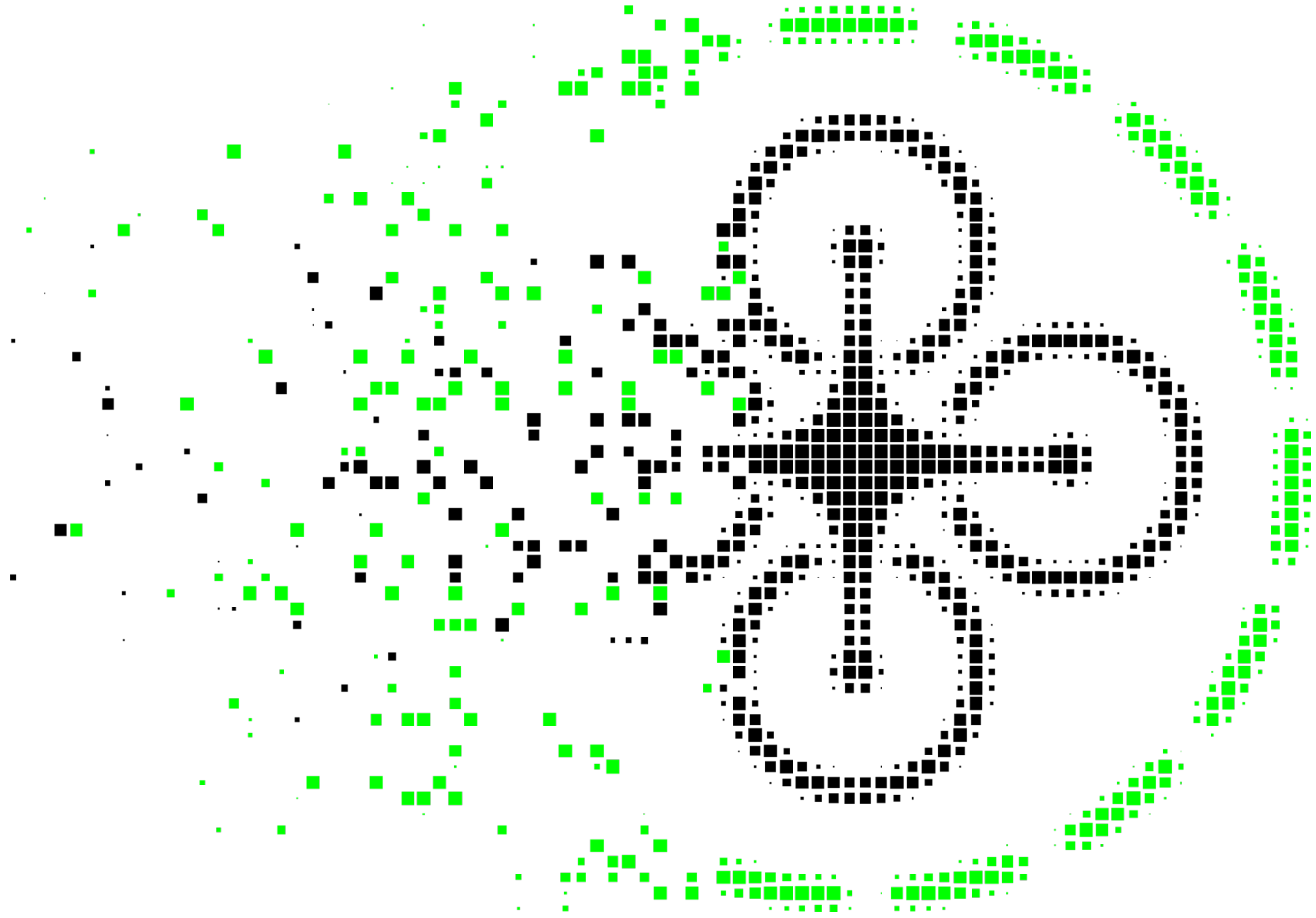
Deloitte.



Unmanned Aircraft Systems (UAS) Risk Management:

Thriving Amid Emerging Threats and Opportunities

November 2018

Introduction 3
Understanding UAS Risk 4
New Risk Realities 6
Understanding Risk Management 9
Assessing UAS Risk & Tailoring UAS Risk Solutions 10
Conclusion 11
For More Information 12
Appendix: Examining the UAS Ecosystem 13

Introduction

On Friday, January 23, 2015 at 3pm, Dubai International Airport (DXB) suspended all air traffic. No hijacking had occurred; no active shooter had been reported; no car bomb had detonated. Instead, the recreational activities of drone enthusiasts had halted operations at the third busiest airport in the world. DXB remained on lockdown for the next 55 minutes while authorities worked to ensure that drones had been removed from the airspace surrounding the airport. The incident cost the United Arab Emirates' economy over $55 million USD over the 55-minute period, as recreational drone interference brought air traffic to a standstill.[1] Since then, drone incidents have continued to disrupt airport and airline operations across the globe, costing commercial and government entities millions of dollars.[2] This incident, and dozens of similar ones in other domains, raise challenging questions around our level of readiness to meet the risk management demands of this rapidly advancing technology.

Drones, also referred to as unmanned aircraft systems (UAS), encompass the unmanned aerial vehicle (UAV) itself, the ground-based controller, and the system connecting the two, thus giving rise to a whole new ecosystem comprising manufacturers, operators, software and service providers, and data analytics purveyors. Like most fast-moving trends, this one is fueled by technological advances, policy changes, and significant cost reduction in parts and manufacturing. Innovative UAS applications are already disrupting a variety of industries from search and rescue to surveying, much of it toward the greater good. However, the DXB example referenced above illustrates how UAS can also create threats to safety and security.

