipment or factory inspection), it is a UAS flight.[4]

What Are Some Examples of Commercial Uses of sUAS?

The commercial uses for sUAS as organizational competitive tools are just starting to be discovered, with new, tactical uses emerging daily. Some examples of how organizations are implementing sUAS as enterprisewide, strategic tools include, but are not limited to:

- Pipeline security, management, maintenance, survey
- Land survey, management
- Real estate sales
- Package delivery
- Monitoring of road races, crowd control/management
- Livestock/range management
- Film making
- Power line maintenance and safety inspection
- Wind turbine maintenance and safety inspection

[1] Lowy, Joan, "FAA contemplating whether millions of drones will fill skies," Associated Press, 16 September, 2016, *http://phys.org/news/2016-09-faa-contemplating-millions-drones.html*

[2] IGI Group Inc., *UAV Market Research Study*—2016 Edition, USA, 2016, *www.igigroup.com/st/pages/2016_uav.html*

[3] U.S. Geological Survey (USGS), "Unmanned Aircraft Systems (UAS) FAQS," *https://www2.usgs.gov/faq/categories/10623/4283*

[4] Recreational flights are governed by Title 14 CFR, Part 101, while UAS fall under several various categories. Purposeful UAS flight requires FAA approval, through Part 107 certification (for sUAS), a certificate of waiver or authorization (COA), Section 333 petition for/grant of exemption, or special airworthiness certificate (restricted or experimental categories).

- Wildlife conservation
- Pinpoint pesticide delivery
- Forest fire fighting assistance
- Traffic monitoring
- Underground sewer, power, utility, maintenance and safety inspection
- High-rise commercial building maintenance and safety inspection
- Photography of previously inaccessible places/spaces/perspectives
- General security surveillance (private residences, corporate offices, public spaces)
- Usage at sporting events (e.g., the Olympics)

Knowing the Jurisdiction

Obviously drone usage is not limited to any geography, country or continent. To the contrary, drones are very much a global phenomenon. That said, chief among the items that must be addressed by an organization seeking to employ drones commercially are regulatory in nature and driven by the constraints of the particular environment and context in which they will operate. For example, the legal and regulatory considerations for the territories in which the organization's drone use will operate fall into this category.

Accordingly, the regulatory frameworks that pertain to air safety vary significantly from jurisdiction to jurisdiction. It is therefore imperative that the organization seeking to employ these technologies understand their regulatory environment and enlist the appropriate expertise such that they account for their regional laws and constraints. Moreover, it means that any usage-focused discussion such as this one will be very much influenced by the regulatory context within which that usage will occur.

This document targets several use cases in the United States commercial market. As such, it must of necessity account for the regulatory context of the US market. Note that other jurisdictions should evaluate and likewise account for the constraints and requirements of these other jurisdictions.

Into the Wild Blue Yonder

The first use case this paper will examine is that of Amazon delivery. Recently, the FAA approved Amazon to begin testing drones for commercial applications. In so doing, Amazon will be required to comply with a bevy of FAA requirements including, but not limited to, reporting monthly to the FAA:

- The number of flights
- Pilot duty time per flight
- Any malfunctions
- Deviation from instructions from air traffic controllers
- Unintended loss of links between the aircraft and remote pilot

As one can see clearly from this list, Amazon's rapid development and advances across multiple technological platforms are outpacing government approvals and the regulations designed to monitor and control this environment. For example, Amazon's ultimate desire to use sUAS to deliver consumer packages is currently stymied by FAA regulations, Part 107, which:

- Does not permit operational capabilities for the transportation of goods for compensation beyond visual line of sight (VLOS). The sUAS remote pilot in command (PIC) or visual observer (VO) must have constant VLOS of the sUAS.
- Permits transportation of property by sUAS for compensation or hire. These operations, however, must be conducted within a confined area.
- Stipulates that when conducting the transportation of property, the transport must occur wholly within the bounds of a state. State lines cannot be crossed; only intrastate operations are permitted at this time.
- Permits operation of sUAS from a moving land or waterborne vehicle over a sparsely populated area. However, operation from a moving aircraft is prohibited. Additionally, sUAS being used to transport another person's property for compensation or hire may not be operated from any moving vehicle (e.g., chase car, delivery van).[5]

Companies wishing to push the rules further—such as flying at night or beyond VLOS—can apply for special exemption. PrecisionHawk, a fixed-wing drone company targeting the agriculture space, has gained a waiver which suggests acknowledgment on the part of at least one regulator that the existing rules might be limiting current potential use cases. A number of companies, including Google, Amazon, Domino's Pizza, DHL, and Flirtey, are exploring using sUAS for delivery, an activity that needs permission beyond VLOS to create a scalable operation.[6]

[5] US Federal Aviation Administration, "Summary of Small Unmanned Aircraft Rule (Part 107)", *FAA News*, 21 June 2016, *www.faa.gov/UAS/media/Part_107_Summary.pdf*. See also: US Federal Aviation Administration, "Small Unmanned Aircraft Systems," *FAA Advisory Circular 107-2*, 21 June 2016, *www.faa.gov/uas/media/AC_107-2_AFS-1_Signed.pdf*

[6] Swinhoe, Dan; "Commercial drones in the US open for business," IDG Connect, 30 August 2016, *www.idgconnect.com/blog abstract/20014/commercial-drones-us-business*

Managing, Monitoring and Controlling sUAS Operations

The FAA's regulation enacted in August 2016, Operation and Certification of Small Unmanned Aircraft Systems, specifically identifies rules for the operation of sUAS in the National Airspace System (NAS). This regulation, known more commonly as Small Unmanned Aircraft Rule (Part 107) or just Rule (Part 107), aims to increase the safety and efficiency of the NAS by addressing the classification of small unmanned aircraft, certification of their remote pilots, registration, approval of operations and operational limits.[7]

sUAS operators and organizations seeking to employ drones as business tools/solutions are required to operate in compliance with Small Unmanned Aircraft Rule (Part 107).

