# Stadium UAS Risk Framework

Sports venue managers need to be aware of risk assessment methodologies to detect threats, identify vulnerabilities, and reduce consequences. Information gathered through this process is extremely valuable for enhancing security measures.

Several risk assessment models exist today. As technology advances and threats evolve, your risk assessment model needs to change as well. Whichever model your organization uses, drone risks can be integrated into your security protocols easily.

Any sporting event with a mass gathering of people makes an attractive target for both unintentional and intentional drone threats. Sports venues are an attractive target for potentially catastrophic consequences. These venues also attract curious drone owners that want to capture a bird's-eye view of the event.

## Identify UAS Risk

During this step, consider these kinds of questions: “why?, what?, when?, where?, how?”

- Why would my stadium be threatened by a drone?
- What would happen if a drone hacked my sporting venue?
- When will this happen, could it happen again?
- Where are my security gaps that would allow such an attack?
- How could my stadium be impacted by drones?

Use these questions to think about event-based scenarios that could happen to your venue. Then establish how these events would impact your organization. Risk identification involves establishing three key concerns: sources of risk, areas of impact, and consequences.

### Sources of Risk

The Department of Homeland Security (DHS) Risk Lexicon, defines a threat as "a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property." Drone threats are a risk that sporting venues face. Risks impacting organizational effectiveness arise from both internal and external sources.

The risks associated with drones are mainly external. External drone threats to stadiums and sporting venues could originate from unintentional or targeted sources.

I. Unintentional: Negligent Drone Pilot

II. Targeted: Domestic/International Terrorist, Hacker, Nefarious Actor/”Lone wolf”

## Areas of Impact

Stadiums have many areas of impact to consider when identifying risks. Areas of impact to consider include: human injury, financial, infrastructural, legality concerns, and adverse effects on brand/reputation.

## Consequences

Brainstorm with a team, include various levels of employees that work in the different areas of impact. Think about all consequences - ranging from a mild inconvenience to a worst-case scenario.

**What would happen if a drone fell on or hit a fan in the stadium?**

Research on drone-human collisions is a great concern to the FAA and other government entities. Research groups are studying these events to establish if it is safe for drones to fly above people. The FAA's Alliance for System Safety of UAS through Research Excellence, or ASSURE, released a detailed study on drone crash tests and digital models of the injuries a falling drone can cause humans. Virginia Tech also researched and published quantitative data on the human injury risks associated with drones. DJI conducted a study and examined the risk of injury drones pose to humans. All found that the likelihood of injury increased proportionally with the size of drone. Larger, heavier drones are more likely to cause more severe injuries.

Virginia Tech's Institute for Critical Technology and Applied Science and its FAA-approved UAS test site teamed up to study and release quantitative data on injury risk associated with potential drone-human collisions.

The team used crash test dummies and measured impacts for different sizes and weights of drones. The study tested popular models such as the DJI Phantom (approx. 3 lbs.), DJI Inspire (approx 7 lbs.), DJI S1000 (approx 21 lbs.) and flew the drones into the dummies from different angles. One test measured a straight-line impact with the drone crashing into dummy's face. Another test measured impact from above, the drone was dropped straight down onto the dummy. Unsurprisingly the researchers observed that heavier drones caused more danger to humans than smaller drones.

SZ DJI Technology Co., the world's largest drone manufacturer, released its study arguing that drones weighing up to 4.9 pounds (2.2 kilograms) pose minimal risk to people. Researchers found that when small consumer drones made of plastic strike an object like a human head, they tend to break apart, lessening the impact and potential risk of injury.

Resources:

FAA's ASSURE: UAS Ground Collision Severity Evaluation Research
Virginia Tech's Institute for Critical Technology and Applied Science Drone-Human Collision Research

**What would happen if a drone was used to drop biological/chemical agents onto the crowd?**

This event would no doubt be devastating to fans and event personnel. It is one of the worst-case scenarios, it would have significant impacts on human health/wellness, to the organization's finances, organization's brand/reputation, and potential loss of ticket sales.

Consumer drones can be modified to carry and release a payload easily. In November of 2017, a California man modified his drone to drop leaflets over two stadiums while NFL games were taking place. Luckily the man was only releasing anti-media propaganda but it does highlight safety concerns, and it is easy to imagine a worse scenario.

