CHAPTER 15

RISK MANAGEMENT

15.1 RISK AS REALITY

Risk is inherent in all activities. It is a normal condition of existence. Risk is the potential for a negative future reality that may or may not happen. Risk is defined by two characteristics of a possible negative future event: probability of occurrence (whether something will happen), and consequences of occurrence (how catastrophic if it happens). If the probability of occurrence is not known then one has *uncertainty*, and the risk is undefined.

Risk is not a problem. It is an understanding of the level of threat due to *potential* problems. A problem is a consequence that has already occurred.

In fact, knowledge of a risk is an opportunity to avoid a problem. Risk occurs whether there is an attempt to manage it or not. Risk exists whether you acknowledge it, whether you believe it, whether if it is written down, or whether you understand it. Risk does not change because you hope it will, you ignore it, or your boss's expectations do not reflect it. Nor will it change just because it is contrary to policy, procedure, or regulation. Risk is neither good nor bad. It is just how things are. Progress and opportunity are companions of risk. In order to make progress, risks must be understood, managed, and reduced to acceptable levels.

Types of Risk in a Systems Engineering Environment

Systems engineering management related risks could be related to the system products or to the process of developing the system. Figure 15-1 shows the decomposition of system development risks.

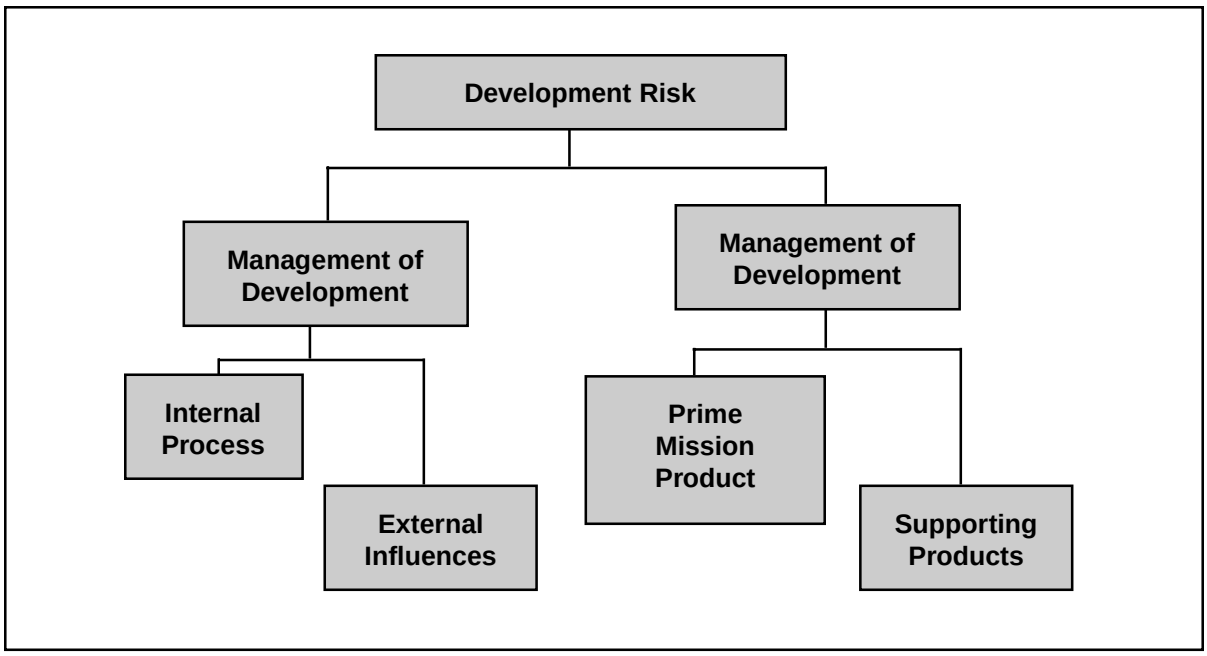

Figure 15-1. Risk Hierarchy

Risks related to the system development generally are traceable to achieving life cycle customer requirements. Product risks include both end product risks that relate to the basic performance and cost of the system, and to enabling products that relate to the products that produce, maintain, support, test, train, and dispose of the system.