Here are several initial internal control and compliance questions an organization must ask prior to the launch of its UAS:

1. Does the organization's sUAS meet the weight requirement as stipulated by Rule (Part 107)? The FAA mandates that unmanned aircraft weigh less than 55 pounds (25 kilograms), including payload, fuel and any other equipment onboard the aircraft required to ensure safe operation.
2. How will the organization's sUAS be capable of being operated (controlled) within the VLOS of its operator? Rule (Part 107) stipulates that the unmanned aircraft must remain within VLOS of the remote PIC and the person manipulating the flight controls of the sUAS.[8]
3. Will the organization's sUAS team have a VO? If the sUAS will not be in the VLOS of the operator, Rule (Part 107) mandates that the sUAS remain within VLOS of the VO and within VLOS proximity to the remote PIC; this is to enable use of first person view (FPV).
4. Will the remote pilot and VO responsible for direct observation of the sUAS be able to see the aircraft with vision unaided by any device other than corrective lenses? The VO acts as a flight crew member who helps the small UA remote PIC and the person manipulating the controls to see and avoid other air traffic or objects aloft or on the ground.
5. How does the organization plan to employ and satisfy the mandatory see and avoid (SAA), also referred to as detect and avoid, requirement for its sUAS? The remote PIC and person manipulating the controls must be able to see the sUAS at all times during flight. Therefore, the sUAS must be operated closely enough to the control station (CS) to ensure visibility requirements are met during sUAS operations.

Sense and Avoid (SAA)

Whether referred to as detect and avoid, sense and avoid or collision avoidance software, the aims of the technology are the same: to detect aircraft and obstacles within the vicinity of the UAV and to execute maneuvers to restore a safe situation if needed. Indeed, sense and avoid is a sequence of functions that, using a combination of airborne and ground-based sensors, are able to perform maneuvers to avoid collisions and serve as a UAV replacement for the traditional see and avoid capability for manned aircraft.[9]

Military, government agencies and other high-end, larger UAS operators seek to employ systems such as traffic alert and collision avoidance systems (TCAS) and automatic dependent surveillance-broadcast (ADS-B) for UAS, resulting in an internal automatic dependent surveillance package. TCAS, for example, keeps an electronic eye on the sky immediately surrounding an airplane. Should another airplane with a similar device fly too close, an alert will prompt the pilot to take action.[10]

The name is self-describing; TCAS sense or detect an object around the aircraft such as other aircraft and natural threats like birds and avoid them to prevent airborne collisions. sUAS need to be able to react to each other and with their surroundings. However, it is the integration and the size, weight and power (SWAP) of small unmanned aerial vehicles (sUAV) that provide challenges. Unlike traditional aircraft and larger sUAS, lower altitudes and speed are contributing factors, too.[11]

The list of initial internal control and compliance questions an organization must ask prior to the launch of its UAS continues with:

[7] VOs and other crew members (e.g., person manipulating controls under supervision of a certified remote PIC) do not require certification.

[8] This is a condition that can be waived, except for transportation of property.

[9] Roden, Megan, "Sense and Avoid: The Technology to Watch," SkyTech, 7 July 2015, *www.skytechevent.com/single-post/2015/07/07/Sense-and-Avoid-The-Technology-to-Watch*

[10] Merlin, Peter; Banke, Jim; "NASA, Industry Complete Third Phase of UAS Flight Testing," National Aeronautics and Space Administration, 16 September 2015, *www.nasa.gov/centers/armstrong/features/detect_and_avoid.html*

[11] Erwin, T.; "Sense and Avoid," Harris Geospatial Solutions, 11 June 2015, *www.harrisgeospatial.com/Company/PressRoom/Blogs/ImagerySpeaksDetail/TabId/901/ArtMID/2927/ArticleID/14506/Sense-and-Avoid.aspx*

6. Has the organization secured the necessary Air Traffic Control (ATC) permissions required to operate in controlled Class B, C, D and E airspace? Operations in Class G (uncontrolled) airspace are allowed without ATC permission. If the organization's sUAS operations team needs to ask what Class B, C, D, E and G airspace is, there may already be a problem with the intended rollout of the sUAS tools.

What Is the Difference Between Controlled Airspace and Uncontrolled Airspace?

Airspace is broadly categorized as either controlled or uncontrolled. In the United States, Class A, B, C, D and E airspace is controlled. Class G airspace is uncontrolled (see **figure 2**).