As the UAS ecosystem evolves, risk management professionals in every organization—from large commercial firms and non-profit universities to federal, state, and local governments—face uncertainty in how to realize the benefits of UAS innovation while mitigating UAS risk across the tactical, operational, and policy levels. By identifying and understanding risk factors and institutional capabilities, organizations are not only able to assess, manage, and mitigate risk, but they can also anticipate it, looking for indicators, warnings, and opportunities that will shape the evolving UAS risk environment. Whether for commercial UAS adopters or government entities charged with creating and enforcing UAS regulations, risk-intelligent decision-making can provide a framework to understand UAS risk and optimize the return on UAS integration through an analytically-driven methodology.

This paper places UAS risk and its associated mitigation strategies in the broader context of the UAS ecosystem. First, we will explore the sources of UAS risk; second, we will examine new risk realities presented by UAS; third, we will conclude by offering techniques for organizations to develop risk-intelligent strategies to proactively assess, understand, and mitigate UAS risk to maximize the value created by UAS integration.

1 "Recreational drones bring Dubai airport traffic to a halt," The National, January 23, 2015.
2 See Transportation Safety Board of Canada, Air Transportation Safety Investigation Report A17Q0162 IN-FLIGHT COLLISION WITH DRONE, October 2017; "Drone causes Gatwick Airport disruption," BBC, July 2017; "Drone in near miss with plane near Edinburgh Airport," BBC, May 2017.

Understanding UAS Risk

UAS operations are projected to increase significantly over the coming years, driving a corresponding increase in UAS risk. Organizations should identify, assess, and prioritize the various forms of physical and non-physical UAS risk.

The growth and rapid development of UAS can be attributed to increased interest in harnessing the technology from commercial operators and hobbyists alike. The FAA estimates that from 2016-2021, the number of domestic commercially-owned small UAVs could grow ten-fold from 42,000 to 420,000. This includes all UAS owned by companies, government, and non-profit organizations. The growth in commercially-owned UAS parallels similar growth in UAS personal ownership by hobbyists, which could grow from 1.1 million to 3.5 million over the same period. This would more than triple the total number of domestic UAS—totaling 3.92 million units—compared to 2016 levels.[3]

The dramatic rise in UAS traffic predicted over the near-term poses a challenge for individuals charged with maintaining the safety and security of their organizations. In some organizations, this individual is the Chief Risk Officer, but in many instances, this responsibility may fall to the Chief Security Officer, Director of Operations, or other individuals who may or may not have training in risk management. UAS risks range from physical—involving kinetic damage or disruptive presence from the UAS itself, or the UAS-borne introduction of explosives, biohazards, etc.—to non-physical, in which UAS capture sensitive data via a variety of sensors, threatening privacy, intellectual property, and/or operational security.

Physical UAS risk

UAS pose physical risk to organizations with assets both in the air and on the ground. Incidents in the sky are most salient. Already, the FAA's reports of drone-safety incidents, defined as flying improperly or getting too close to other aircraft, now average almost 250 a month, up more than 50% year-over-year since 2016.[4] In September 2017 a quadcopter UAS hit the side of a US Army Black Hawk helicopter, representing the first confirmed in-flight collision between a drone and a piloted aircraft in the United States. The incident cost the Army upwards of $220,000 to replace the damaged rotor blade and repair the door—though fortunately not the lives of its helicopter crew.[5] UAS may also threaten people and assets on the ground. Both legitimate and illegal UAS activities have the potential to damage or injure any assets or people that might be below an operation gone awry, especially in the nascent stages of UAS airworthiness and safety standards. Authorities struggle to deter curious hobbyists who fly over critical infrastructure, professional sporting venues, and other large gatherings, for fear of a crash that might damage assets and injure unsuspecting people or worse—an attack with explosives, biohazards, or other harmful agents.[6] Even the most secure organizations and facilities are likely vulnerable to penetration from the sky. From interfering with aircraft and breaching secure perimeters to crashing and causing wildfires, UAS have proven that their associated physical risk scenarios are limited only by the imagination—and they can affect not only the individuals and organizations that operate them, but the people, structures, and organizations in their vicinity as well.[7]

3 Federal Aviation Administration, "FAA Aerospace Forecast, Fiscal Years 2017-2037," TC17-002, 2017.
4 Federal Aviation Administration, "Request for Emergency Processing of Collection of Information by the Office of Management and Budget; Emergency Clearance To revise Information Collection 2120-0768, Part 107 Authorizations and Waivers," 2017-21878, October 11, 2017.
5 Tim Wright, "Army Blackhawk Collides with Drone Over NYC," Air & Space Magazine, September 27, 2017.
6 CBS/Associated Press, "FAA criminalizes flying drones near certain locations," CBS News, October 29, 2014.
7 Trevor Mogg, "A consumer drone crashed and burned, and then caused a wildfire," Digital Trends, March 12, 2018.

