Some Considerations for Implementing Risk Management in Defense Programs

A Faithfully Followed, Structured Risk Management Process is Critical to Maximizing Program Success

EDMUND H. CONROW • MARK A. FREDRICKSON

Risk management is mandated for defense programs in several Department of Defense (DoD) directives and initiatives, including: DoDD 5000.1, *Defense Acquisition Management*, February 23, 1991; DoDI 5000.2, *Defense Acquisition Management Policies and Procedures*, February 26, 1993; DoDD 5000.2-M, *Defense Acquisition Management Documentation and Reports*, March 5, 1993; and DoDD 4245.7-M, *Transition from Development to Production*, September 1985. For example, DoDD 5000.1 states:

> Risk areas to be assessed at milestone decision points include: threat, technology, design and engineering, support, manufacturing, cost, and schedule.[1]

In addition, Defense Systems Management College publications, including *Risk Management Concepts*

Dr. Conrow is an independent management and technical consultant in Redondo Beach, Calif., specializing in defense and large-scale commercial projects. He has authored numerous articles for Program Manager and Acquisition Review Quarterly, and was recently awarded the David D. Acker Award for Skill in Communication at the DSMC-sponsored Acquisition Research Symposium, 1995. Mr. Fredrickson is a systems engineering program manager at Science Applications International Corporation, Torrance, Calif.

and Guidance (1989), provide approaches for assessing and managing program risk. Despite these guidelines and reference documents, the risk management process has been inadequately implemented in some defense programs. For example, the Air Force Acquisition Process Review Team on Clear Accountability in Design stated:

> The contractor and government program management team overestimates technology readiness, downplays potential problems, and fails to plan and perform adequate risk management at program initiation and throughout the program, resulting in unexpected cost overruns, schedule delays, and technical compromise. Initial impacts surface as early as Demonstration/Validation (DEM/VAL) and continue throughout succeeding program phases. These effects exist on all programs to varying degrees.[2]

In this article we will discuss some typical deficiencies associated with risk management processes for DoD programs. We will also examine in greater detail how the risk management process was improved for one DoD program.

Inadequate risk management by contractors and government program management teams results in unexpected cost overruns, schedule delays, and technical compromise.

Some Common Risk Management Deficiencies

The following paragraphs briefly describe four risk management deficiencies observed in several DoD programs that were in the DEM/VAL or Engineering and Manufacturing Development (EMD) program phases.

First Deficiency. The risk management process is often weakly structured or 'ad hoc' for both the government and contractors. There may be no clearly delineated mechanism in-place for managing program risk (e.g., organizational responsibilities, analyses, products, etc.), or if a risk management process exists, it may be present on paper only.

Second Deficiency. The risk assessment portion of the risk management process is often too subjective and not adequately documented.

- The prescribed risk assessment categories may be overly broad (e.g., management, technical), leading to difficulty in evaluating results and implementing a viable, measurable risk mitigation strategy.
- A weak risk assessment methodology may be used, which introduces considerable doubt as to the accuracy and value of the results for senior management use.
- Ordinal risk assessment scales are often incorrectly applied. Mathematical operations cannot be applied to scores obtained from uncalibrated ordinal risk assessment scales. Risk values generated by mathematical operations are generally meaningless and may hide true risk issues.[3]
- The risk assessment results may be summarized into broad categories (e.g., low, medium, and high) without sufficient backup to understand the nature of the risk present.
- The government and contractors may use different, incompatible risk assessment methodologies making comparing results difficult, if not impossible.

The government and each contractor team used widely dissimilar and incompatible risk assessment methodologies, making comparison of results very difficult.

Third Deficiency. The emphasis of the risk assessment process is generally on the uncertainty associated with a specific event occurring, with less attention given to the consequence of the event occurring. Risk is often inaccurately referenced as only the uncertainty term. However, it is the product of the uncertainty and consequence terms that yields risk.[4,5] In addition, both the uncertainty and consequence terms require evaluation and tracking over time.

