

RISK MANAGEMENT PROCESS

Last Updated: 13 August 2014

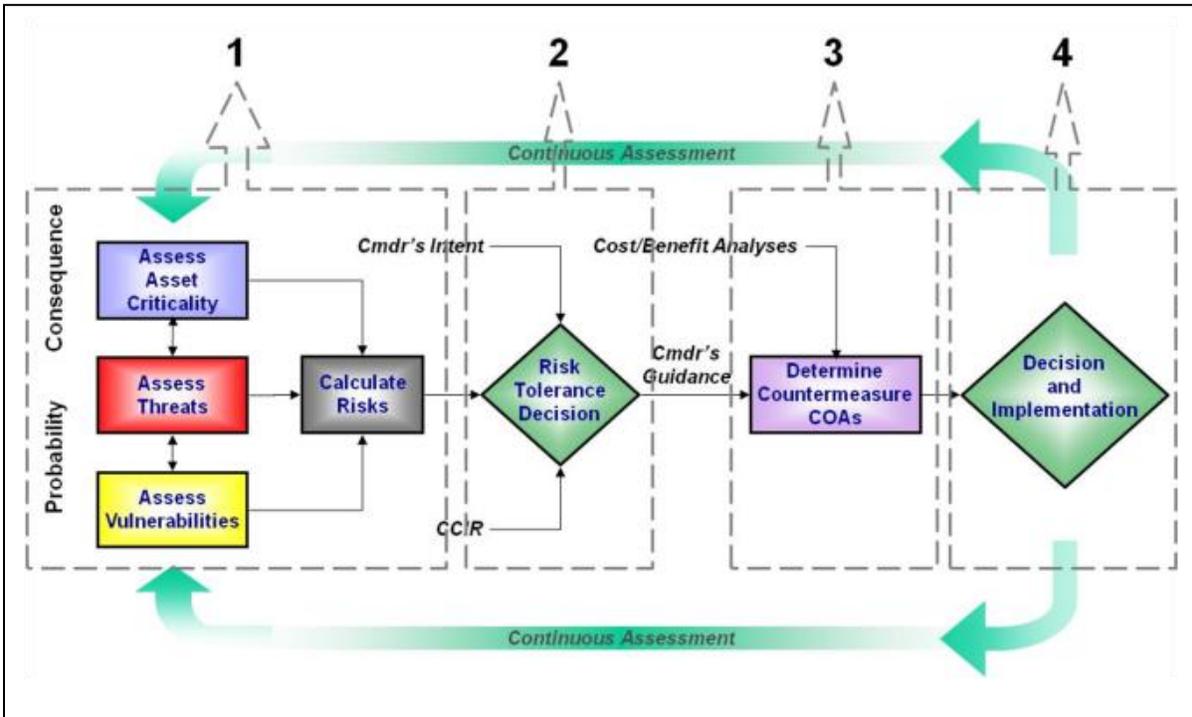
Commanders, with input from appropriate staff, determine how best to manage risks. The Air Force defines [risk management](#) (RM) as **the process of identifying critical assets; understanding the threat; understanding Air Force vulnerabilities to the threat; determining risk to personnel, assets, and information; and assuming risk or applying countermeasures to correct or mitigate the risk.**¹ In all cases, as part of the installation all-hazards emergency management program, the assessments include hazards as well as threats. This RM process consists of the following elements: prioritizing assets and resources by a **criticality assessment**, identifying potential threats through a **threat assessment**, analyzing resource and asset vulnerabilities through a **vulnerability assessment**, determining the risks acceptable to them for a given operation by conducting a **risk assessment**, then supervising and reviewing the effort to eliminate or mitigate the risks that are not acceptable. A safety and RM focus ensures maximum protection of people and physical resources. This kind of risk-based focus is critical to warfighting success. [Operations security](#) should be considered during the risk management process, as well.

Safety, as applied via RM, is a major element of FP planning and should be used in the risk assessment phase of the RM process when planning to counter a threat. The risk management process established in Air Force safety channels, from identifying a hazard through implementing risk control measures and supervision and review of the effort, lends itself ideally to planning for FP efforts.² Safety has a strong impact on FP's overall effectiveness.³ The figure, The Risk Management Process, is an illustration of the RM process for FP focusing on threats.

