

The **Risk Based Assessment** process can include the following steps:

1. Identify the assets.
2. Determine the criticality of assets.
3. Identify the threats to each critical asset.
4. Identify the existing countermeasures (*Existing Security* is existing countermeasures).
5. Determine the vulnerability level of each critical asset.
6. Determine the risk level of each critical asset.
7. Recommend security upgrades to reduce high levels of risk.
8. *Perform a cost-benefit analysis in support of upgrade recommendation. (This will be done as a good business practice).*

An **asset** is a person, place or thing. Its value may be quantifiable in terms of dollars. The total cost of damage to or loss of an asset is evaluated in the process. This may include replacement cost, repair cost, and the financial impact (consequence cost) of the loss event.

A **loss event** is defined as physical damage to, or destruction of, an asset. While human life is priceless, the process requires that each asset be given a value.

The **level of criticality of an asset** is determined by the impact its damage or loss will have on the capability of the facility or the organization to perform its mission. Criticality values are assigned on a scale of 1 through 4.

The four levels of criticality are:

Rating Interpretation Impact of Loss

1 Essential

Total destruction of (or severe damage) to the asset would cause complete loss of mission capability. This is a *catastrophic loss*.

2 Critical

Total destruction of (or severe damage) to the asset would cause severe impairment of mission capability. This is a *serious loss*.

3 Important

Total destruction of (or severe damage) to the asset would cause noticeable impact on mission capability. This is a *moderate loss*.

4 Not important

Total destruction of (or severe damage) to the asset would cause no noticeable impact on mission capability. This is a *minor loss*.

A **threat** is any action or event, whether human or natural in origin, that can result in a loss event.

“What is the probability of a specific threat successfully causing a loss event?” not “What is the probability of the threat occurring?” This distinction is important and requires that the threats established be credible and realistic. A credible threat package should be established and is paramount to a successful Facility Security Assessment.

Given recent threat data, such as facility bombings, computer information theft and/or sabotage, workplace violence / disgruntled employees, and potential stowaway personnel from vessels, all possible threats must be carefully considered.

A **countermeasure** is any action or combination of actions involving physical, technical, administrative, procedural, or other measure(s) that is/are taken to reduce the severity of an identified risk.

Viewed from this perspective, the question that is asked has two parts. The first part is: “What credible threat(s) is/are associated with a particular asset?” The second part of the question is: “Should that threat occur, what is the probability that the threat will produce a loss event?” Hence, vulnerability is defined as any condition or situation that increases the likelihood that a threat, if it occurs, will result in a loss event associated with a particular asset.

The level of vulnerability of an asset is determined by contrasting the threats with the existing countermeasures. If the existing countermeasures are effectively protecting the asset from all threats, then vulnerability will be low. If, however, the existing countermeasures are not adequate to prevent or withstand an attack, vulnerability is higher. Vulnerability is measured in terms of the probability of a loss event occurring. Vulnerability values are assigned on a scale of A through D. The levels of vulnerability and the corresponding definitions are provided below.

Asset Vulnerability Rating

Interpretation Probability of Loss

A Extremely high

The magnitude of the vulnerability is such that if a threat occurs there is an *extremely high probability* that it will be successful in causing a loss event.

B High

The magnitude of the vulnerability is such that if a threat occurs there is a *high probability* that it will be successful in causing a loss event.

C Medium

The magnitude of the vulnerability is such that if a threat occurs there is a *medium probability* that it will result in a loss event.

D Low

The magnitude of the vulnerability is such that if a threat occurs there is a *low probability* that it will result in a loss event.

In order to provide the necessary data for making risk management decisions, it is necessary to provide an orderly and logical presentation of risk data information. This is done by combining the criticality and vulnerability data associated with specific assets in such a way as to indicate the combined severity of impact and the probability of a loss event occurring. The criticality and vulnerability ratings assigned to the major assets are entered in a risk logic matrix to determine the overall risk probability rating as shown below.

Risk Categories

Asset Vulnerability		Asset Criticality		
	1 Essential	2 Critical	3 Important	4 Not Important
(A) Extremely High	1A	2A	3A	4A
(B) High	1B	2B	3B	4B
(C) Medium	1C	2C	3C	4C
(D) Low	1D	2D	3D	4D

The matrix presentation permits extrapolating risk information pertaining to assets in such a way that there is a clear perception of where the crucial decision boundaries are to be found. This table indicates how the risk categories may be interpreted.

Risk Matrix Management Guide

Asset Risk Category	Interpretation
1A 1B 1C 2A 2B 3A	These risks are very high and it is recommended that measures be taken to eliminate them.
1D 2C 2D 3B 3C	These risks are moderate.

	Management may determine to address these risks.
3D 4A 4B 4C 4D	These risks are low.

Once the level of risk is determined for each asset, recommendations for security upgrades are made, if warranted. The first goal of the upgrades is to reduce the level of risk to those assets that are in the very high category to the greatest degree practical.

A secondary goal is to reduce the level of risk to the assets in the moderate category (yellow) to the greatest degree practical. If there are constraints that preclude the immediate or near term reduction of risks, then recommendations should include planning and budgeting to accomplish this in the future.

Risk Category	Priority