Non-physical UAS risk

UAS risks to privacy, intellectual property, and operational security are similarly broad. Risk management professionals must consider how to protect their organizations from unwanted data collection by outsider UAS, as UAS-borne platforms and sensors become increasingly sophisticated and attainable. Foreign governments, competitors, criminal organizations, and other non-state actors regularly engage in information gathering and corporate espionage. From capturing sensitive documents, meetings, and research & development activities to tracking movement of key personnel and materiel, drones represent yet another threat vector to mitigate. Drones are even marrying physical risk to cyber risk—by landing on the roof of a target building, for example, drones can provide the physical proximity necessary to collect sensitive information, exploit cyber vulnerabilities, and conduct a wide range of cyber attacks to devastating effect.[8]

Risk management professionals must also consider the information security risk posed by their own organization's UAS operations, if applicable. Data collected from UAS operations may be particularly sensitive, and must be appropriately managed and secured from cyber risk and supply chain risk, especially for hardware and software manufactured abroad or data sent to foreign servers. Data collected from legitimate UAS operations present legal and regulatory risk as well. Privacy advocates and watchdog groups are concerned by the collection, use, and protection of data collected by UAS, and the regulatory framework is beginning to catch up—especially in Europe.[9] Data spills and misuse will be costly. Comprehensive UAS risk management spans both risk to data and risk from data.

Regulatory trends affecting UAS risk

The existing regulatory framework is not equipped to handle the myriad questions that stem from the rapid proliferation of UAS operations. FAA, DHS, state and local governments, and other government stakeholders are working to integrate UAS into the national airspace while weighing safety, security, privacy, and a host of other concerns. In 2017 alone, the FAA went from maintaining a UAS registration database,[10] to this requirement being struck down in court, to its being reinstated.[11] The FAA Reauthorization Act of 2018, signed into law on October 5, 2018, includes many key provisions needed for UAS integration, from receiving the authority to impose remote tracking and identification requirements to establishing a process for developing risk-based, consensus-driven industry standards for airworthiness certification.[12] In addition, the law authorizes DHS and DOJ to mitigate UAS that threaten public safety, but the capabilities and processes to safely do so—especially in the complicated interagency environment—are far from certain.[13] Translating this new legislation into actionable policies will require significant resources from the policy-setting community, and will have a major impact on the rest of the UAS ecosystem.[14]

Meanwhile, UAS continue to grow in both number and capabilities. UAS technology is advancing rapidly, allowing for features such as sophisticated cameras, sensors, and remote, pre-programmed, or autonomous flight control beyond visual line of sight that can take dynamic variables and objectives into account. As these capabilities evolve, they continue to outpace not only government regulation, but also user training programs and user knowledge. This broadens the spectrum of risk from commercial users, hobbyists, and nefarious actors, whether accidental or intentional, thereby increasing risk to organizations.

8 Patrick Howell O'Neill, "Drones emerge as new dimension in cyberwar," Cyberscoop, February 5, 2018.
9 Colin Snow and Charlotte Ziems, "Commercial Drones and GDPR: What You Need to Know," Drone Analyst, May 18, 2018.
10 See the Federal Aviation Administration "Geographic (City, State, Zip) Listing of sUAS Registry Enrollments and Registrants" at the following link: https://www.faa.gov/foia/electronic_reading_room/#geo_list.
11 April Glaser, "Americans no longer have to register non-commercial drones with the FAA," Recode, May 19, 2017; Ben Popper, "New law reinstates small drone registration in the US," The Verge, December 12, 2017.
12 For more information, see H.R. 302 – FAA Reauthorization Act of 2018, Congress.gov, https://www.congress.gov/bill/115th-congress/house-bill/302?q=%7B%22search%22%3A%5B%22FAA+Reauthorization+Act+of+2018%2 2%5D%7D&r=3
13 Betsy Lilian, "Drone Groups Give Blessing to FAA Reauthorization, Now OK'd by Congress," Unmanned Aerial Online, October 3, 2018.
14 US Department of Homeland Security, "Secretary Kirstjen M. Nielsen Statement on Passage of Legislation to Counter Dangerous Unmanned Aerial Systems," October 3, 2018

New Risk Realities

UAS present new risks to critical infrastructure and assets from both malicious and unintentional actors.

As entities both adopt and defend against this evolving and emerging technology, the increasing presence of UAS creates a broad array of never-before-seen risk realities, or scenarios, that can affect and damage physical assets, personnel, operations, and intellectual property. Existing access control measures are designed to detect and prevent unapproved ground-based and cyber-based access; almost none are designed to prevent unapproved aerial-based access. These scenarios can be carried out either by malicious actors intending to cause harm via UAS, or UAS users who are not following approved guidelines and have not applied ORM principles as best practices for aviation safety. These unintentional actors may operate within restricted areas, including those employed by the entity itself to leverage UAS for its own operations. Stakeholders in government, commercial, and non-profit sectors should acknowledge these risks and determine how to confront and shape them.

The UAS Risk Scenarios Matrix below (Figure 1) connects plausible scenarios to the sectors most likely to be impacted and the potential threat actor—a UAS user who either maliciously or unintentionally introduces risk in each scenario.

