DEDICATED TO HELPING BUSINESS ACHIEVE ITS HIGHEST GOALS.

NBAA

SECURITY RISK ASSESSMENT FOR BUSINESS AVIATION

Table of Contents

Introduction

In the post-9/11 world, aviation security has become the responsibility of individuals and organizations across the aviation industry – from ground crews and schedulers, to pilots and business leaders, to government officials. As threats and threat actors evolve, continued enhancement of corporate aviation security is a critical component to national security. Across the aviation industry, standards for safety and security have traditionally been set by large governing bodies, including the US Department of Homeland Security, Transportation Safety Administration, the Federal Aviation Administration, the National Transportation Safety Board and the International Civil Aviation Organization. For the general aviation (GA) community – and particularly business aviation – these standards must be viewed by corporate directors of aviation and security as a starting point for their aviation safety and security programs.

The National Business Aviation Association (NBAA) supports the continued adoption, implementation and enhancement of many security requirements, programs and best practices that reduce business aviation's vulnerability to terrorist threats. Risk assessments are a critical part of any organization's security process. Proper risk assessment provides security teams with the necessary data points to mitigate or accept any residual risk.

This Security Risk Assessment process, developed and produced by the NBAA Security Council specifically for business aviation professionals, provides a simple product for assessing risk in a variety of business aviation-related areas. This assessment does not require significant security training or background, making it a useful tool across any organization. The instructions and format are designed to allow users from across an organization to be effective risk assessors with minimal additional training.

This product is not designed to replace any other security procedure or process, but to serve as supporting effort to existing and growing risk assessment and mitigation processes. For questions or comments about this resource, please contact Sarah Wolf at swolf@nbaa.org.

Security Risk Assessment Process

The assessment process is intended to provide guidance for analyzing the risk levels associated with your future operations. While each organization will have different approaches to quantifying risk to company assets, which include personnel, aircraft, productivity and public image, the general methodology for evaluating the security risk level is widely applicable: Identify, assess and mitigate. For the aviation department, make sure you are aware of your company's major security risks domestically and abroad.

The user should ask the following questions:

1) Would a reasonable person in the same and similar situation come to the same conclusions?

2) Is this operation unique, or is there guidance from other sources?

3) Are the risk prevention and mitigation tools adequate for my operation?

4) Are industry best practices employed, both in the flight planning process and during the mission?

Answering these questions thoroughly requires working knowledge (within your organization or through a third-party source) of current issues and pain points in the region or country that you are traveling to. For a list of resources to help keep you abreast on political, cultural and other relevant factors on the ground where you're traveling, see Appendix 4: Additional Resources.

Ultimately, risk determination is subjective and even the most stringent mitigation process cannot guarantee 100 percent security. Under some circumstances, the operation may have to go forward regardless of risks identified beforehand. However, by following this process you are ensuring preparedness for whatever may arise during the course of the mission.

STEP 1: DETERMINE POTENTIAL RISKS

Thorough and precise evaluation of potential risk factors is paramount when assessing the overall risk level of an operation. As an example, consider the airport of arrival as the **operational component** and a specific vulnerability within that broad category, such as poor perimeter security where the aircraft will be parking, as the **risk factor** to be assessed.

For some operations, the specific region in which the operation occurs will present risks. In this case, consider location as the operational component and the potential for damages as a result of political unrest as the specific risk factor. Remember that risk is always present at some level. Additional risks may be present only when your operation arrives in the region because someone is targeting your company or a specific person.

Example: The next mission will be landing at an airport that has seen several security breaches over the last decade. As part of determining potential risks, your flight department analyzes these incidents for specific risk factors that could lead to a similar security breach while the aircraft is on the ground.

STEP 2: DETERMINE RISK PROBABILITY

The probability of an identified risk affecting your operation should be based on several factors: historical data, current circumstances, and any unique factors that may heighten risk (e.g., CEO has received credible threats). The following table provides the metrics we'll be using for this assessment.