The task of arming a drone to carry a chemical agent is technically possible, as seen in crop dusting use. Agricultural drones are equipped with chemical sprayers. Also chemical sprayer kits are available, these kits attach to larger drones and allow for easy drone modification.

**What would happen if a drone armed with a bomb or other deadly device attacked my venue?**

This is another worst-case scenario event that would have horrendous consequences, most likely severe injuries, casualties, and significant structural damages. The incident would impact many areas of the organization; impacts would be immediate and future-oriented.

**Are these worst-case scenarios actual risks?**

In fact, they are. In November of 2017, Homeland Security released an updated terror bulletin that highlights the threat of weaponized drones, chemical attacks and the continued targeting of commercial planes.

During the U.S. Committee on Homeland Security and Governmental Affairs, Annual Threats to The Homeland Hearing, Nicholas Rasmussen, the director of the National Counterterrorism Center, spoke to a Senate panel about the growing threat and possibility of terrorists using drones to drop explosives or even unleash biological attacks on U.S. soil. Rasmussen, also told the committee, "A year ago this was an emerging problem. Now it's a real problem."

During a security committee briefing on drone risks, FBI director remarks that terrorists have shown an interest using drone overseas and "the expectation is, it's coming here imminently." Drones are easy to acquire and operate, but they are difficult to disrupt and monitor. The FBI is

working with agencies to figure out a solution. Video can be watched on Youtube: FBI director discusses threats of terrorist drones.

To watch the entire committee hearing, click the link: Threats to the Homeland Committee Hearing Video.

Risk cannot be eliminated entirely from the environment, but with careful planning, it can be managed. Your organization may already has protocols for these types of worst-case scenario, and the same procedures can be applied whether it can the threat came from an existing perimeter breach or an above perimeter(sky) breach.

## Analyze the Level of Risk

The next step is to identify the level of risk. The level of risk can best be understood as the probability of the event occurring and the product of the consequence of an event: Risk = Probability x Consequence.

***Level of Risk = Probability x Consequence***

The assessment of probability and consequence is somewhat subjective but can be more quantitative by using data or facts collected from a range of available internal and external information.

### Probability

When determining the likelihood of an event or risk, it can seem hard to have a precise frequency. For instance, you may want to determine the frequency of drones operating near or above your stadium. First, you can ask personnel of all levels to report drone sighting and keep records of the events. This may not give you an exact number but can indicate if there is a problem, or if it's a growing concern.

Another way to determine the frequency of drone sightings is to monitor drones with drone detection technology. Reputable companies will allow you to try out or rent drone detection equipment for a trial period (30-day or 60-day trial), this will give the most accurate numbers to access the actual probability.

Probability Scale

| Level | Probability | Description |
|---|---|---|
| 4 | Very likely | Has occurred 2-3 times in the past year |

| | | |
|---|---|---|
| | (frequent) | |
| 3 | Likely (probable) | Occurred more than 4-5 times over 5 years in this organization or in other similar organizations; is known to have occurred in the past year |
| 2 | Unlikely (uncommon) | Has occurred 2 or 3 times over 10 years in this organization or similar organizations |
| 1 | Very unlikely (rare) | Has never happened in this industry |

## Consequence

Consequences will range from marginal/slight inconveniences to major/catastrophes. Determine how the events will impact different areas of your organization: will they affect human life, daily operations, information and technology, financial, etc.

### Consequence Scale

| Level | Consequence | Areas of Impact | | |
|---|---|---|---|---|
| | | Human Injury | Business Operations | Financial |
| **4** | Severe | Death; human casualties | Complete shutdown of operation; halt core operations; major revenue loss | Severe financial loss; Significant budget overrun with no capacity to adjust existing budget/resources; Ticket sales loss/ extremely low attendance numbers |
| **3** | High | Multiple severe injuries | Shutdown of key operations; service delays, revenue loss | Major financial loss; Requires significant adjustment to funded projects/programs/ business activities; Noticeable impact on ticket sales/attendance |
| **2** | Moderate | Injuries may require hospitalization | Reduced performance may result in minor revenue loss; Organization existence is not threatened | Significant financial loss; Impact may be reduced by reallocating resources: Minor impact on ticket sales |

| | | | | |
|---|---|---|---|---|
| **1** | Low | No human impact, minor injury | No impact to daily operations, Minimal impact on non-core operations. | Minor financial loss; Unlikely to impact budget or business activities; No impact on ticket sales |