¹ See AFI 31-101, *Integrated Defense*. This Air Force definition accords with and supports the joint definition of risk management: "The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits." (JP 1-02)

² See AFI 90-802, [Risk Management](#), and AFD 10-24, [Critical Asset Risk Management](#).

³ See the 91-series of Air Force instructions for information on Air Force safety programs.



The Risk Management Process.
(Derived from AFI 31-101, *Integrated Defense*)

Criticality Assessment

A commander should know and identify those assets critical to mission execution. A criticality assessment is a systematic effort to identify key assets and infrastructure and evaluate the effect of temporary or permanent loss of the same on the installation's or a unit's ability to perform its mission. This assessment should examine costs of recovery and reconstitution including time, funds, capability, and infrastructure support.

Assessments of non-mission essential assets should also be considered, such as high-population facilities; mass gathering activities; and other facilities, equipment, services, or resources deemed important by the commander to ensure continued effective operation. This assessment also assists the commander in identifying assets that are priorities for FP resource allocation.

The criticality assessment identifies the relative criticality of assets based upon mission criticality, impact on national defense, replaceability and monetary value. An asset is anything of value, including people, information, equipment, facilities and infrastructure. Assets can also extend to more general or intangible items such as operations, systems, strategic advantage, morale and reputation. The primary objectives in the effective asset criticality assessment are to identify key assets, determine if critical functions can be duplicated, identify the resources required for duplication, and determine the priority of response.

Assessing criticality requires judgment and analysis. For example, the enemy's destruction of an asset not considered essential to mission success or necessary for continued efficient operations may still be critical, if the enemy perceives it to be symbolic. Such an asset may warrant protection because its loss may give an enemy the media coverage they seek or cause personnel to doubt a commander's ability to keep them safe. Complete protection of every asset is not possible, but the more difficult it is for the enemy to attack an asset, the less likely he is to attack. The [critical asset risk management program](#)⁴ enhances the risk management decision-making capability at all levels to ensure that Air Force critical assets are available when required to support mission requirements in an all threats and hazards environment. This risk management approach supports the prioritization of scarce resources across the Air Force, focusing priorities on the greatest risk based on assessed criticality, threat, vulnerability, and risk.

Threat Assessment

A commander should know what threat is anticipated in order to devise an effective means to counter or mitigate it. Without this knowledge, the commander is acting blindly. A thorough threat assessment reviews the factors of a threat's existence, capability, intention, history, and targeting, as well as the operating environment within which friendly forces operate. Analyzing and synthesizing this information are essential precursor steps in identifying the probability of attack. [Air Force Office of Special Investigations](#) (AFOSI) and other Service counterparts produce a local threat assessment that should be used as a baseline product for adversarial threats in the FP effort. At the installation level, the threat working group or other intelligence fusion and analysis cell (e.g., joint intelligence support element, etc.) should assist in producing a localized threat assessment and recommend courses of action to the commander to mitigate or counter threats.

In the complex environment of [irregular warfare](#) (IW), [ISR](#) forces should use information collected from a variety of sources to provide or collect information to fill intelligence gaps. ISR personnel should validate the credibility of these various sources to overcome adversary denial and deception, and information operations. Though [rules of engagement](#) and operational objectives drive operations, analysts should craft their [intelligence requirements](#) to help protect the population against both kinetic and non-kinetic capabilities. Analysts should recognize an increased need to make correlations between various development projects and levels of cooperation with the local nationals. Additionally, ISR forces should be aware that one of the basic underpinnings of successful IW operations is the capability to train partners to conduct independent operations and participate in coalition operations.