Fourth Deficiency. Program risk assessments and mitigation plans are often unlinked. In addition, they may be prepared on an as-needed basis with limited tracking against key program milestones.

Risk Management Implementation in One DoD Program

The following paragraphs discuss how the risk management process was improved for one major DoD program during the DEM/VAL phase. (Four prime contractor teams initially existed during this program phase. Two contractor teams remained following a down-selection approximately 2 years later.)

Initial System Program Office (SPO) Risk Management Status. Risk management activities began early in the DEM/VAL program phase to assess whether or not critical program technologies existed or a viable path to their availability was in-place. Initial risk management activity was done in an “ad hoc” fashion by relevant experts. Organizations and individuals supporting risk management were not initially identified, nor were the analyses or products structured or maintained. The first program risk assessment was generated by a non-SPO organization. It did not adequately reflect the program’s Work Breakdown Structure (WBS) nor accurately reflect the level of risk present.

The government and each contractor team used widely dissimilar and incompatible risk assessment methodologies, making comparison of results very difficult. Different ordinal scales with inadequate definitions were used in each risk assessment. Mathematical operations were performed on the risk scores, which rendered the results nearly meaningless. Insufficient backup generally existed to permit independent understanding of the results. In addition, the government and contractor teams evaluated a somewhat different set of risk categories which made comparing results difficult.

The main emphasis was evaluating the uncertainty term of risk. In all cases except cost and schedule risk the consequence term was derived from an uncalibrated ordinal scale. When it was estimated, the consequence term was often multiplied by the uncertainty term. Although this should yield risk, the mathematical operation was invalid for all but cost and schedule risk since both the uncertainty and consequence terms were derived from ordinal scales.[3] Finally, little emphasis was placed on developing risk mitigation plans.

Modified SPO Risk Management Process. The SPO director (O-6) recognized that deficiencies existed in the risk management process. As a result, the deputy SPO director (O-5) was named the focal point for program risk management. The deputy director formed a Risk Management Working Group (RMWG) composed of chiefs of the SPO system engineering, technology, and test divisions (O-4s and O-5s), the SPO focal point for producibility, and appropriate other government and support contractor personnel.

The purpose of the RMWG was to provide risk-related products and recommendations to the SPO director for decision and implementation approval. Some of the RMWG’s key responsibilities included:

- establishment, adoption, and application of risk management methodology;
- identification of all program risks;

- generation, control, and update of all approved program risk assessments;
- coordination with government agencies, laboratories, and contractors for risk assessment inputs, updates, and reviews;
- integration and verification of risk assessment inputs and updates;
- validation of program risk assessments;
- documentation of risk assessments and risk mitigation plans;
- evaluation of the feasibility of proposed risk mitigation alternatives;
- tracking risk mitigation progress over time; and
- review of program contract-related items for content necessary to permit support of risk assessment activities.

Membership on the RMWG was limited in size to facilitate working in a "shirt sleeve" environment. Over time, RMWG membership evolved to reflect changes in SPO organizational structure and the addition of new risk categories requiring evaluation. As needed, RMWG splinter groups were formed to resolve issues and action items that required specialized attention.

The responsibility for generating cost risk assessments remained with the SPO Program Control Division. (Both the government and contractors had suitable software tools for performing cost risk assessments.)

Initial RMWG meetings occurred to generate SPO-position risk assessments. The appropriate WBS level to perform the risk assessment varied between risk categories. For example, threat risk assessments were typically performed at a high WBS level (e.g., level 2), while technology risk assessments were typically performed at lower WBS levels to reflect key assembly items or parts (e.g., levels 5 or 6).

The reason for performing the risk assessments was twofold. First, it provided suitable material for the SPO director to respond to requests for risk assessments by DoD personnel. Second, it permitted the identification of moderate- and high-risk items potentially present in the contractor designs. This facilitated the generation of a prioritized list of risk items critical to the program. It also permitted the SPO director to apply available resources and defend the need for additional resources for critical supporting programs both within and outside the SPO's jurisdiction.