Risk Probability Descriptors
Near Certainty – An event is extremely likely to occur
Likely – An event is more likely than not to occur
Unlikely – An event is unlikely to occur but still possible
Remote – An event is highly unlikely to occur

Probability of Operational Impact

Risk Value	Description
4	Near Certainty
3	Likely
2	Unlikely
1	Remote

Example: Based on analysis of previous incidents and current conditions on the ground, you decide there's a likely chance that the identified risk factor will have an operational impact. This is quantified as a "3" for the assessment.

STEP 3: DETERMINE RISK SEVERITY

After determining the probability of a risk impacting your operation, you will want to determine (using your company's internal methodology) the potential impact of the risk using several categories. As an example, an organization may be most concerned with the potential impact on three categories: personnel safety, asset damage and interruption to business activity.

Risk Severity	
Risk Value	**Description**
4	Catastrophic
3	Major
2	Marginal
1	Negligible

Risk Severity Descriptors

Catastrophic – Results in fatalities and/or total loss
Major – Results in severe injury and/or major damage
Marginal – Results in minor injury and/or minor damage
Negligible – Results in less than minor injury and/or damage

Example: Previous incidents at this airport resulted in operational disruption but no significant damage to asset or personnel. As such, you decide the risk severity is marginal and quantify that with a "2" for the assessment.

STEP 4: DETERMINE OVERALL RISK LEVEL

This chart provides an example of how companies may calculate overall risk level by multiplying the probability of a risk occurring with the severity that risk entails. Keep in mind when flying into certain regions with higher risk factors, such as ones with recent political, cultural or military turmoil, you may wish to factor that into the equation.

For this assessment, there are five possible levels of overall risk:

Risk Assessment Matrix				
Probability	**Severity of Potential Risk**			
	Catastrophic (4)	**Major (3)**	**Marginal (2)**	**Negligible (1)**
Near Certainty (4)	Critical (16)	Very High (12)	High (8)	Medium (4)
Likely (3)	Very High (12)	High (9)	Medium (6)	Low (3)
Unlikely (2)	High (8)	Medium (6)	Medium (4)	Low (2)
Remote (1)	Medium (4)	Low (3)	Low (2)	Low (1)

Critical (13+): This level represents an unacceptable risk. Operations at this level should STOP. This level is coded **Black**.

Very High (10-12): The highest level of potentially acceptable risk. Implementation of risk prevention and mitigation should occur immediately. Operations at this level should likely STOP. This level is coded **RED**.

High (7-9): This level is at the upper end of normal operational range. Implementation of risk prevention and mitigation should occur as soon as possible. Operations may continue at this level provided all team members are aware of the potential risk, and all team members accept the mitigated risk. This level is coded **ORANGE**.

Medium (4-6): This level is within a normal operational range. Implementation of risk prevention and mitigation should occur as soon as practical. Each team member should conduct operations at an elevated level of consciousness. This level is coded **GREEN**.

Low (1-3): This is the lowest level of risk. Implementation of risk prevention and mitigation is at its lowest achievable level. Risks can usually be addressed by following best practices. This level is coded **GREY**.

Example: Since you determined risk probability is **3** and risk severity is **2**, you calculate an overall risk level of **6 (Medium)**. For mission planning purposes, this means the airport represents a risk within normal operational range. Crew should conduct operations at an elevated level of consciousness.

Examples of Risk Assessment

Created by NBAA and its Security Council, this reference table provides a look at common risks factors and potential mitigation strategies. While this is not a comprehensive review of all the risks your operation may face, it offers examples of how your organization will want to analyze and develop mitigation strategies for potential risks.