Threat assessments fuse information and intelligence from open source, law enforcement, government intelligence, medical intelligence, and counterintelligence

⁴ For additional information on the critical infrastructure program, see Air Force Policy Directive (AFPD) 10-24, [Critical Infrastructure Program](#). This supports Homeland Security Presidential Directive 7, [Critical Infrastructure Identification, Prioritization, and Protection](#), and DODD 3020.40, [DOD Policy and Responsibilities for Critical Infrastructure](#).

information, along with local, state, and federal information to create a cohesive threat picture for FP decision-makers. By synthesizing law enforcement, intelligence, medical intelligence, and counterintelligence information, analysts can identify indicators of future attacks. The more common sources are described in the figure, Sources of Intelligence and Counterintelligence.⁵

OPEN SOURCE INFORMATION: —News media, hearings, publications, reference services, publicly available internet sites/data
LAW ENFORCEMENT INFORMATION: —Collection, retention, and dissemination regulated by law enforcement channels —Law enforcement information
GOVERNMENT INTELLIGENCE AND COUNTERINTELLIGENCE INFORMATION: —Products and reporting from the US intelligence community
LOCAL, STATE, AND FEDERAL INFORMATION (including host nation): —Service member, civil servant, individuals with regional knowledge —Counterintelligence force protection operations—information gleaned from the streets

Sources of Intelligence and Counterintelligence.

Considering the wide range of possible threats, FP personnel should focus on developing a robust [force protection intelligence](#) (FPI) threat picture to support unit deployments, readiness training, mission planning, and other mission execution functions such as integrated defense, the critical infrastructure program, and emergency management.⁶ Commanders should develop priority intelligence requirements to guide FPI work supporting their decision-making and operations. FP personnel should coordinate with their cross-functional counterparts to ensure information requirements are satisfied. Once FP information has been fused, the end product should be provided to the commander to guide intelligence-driven and risk-based measures or operations, such as [counterthreat operations](#), to preempt, deter, mitigate, or negate threats. FPI provides support to all phases of FP operations.⁷

The AFOSI's defense threat assessment is a good starting point for general information on the security threats facing an installation. However, when more specific local threat information is required, it can be obtained from multiple sources through AFOSI's liaison

⁵ See JP 3-07.2, [Antiterrorism](#).

⁶ See AFI 31-101, [Integrated Defense](#); AFPD 10-24, [Air Force Critical Infrastructure Program \(CIP\)](#); and AFI 10-2501, [Air Force Emergency Management \(EM\) Program Planning and Operations](#), for more information on these functions.

⁷ For additional information, see AFI 14-119, [Intelligence Support to Force Protection \(FP\)](#).

with federal, state, local and foreign national law enforcement, counterintelligence and security agencies.⁸

Vulnerability Assessment

Once the threat assessment is complete, commanders should prepare a vulnerability assessment of their personnel, equipment, facilities, installations, and operating areas. This assessment should address the broad range of medical and physical threats to the security of the commander's personnel and assets. The vulnerability assessment then considers the identified and projected threats against personnel, facilities, or other assets to identify those areas where resources are susceptible to actions which may reduce or diminish operational effectiveness. This includes the local populace and infrastructure due to association or proximity with Air Force operations.

[Airmen](#) should consider both the threat and existing vulnerabilities, but should not rely exclusively on the assessed threat. For example, terrorists successfully attacked military targets, such as Khobar Towers, the USS Cole, and three residential compounds in Riyadh, Saudi Arabia, even though those locations were in [force protection condition](#) (FPCON) Bravo. Non-military targets, such as the US embassies in Tanzania and Kenya or the World Trade Center, have been attacked when the country terrorist threat assessments for those locations were moderate, low, or negligible. History shows that the assessed threat is not necessarily an accurate reflection of the actual threat. As a result, identifying vulnerabilities is critical. Once identified, steps to mitigate the vulnerabilities should be undertaken to increase survivability for Air Force personnel and assets.

Risk Assessment

The Risk Assessment compares the relative impact of any loss or damage to an asset (criticality) with the relative probability of an unwanted event. When combined in a quantified fashion, these elements analyze and measure the risks associated with an unwanted event. Upon completion of the criticality, threat, and vulnerability assessments, commanders should have the information they need to make decisions regarding what level of risk they are willing to accept. Ultimately commanders decide what level of risk to accept. However, risks to the most critical Air Force assets should be mitigated or eliminated whenever possible. If risks cannot be eliminated, commanders should implement measures to mitigate them to the greatest extent possible.

⁸ AFPD 71-1, [Criminal Investigations and Counterintelligence](#); AFI 14-119, [Intelligence Support to Force Protection](#).