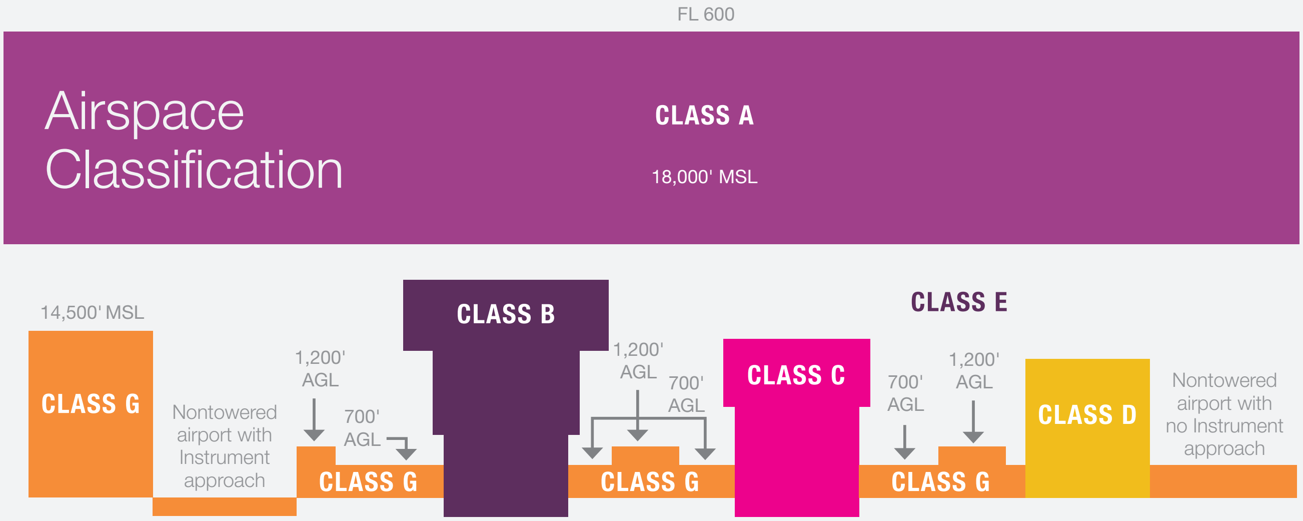
In controlled airspace, air traffic controllers are generally responsible for separating aircraft flying under instrument flight rules (IFR) from one another. In uncontrolled airspace (Class G), ATC does not provide that service. The distinction of controlled and uncontrolled airspace has nothing to do with whether the federal aviation regulations (FARs) are enforceable or not; the FARs are in effect in all US airspace.[12] **A concern for the widespread operation of sUAS is that they may be too small to see, either visually or on radar, and can therefore present a hazard to manned aviation.**

Remote Pilot in Command Certification and Responsibilities

Rule (Part 107) has specific requirements aimed at the remote pilot and mandatory compliances for this operator. To ensure compliance, the following questions should be asked:

1. First and foremost, has the organization established a remote PIC position? Just like a manned aircraft, the remote PIC of an sUAS is directly responsible for, and is the final authority as to, the operation of that UAS.The position, along with an appropriately defined job description, should be developed in cooperation with the organization's human resources/personnel and legal departments in addition to an external subject matter expert (SME) having specific knowledge of pilot requirements, capabilities and experience necessary to command and operate this particular type of aircraft.
2. Does the organization's sUAS pilot hold a remote pilot airman certificate with a small UAS rating? The remote PIC must have this certificate easily accessible during flight operations.
3. Is the certificate valid, current and substantiated by both the experience and testing required to obtain such a certificate? It should be emphasized that experience is not needed to obtain a certificate; one must simply pass a test.

FIGURE 2: Types of Controlled Airspace



SOURCE: FAA Safety Team, "ALC-42: Airspace, Special Use Airspace and TFRs – Types of Controlled Airspace," *www.faasafety.gov/gslac/ALC/course_content.aspx?cID=42&sID=505&preview=true*

[12] Marcus, Ben; "Proposed FAA Small UAS Rule—What is Class B, C, D, and E airspace?," Medium, 22 February 2015, *https://medium.com/future-of-flight/proposed-faa-small-uas-rule-what-is-class-b-c-d-and-e-airspace-81e760a36db1#.dxc2ze1sc*

4. Does the remote PIC possess demonstrated experience, i.e., the applicable knowledge, including appropriate flight time, to support the exam-based certificate?
5. If not, is this pilot under the direct supervision of a person who does hold a remote pilot certificate (remote PIC)? How is this direct supervision substantiated?

The goal of the airman certification process is to ensure the applicant possesses knowledge consistent with the privileges of the remote pilot certificate with an sUAS rating being exercised, as well as the ability to manage the risks of flight in order to act as a remote PIC.[13]

Upon request from the FAA, the remote PIC must make available to the FAA the organization's sUAS for inspection or testing, along with any associated documents/records required to be kept under the rule.

Is the Organization's sUAS Flight-ready and Airworthy?

An sUAS must be maintained in a condition for safe operation. Prior to flight, the remote PIC is responsible for conducting a check of the sUAS and verifying that it is in a condition for safe operation.

Asking and answering the following questions will help determine that the sUAS remains in flight-ready and airworthy condition:

1. What is the organization's maintenance, inspection and testing policy?
2. Who is responsible for maintaining this policy and all forthcoming documentation?
3. Who is responsible for the actual field-level inspection and maintenance of the sUAS? Who is responsible for testing of the sUAS?
4. Is this (or are these) individuals certified to perform this inspection/maintenance and/or testing process? If so, what is the date of their last certification exam or review?
5. What is the risk/exposure to the organization if an unqualified individual is performing the inspection, maintenance or testing of the organization's sUAS?
6. What liabilities exist if the organization is unable to provide the inspection, maintenance or testing documentation when requested by the FAA?
7. Does evidence exist to substantiate that the individual responsible for sUAS inspection and maintenance and determining that the sUAS is in a condition for safe operation utilizes an FAA-approved maintenance schedule for all the sUAS aircraft, incorporating into this schedule manufacturer guidance as well as industry best practices?[14]

The FAA may take appropriate action against an sUAS owner, operator, remote PIC or anyone else who fraudulently or knowingly provides false records or reports or otherwise reproduces or alters any records, reports or other information for fraudulent purposes. Such action could include civil sanctions and the suspension or revocation of a certificate or waiver.