Operational Component	Risk Factor	Risk Observations/Assessments	Risk Mitigation Methods
Airport	Lack of Airport Security	• Does the aircraft parking area have adequate lighting, and have you verified the lighting is operational? • Is the entire facility surrounded by a fence of sufficient height and design? Is the fence inspected regularly? • What kind of access control is in place at the FBO/GA area? Are entry points manned or unmanned? • Are the airport and GA areas open 24/7 and how busy are the areas? • What is the FAA IASA security rating for the location and what concerns are stipulated, if any? • Is there an active security committee and a written security plan for the airport?	• Security Contractors • Internal Aircraft Storage • Airport Analysis/Audit • Reposition Aircraft • Alternate ARR/DEP Times • External Aircraft Locks and Equipment
Aircraft	Unattended Aircraft (Overnight)	• Same as above	• Airport Lights • 24/7 FBO Operations • Ramp Security • Aircraft Locks
ATC	Aircraft Intercept Over Foreign Airspace	• Has the crew been trained and made aware of the procedures to follow?	• ATC Emergency Communication and Contacts • Pre-Trip Crew Briefing • Flight Following Procedures • Embassies and Consulates
ATC	DCA Access	• Is the crew DCA trained and licensed? • Is an armed and licensed armed security officer (compliant with regulations) available for the flight?	• DCA Access Training • Briefing • Checklist Usage • Contingency Planning and Gateways • Armed Service Officer Briefing • Firearm Knowledge
Country	Civil/Political Unrest	• Have passengers received and read through a pre-trip intelligence briefing? • Have any ongoing or potential protests or demonstrations been reported that could coincide with the trip? • Are there any upcoming dates of significance that could trigger unrest? • Are the itinerary and travel schedule planned to avoid any known demonstrations or other potential targets for unrest, such as government or police stations?	• Regional Awareness • Security Contractors • Emergency Response Plan • Cultural Awareness Training • Regional Security Contacts • Contingency Planning

Operational Component	Risk Factor	Risk Observations/Assessments	Risk Mitigation Methods
Crew	Overnight in Foreign Country	• Are your passport and essentials on your person at all times? • Are you familiar with the broad outline of the city and major landmark locations? • Have you checked for any local customs/cultural highlights you should be aware of at both business and tourist levels? • Do you have emergency communications and contingencies planned? • Do you know where other team members are located? • Have you contacted your Embassy/Consulate?	• Cultural Awareness Training • Crew Pairing • Scheduled Crew Check-Ins • Pre-Trip Crew Briefing • Embassy/Consulate Contacts • STEP Registration
Crew	Incapacitated/ Missing Crew	• Do you know where the nearest quality emergency room is located and is it open 24/7? • Do the staff speak English if international? • Does your insurance provide coverage at this location? • Do you know who to contact within your organization in case of injured/missing crew? • Did you register with State Dept's STEP program before departing? • Who is your company contact in case of emergency? • Have you contacted your Embassy/Consulate?	• Cultural Awareness Training • Contingency Planning • Language Fluency • Criminal Activity Awareness Training
Crew	Natural Disaster/ Emergency	• Who is your company contact in case of emergency? • Do you know where all of your team is supposed to be? • Do you have an assigned rendezvous point in case communications are out? • Do you know how to reach or contact your Embassy/Consulate? • Can the crew get to the airport safely to secure the aircraft?	• Emergency Response Plan • Communication • Regional Disaster Awareness Training
Crew	Identification as Crew Members	• Do you have guidelines for traveling safely in higher threat/crime locations? • Have you considered securing ID and name badges or flight charts out of sight? • Are you able/permitted to change or use casual outerwear to cover uniforms when outside the airport? • Have you secured jewelry, watches and other valuables out of sight before leaving the airport, or preferably before leaving home?	• Limit Use of Personal Identification • Secure Valuables • Cultural Blending and Customs • Apparel
Crew	Complacency	• Do you have a checklist for pre-trip planning? • How/when are security and safety addressed in the pre-planning effort? • Has the crew been provided an overview (intelligence briefing) of conditions and basic travel knowledge of the destinations involved? • Do you have a means to get incident alerts during a trip that could impact safety/security?	• Flight Planning Providers • Advocacy Groups • Intelligence Briefings • International NOTAMS • Proactive Outreach to Embassy/ Consulate