The RMWG operations concept was to have a small splinter group develop strawman risk assessments for each item identified in the baseline design. These strawman assessments were then evaluated by technical experts associated with each hardware or software WBS area. A 1-day RMWG meeting was then held to generate final risk assessment scores and supporting rationale. An advantage of using this tiered assessment approach was that reliable risk assessments were generated in a relatively short period of time while placing only a slight burden on personnel. The period of time typically necessary to perform a program risk assessment was less than 3 calendar weeks, with most of the work performed in less than 1 week.

The risk assessment process was part of a larger multi-step SPO risk management process. Risk assessment outputs were inputs to a supporting program assessment, necessary to identify critical technology and manufacturing programs needed for the program. Items identified as having high design and engineering, manufacturing, or technology risk would likely require a breadboard, prototype, and prototype qualification to eventually lead to a low risk level, while items identified as moderate risk would likely require a prototype and prototype qualification. Potential Milestone II exit criteria were evaluated against various program options to identify critical issues and develop suitable implementation plans. A risk mitigation plan was developed for technology and manufacturing supporting programs, and an issue resolution plan was developed for test experiment programs.

Of key importance was how the risk mitigation plans were implemented over time, and whether suitable progress was being made to reduce the identified level of risk present.

Technical performance measurements were identified and used to aid in tracking the risk mitigation process for design and engineering, manufacturing, and technology risk issues. Of key importance was how the risk mitigation plans were implemented over time, and whether suitable progress was being made to reduce the identified level of risk present. (For example, were planned experiments performed on-time, and were the results achieved from the experiments consistent with anticipated performance goals?)

Critical to the success of the risk management process was the derivation and acceptance of risk assessment ground rules and assumptions. A key ground rule necessary for any risk assessment is the reference time frame. We assumed that the risk assessment represented the current [today's] status for each item evaluated, and not a projected status at some future time. Future time frames generally have too many uncertainties to permit an accurate, consistent evaluation. In addition, several assumptions had to be developed and applied across the board to the risk assessment process. These assumptions included information pertaining to:

- mission objective requirements;
- threat evolution;
- design life and mean mission duration;
- parts quality;
- hardness levels;
- technology freeze and initial operational dates; and
- annual production rates and total production quantity.

Existing design and engineering, manufacturing, and technology ordinal risk (uncertainty) scales were modified to reduce inconsistencies and improve assessment accuracy. Supporting text, including definitions of key terms, was generated to further assist risk analysts. Surprisingly, even a common term such as "prototype" may represent different levels of hardware maturity between the Services and other government agencies.

Those responsible for program risk management must recognize that having a faithfully followed, structured risk management process is critical to maximizing program success.

A matrix of risk scores composed of each WBS item and category was generated and reported. Thresholds were identified for summarizing risk assessment results to low-, moderate-, and high-risk levels, and a set of summary charts condensing the risk results into these categories was developed. Detailed results were presented in quad charts to provide senior SPO management with information to make rapid, accurate, high-confidence decisions regarding resource allocation and critical program-level decisions.

Risk assessment summary level charts, detailed matrix charts, and quad charts were successfully used by the SPO director on several occasions to brief the program to higher-level DoD and Service management. They were also used to measure the claims of outside technology programs in terms of how they benefited the program. In some cases the risk assessment results shaped the direction of outside technology programs to increase the likelihood that they would yield products useful to the program. Finally, DoD recommended that related programs consider implementing the risk management process developed by this program.

The SPO risk management process was provided to the contractors at a major program milestone. The contractors were given some of the risk (uncertainty) assessment scales and supporting rationale to interpret the scale definitions. We found that without supplemental clarifying information, analysts often assigned incorrect risk scores. The contractors were instructed not to perform mathematical operations on uncalibrated ordinal risk scales (as each had previously done). They were, however, encouraged to investigate using enhanced risk assessment approaches if possible (e.g., quantitative analyses based on cardinal numbers). The contractors were contractually required to submit annual Risk Assessment Reports, including detailed risk assessments and risk mitigation plans for any item identified as having a moderate or high score for the required risk categories.