Risks relating to the management of the development effort can be technical management risk or risk caused by external influences. Risks dealing with the internal technical management include those associated with schedules, resources, work flow, on time deliverables, availability of appropriate personnel, potential bottlenecks, critical path operations and the like. Risks dealing with external influences include resource availability, higher authority delegation, level of program visibility, regulatory requirements, and the like.

15.2 RISK MANAGEMENT

Risk management is an organized method for identifying and measuring risk and for selecting, developing, and implementing options for the handling of risk. It is a process, not a series of events. Risk management depends on risk management planning, early identification and analysis of risks, continuous risk tracking and reassessment, early implementation of corrective actions, communication, documentation, and coordination. Though there are many ways to structure risk management, this book will structure it as having four parts: Planning, Assessment, Handling, and Monitoring. As depicted in Figure 15-2 all of the parts are interlocked to demonstrate that after initial planning the parts begin to be dependent on each other. Illustrating this, Figure 15-3 shows the key control and feedback relationships in the process.

Risk Planning

Risk Planning is the continuing process of developing an organized, comprehensive approach to risk management. The initial planning includes establishing a strategy; establishing goals and objectives; planning assessment, handling, and monitoring activities; identifying resources, tasks, and responsibilities; organizing and training risk management IPT members; establishing a method to track risk items; and establishing a method to