Operational Component	Risk Factor	Risk Observations/Assessments	Risk Mitigation Methods
Crew	Uncontrolled Baggage	• How is luggage handled within the airport perimeter? • Is luggage screened and secured within the airport grounds prior to loading? • Do you have a reliable bag identification and retrieval process in place? • Does the airport have the necessary equipment to screen baggage prior to getting it on the aircraft? (X-ray machines, body scanning, dogs, etc.)	• HAZMAT Awareness Training • Positive Bag Identification Control • Controlled Loading • Baggage Screening/Monitoring • Passenger Luggage Briefing
FBO	Catering	• Does the catering provider have on-site food preparation? • What is the reputation of the caterer? • Does the caterer use locally sourced food/ingredients? • Does the caterer have required local licensing and certifications and are they posted and available?	• Tamper-Proof Containers/ Equipment • Food Handling Training • Catering Control Measures • Vetting Caterers
FBO	Ramp Control	• Are any overt signs of security ramp challenges known or detected? • Do private vehicles have access to the ramp? • How is ramp access controlled/monitored? • Are badges visible? Proper badge security enforced? • Is access to active ramp areas controlled by card? • Is there a security plan in place for the FBO?	• Security Identification Display Area Badging • Dedicated Security Personnel • Airport Watch Program
IT	Cybersecurity	• Have the passengers been briefed on essentials of cybersecurity? • Have passengers been trained on password security best practices? • Have specific concerns with high-risk destinations (e.g., China, Russia) been addressed? • Do you have a company policy addressing cybersecurity and use of electronic devices? • What methods are in place for passengers to reduce risk in connecting to an unknown internet source? • Have aircraft systems been evaluated for vulnerability to cyber attacks?	• Cybersecurity Training • Hardware Protective Devices • Security Protocols • Software Vetting and Encryption • Strong Passwords
Lodging	Hotel Accommodations	• Have you reviewed hotel location and access to main roads? Is it possible to get in/out easily? • Does the hotel have cleared access to and within stairwells, as well as unblocked emergency exit doors? • Are the common areas organized and cleared of clutter and people during normal operations? • Are sprinkler systems visible and fire extinguishers present in common areas, hallways, rooms, etc.? • Is the front desk staffed 24/7 and are the staff visible and reachable by phone? • Does hotel have restricted access after-hours? If so, does this restricted access include outer doors and elevators? • Does hotel offer necessary amenities to limit need for additional travel?	• Room Security Awareness Training • Personal Security Measures • Establish Crew Communication Plan • Awareness Briefing • Contingency Plan • Crew Amenities Available at Hotel

Operational Component	Risk Factor	Risk Observations/Assessments	Risk Mitigation Methods
Lodging	Room Access	• Does each room have a visible and clearly marked emergency exit plan? • Were you supplied with properly working keys? • Does the hotel have audit capability on door readers if needed for post-incident assessment? • Does each room have multiple door latches/ bolts? • Is the room's door or windows/porch accessible from the ground or any nearby structures? • Do the front desk personnel engage in proper etiquette/confidentiality of room numbers?	• Awareness Training • Case Studies • Embassy/Consulate Contacts • Contingency Planning
Maintenance	Third-Party Vendors	• Do primary and secondary vendors have insurance/licensing to support risks from third-party vendors? • To what standards are all elements of the vendor chain held responsible? • Are regular checks/inspections carried out including background checks of personnel with access to the aircraft and sterile area? • How often, if ever, are the vendors audited for performance and service level? • Are "secret shopper"-type inspections conducted for each vendor?	• Assigned Duties • Packaging Awareness Training • Material Safety Data Sheet Training and Safety Equipment
Scheduling & Dispatching	Demonstrations/ Special Events/ Holidays	• Have you checked your itinerary against possible conflicts like holidays, parades, demonstrations, sporting events or other local events?	• Pre-Trip Crew Briefing • Alternate Accommodations • Contingency Plan • Emergency Response Plan
Transport	General Ground Transportation	• Are details about vehicle and driver provided in advance? Are these details visually confirmed onsite before getting in the vehicle? • Does the driver ask for your photo identification to confirm identity of his passenger(s)? • Are you monitoring driver distractions and checking that the driver is following direct routes (using GPS)? • Have you ensured rear door child locks are disengaged before entering the vehicle? • Are you keeping your luggage/valuables in active sight and secured? • Have you ensured driver knows your itinerary in advance, preferably when booking?	• Vetting Contractors • Confirm Positive ID of Driver and Vehicle • Routing Best Practices • Establish Emergency Contacts and Contact with Embassy

Appendix 1: Security Risk Assessment Worksheet

Based on the process detailed in the Security Risk Assessment for Business Aviation resource, this worksheet offers a simple on-the-go tool for gauging potential security risks. As you plan your mission, use the charts below to guide your thought process as you analyze risks to the operation. Additional worksheet pages are available at nbaa.org/security.