Several follow-ups were needed with each contractor team over the next year to insure that the risk management process had been properly assimilated. One key SPO concern was that artificially low risk scores and overly optimistic risk mitigation plans might result since the two remaining contractor teams were still in competition. The contractors were instructed that realism in assessing and documenting risk and generating suitable risk mitigation plans was of paramount importance. Artificially low risk scores and unrealistic risk mitigation plans were unacceptable to the SPO.

Risk (uncertainty) assessment methodologies were also developed for a number of risk categories. Ordinal scales were developed for evaluating design and engineering, support, and technology software risk, support risk, threat risk, hardware/software integration risk, and test procedures risk. Ordinal scales were also developed for assessing the ability to meet mission objectives.

In addition, several ordinal scales initially developed to categorize mission failures associated with a historical database were transformed to consequence of occurrence scales. The resulting consequence of occurrence scales were far better suited for use by the program than the single scale used earlier by the RMWG.

We used ordinal scores in assessing all but cost and schedule risk. (Cost and schedule risk were assessed using Commercial Off The Shelf software that yields risk – encompassing both the uncertainty and consequence terms.) Although suitable ordinal scales can clearly be developed for the required risk categories, some substantial limitations exist in their use.

First Limitation. Ordinal scales yield a rank-ordered list of risk (uncertainty) ratings with generally nonlinear scale increments.

Second Limitation. Since the scores are ordinal, they are not mathematical probabilities, which are cardinal numbers.

Third Limitation. Some correlation may exist between risk subcategories and categories.

Fourth Limitation. The scale categories may not be composed of a complete set of subcategories.

Fifth Limitation. It is not mathematically possible to generate confidence intervals for ordinal scales.[3]

Future Direction

An enhanced risk management process was derived based upon experience obtained from two separate programs. Here, the RMWG functions have been split into a Risk Management Advisory Group composed of analysts, which develops, reviews, and revises risk assessments and risk mitigation plans, and a Risk Management Board composed of senior SPO managers, which is responsible for prioritizing risks and allocating resources to mitigate risks. Improved methods for performing risk assessments, planning risk mitigation, and reporting results were also developed for use by government and contractor analysts.

Closing Comments

The risk management process and information available to senior management for critical decision making was substantially improved over a 3-year period. However, as one would expect in this difficult program management area, some deficiencies can still be identified. Most of these deficiencies relate to cognitive issues associated with the reluctance to address program risk in an unbiased fashion. These problems are generally difficult to solve or even identify. For example, the National Research Council stated that the risk assessment process can be adversely impacted by:

- an inappropriate reliance on limited data;
- the tendency to impose order on random events;
- the tendency to fit ambiguous evidence into predispositions;
- the tendency to systematically omit components of risk; and
- overconfidence in the reliability of analyses.[6]

In addition, when faced with ambiguous or uncertain information, people have a tendency to interpret it as confirming their preexisting beliefs; with new data they tend to accept information that confirms their beliefs but to question new information that conflicts with them.[7]

Those responsible for program risk management must recognize that having a faithfully followed, structured risk management process is critical to maximizing program success. However, for the risk management process to yield worthwhile results it must be embraced by the senior SPO leadership and applied in an unbiased fashion.

References

1. “U. S. Air Force Acquisition Process Review Team: Clear Accountability in Design,” Final Report, April 1991, p. 3.

2. Department of Defense Directive 5000.1, *Defense Acquisition Management*, pp. 1-5, February 23, 1991.

3. Conrow, Edmund H., “The Use of Ordinal Scales in Defense Systems Engineering,” *Proceedings of the 1995 Acquisition Research Symposium*, 1995, pp. 455-463.

4. *Systems Engineering Management Guide*, Defense Systems Management College, January 1990, p. 15-1.

5. *Risk Management Concepts and Guidance*, Defense Systems Management College, March 1989, p. 3-1.

6. *Improving Risk Communication*, National Research Council, National Academy Press, 1989, pp. 45-47.

7. Ibid, p. 46.