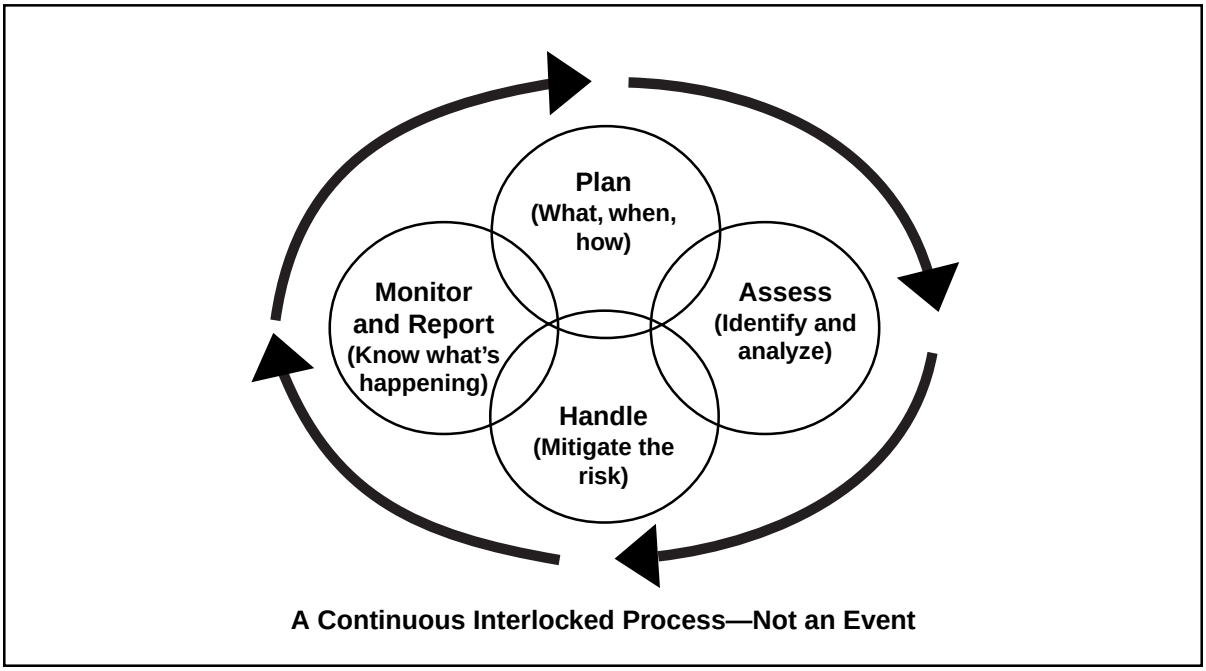

Figure 15-2. Four Elements of Risk Management

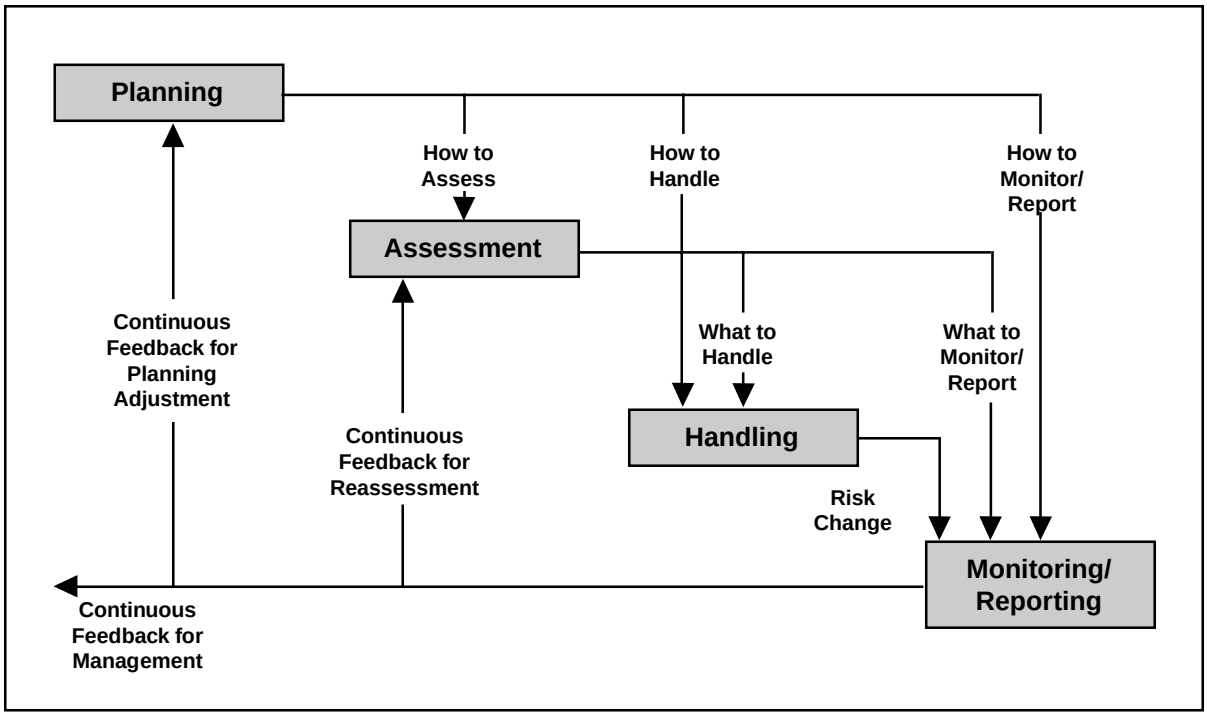

Figure 15-3. Risk Management Control and Feedback

document and disseminate information on a continuous basis.

In a systems engineering environment risk planning should be:

- Inherent (imbedded) in systems engineering planning and other related planning, such as producibility, supportability, and configuration management;
- A documented, continuous effort;
- Integrated among all activities;
- Integrated with other planning, such as systems engineering planning, supportability analysis, production planning, configuration and data management, etc.;
- Integrated with previous and future phases; and
- Selective for each Configuration Baseline.

Risk is altered by time. As we try to control or alter risk, its probability and/or consequence will change. Judgment of the risk impact and the method of handling the risk must be reassessed and potentially altered as events unfold. Since these events are continually changing, the planning process is a continuous one.

Risk Assessment

Risk assessment consists of *identifying* and *analyzing* the risks associated with the life cycle of the system.

Risk Identification Activities

Risk identification activities establish what risks are of concern. These activities include:

- Identifying risk/uncertainty sources and drivers,
- Transforming uncertainty into risk,
- Quantifying risk,
- Establishing probability, and
- Establishing the priority of risk items.