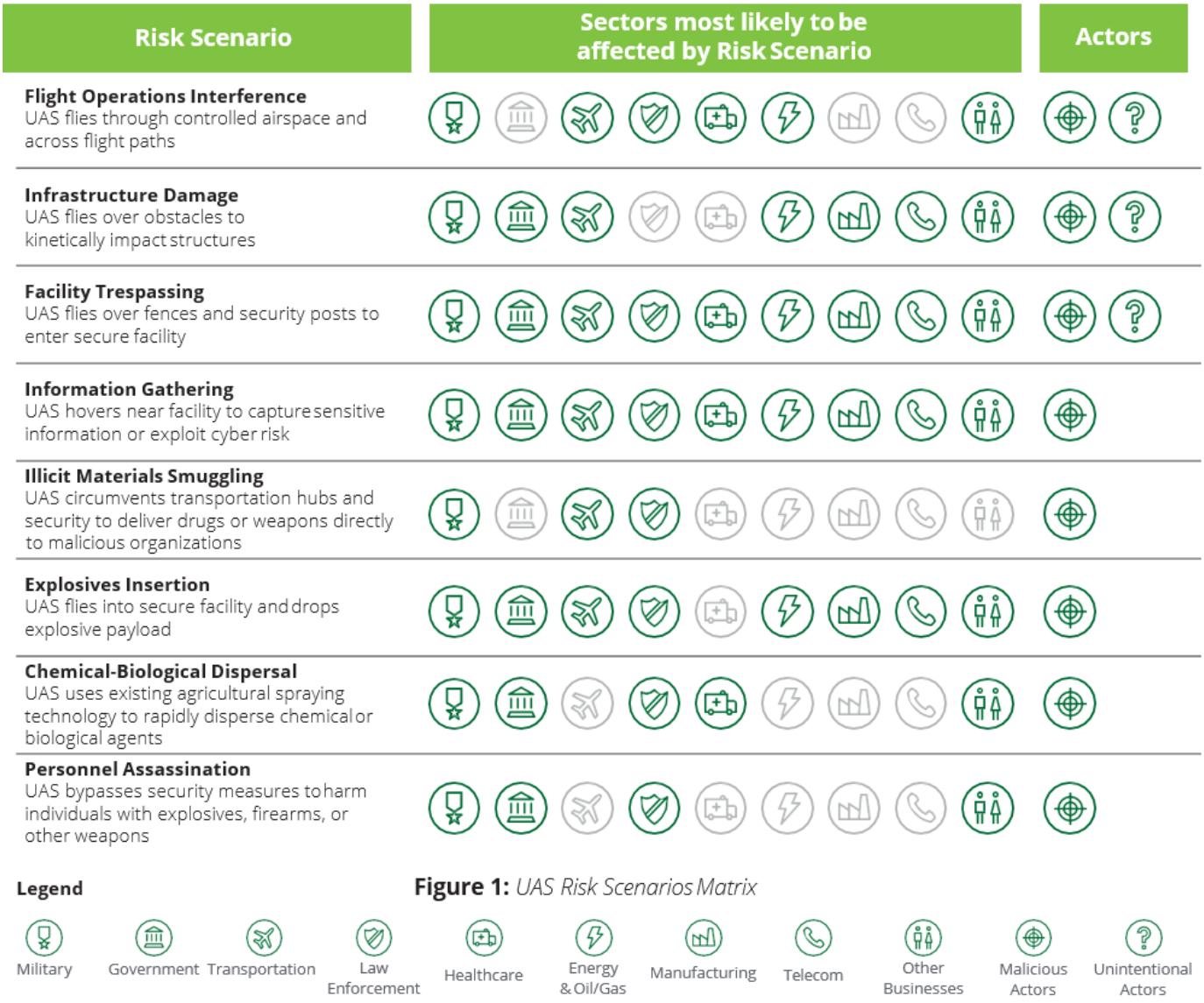


Figure 1: *UAS Risk Scenarios Matrix*

Each organization should consider which scenarios are most threatening in the short-term and long-term, as well as how current risk management protocols perform against them. For example, barriers and fences that are traditionally designed to prevent unapproved off-road access are capable of being circumvented by UAS flying over fence lines to kinetically impact structures. One example includes unauthorized surveillance and delivery by UAS where a malicious actor operating outside the law used UAS to drop a package containing heroin, marijuana, and tobacco over an Ohio prison yard, effectively functioning as a drug mule.[15] Another poignant example of malicious actor exploitation occurred in Venezuela in 2018, when UAS armed with explosives targeted the president of the country.[16] Additionally, while private companies and government organizations may employ security personnel, employee vetting to guard against insider threats, and network defense solutions, the ability of UAS to hover near buildings presents a challenge for stakeholders aiming to protect sensitive information, since this technology is often designed to capture video, photographs, or other data, even through a building's windows.

These risk scenarios have the potential to significantly impact the daily operations of entities. UAS are unique in the risk management space due to the combination of a relatively low cost of purchase, high-tech capabilities, and the ability to overcome aerial barriers with ease. On top of these outsider risks, an entity may pose a risk to itself as it takes advantage of opportunities to employ UAS for its own operations. Risk management professionals should implement a comprehensive risk management framework to prepare for, influence, and act upon UAS risk from both inside and outside their organization.

15 Lorenzo Ferrigno, "Ohio prison yard free-for-all after drone drops drugs," CNN, August 5, 2015.
16 Ana Vanessa Herrero, "Venezuelan President Targeted by Drone Attack, Officials Say," New York Times, August 4, 2018.

Understanding Risk Management

Before an organization can develop a UAS risk management strategy, it should consider the principles that define a risk-intelligent framework.

Deloitte's risk management philosophy—Risk Intelligence (RI)—is about striking the right balance between risk and reward.[17] At a high level, it involves identifying, assessing, and prioritizing potential risks against an organization's risk tolerance, and creating risk mitigation strategies that are continually monitored and updated in accordance with the evolving risk environment.

