

# Robust, Replicable and Defensible Risk Management

At Headquarters or the Front

*Eugene A. Razzetti*

**T**erms like risk analysis, risk assessment, and risk management often are used interchangeably and can include a variety of different concepts or strategies. Approaches can be simple or complex, although simpler is almost always better. Properly conducted risk management permits decision making based on realistic scenario assumptions and provides defensible justification, before limited resources are committed.

The risk management model described in the pages that follow is based on what I like to call “disciplined subjectivity.” Risk planners can use it to subjectively identify and assess mission threats, criticalities and vulnerabilities—applying the best knowledge and experience available. The discipline comes when they assign consistent, replicable, numerical values to them in accordance with established criteria. (I do not recommend that planners do risk management either in their heads or by themselves.)

I have used this model with clients both in and out of the military for more than 10 years.

**Razzetti**, a retired U.S. Navy captain, is a management consultant and military analyst. He is the author of five management books and has served on the advisory boards of two business schools.





**Table 1. The Criteria**

Level	Scale	Threat Criteria	Criticality Criteria	Vulnerability Criteria
Lowest	1, 2	Never occurred before—unlikely; minimally effective due to physical area/environment; not a significant source of disruption	Minimally disruptive to mission if used	Minimally vulnerable to attack, due to own tactics, equipment, physical surroundings
Low	3, 4	Has occurred before—possible; effective in physical area for short period; potential source of disruption	Disruptive to mission if used; minor mission degradation	Susceptible to attack, but history and physical surroundings make attack unlikely
Medium	5, 6	Occurs periodically and predictably; likely to encounter; disruptive when occurring	Mission degraded, but can continue if attacked; some casualties	Highly vulnerable to attack, due to own tactical limitations and physical surroundings
High	7, 8	Occurs often; enemy has expertise; utility in area against missions; expect to encounter; highly disruptive	Mission seriously degraded, but can continue marginally if attacked; significant casualties possible	Extremely vulnerable due to tactical and equipment limitations and physical surroundings
Highest	9, 10	High probability of use; enemy proficient in use; unlimited utility and effectiveness against most missions; catastrophic if used	Mission failure; much disruption likely	Imminent danger, due to nature of operations, plus equipment limitations

**I. In General**

$$\text{Risk} = \text{Criticality} \times \text{Vulnerability} \times \text{Threat}$$

A spreadsheet model consisting of a set of connected worksheets can be a priceless management tool for the program manager (PM), enabling him or her to identify major potential threats to the mission of the organization and prioritize them, by assigning a numerical value to each. The PM also could assess the criticality of each threat to the mission expressed as a numerical value, and the vulnerability of the mission or organization to the threats expressed as a numerical value.

Then (and unlike other risk models) this model also helps to predict the impact on risk of one or more external or environmental factors, and the change to the risk if a selected course of action (COA) is implemented. With this last step, risk assessment becomes risk management.

**II. In the Headquarters**

**Creating Criteria**

For risk assessments to be consistent and reports to be uniform among reporting subordinates, the model requires an established set of numerical values or “criteria.” The criteria Table 1 uses numerical values from 1 to 10 and describes each in terms of threat, criticality and vulnerability (to a mission).

**Step 1. Developing the Threat Assessment Matrix**

PMs and staffs identify the threats, and then assign numbers based on their knowledge and experience. The spreadsheet automatically computes the total and the average threat. The model uses average threats in all the calculations. This is a simple way to quantify threats in a “multi-threat” scenario. You may have another way, but you must be consistent in whatever method you use. Some variations may prove misleading or self-defeating (such as assigning zeros). The shaded columns are computed and posted automatically by the software.