It is important to note that, according to Rule (Part 107), a person may not operate or act as a remote PIC or VO in the operation of more than one UA at the same time. To test this, the following question should be asked:

8. If your organization operates (or intends to operate) more than one sUAS concurrently, does the organization employ multiple PICs and VOs?[15]

All sUAS operating in the NAS in accordance with Title 14 of the Code of Federal Regulations (14 CFR), Part 48, are limited to not more than 55 pounds (25 kilograms) and must be registered prior to operating under Rule (Part 107). Answers to the following questions will help test compliance with this requirement:

9. Are all the organization's flight-ready sUAS properly registered in compliance with 14 CFR, Part 48?
10. Who is responsible for the registration process, record retention and the renewal process when required?
11. How is registration substantiated for proper compliance to 14 CFR, Part 48?

Rule (Part 107) prohibits operation of an sUAS at night, which is defined as the time between the end of evening civil twilight and the beginning of morning civil twilight, as published in The Air Almanac[16], converted to local time. This can be tested by answering the following question:

12. Does the organization physically secure all sUAS to prevent their usage outside of the regulated daylight hours as described by The Air Almanac?[17]

[13] US Federal Aviation Administration, "Remote Pilot—Small Unmanned Aircraft Systems Airman Certification Standards," July 2016, *www.faa.gov/training_testing/testing/acs/media/uas_acs.pdf*

[14] For guidance regarding how to determine that an sUAS is in a condition for safe operation, see: US Federal Aviation Administration, "Small Unmanned Aircraft Systems," *FAA Advisory Circular 107-2*, 21 June 2016, *www.faa.gov/uas/media/AC_107-2_AFS-1_Signed.pdf*

[15] An organization may apply for a waiver of the VO requirement if the PIC proves the proposed flight will be conducted safely under a waiver.

[16] Nautical Almanac Office; *The Air Almanac 2016*, US Department of Defense, Navy, Nautical Almanac Office, 2016, *http://aa.usno.navy.mil/publications/docs/aira.php*

[17] sUAS operation may be allowed to deviate from certain operating rules if the FAA finds that the proposed operation can be performed safely. For example, when sUAS operations are conducted during civil twilight, the small UA must be equipped with anti-collision lights that are capable of being visible for at least three statute miles.

Securing and Controlling the Organization's sUAS Initiatives

According to Dedrone CEO and co-founder Joerg Lamprecht, "Any institution with an elevated need for security must now protect its airspace against intrusion from drones."[18]

The security threats from sUAS are real. **Figure 3** discusses just some of the issues associated with emerging UAS usage and considerations on how organizations will address the issues.

Before an organization commits to implementing and launching an sUAS program, the following critical questions must be addressed and answered:

1. Is the organization prepared to operate and manage an internal aviation department?
2. Is running an aviation operation in line with the organization's mission, core business and capabilities?
3. Who is the individual primarily responsible for the organization's sUAS program?
4. Who is responsible for assessing and authorizing applications of the sUAS technology to specific business usages/purposes?
5. Are uses of the organization's sUAS consistent with the organization's ethics policy?
6. Has the organization secured a certificate of authorization (COA) prior to any launch of the corporate sUAS?
7. Is the organization ready to assume the responsibilities of flight operations?
8. Has the organization identified all the complexities and challenges of operating an internal certified flight operations function?
9. Does sUAS technology pose a risk to the organization? If so, what type? How is this risk expected to be mitigated?

FIGURE 3: UAS Usage Issues

SECURITY	
Threat	A breach of the organization's perimeter, buildings, offices, storage facilities, meeting spaces, etc.
Vulnerability	A UAS outfitted with a laser microphone could be stationed outside the 30th-floor boardroom.
Impact	The unauthorized monitoring, recording, disclosure and use of confidential corporate intelligence, information, or activities, by an external competitor, third party or nation-state.
TECHNICAL RISK	
Threat	Unauthorized physical and/or logistical access to the sUAS's onboard technology, programming, sensing and recording equipment.
Vulnerability	Unauthorized software changes or modifications to the sUAS guidance, geolocation, (e.g., GPS sense and avoide/detect and avoid software/hardware) and/or the sUAS's operating protocols.
Impact	The weaponization (intentionally or unintentionally) of the organization's benign sUAS.
DATA MANAGEMENT	
Threat	The unauthorized access to and use of data (e.g., audio, video, other) held by the organization, which is captured, collected, recorded and archived by the UAS.
Vulnerability	Failure to address how information acquired by sUAS is gathered through remote sensing technology, including but not limited to photography (e.g., RGB, infrared), audio or video recording, etc.
Impact	Noncompliance with or violation of local, state or federal laws, such as: **1.** Texas HB 912 criminalizes the use of drones to capture images and possess or distribute them. **2.** North Carolina SB 744 creates regulations for the public, private and commercial use of UAS. This law prohibits any entity from conducting UAS surveillance of a person or private property. It also prohibits taking a photo of a person for the purpose of distributing it without his or her consent.[19]

[18] Dedrone, "Fast-Growing Dedrone Raises $10M Series A, 17 May 2016, *www.dedrone.com/en/newsroom/press-detail/fast-growing-dedrone-raises-10m-series-a*

[19] National Association of Mutual Insurance Companies, "A Compendium of State Laws and Proposed Legislation Related to Unmanned Aerial Systems/Drones," September 2015, *www.ntia.doc.gov/files/ntia/publications/namic-ntia-drones_final.pdf*