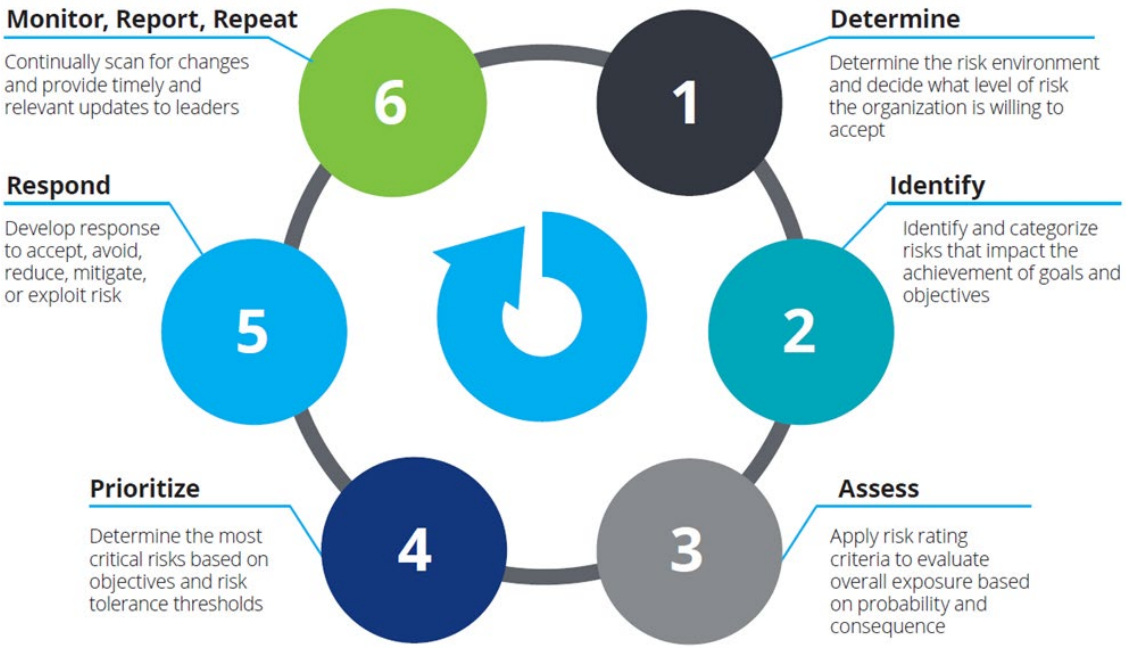


Figure 2: *Risk Management Process*

Similarly, the Federal Aviation Administration (FAA) System Safety Handbook offers the FAA perspective on Operational Risk Management (ORM), which is "a decision-making tool to systematically help identify operational risks and benefits and determine the best courses of action for any given situation"[18] that it instructs all pilots to apply prior to flight. ORM defines risk as "the probability and severity of accident or loss from exposure to various hazards, including injury to people and loss of resources." It goes on to say that risk management is "pre-emptive, rather than reactive."[19] Understanding risk management as proactive, analytically-driven, and rooted in strategy will be critical to leveraging it for UAS integration.

17 For more information regarding the risk-intelligent enterprise, see Deloitte's Enterprise Risk Management: A Risk-Intelligence Approach, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-erm-a-risk-intelligent-approach.pdf.
18 Federal Aviation Administration System Safety Handbook, "Chapter 15: Operational Risk Management," 2000.
19 Ibid.

Assessing UAS Risk & Tailoring UAS Risk Solutions

Emerging UAS technology creates the need for customizable solutions to proactively mitigate risk and realize the reward of UAS integration.

As emerging UAS technology creates new and startling risk scenarios, risk managers can methodically assess the impact that UAS will have on their enterprise. A UAS Risk Solution Development framework (see Figure 3, below) can provide a foundation for incorporating UAS into an organization's broader risk management portfolio in a risk-intelligent manner. The solutions described below are not meant to serve as an exhaustive list, but rather describe some of the most applicable UAS risk management solutions for a broad range of sectors.