As shown by Figure 15-4 the initial identification process starts with an identification of potential risk items in each of the four risk areas. Risks related to the system performance and supporting products are generally organized by WBS and initially determined by expert assessment of teams and individuals in the development enterprise. These risks tend to be those that require follow-up quantitative assessment. Internal process and external influence risks are also determined by expert assessment within the enterprise, as well as through the use of risk area templates similar to those found in DoD 4245.7-M. The DoD 4245.7-M templates describe the risk areas associated with system acquisition management processes, and provide methods for reducing traditional risks in each area. These templates should be tailored for specific program use based on expert feedback.

After identifying the risk items, the risk level should be established. One common method is through the use of a matrix such as shown in Figure 15-5. Each item is associated with a block in the matrix to establish relative risk among them. On such a graph risk increases on the diagonal and provides a method for assessing relative risk. Once the relative risk is known, a priority list can be established and risk analysis can begin.

Risk identification efforts can also include activities that help define the probability or consequences of a risk item, such as:

- Testing and analyzing uncertainty away,
- Testing to understand probability and consequences, and
- Activities that quantify risk where the qualitative nature of high, moderate, low estimates are insufficient for adequate understanding.

Risk Analysis Activities

Risk analysis activities continue the assessment process by refining the description of identified risk event through isolation of the cause of risk, determination of the full impact of risk, and the