FIGURE 3: UAS Usage Issues *(continued)*

PRIVACY	
Threat	The impact on privacy in general and specifically on the protection of personally identifiable information (PII).
Vulnerability	An aircraft traveling over an individual's land does not constitute a trespass, but the "immediate reaches" around the property still belong to the owner. UAS flying within the immediate reaches of one's personal property could be considered trespassing.
Impact	Noncompliance with or violation of local, state or federal laws, such as: **1.** Florida SB 766 prohibits the use of a drone to capture an image of privately owned property or the owner, tenant or occupant of such property without consent if a reasonable expectation of privacy exists. **2.** Mississippi SB 2022 specifies that using a drone to commit Peeping Tom activities is a felony. **3.** Tennessee SB 1892 prohibits drone use to intentionally conduct surveillance of an individual or his/her property.[20]
LEGAL	
Threat	Operational failure (e.g., mechanical, physical, logical or operator) of the organization's UAS. Intentional disabling another UAS via electronic jamming, passing malware to an onboard CPU via near-field communications (NFC).
Vulnerability	Uncontrolled or intentional downing (i.e., crash) of UAS into crowds, individuals, commercial aircraft, private/public property, etc.
Impact	Legal and financial impacts to both operator and organization. In addition, noncompliance with or violation of local, state or federal laws, such as: Idaho's SB 1134 requires warrants for drone use by law enforcement, establishes guidelines for use by private citizens and provides civil penalties for damages caused by improper use.[21]

10. What procedures exist to attest that any organizational use of sUAS technology: (a) is legal; (b) is authorized and approved by executive management; (c) is conducted according to established operational protocols; and (d) meets or exceeds legal compliance requirements?

11. How is sUAS technology classified within the organization? Is it IT? Is it operations?

12. Does organizational sUAS operations maintain its own functional department?

13. Will the organization be able to immediately (required prior to the maiden launch of the organization's sUAS) comply with federal legislation and state and local regulations for the safe and proper operation of its sUAS fleet?

14. What added risk and liabilities will the organization encounter once it establishes an aviation function/department and is responsible for all of the compliance requirements associated with this function?

15. Does the organization possess the knowledge and skill set necessary to perform an audit of the aviation department?

16. Who oversees the PIC and VO licensing/qualification process? Is it IT, operations, human resources or another department?

17. What would be the impact on the organization's insurance coverage if the company's UAS operators were not qualified or certified?

18. Does the organization maintain a policy for acceptable use of sUAS technology within the organization? If not, does the absence of such a policy represent a potential liability to the organization?

19. Does the organization maintain appropriate levels of insurance, covering the operation, maintenance, storage and security of the sUAS and its related technologies?

20. Does the organization have up-to-date, operational lost link and fly away profiles, operating limitations and emergency procedures for each of its FAA-approved sUAS vehicles?[22,23]

[20] *Ibid.*

[21] *Ibid.*

[22] Lost link refers to an interruption or loss of the control link, or when the pilot is unable to effect control of the aircraft and, as a result, the UA will perform a predictable or planned maneuver. Source: U.S. Department of Transportation Federal Aviation Administration, "Unmanned Aircraft Systems (UAS) Operational Approval, N 8900.227," 30 July2013, *www.faa.gov/documentlibrary/media/notice/n_8900.227.pdf*

[23] Fly-away refers to an interruption or loss of the command and control link where the pilot is unable to affect control of the aircraft and the aircraft is no longer following its preprogrammed procedures resulting in the UAV not operating in a predictable or planned manner. Source: Transport Canada, "Staff Instruction (SI) No. 623-001, Review and Processing of an Application for a Special Flight Operations Certificate for the Operation of an Unmanned Air Vehicle (UAV) System, Document No.: SI 623-001," 19 November 2014, *www.tc.gc.ca/eng/civilaviation/standards/general-recavi-uav-4161.html*

21. How are sUAS that are decommissioned purged of any sensitive technology, data and data retention/storage capability prior to their disposal?
22. How are data obtained in full compliance with the law, via sUAS technology, protected as company propriety information? How are the data protected as intellectual property?
23. What procedures exist to guide the organization in the acquisition of appropriate, justified and cost-effective corporate sUAS?
24. How will the organization ensure that when outside service providers are hired to manage, maintain and/or operate the organization's UAS program, those providers can maintain adequate and reasonable security and meet all legal compliances?
25. How will the organization demonstrate the capability to provide appropriate oversight of all third-party providers entrusted with managing, maintaining and/or operating the organization's UAS program?

Organizational Preparedness—Additional Requirements

Though neither the person manipulating the controls of an sUAS nor the VO is required to obtain an airman medical certificate, these individuals may not participate in the operation of an sUAS if they know or have reason to know that they have a physical or mental condition that could interfere with the safe operation of the sUAS.[24]

The following questions can help the organization determine its readiness to meet this requirement:

1. Is the organization ready to identify, collect, retain and manage the sensitive, private medical information that is required to ascertain the medical flight readiness of the sUAS PIC and VO?
2. Exactly what information will these employees (or third-party contractors) be required to submit to substantiate that they are medically fit to operate the sUAS?
3. It is the remote PIC's responsibility to ensure no crew members are participating in the operation while impaired. How does the PIC determine and substantiate that all sUAS operational personnel are fit to participate in the flight operations of the sUAS?
4. What risk does the organization face if the PIC or VO operate the sUAS in an impaired medical state?