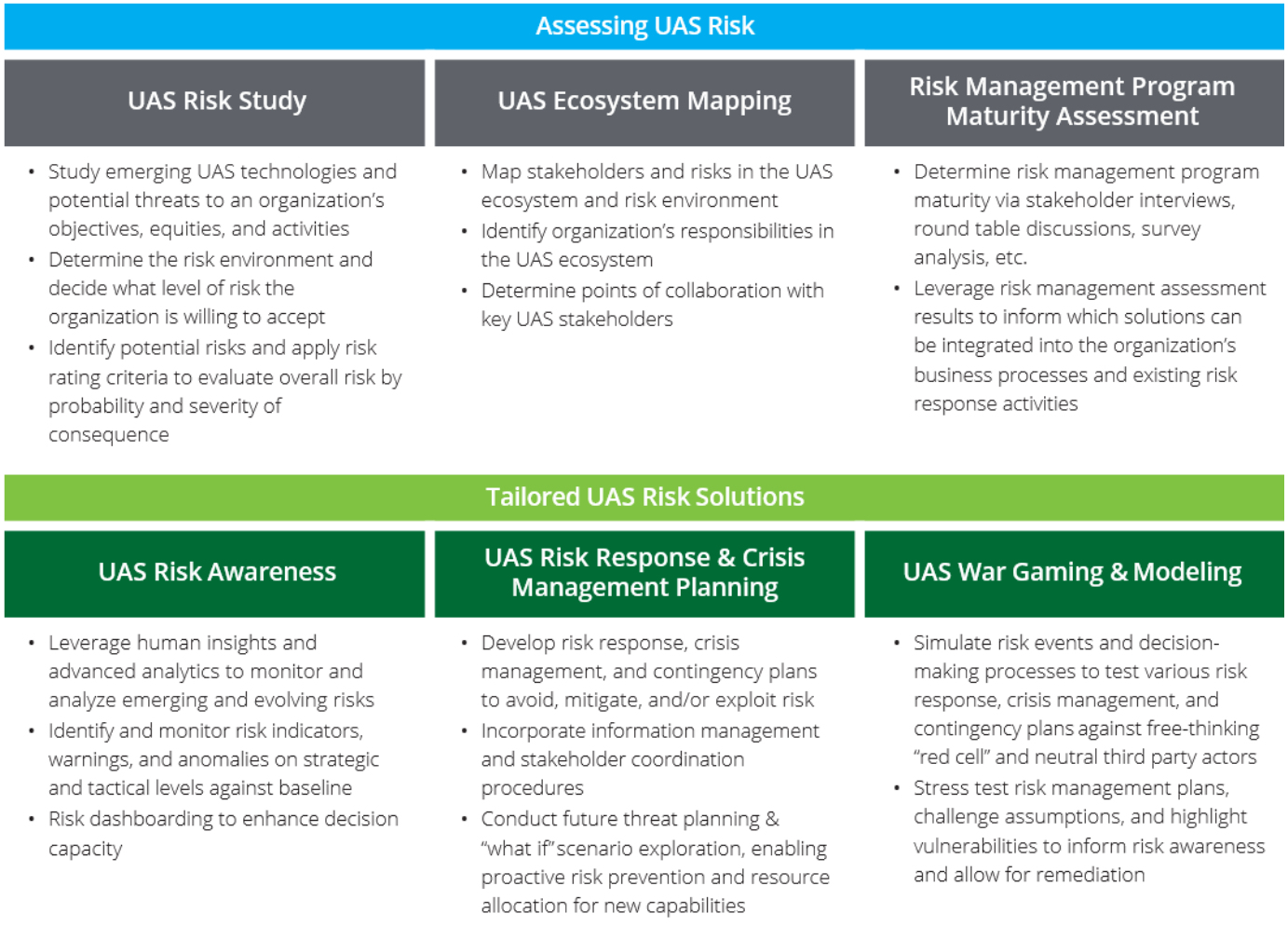


Figure 3: *UAS Risk Solution Development Framework*

Conclusion

The impact of UAS risk

As UAS proliferation continues, risk management professionals tasked with managing the safety and security of their organization's assets and personnel will face an increasingly complex risk environment. Opportunity and risk from UAS—both physical and non-physical—will continue to grow.

Given the pace of UAS innovation and disruption, it will be more important than ever for risk management professionals to develop a strong risk management framework that balances UAS risk and reward in a risk-intelligent manner. However, the responsibility to understand and mitigate risk extends beyond a single agency or entity—it requires an ecosystem approach. A collective effort is needed to support the adoption of this new technology, accounting for emerging and future UAS applications, implications, and risks. From countering unwanted data collection to mitigating physical risk to critical infrastructure, organizations should develop strategies to identify, assess, prioritize, and mitigate risk in accordance with their risk tolerance. But they must do so as part of the larger UAS ecosystem, understanding that their success—or failure—will impact the broader UAS industry.

UAS adoption, proliferation, and evolution have the potential to result in mishaps and risk to people, property, and infrastructure. Commercial, government, and non-profit entities will need to prepare for, respond to, and learn from these incidents—thereby impacting the shape of the overall UAS ecosystem. While risk management practices, methodologies, and processes are not new, UAS technology presents a unique challenge in terms of risk. Industry, academia, and government agencies need an integrated and collaborative approach to fully understand the existing and emerging risk landscape to identify and develop effective risk mitigation and response measures, both for their own UAS operations and outsider UAS operations in their vicinity.

The responsibility to understand and mitigate risk extends beyond a single agency or entity—it requires an ecosystem approach. A collective effort is needed to support the adoption of this new technology, accounting for emerging and future UAS applications, implications, and risks.

For more information

Please Contact:

Peter Liu
Program Managing Director
Deloitte US Drone Services
Deloitte Consulting LLP
peteliu@deloitte.com

Chris Hewlett
Program Leader
Deloitte US Drone Services
Deloitte Consulting LLP
chewlett@deloitte.com

Sevan Mehrabian
Government Market Leader
Deloitte US Drone Services
Deloitte Consulting LLP
smehrabian@deloitte.com

Mat Rommel
Commercial Market Leader
Deloitte US Drone Services
Deloitte Consulting LLP
mrommel@deloitte.com

Nick Buck
Solutions Leader
Deloitte US Drone Services
Deloitte Consulting LLP
nibuck@deloitte.com

Brad Davidson
Counter-UAS Leader
Deloitte US Drone Services
Deloitte Consulting LLP
bradavidson@deloitte.com

Contributors:

Claire Porté
Consultant
Deloitte Consulting LLP

Nicholas Bellomy
Manager
Deloitte Consulting LLP

Elton Parker
Specialist Leader
Deloitte & Touche LLP

Alexa Monti
Senior Consultant
Deloitte Consulting LLP

The authors would like to acknowledge the contributions of Bill Eggers, Joe Mariani, and Felix Martinez of Deloitte Services LP; David Schatsky of Deloitte LLP; Matt Gentile of Deloitte & Touche LLP; Bill Miracky, Robert Krawiec, Alex Mirkow, Elizabeth Nelson, Anton Attard, Christos Pissios, Walter Jones, and Drew Tucker of Deloitte Consulting LLP.

Appendix

Examining the UAS ecosystem

Rapid technological evolution, policy advances, and significant retail cost reduction have all contributed to the emergence of a global market for UAS products and services. This market exhibits the characteristics of a dynamic business ecosystem: a diverse and ever-expanding group of stakeholder entities—from individual hobbyists, commercial businesses, and academic institutions to government agencies and non-profit organizations—that interact, collaborate, and compete to create value under the umbrella of UAS integration. Figure 4 groups UAS stakeholders into various communities and describes the value they create.