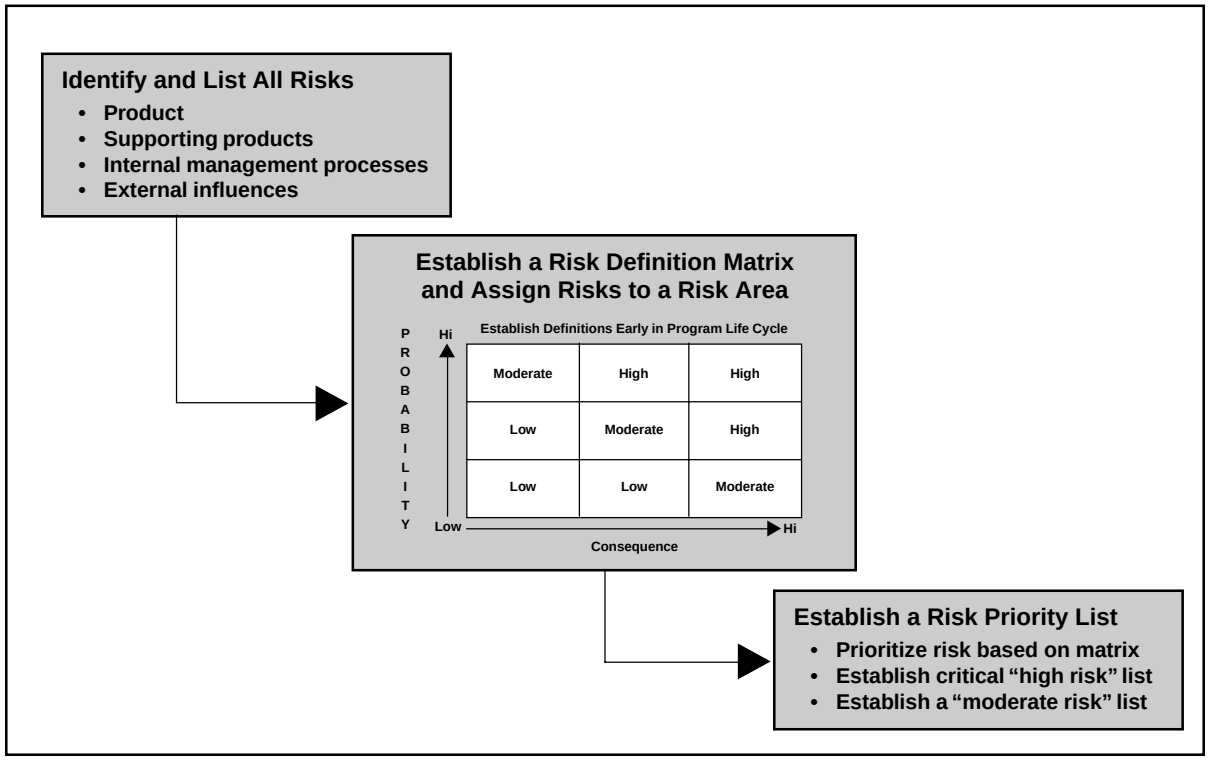

Figure 15-4. Initial Risk Identificaiton

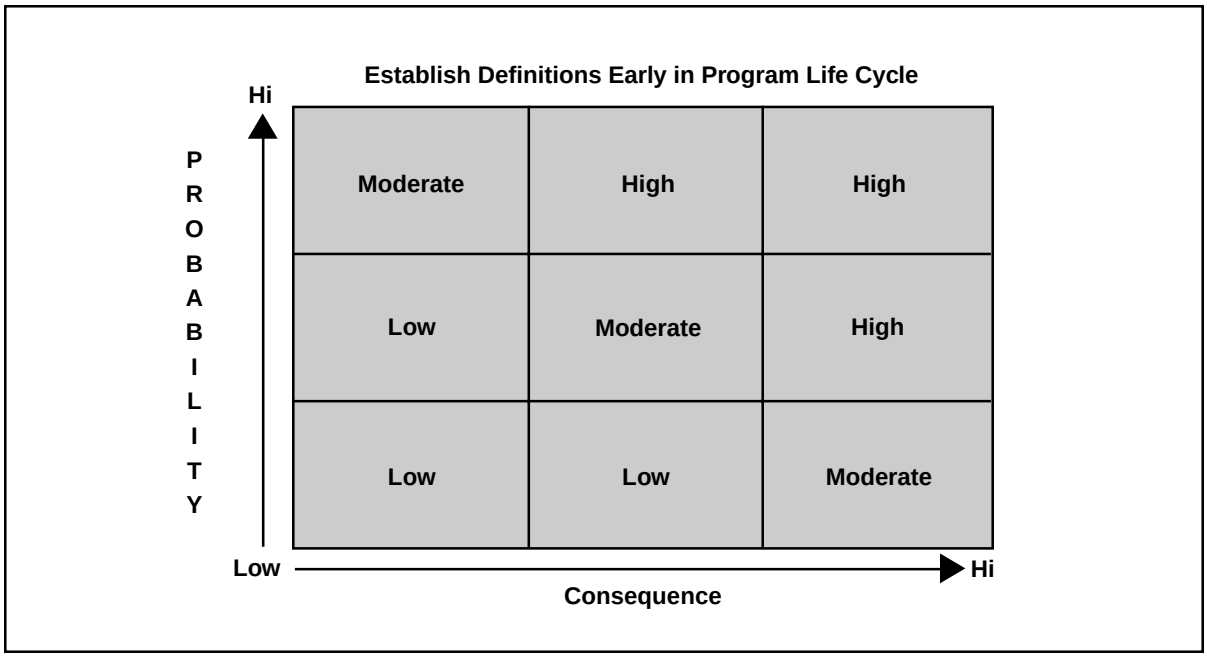

Figure 15-5. Simple Risk Matrix

determination and choose of alternative courses of action. They are used to determine what risk should be tracked, what data is used to track risk, and what methods are used to handle the risk.

Risk analysis explores the options, opportunities, and alternatives associated with the risk. It addresses the questions of how many legitimate ways the risk could be dealt with and the best way to do so. It examines sensitivity, and risk interrelationships by analyzing impacts and sensitivity of related risks and performance variation. It further analyzes the impact of potential and accomplished, external and internal changes.

Risk analysis activities that help define the scope and sensitivity of the risk item include finding answers to the following questions:

- If something changes, will risk change faster, slower, or at the same pace?
- If a given risk item occurs, what collateral effects happen?
- How does it affect other risks?
- How does it affect the overall situation?
- Development of a watch list (prioritized list of risk items that demand constant attention by management) and a set of metrics to determine if risks are steady, increasing, or decreasing.
- Development of a feedback system to track metrics and other risk management data.
- Development of quantified risk assessment.