In the development of risk assessment criteria, sUAS remote PICs are expected to develop risk acceptance procedures, including acceptance criteria and designation of authority and responsibility for risk management decision making. The acceptability of risk can be evaluated using a risk matrix as shown in **figure 4**.[25]

Once again, even if the organization were to outsource its sUAS operation, this does not relieve the organization from the risk and responsibilities associated with any wrongdoing associated with the operation of the sUAS.

The remote PIC must complete a preflight familiarization and inspection, and perform other actions such as crew member briefings, prior to beginning flight operations. The FAA has produced many publications providing in-depth information on topics such as aviation weather, aircraft loading and performance, emergency procedures, Aeronautical Decision Making (ADM), and airspace, which should all be considered

FIGURE 4: Safety Risk Matrix

RISK LIKELIHOOD		RISK SEVERITY				
		Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely Improbable	1	1A	1B	1C	1D	1E

SOURCE: US Federal Aviation Administration, "Small Unmanned Aircraft Systems (sUAS), FAA Advisory Circular 107-2," 21 June 2016, *www.faa.gov/documentlibrary/media/advisory_circular/ac_107-2.pdf*

[24] US Federal Aviation Administration, "Small Unmanned Aircraft Systems," FAA Advisory Circular 107-2, 21 June 2016, *www.faa.gov/uas/media/AC_107-2_AFS-1_Signed.pdf*

[25] *Ibid.*

prior to operations.[26] Answering the following question will continue the process of helping the organization gauge its readiness for flight:

5. What procedures are in place to validate that the PIC has properly and completely performed the preflight check, as prescribed by the FAA, prior to beginning flight operations?

The FAA encourages the remote PIC to conduct the overall safety risk assessment as a method of compliance with the prohibition on operations by certain persons and the requirement to remain clear of other aircraft. The answer to the following question will inform the organization if it is in compliance with the FAA's rules:

6. What evidence exists to substantiate that this recommended safety risk assessment has been conducted by the PIC?

Flying an sUAS while driving a moving vehicle is considered careless or reckless because the person's attention would be hazardously divided. The organization should ask itself the following questions to ensure this hazard is avoided:

7. Do procedures exist that prevent the remote PIC or person manipulating the flight controls from operating the sUAS while concurrently driving a moving vehicle?
8. Is the PIC aware of and has the PIC reviewed all applicable state and local privacy-related laws specific to UAS operations within the intended area of operation, prior to operating their sUAS?

Lastly, prior to launch, this question should be considered:

9. Is the PIC aware of and has the PIC been advised that individuals involved in operating an sUAS are responsible for complying with all applicable laws and not just the FAA's regulations?

In Conclusion: Be Prepared

sUAS are very capable of invading privacy, breaching security and compromising internal controls on many different levels. A mobile phone is equally capable of doing the same, while also making it easier to get closer to a person or intended internal corporate target than with an sUAS and providing less probability of being detected. However, with a mobile phone, for the most part, targets know the person is in front of them taking their picture. The organization can prevent the phone's access to its IT infrastructure or the device's entry into a facility. The same cannot be said of an sUAS or its potential technological payload.

sUAS are in the news almost daily, most often for their role in military operations and capacities. As the technology becomes cheaper and easier to operate, the spread of sUAS technology and its usage into the mainstream population is only a matter of time.

There is hardly any other single technology currently developing as fast as sUAS technology. However, the increase in sUAS efficiency also means more opportunities for individuals, organizations and nation-states to misuse this technology.

The ongoing miniaturization of fully functional sUAS, the emergence of newer sUAS technologies, and the application of sUAS into general and specific business processes to achieve a competitive advantage will only contribute to organizations' desire to adopt and implement sUAS tools—at times doing so without the proper planning or forethought.

Before an organization embarks upon implementing its own sUAS strategy, it must be very sure that it is properly prepared to do so.

[26] *Ibid*

Glossary

Acceptable level of safety performance (ALoSP)

The minimum level of safety performance of civil aviation in a state, as defined in its state safety program, or of a service provider, as defined in its safety management system, expressed in terms of safety performance targets and safety performance indicators

Accident (aircraft)

An occurrence associated with the operation of an aircraft that takes place between the time any person boards the aircraft with the intention of flight until all such persons have disembarked, in which a person is fatally or seriously injured, the aircraft sustains substantial damage, or the aircraft is missing or is completely inaccessible

Accountability

The ability to map a given activity or event back to the responsible party.

Scope note: In the context of a safety management system (SMS), accountability means being ultimately responsible for safety performance, whether at the overall SMS level (accountable executive) or at specific product and/or process levels (other applicable members of management).

Advanced qualification program (AQP)

A training and evaluation program that is an alternative method of complying with the traditional training requirements prescribed by a regulatory authority. Such advanced or alternative training and evaluation programs are typically established to allow a greater degree of flexibility in the approval of innovative training programs, and can be used to qualify and certify, as applicable, flight crew members, cabin crew members, flight dispatchers/flight operations officers (FOOs), instructors, evaluators and other operations personnel.

Air operator

The holder of an air operator certificate (AOC) issued by the certifying authority

Air traffic management (ATM)

The integrated management of air traffic and airspace for the purpose of providing the safe movement of aircraft in the air and on the ground. ATM comprises three complementary systems:

1. Airspace management
2. Air traffic flow and capacity management
3. Air traffic control (ATC)

Aircraft

Any machine that can derive support in the atmosphere from the actions of the air

Aircraft maintenance

The performance of tasks required to ensure the continuing airworthiness of an aircraft, including any one or a combination of overhaul, inspection, replacement, defect rectification, and the embodiment of a modification or repair

Aircraft operations

All activities associated with the operation of an aircraft on the ground and in the air

Aircraft technical log (ATL)

The record of reported or observed malfunctions, failures or defects in the airframe, power plant or appliances on an aircraft, including information concerning repairs, replacements, adjustments or deferrals. The log normally resides in the aircraft.