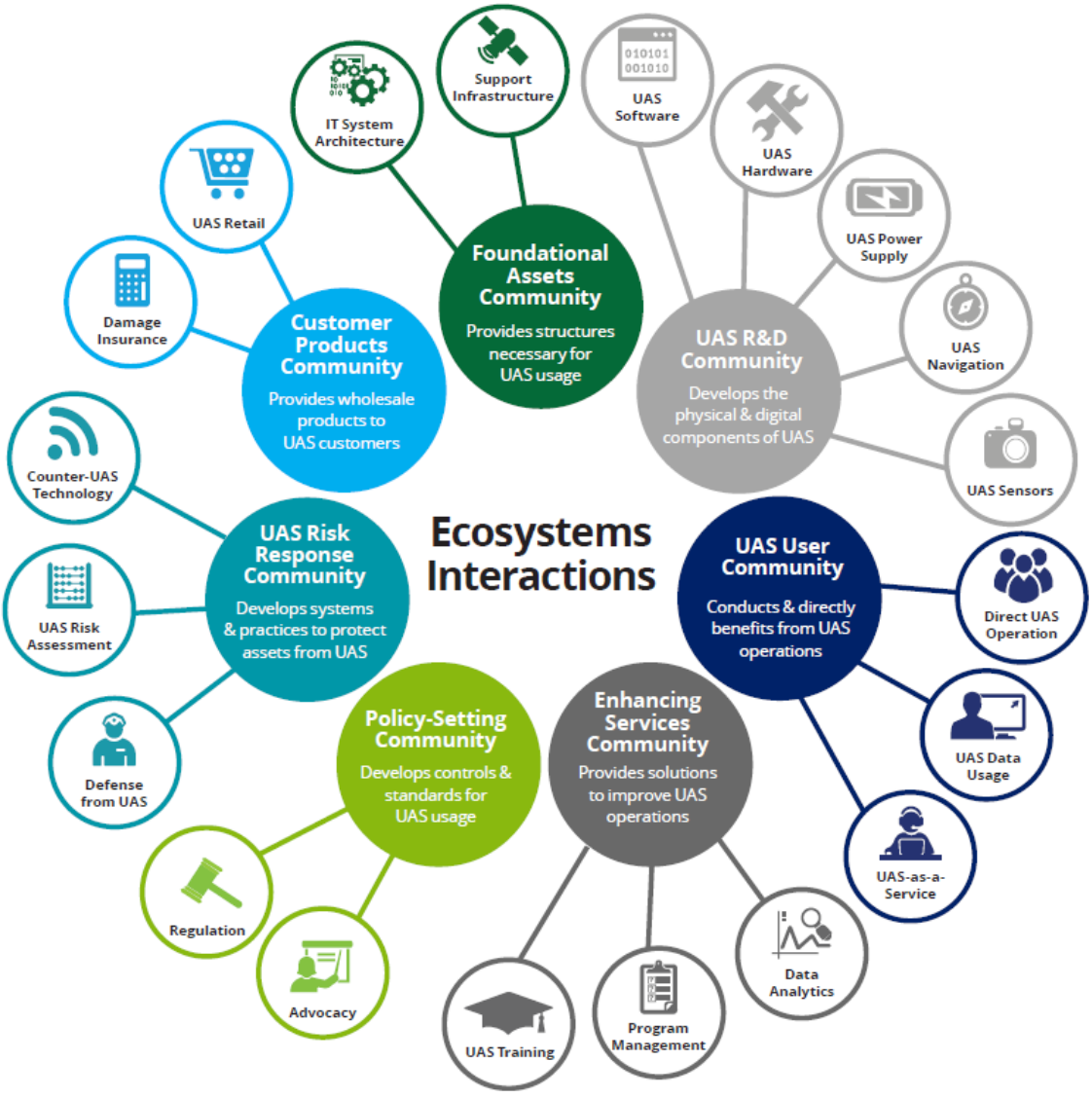


Figure 4: *UAS Ecosystem*

The current UAS Ecosystem's seven major communities are:

- **UAS R&D Community:** This group serves as the traditional core and original 'product creator' of the UAS ecosystem. Entities within this community are focused on the research, design, development, and manufacturing of UAS components. These organizations often lead innovation in UAS power supply systems, navigation systems, data-collecting sensors, and software. This community covers a broad diversity of entities, from large multinational UAS corporations and government laboratories to small hobbyist developers and non-profit educational organizations.

- **Foundational Assets Community:** Entities within this community provide the basic physical and digital infrastructure necessary for UAS operations. This includes government operators and owners of the Global Positioning System (GPS) constellation, which enables UAS GPS-based navigation. Major information technology companies also participate in this community by providing the system architecture through which UAS data is collected, analyzed, and stored. Unlike the other communities in the ecosystem, most entities in the Foundational Assets Community only support UAS as a tangential outcome of their other non-UAS primary activities. Thus, entities in this group are the least likely to see themselves as similar to one another or even as part of the UAS ecosystem—despite the criticality of their value propositions to UAS operations.

- **UAS User Community:** This group serves as the traditional 'end user' of UAS products and services. Entities within this community operate UAS or benefit from UAS-collected data. As the largest and most diverse community in the ecosystem, the UAS User Community expands exponentially as new individuals, companies, and organizations adopt UAS technology. The newest value proposition within this community are entities that provide UAS-as-a-Service. These companies own fleets of UAS and conduct flight operations to execute projects for their businesses.

- **Enhancing Services Community:** This group of mostly commercial entities provides various solutions to help improve UAS users' operations. This includes supporting the stand-up and operation of a UAS capability via program management, developing data analytics solutions to help UAS users better understand and visualize their collected data, and providing training to help customers understand both how to fly UAS and incorporate UAS into their daily operations.