Formula for Computing Risk Level of an Operational Component

1. Determine risk probability

Based on historical trends and current factors, find the probability closest to your analysis on this chart and use that number for your calculations.

Probability of Operational Impact	
Risk Value	Description
4	Near Certainty
3	Likely
2	Unlikely
1	Remote

2. Determine risk severity

Based on your organization's assets and operational needs, find the risk description that best matches your internal data and use that number for your calculations.

Risk Severity	
Risk Value	Description
4	Catastrophic (Results in fatalities and/or total loss)
3	Major (Results in severe injury and/or major damage)
2	Marginal (Results in minor injury and/or minor damage)
1	Negligible (Results in less than minor injury and/or damage)

3. Determine overall risk level

Multiply both numbers together to arrive at the overall risk level for this operational component. Combine this with your organization's tolerance for risk to determine if mitigation methods are needed.

Risk Assessment Matrix				
Probability	Severity of Potential Risk			
	Catastrophic (4)	Major (3)	Marginal (2)	Negligible (1)
Near Certainty (4)	Critical (16)	Very High (12)	High (8)	Medium (4)
Likely (3)	Very High (12)	High (9)	Medium (6)	Low (3)
Unlikely (2)	High (8)	Medium (6)	Medium (4)	Low (2)
Remote (1)	Medium (4)	Low (3)	Low (2)	Low (1)

Operational Component	Specific Risk	Risk Severity	Risk Probability	Risk Rating (Combined)	Risk Observations/Assessments

Appendix 2: Security Risk Assessment Case Study #1

International Airport Example

This airport is the primary international airport in the country. Built for military purposes originally, this airport hosts approximately 20 million passengers a year. The airport itself as well as the surrounding perimeter has very tight security and is one of the safest airports to operate into and out of in the world. Border police soldiers accompany uniformed and ununiformed security officers.

There is a high level of threat severity. There is a higher risk of terrorist attacks in urban areas of this country. The city this airport is located in, like most cities around the world is, for the most part, a safe area to travel to and be in. Areas of random violence and conflict continue to provide threat of civil unrest, however.

The crew will be housed at a worldwide hotel chain, between the city and the airport. All crew members will be at the same hotel. Transportation from the airport to the hotel is provided by a vetted operator through coordination with the FBO. The crew will only be staying at the hotel for one night, and will not have sufficient time for personal exploration of the local area.

Operational Security Risk Assessment					
Operational Component	**Specific Risk**	**Risk Severity**	**Risk Probability**	**Risk Rating (Combined)**	**Risk Observations/Mitigations**
Aircraft	Unattended Aircraft (Overnight)	3	1	**3 (Low)**	
ATC	Aircraft Intercept Over Foreign Airspace	4	2	**8 (High)**	• ATC Emergency Communication and Contacts
Country	Civil/Political Unrest	4	2	**8 (High)**	• Regional Awareness
Crew	Overnight in Foreign Country	2	2	**4 (Medium)**	
Crew	Incapacitated/Missing Crew	4	2	**8 (High)**	• Embassy/Consulate Contacts
Crew	Natural Disaster/Emergency	4	2	**8 (High)**	• Regional Disaster Awareness Training
Crew	Identification as Crew Members (Off-Airport)	2	2	**4 (Medium)**	
IT	Cybersecurity	3	1	**3 (Low)**	
Lodging	Hotel Accommodations	3	2	**6 (Medium)**	• Personal Security Measures • Crew Amenities Available at Hotel
Lodging	Room Access	2	1	**2 (Low)**	
Scheduling & Dispatching	Demonstrations/Special Events/ Holidays	3	4	**12 (Very High)**	• Alternate Accommodations • Emergency Response Plan
Transport	General Ground Transportation	3	2	**6 (Medium)**	

Appendix 3: Security Risk Assessment Case Study #2

Domestic Airport Example

This is the city's second largest commercial and general aviation airport, located approximately 7 miles south of downtown. The airport services four commercial airlines totaling more than 13 million passengers annually. The airport operates with standard security measures in place for both the commercial terminal and the FBOs inside the perimeter.