Quantified risk assessment is a formal quantification of probabilities of occurrence and consequences using a top-down structured process following the WBS. For each element, risks are assessed through analysis, simulation and test to determine statistical probability and specific conditions caused by the occurrence of the consequence.

Cautions in Risk Assessments

Reliance solely on numerical values from simulations and analysis should be avoided. Do not lose sight of the actual source and consequences of the risks. Testing does not eliminate risk. It only

provides data to assess and analyze risk. Most of all, beware of manipulating relative numbers, such as 'risk index" or "risk scales," even when based on expert opinion, as quantified data. They are important information, but they are largely subjective and relative; they do not necessarily define risk accurately. Numbers such as these should always be the subject of a sensitivity analysis.

Risk Handling

Once the risks have been categorized and analyzed, the process of handling those risks is initiated. The prime purpose of risk handling activities is to mitigate risk. Methods for doing this are numerous, but all fall into four basic categories:

- Risk Avoidance,
- Risk Control,
- Risk Assumption, and
- Risk Transfer.

Avoidance

To avoid risk, remove requirements that represent uncertainty and high risk (probability or consequence.) Avoidance includes trading off risk for performance or other capability, and it is a key activity during requirements analysis. Avoidance requires understanding of priorities in requirements and constraints. Are they mission critical, mission enhancing, nice to have, or "bells and whistles?"

Control

Control is the deliberate use of the design process to lower the risk to acceptable levels. It requires the disciplined application of the systems engineering process and detailed knowledge of the technical area associated with the design. Control techniques are plentiful and include:

- Multiple concurrent design to provide more than one design path to a solution,
- Alternative low-risk design to minimize the risk of a design solution by using the lowest-risk design option,
- Incremental development, such as preplanned product improvement, to dissociate the design from high-risk components that can be developed separately,
- Technology maturation that allows high-risk components to be developed separately while the basic development uses a less risky and lower-performance temporary substitute,
- Test, analyze and fix that allows understanding to lead to lower risk design changes. (Test can be replaced by demonstration, inspection, early prototyping, reviews, metric tracking, experimentation, models and mock-ups, simulation, or any other input or set of inputs that gives a better understanding of the risk),
- Robust design that produces a design with substantial margin such that risk is reduced, and
- The open system approach that emphasizes use of generally accepted interface standards that provide proven solutions to component design problems.

Acceptance

Acceptance is the deliberate acceptance of the risk because it is low enough in probability and/or consequence to be reasonably assumed without impacting the development effort. Key techniques for handling accepted risk are budget and schedule reserves for unplanned activities and continuous assessment (to assure accepted risks are maintained at acceptance level). The basic objective of risk management in systems engineering is to reduce all risk to an acceptable level.

The strong budgetary strain and tight schedules on DoD programs tends to reduce the program manager's and system engineer's capability to provide reserve. By identifying a risk as acceptable, the worst-case outcome is being declared acceptable. Accordingly, the level of risk considered acceptable should be chosen very carefully in a DoD acquisition program.

Transfer

Transfer can be used to reduce risk by moving the risk from one area of design to another where a design solution is less risky. Examples of this include:

- Assignment to hardware (versus software) or vice versa; and
- Use of functional partitioning to allocate performance based on risk factors.

Transfer is most associated with the act of assigning, delegating, or paying someone to assume the risk. To some extent transfer always occurs when contracting or tasking another activity. The contract or tasking document sets up agreements that can transfer risk from the government to contractor, program office to agency, and vice versa. Typical methods include insurance, warranties, and incentive clauses. Risk is never truly transferred. If the risk isn't mitigated by the delegated activity it still affects your project or program.

Key areas to review before using transfer are:

- How well can the delegated activity handle the risk? Transfer is effective only to the level the risk taker can handle it.
- How well will the delegated activity solution integrate into your project or program? Transfer is effective only if the method is integrated with the overall effort. For example, is the warranty action coordinated with operators and maintainers?
- Was the method of tasking the delegated activity proper? Transfer is effective only if the transfer mechanism is valid. For example, can incentives be "gamed?"
- Who has the most control over the risk? If the project or program has no or little control over the risk item, then transfer should be considered to delegate the risk to those most likely to be able to control it.