**Table 2. Threat Assessment Matrix**

Program Management	Terrorist Attack	Utility Loss	Hacker or Cyber Attack	Industrial Espionage	Strike	Contractor Default	Natural Disaster	Falsified Reporting	Total	Average
Concept Design	9	4	9	9	3	5	8	8	55	7
Systems Engineering	4	4	9	9	3	5	8	8	50	6
Reliability & Maintainability	9	9	9	5	3	5	8	8	56	7
Manufacturing & Logistics	9	4	9	5	6	5	8	8	54	7
Environmental Planning	9	4	6	5	6	5	8	8	51	7
Safety/Security Plan	6	4	6	5	3	5	8	8	45	6
Software Engineering Plan	4	4	6	5	3	5	8	8	43	5
Quality Engineering	4	4	7	5	3	5	8	8	44	6

**Table 3. Computing Basic Risk, Environmental Adjustment and Adjusted Risk**

(Criticality × Vulnerability × Threat)

Program Management	Criticality	Vulnerability	Threat	Risk	Environment Adjustment	Adj Risk (1)	Revised Vulnerability	Adj. Risk (2) (COA)
Concept Design	8	6	7	330	0.9	297	5	248
Systems Engineering	8	5	6	250	0.2	50	4	40
Reliability & Maintainability	8	5	7	280	0.4	112	3	67
Manufacturing & Logistics	8	4	7	216	0.5	108	2	54
Environmental Planning	5	5	6	159	0.3	48	2	19
Safety/Security Plan	7	6	6	236	0.7	155	4	110
Software Engineering Plan	4	7	5	151	0.9	135	4	77

Table 2 is a threat assessment matrix. This matrix (worksheet) is the basis for all subsequent computations. There is an abbreviated list of program management tasks on the vertical axis and identified potential threats along the horizontal axis. It remains only to assign subjective numerical values from the criteria table.

**Step 2. Computing Basic or “Unadjusted” Risk**

The next worksheet (see Table 3) automatically copies the computed average threat from Table 2 for each program management sub-category. Planners then compute unadjusted (i.e., basic) risk according to the formula:

$$\text{Risk} = \text{Criticality} \times \text{Vulnerability} \times \text{Threat}$$

Planners assign numerical values from the (same) criteria table for the criticality of the threat incident or adverse event (if it happened) to the specific mission task and the resultant vulnerability of the mission.

When planners update the spreadsheet model displayed in Table 3 they automatically revise its associated graph shown in Figure 1. The first bar in Figure 1 (automatically formed by the spreadsheet software) displays basic or “unadjusted” risk. This often is the final step in risk assessment, but it is only the beginning of risk management, as shown in the last four columns on the right-hand side of Table 3. The reader will need to refer to Table 3 periodically as the risk management picture develops.

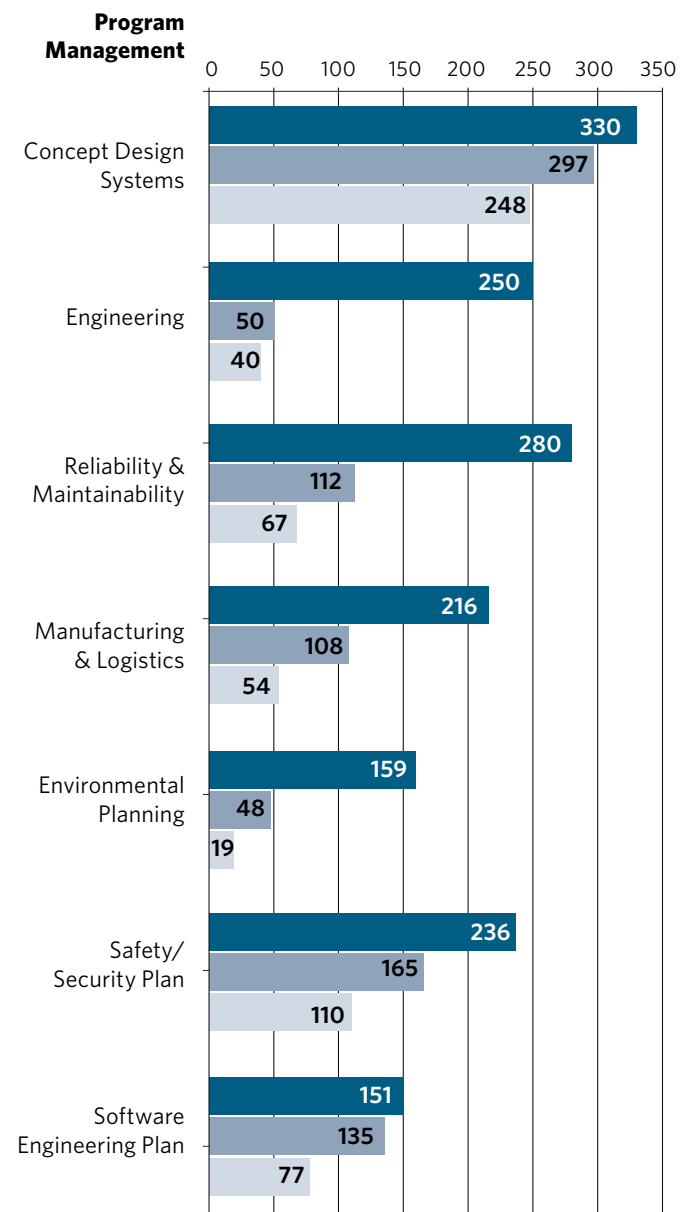
**Step 3. Assessing Impact of the External Environment**