- **Policy-setting Community:** Entities within this community are responsible for influencing and developing policies, rules, and standards for UAS operations. Federal and state governments are the most visible members of this community, but have been joined by advocacy groups. These new entities look to leverage joint action among UAS users, commercial entities, or concerned constituents to influence the policy-making process.

- **UAS Risk Response Community:** This relatively new group of entities emerged to help organizations and individuals protect their assets and operations amidst the increasing global proliferation of UAS. Entities within this community assess the risks posed by UAS, develop or acquire technological solutions to degrade or defeat malicious UAS, and defend physical locations from unauthorized UAS operations. This community originally consisted predominantly of government and military entities, but has diversified as commercial entities incorporate UAS into their risk portfolios.

- **Customer Products Community:** Entities within this community offer discrete whole products to UAS customers. This includes retail companies that sell complete UAS packages. A new and growing value proposition in this community comes from companies that provide insurance coverage to UAS owners. Similar to automobile insurance, governments are increasingly requiring UAS owners to purchase insurance in order to mitigate the costs of accidents or damage to infrastructure.

Examining the UAS Risk Response Community

In response to new technologies, innovative use cases, and evolving regulations, entities within the UAS Risk Response Community are building risk mitigation frameworks and counter-UAS (C-UAS) technologies to protect assets and operations from UAS risk. UAS adopters are incorporating operational risk management techniques to limit risks to safety from legitimate UAS operations. Meanwhile, federal, state, and local governments, along with many commercial entities and private citizens, are looking toward technical and regulatory solutions to mitigate UAS risk from both malicious and unintentional actors.

Public and private sector entities are actively researching, testing, and evaluating technology to detect, identify, track, and mitigate UAS while limiting collateral damage and providing flexibility to operations in multiple mission environments. C-UAS technologies can be divided into kinetic and non-kinetic counter-measures. Kinetic counter-measures include lasers, nets, eagles, defensive drones, modified surface to air missiles, and other projectiles. Non-kinetic counter-measures consist of detection and tracking technologies, including radar, radio frequency, optical, infrared, and acoustic sensors, as well as mitigation technologies, which include jamming communication links and "spoofing" command signals to take control of a drone.

Key US government players in the UAS Risk Response Community

Development of counter-UAS technologies by public and private sector entities is occurring in tandem with efforts to define legal authorities for their deployment. While the Emerging Threats Act, signed into law as part of the FAA Reauthorization Act in October 2018, provides C-UAS authorities to the Department of Homeland Security and Department of Justice, the interactions between various government stakeholders have yet to be determined. The following is a non-exhaustive list of key US government players in the UAS Risk Response Community.

- **Department of Defense:** DOD has authority from the 2018 National Defense Authorization Act (NDAA) to counter drones that threaten certain key DOD installations.[20]
- **Department of Energy:** Given DOE's role in safeguarding nuclear facilities, materials, and technologies, the NDAA also provides authority for DOE to counter drones at sensitive nuclear sites.[21]
- **Department of Homeland Security:** DHS received authority from the Emerging Threats Act of 2018 to "mitigate a credible threat" from UAS to "the safety or security of a covered facility or asset," which include many DHS functions: U.S. Coast Guard Operations, U.S. Customs and Border Patrol operations, federal law enforcement operations, etc.[22]
- **Department of Justice:** DOJ also received authority from the Emerging Threats Act of 2018 to mitigate threats from UAS. Covered facilities or assets under DOJ include DOJ operations, federal law enforcement investigations, federal prisons, national security special events, etc.[23]
- **Federal Aviation Administration:** As part of the Department of Transportation, FAA is responsible for safely integrating UAS into the National Airspace System (NAS). FAA creates requirements and restrictions for UAS operations and may take civil enforcement actions to enforce compliance with regulations.[24]
- **State and Local Law Enforcement:** While state and local law enforcement do not yet have the authority to counter drones, they cooperate with FAA to report suspected cases of unauthorized UAS activity. State and local law enforcement are responsible for enforcing state and local drone laws, and will be indispensable partners to the FAA, DHS, DOJ, and other government entities in maintaining safety and security.[25]

Risk management in today's UAS ecosystem

Today's complex UAS ecosystem contains risk from both malicious actors—who see the threat potential of UAS and exploit them for nefarious purposes or commercial gain—and unintentional actors, who pose a hazard to safety, operations, and infrastructure. Given the evolving nature of UAS risk, members of the UAS Risk Response Community will have to partner with all members of the UAS ecosystem, especially the Policy-setting, R&D, and User Communities, to shape the industry in a way that balances risk and reward to maximize the benefits of UAS integration in a risk-intelligent manner.

---

20 National Defense Authorization Act for Fiscal Year 2018, Public Law 115–91, § 1692.
21 National Nuclear Security Administration, "NNSA deploys its first counter-unmanned aircraft system," Energy.gov, November 19, 2018; National Defense Authorization Act for Fiscal Year 2017, Public Law 114–328 § 3112, https://www.congress.gov/bill/114th-congress/senate-bill/2943/text
22 Preventing Emerging Threats Act of 2018, Public Law 115–254, § 1601- § 1603.
23 Ibid.
24 FAA Modernization and Reform Act of 2012, Public Law 112–95.
Federal Aviation Administration, "Law Enforcement Guidance for Suspected Unauthorized UAS Operations," June 5, 2017, https://www.faa.gov/uas/resources/law_enforcement/media/FAA_UAS-PO_LEA_Guidance.pdf

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.