There is a medium level of threat severity in the city and in the area immediately around this airport, primarily due to the risk of crime. There is no specific risk of terrorism related to this location other than exists as background concerns in most major aviation facilities. Within this large city, wealthy and disadvantaged areas are often in close proximity to each other, which can present inadvertent exposure to crime and related threats for those unfamiliar with traveling through the city. Taxis and ride-share services, along with nearby hotel shuttles, are relatively safe, though caution with unknown drivers should always be exercised.

On this flight, there is a contract flight attendant. The three crewmembers will be housed in a hotel near the airport and will not be renting a car. Transportation from the FBO is provided by a ride-share service. The hotel does not have a restaurant in it but there are number of options within the surrounding area, some that can be walked to easily from the hotel. The crew will be at the hotel for two nights.

Operational Security Risk Assessment					
Operational Component	**Specific Risk**	**Risk Severity**	**Risk Probability**	**Total Risk Rating**	**Risk Observations/Mitigations**
Airport	Lack of Airport Security	2	1	**2 (Low)**	• Internal Aircraft Storage
Aircraft	Unattended Aircraft (Overnight)	2	1	**2 (Low)**	
Crew	Incapacitated/Missing Crew	3	3	**9 (High)**	• Criminal Activity Awareness Training
Crew	Natural Disaster/ Emergency	4	1	**4 (Medium)**	
Crew	Identification as Crew Members (Off-Airport)	3	2	**6 (Medium)**	• Limit Use of Personal Identification • Secure Valuables
Crew	Inadequate Pre-Trip Planning	2	2	**4 (Medium)**	
Crew	Uncontrolled Baggage	3	1	**3 (Low)**	• Positive Bag Identification Control
FBO	Catering	2	1	**2 (Low)**	
IT	Cybersecurity	2	1	**2 (Low)**	
Lodging	Room Access	2	2	**4 (Medium)**	• Contingency Planning
Maintenance	Third-Party Vendors	2	2	**4 (Medium)**	
Transport	General Ground Transportation	2	2	**4 (Medium)**	• Confirm Positive ID of Driver and Vehicle

Appendix 4: Additional Resources

- US State Department Travel Warnings
  www.travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html
- Smart Traveler Enrollment Program (STEP)
  https://step.state.gov/step/
- OSAC Crime and Safety Reports
  https://www.osac.gov/Pages/Home.aspx
- ATA Travel Information Manual
  www.iata.org/publications/timatic/Pages/tim.aspx
- Individual state Aeronautical Information Publications (AIPs)
  www.eurocontrol.int/articles/ais-online
- IATA Travel Centre
  www.iatatravelcentre.com
- US Customs and Border Protection
  www.cbp.gov/travel
- NBAA's List of Flight Planning and Flight Support Companies
  www.nbaa.org/about/contact/air-traffic-services/fpsp/
- The CIA World Fact Book
  www.cia.gov/library/publications/the-world-factbook/
- The Centers for Disease Control
  www.cdc.gov
- International Business Aviation Council (IBAC)
  www.ibac.org
- NBAA Professional Development Courses
  www.nbaa.org/pdp
- Australian Foreign Travel Information
  www.smartraveller.gov.au/
- British Foreign Travel Advice
  www.gov.uk/foreign-travel-advice
- Canadian Foreign Travel Advice
  www.travel.gc.ca/travelling/advisories
- Additional Travel Registration Programs:

  Australia: https://www.orao.dfat.gov.au

  Canada: https://www.voyage2.gc.ca/minroca/std/main-en.htm

  France: https://pastel.diplomatie.gouv.fr/fildariane/dyn/public/login.html

  Ireland: https://citizensregistration.dfa.ie/

  Mexico: https://sirme.sre.gob.mx/

  New Zealand: https://register.safetravel.govt.nz/login

ACKNOWLEDGMENTS
The National Business Aviation Association wishes to thank the members of its Security Council for their work developing this resource.

ABOUT NBAA
Founded in 1947 and based in Washington, DC, the National Business Aviation Association (NBAA) is the leading organization for companies that rely on general aviation aircraft to help make their businesses more efficient, productive and successful. Contact NBAA at 800-FYI-NBAA or info@nbaa.org. Not a member? Join today by visiting www.nbaa.org/join.