$$\text{Risk} = \text{Criticality} \times \text{Vulnerability} \times \text{Threat} \times \text{Environmental Adjustment}$$

The next step in the modeling process assesses the impact of external factors over which planners may have little or no control, such as host nation support of logistical operations in theater. In some cases, host nation support and/or involvement is invaluable, as in assigning interpreters or counterparts.

**Figure 1. The Total Risk Management Picture for the Headquarters**

(Composite Risk and Adjusted Risks From Table 3)



# Risk assessment becomes risk management when the PM goes beyond what he has just completed, to identify and evaluate potential courses corrective COAs before expending any time or funding.

In other cases, (e.g., corrupt bureaucracies), U.S. Forces are often better left alone.

Planners wanting to separately reflect external variables on risk can add this step to assess (among other variables):

- Foreign country support (receipt, transportation, customs, etc.)
- Supply chain security
- Outsourcing (foreign or domestic)
- Special laws, regulations or protocols
- Anything else you want to separate from the internal processes but feel must be included in the overall risk assessment process.

For example, if the addition of a certain procedure or custom in the country where your operations are based cuts the risk in half, you multiply the risk figure by ".5." If the practice makes no appreciable difference, multiply the risk by "1" (no change). If a procedure makes it half again as difficult or risky, multiply by "1.5." Again, this will not corrupt or hinder your computations, as long as you apply it consistently. Planners not wishing to go through this step may either remove the "Environmental Adjustment" column from the spreadsheet or leave it in and place the number "1" in each row.

## Graphing Unadjusted and Adjusted Risk

Thus far, we have quantified (1) the unadjusted risk and (2) the impact of the environmental factors, providing a more realistic assessment of the actual risk. The second bar in Figure 1 displays the change (for better or worse) brought about by external factors.

## Step 4. Identifying and Assessing Potential Actions

**Reduce Risk by Reducing Vulnerability.** Identifying threats, criticalities and vulnerabilities in accordance with a standard set of numerical values to provide a "snapshot" of operations normally is the extent of risk assessment as currently practiced.

However, risk assessment becomes risk management when the PM goes beyond what he has just completed, to identify and evaluate potential corrective COAs before expending any time or funding.

Identifying potential COAs and modeling them in the spreadsheet can show one of the following:

- Measurable potential reductions of risk in one or more mission areas if implemented (good)
- Small or insignificant potential changes of risk if implemented (neither good nor bad; not worth the time or expense)
- A measurable increase in risk to another part of the mission if implemented (bad)

Implementing a new course of action for an existing mission, operation or project does not change the threat to the mission. Neither does it change the criticality of the mission. It does (or should), however, measurably reduce the vulnerability of the mission. For example, posting extra security personnel or adding alarm systems can decrease an organization's vulnerability to a break-in. The alarm systems have not decreased the threat of a break-in, or the criticality of a break-in—only the vulnerability.