Monitoring and Reporting

Risk monitoring is the continuous process of tracking and evaluating the risk management process by metric reporting, enterprise feedback on watch list items, and regular enterprise input on potential developing risks. (The metrics, watch lists, and feedback system are developed and maintained as an assessment activity.) The output of this process is then distributed throughout the enterprise, so that all those involved with the program are aware of the risks that affect their efforts and the system development as a whole.

Special Case – Integration as Risk

Integration of technologies in a complex system is a technology in itself! Technology integration during design may be a high-risk item. It is not normally assessed or analyzed as a separately identified risk item. If integration risks are not properly identified during development of the functional baseline, they will demonstrate themselves as serious problems in the development of the product baseline.

Special Case – Software Risk

Based on past history, software development is often a high-risk area. Among the causes of performance, schedule, and cost deficiencies have been:

- Imperfect understanding of operational requirements and its translation into source instructions,
- Risk tracking and handling,
- Insufficient comprehension of interface constraints, and
- Lack of sufficient qualified personnel.

Risk Awareness

All members of the enterprise developing the system must understand the need to pay attention to the existence and changing nature of risk.

Consequences that are unanticipated can seriously disrupt a development effort. The uneasy feeling that something is wrong, despite assurances that all is fine may be valid. These kinds of intuitions have allowed humanity to survive the slings and arrows of outrageous fortune throughout history. Though generally viewed as non-analytical, these apprehensions should not be ignored. Experience indicates those non-specific warnings have validity, and should be quantified as soon as possible.

15.3 SUMMARY POINTS

- Risk is inherent in all activities.
- Risk is composed of knowledge of two characteristics of a possible negative future event: probability of occurrence and consequences of occurrence.
- Risk management is associated with a clear understanding of probability.
- Risk management is an essential and integral part of technical program management (systems engineering).
- Risks and uncertainties must be identified, analyzed, handled, and tracked.
- There are four basic ways of handling risk: avoidance, transfer, acceptance, and control.
- Program risks are classified as low, moderate, or high depending on consequences and probability of occurrence. Risk classification should be based on quantified data to the extent possible.

SUPPLEMENT 15-A

RISK MANAGEMENT IN DOD ACQUISITION

Policy

DoD policy is quite clear in regard to risk management: it must be done.

The PM shall identify the risk areas in the program and integrate risk management within overall program management. (DoD 5000.2-R.)

In addition, DoDD 5000.4 identifies risk and cost analysis as a responsibility of the program manager.

Risk Management View

A DSMC study indicates that major programs which declared moderate risk at Milestone B have been more successful in terms of meeting cost and schedule goals than those which declared low risk (DSMC TR 2-95). This strongly implies that program offices that understand and respect risk management will be more successful. For this reason, the program office needs to adopt a systems-level view of risk. The systems engineer provides this view. Systems Engineering is the cornerstone of program office risk management program because it is the connection to realistic assessment of product maturity and development, and the product is, in the final analysis, what system acquisition is really about.

However, the program office has external risks to deal with as well as the internal risks prevalent in the development process. The Systems Engineer has to provide the program manager internal risk data in a manner that aids the handling of the external risks. In short, the systems engineer must present bad news such that it is reasonable and compelling to higher levels of authority. See Chapter 20 for further discussion on this topic.

Factoring Risk Management into the Process

Risk management, as an integral part of the overall program planning and management process, is enhanced by applying a controlled, consistent, approach to systems engineering and using integrated teams for both product development and management control. Programs should be transitioned to the next phase only if risk is at the appropriate level. Know the risk drivers behind the estimates. By its nature there are always subjective aspects to assessing and analyzing risk at the system level, even though they tend to be represented as quantitative and/or analytically objective.

Risk and Phases

Risk management begins in the Concept and Technology Development phase. During Concept Exploration initial system level risk assessments are made. Unknown-unknowns, uncertainty, and some high-risk elements are normal and expected. When substantial technical risk exists, the Component Advanced Development stage is appropriate, and is included in the life-cycle process specifically as an opportunity to address and reduce risks to a level that are consistent with movement into systems acquisition.