Aircraft tracking	A process established by an operator that maintains and updates, at standardized intervals, a ground-based record of the four dimensional positions of an individual aircraft in flight
Airworthiness	The status of an aircraft, engine, propeller or part when it conforms to its approved design and is in a condition for safe operation
Authority (regulatory)	A government agency or other administrative body that exercises regulatory or oversight control over operations or activities within a defined jurisdiction
Base maintenance	Any maintenance task falling outside the criteria for line maintenance
Certificate of waiver or authorization (COA)	An authorization issued by the air traffic organization to a public operator for a specific unmanned aircraft activity. In the United States, after a complete application is submitted, the Federal Aviation Administration conducts a comprehensive operational and technical review.
Compliance	Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies
Control station (CS)	An interface used by the remote pilot or the person manipulating the controls to control the flight path of the small unmanned aircraft
Corrective action	Action to eliminate the cause(s) and prevent recurrence of an existing (detected) nonconformance or an existing (detected) undesirable condition or situation
Covered data	Information collected by an unmanned aircraft system that identifies a particular person. If data collected by an unmanned aircraft system likely will not be linked to an individual's name or other personally identifiable information, or if the data are altered so that a specific person is not recognizable, the data are not covered data.
Evidence	Information that an auditor gathers in the course of performing an information systems (IS) audit; relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support.
Flight recorder	Any type of recorder installed in the aircraft for the purposes of complementing accident/incident investigation

Flight safety analysis program

A support management function that specializes in the collection and analysis of operational information and data for the purpose of identifying hazards and supporting the risk management process in order to prevent accidents or incidents associated with aircraft operations. Typical program elements include:

1. Investigation of operational accidents, incidents and irregularities
2. Liaison with regulatory and investigative authorities
3. Collection and analysis of flight data and information
4. Review and analysis of flight safety and confidential human factors reports
5. Issuance of operational safety publications
6. Generation of operational safety statistics
7. Maintenance of a flight safety database

Flight training device (FTD)

A device that replicates aircraft flight deck instruments, equipment, panels and controls in an open or enclosed area; includes the assemblage of equipment and computer software programs necessary to represent the aircraft in ground and flight conditions to the extent of the systems installed in the device; does not require a force (motion) cueing or visual system

Incident (aircraft)

An occurrence other than an aircraft accident, associated with the operation of an aircraft, that affects or could affect the safety of operations

Life status

The accumulated cycles, hours or any other mandatory replacement limit of a life-limited part

Life-limited part (LLP)

Any part for which a mandatory replacement limit is specified in the type design, the Instructions for Continued Airworthiness, or the maintenance manual

Line maintenance

Any maintenance that must be carried out before flight to ensure the aircraft is fit for the intended flight. It may include:

- Troubleshooting
- Defect rectification
- Component replacement with use of external test equipment, if required
- Component replacement (may include components such as engines and propellers)
- Scheduled maintenance and/or checks, including visual inspections that will detect obvious unsatisfactory conditions or discrepancies but do not require extensive in-depth inspection

It may also include internal structure, systems and power plant items, which are visible through quick opening access panels/doors, and minor repairs and modifications, which do not require extensive disassembly and can be done by simple means.

For temporary or occasional cases, the quality manager may accept base maintenance tasks to be performed by a line maintenance organization, provided all requirements are fulfilled.

Lost link protocol	The intent of any lost link procedure is to ensure airborne operations remain predictable (e.g., lost link orbit points, communications procedures, and pre-planned flight termination points (FTP) or other contingency planning measures in the event recovery of the unmanned aircraft system is not feasible). There are two types of links: **1.** An uplink that transmits command instructions to the aircraft **2.** A downlink that transmits the status of the aircraft and provides situational awareness to the pilot
Maintenance (aircraft)	Those actions required for restoring or maintaining an aircraft, aircraft engine or aircraft component in an airworthy and serviceable condition, including repair, modification, overhaul, inspection, replacement, defect rectification and determination of condition
Maintenance program	A document that describes the specific scheduled maintenance tasks and their frequency of completion and related procedures, such as a reliability program, necessary for the safe operation of those aircraft to which it applies
Maintenance records	Specific records that contain the details of maintenance performed on an aircraft, aircraft engine or aircraft component, typically including the data used, certification for such maintenance and names of persons who accomplished the maintenance
National Airspace System (NAS)	A network of air navigation facilities, air traffic control facilities, airports, technology, and appropriate rules and regulations needed to operate the system
Person manipulating the controls	A person other than the remote pilot in command (PIC) who is controlling the flight of a small unmanned aircraft system under the supervision of the remote PIC
Preventive action	Action to eliminate the cause(s) and prevent occurrence of a potential nonconformance or potential undesirable condition or situation
Regulatory authority	An organization designated or otherwise recognized by the government of a state for regulatory purposes, which issues rules and regulations in connection with protection and safety
Remote pilot in command (remote PIC or remote pilot)	A person who holds a remote pilot certificate with a small unmanned aircraft system (sUAS) rating and has the final authority and responsibility for the operation and safety of an sUAS operation conducted under Small Unmanned Aircraft Rule (Part 107)
Safety audit	An independent and documented examination of activities, records, systems, programs, processes, procedures, resources and/or other elements of operations to verify an operator’s safety performance and validate the effectiveness of existing risk controls