Accordingly, you reduce risk by reducing vulnerability. Recognizing this fact and using it to predict changes in risk is an indispensable to program management in general and risk management in particular.

The following formula computes the impact of the COA on the risk computed earlier:

$$\text{Risk} = \text{Threat} \times \text{Criticality} \times \text{Revised Vulnerability} \times \text{Environmental Adjustment}$$

The third bar in Figure 3 displays the application of the revised vulnerability and, accordingly, the revised risk resulting from implementing a (notional) course of action. The graph displays at a glance:

- The unadjusted (basic) risk assessment
- The impact of the external environment
- The impact of a notional course of action, which is the result of revising the numerical value for vulnerability.

We have not only a realistic snapshot of the present, but our best possible prediction (albeit subjective) of the future, if we were to implement specific courses of action.

Revisions that reflect changing situations and the immediate feedback provided by the graphs make the model a dynamic management tool for evaluation, prioritization

**Table 4. Threat Matrix Closer to the Front**

Program Management	Terrorist Attack	Utility Loss	Hacker/Cyber Attack	Industrial Espionage	Strike	Contractor Default	Natural Disaster	Falsified Reporting	Total	Average
Security/Surveillance										
Detecting/Identifying unauthorized movement-personnel	9	4	9	9	3	5	8	8	55	7
Detecting/Identifying unauthorized movement-vehicles	9	4	9	9	3	5	8	8	55	7
Surveillance of restricted areas	4	4	9	9	3	5	8	8	50	6
Securing Incident Sites	9	9	9	5	3	5	8	8	56	7
Detection of unauthorized material	9	4	6	5	6	5	8	8	54	7
Surveillance of access points	9	4	6	5	6	5	8	8	51	6
Harbor Surveillance	6	4	6	5	3	5	8	8	45	6
Automatic Security Systems	4	4	6	5	3	5	8	8	43	5

and presentation, as well as a timely, stand-alone report to higher authority.

It is not unusual to discover that modeling potential courses of action (i.e., “gaming” them) predicts only small or insignificant changes. Modeling can show PMs in advance that certain courses of action simply may not be worth expending limited resources.

### III. Risk Management at the Front

This includes identifying (as appropriate):

- Physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action

- Operational threats and risks, including the control of security, human factors and other activities that affect the organization’s performance, condition or safety
- Environmental or cultural aspects that may either enhance or impair operations
- Factors outside of the commander’s control, such as failures in externally supplied (e.g., host nation) equipment and services
- Contractor and host nation challenges, such as local regulatory requirements
- Facilities and equipment, including information, data and communications management systems
- Any other threats to the continuity of operations


Commanders and planners closer to the front can use the model and approach to assess actual operations.

Table 4 contains a threat matrix for a key mission set of a (notional) deployed unit: “Security/Surveillance.” A corresponding risk table and graph are not shown, due to space constraints.

### Summary

Properly conducted risk assessments based on lifelike scenario assumptions lead PMs to either justify or preclude commitments of time and funding in making their decisions.

There are many approaches to meaningful risk management. This model provides risk planners with a simple but comprehensive management tool for identifying mission threats, criticalities and vulnerabilities. It can help identify and assess potentially mitigating courses of action.

Regardless of where the assessment leads, completing this model will provide a rigorous and structured process to help PMs and commanders arrive at logical and defensible conclusions. 

The author can be contacted at [generazz@aol.com](mailto:generazz@aol.com).

## MDAP/MAIS Program Manager Changes

With the assistance of the Office of the Secretary of Defense, *Defense AT&L* magazine publishes the names of incoming and outgoing program managers for major defense acquisition programs (MDAPs) and major automated information system (MAIS) programs. This announcement lists all such changes of leadership, for both civilian and military program managers for March and April 2016.

### Navy/Marine Corps

**CAPT Todd St. Laurent** relieved **CAPT Leon R. Bacon** as Program Manager for the T-6B Joint Primary Aircraft Training System (JPATS) program (PMA 273) on March 4.

**Patrick Fitzgerald** relieved **Laura Knight** as program manager for the Sea Warrior program (PMW 240) on April 1.