## Determine Risk Mitigation

Risk mitigation involves deciding what the acceptable and unacceptable risk levels are for your organization. It also involves identifying solutions or ways to treat the risks. Unacceptable risks range in severity; some risks will require immediate treatment while others can be monitored and treated later.

For example, you may decide the probability of a drone releasing biological weapon is 'unlikely' (a score of 2) but the consequences are 'severe' (a score of 4). Using the tables and formula above, a biological drone attack therefore has a risk rating of 8 (i.e. 2 x 4 = 8).

# Risk rating table

| Risk rating | Description | Action |
|---|---|---|
| 12-16 | Severe | Needs immediate corrective action |
| 8-12 | High | Needs corrective action within 1 month; monitor risk and re-evaluate at a later date |
| 4-8 | Moderate | Needs corrective action within 3 months; monitor risk and re-evaluate at a later date |
| 1-4 | Low | Does not currently require corrective action; monitor risk |

Risks can be managed by one of four distinct methods: risk acceptance, risk avoidance, risk control (or reduction), and risk transfer (deflection).

Risk Management Strategies:

| | Definition |
|---|---|
| Risk Acceptance | An explicit or implicit decision not to take an action that would affect a particular risk. |
| Risk Avoidance | A strategy or measure which effectively removes the exposure of an organization to a risk. |
| Risk Control (or reduction) | Deliberate actions taken to reduce a risk's potential for harm or maintain the risk at an acceptable level. |
| Risk Transfer (or deflection) | Shifting some or all of the risk to another entity, asset, system, network, or geographic areas. |

Source: Homeland Security: Risk Management Fundamentals (page 23)

It is up to owners and facility/asset managers to determine what risk is acceptable and unacceptable. Severe risks that cause a high degree of loss and occur frequently should be avoided at all costs. Minor risks with a low degree of loss may be acceptable. Not all the risk strategies can be implemented easily, discuss the best course of actions for your organization with your entire team.

Risk Acceptance:
Accept all risk of the event and consequences that come with the event occurring. Regarding drone risk, you accept the risk of human injury and the impacts it comes with, which could be financial, adverse impact on reputation, legal liability.

Risk Avoidance:
How might you remove your venue from exposure to a drone causing injury or worse, attacking the stadium? For an exposed open stadium, it is impossible to remove itself from aerial threats completely. Installing a retractable roof may help. This is a very costly and time-consuming solution and doesn't address the problem of aerial threats. When the roof is open, the vulnerability remains.

Risk Control (Reduction):
Facility managers can reduce risk through staff training, preventative maintenance, and development of a risk management plan as the standard operating procedure.

Communicate with all levels of employees the risk, from seat ushers to high-level managers; everyone needs to be aware of the dangers. If a seat usher or concession worker sees a drone, they need a procedure on who to tell; they need to be able to talk to those in the chain of command as well.

Facility and security managers can access the risk, and if they determine it needs a more advanced solution, a drone detection system can integrate into existing security protocols. As stated before, reputable companies will allow you to set up drone detection systems on a trial basis before investing in an expensive system you don't need yet.

Drone threats and risk impact the whole organization not just the security team, all teams can allocate or budget money to mitigate the costs. This will control the risk while reducing the financial burdens.

Risk Transfer (Deflection):
Sometimes managers will want to transfer the risk to someone else who is willing to assume the risk. The facility manager may decide to pay an insurance company to cover physical and financial damages. This may not apply to drone threats, but if the attack were deemed a terrorist attack, the government would provide financial assistance to those impacted by terrorism.

Risk management is an ongoing process. Whether you take action now or choose to monitor the situation, facility managers must re-evaluate risks on a continuous basis. Security perimeters are not just ground entry points, security and facility managers need to consider the perimeters extending above the stadium as well.