Safety risk	The projected severity and likelihood of occurrence of an adverse consequence or outcome from an existing hazard. A projected outcome could be an accident, but an intermediate unsafe event or consequence might be identified as the most credible outcome.
Safety risk assessment (SRA)	A formal process used to determine safety risk by assessing the potential severity and likelihood of occurrence of an adverse consequence or outcome from an existing hazard
Safety risk management	The component of a safety management system that includes the organizationwide implementation of safety risk assessment processes for the purpose of ensuring safety risk is mitigated or controlled
Safety risk mitigation	The development and implementation of action(s) or measures designed to reduce a safety risk to, and maintain such risk at or below, an acceptable level in accordance with an organization's safety risk tolerability
Safety risk tolerability	The level of safety risk that is acceptable (or unacceptable) to an organization based on the risk acceptance criteria of that organization
Security control	A means by which the introduction of weapons, explosives, or other dangerous/prohibited devices, articles or substances that could be utilized to commit an act of unlawful interference can be prevented
Small unmanned aircraft (UA)	An unmanned aircraft weighing less than 55 pounds (25 kilograms), including everything that is onboard or otherwise attached to the aircraft, and can be flown without the possibility of direct human intervention from within or on the aircraft
Small unmanned aircraft system(s) (sUAS)	A small unmanned aircraft and its associated elements (including communication links and the components that control the small unmanned aircraft) that are required for the safe and efficient operation of the small unmanned aircraft in the National Airspace System
Swarm robotics	A field of study that examines how large groups of robots can interact with each other in simple ways to solve relatively complex tasks cooperatively
Unmanned aircraft (UA)	An aircraft operated without the possibility of direct human intervention from within or on the aircraft
Unmanned aircraft system(s) (UAS)	An unmanned aircraft (an aircraft that is operated without direct human intervention from within or on the aircraft) and associated elements (including communication links and components that control the unmanned aircraft) that are required for the pilot or system operator in command to operate safely and efficiently in the National Airspace System
Visual observer (VO)	A person acting as a flight crew member who assists the small unmanned aircraft remote pilot in command and the person manipulating the controls to see and avoid other air traffic or objects aloft or on the ground

The terms in this glossary have been compiled from multiple sources, including, but not limited to, the following publications:

- International Air Transport Association, *IATA Reference Manual for Audit Programs Ed 7*, June 2016, *http://extranet.iata.org/audit-program-documentation/SitePages/default.aspx*
- US Federal Aviation Administration, “Small Unmanned Aircraft Systems (sUAS), *FAA Advisory Circular 107-2*,” 21 June 2016, *www.faa.gov/uas/media/AC_107-2_AFS-1_Signed.pdf*
- US Federal Aviation Administration, “ALC-42: Airspace, Special Use Airspace and TFRs,” *www.faasafety.gov/gslac/ALC/course_content.aspx?cID=42&sID=505&preview=true*
- US Federal Aviation Administration, “Summary of Small Unmanned Aircraft Rule (Part 107),” 21 June 2016, *www.faa.gov/UAS/media/Part_107_Summary.pdf*
- The White House, “Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems,” 15 February 2015, *www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness while-safegua*

ISACA®

ISACA (*isaca.org*) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

This is an educational resource and is not inclusive of all information that may be needed to assure a successful outcome. Readers should apply their own professional judgment to their specific circumstances.

Reservation of Rights

ISACA®
Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

Web site: *www.isaca.org*

Provide feedback:
www.isaca.org/drones

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Follow ISACA on Twitter:
https://twitter.com/ISACANews

Join ISACA on LinkedIn:
www.linkd.in/ISACAOfficial

Like ISACA on Facebook:
www.facebook.com/ISACAHQ

Acknowledgments

ISACA wishes to recognize:

Authors

Albert J. Marcella, Jr.
Ph.D., CISA, CISM, Business Automation Consultants, LLC, USA

Brent A. Terwilliger
Ph.D., Embry-Riddle Aeronautical University, USA

Expert Reviewers

Christopher Gourdine
DMGT, Lindenwood University, USA

Brian K. Maddocks
Ticom Geomatics, Inc., USA

Board of Directors

Christos K. Dimitriadis
Ph.D., CISA, CISM, CRISC
INTRALOT S.A., Greece, Chair

Theresa Grafenstine
CISA, CGEIT, CRISC, CIA, CGAP, CGMA, CPA
U.S. House of Representatives, USA, Vice-chair

Robert Clyde
CISM
Clyde Consulting LLC, USA, Director

Leonard Ong
CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM, CIPT, CISSP, ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA
Merck, Singapore, Director

Andre Pitkowski
CGEIT, CRISC, OCTAVE CRMA, ISO27kLA, ISO31kLA
APIT Consultoria de Informatica Ltd., Brazil, Director

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP
USA, Director

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, FACS CP
BRM Holdich, Australia, Director

Tichaona Zororo
CISA, CISM, CGEIT, CRISC, CIA, CRMA
EGIT | Enterprise Governance (Pty) Ltd., South Africa, Director

Zubin Chagpar
CISA, CISM, PMP
Amazon Web Services, UK, Director

Rajaramiyer Venketaramani Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India, Director

Jeff Spivey
CRISC, CPP
Security Risk Management, Inc., USA, Director

Robert E Stroud
CGEIT, CRISC
Forrester Research, USA, Past Chair

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA
Queensland Government, Australia, Past Chair

Greg Grocholski
CISA, SABIC
Saudi Arabia, Past Chair

Matt Loeb
CGEIT, FASAE, CAE
ISACA, USA, Director