The S&T community has a number of vehicles available that are appropriate for examining technology in application and for undertaking risk reduction activities. These include Advanced Technology Demonstrations, Advanced Concept Technology Demonstrations, as well as Joint Warfighting Experiments. The focus of the activities undertaken during these risk reduction stages include:

- Testing, analyzing, or mitigating system and subsystem uncertainty and high risk out of the program.

- Demonstrating technology sufficient to uncover system and subsystem unknown-unknowns (especially for integration).

- Planning for risk management during the transition to and continuation of systems acquisition during the System Development and Demonstration phase, especially handling and tracking of moderate risk.

System Development and Demonstration requires the application of product and manufacturing engineering, which can be disrupted if the technology development is not sufficient to support engineering development. Risk management in during this phase emphasizes:

- Reduction and control of moderate risks,

- All risks under management including emerging ones, and

- Maintenance of risk levels and reaction to problems.

Objective Assessment of Technology

The revised acquisition process has been deliberately structured to encourage and allow programs to progress through appropriate risk reduction stages and phases, based on an objective assessment of the maturity levels associated with the products and systems under development. It is therefore, particularly important that program managers and their staffs ensure that the decisions made regarding recommendations to proceed, and the paths to be taken, be based on as impartial and objective opinions as possible. The temptation is always to move ahead and not to delay to improve the robustness of a given product or system. When systems are hurried into engineering development and production, in spite of the fact that the underlying technologies require further development, history indicates that the results will eventually show the fallacy of speed over common sense. And to fix the problem in later stages of development—or even after deployment—can be hugely expensive in terms of both monetary cost and human lives.

The prevailing presumption at Milestone B is that the system is ready for engineering development. After this, the acquisition community generally assumes that risk is moderate to low, that the technology is "available." There is evidence to support the assertion that programs often progress into engineering development with risks that actually require substantial exploratory and applied research and development to bring them to the moderate levels of risk or lower. One approach that has proven successful in making objective risk assessments is the use of independent evaluation teams. Groups that have no pre-determined interest to protect or axe to grind are often capable of providing excellent advice regarding the extent to which a system is ready to proceed to the next level of development and subsequent phases.

Risk Classification on the System (Program) Level

Classification definitions should be established early and remain consistent throughout the program. The program office should assess the risks of achieving performance, schedule, and cost in clear and accurate terms of both probability and consequence. Where there is disagreement about the risk, assessment efforts should be immediately increased. Confusion over risk is the worst program risk, because it puts in doubt the validity of the risk management process, and therefore, whether program reality is truly understood.

The system level risk assessment requires integration and interpretation of the quantified risk assessment of the parts. This requires reasonable judgement. Because integration increases the potential for risk, it is reasonable to assume overall risk is not better than the sum of objective data for the parts.

Reality Versus Expectations

Program managers are burdened with the expectations of superiors and others that have control over the program office's environment. Pressure to accommodate these expectations is high. If the systems engineer cannot communicate the reality of risk in terms that are understandable, acceptable, or sufficiently verifiable to management, then these pressures may override vertical communication of actual risk.

Formal systems engineering with risk management incorporated can provide the verifiable information. However, the systems engineer also has the responsibility to adequately explain probability and consequences such that the program manager can accept the reality of the risk and override higher level expectations.

Uncertainty is a special case, and very dangerous in an atmosphere of high level expectations. Presentation of uncertainty issues should strongly emphasize consequences, show probability trends, and develop "most likely" alternatives for probability.

SUPPLEMENT 15-B

MODEL FOR SYSTEM LEVEL RISK ASSESSMENT

The following may be used to assist in making preliminary judgments regarding risk classifications:

	Low Risk	Moderate Risk	High Risk
Consequences	Insignificant cost, schedule, or technical impact	Affects program objectives, cost, or schedule; however cost, schedule, performance are achievable	Significant impact, requiring reserve or alternate courses of action to recover
Probability of Occurrence	Little or no estimated likelihood	Probability sufficiently high to be of concern to management	High likelihood of occurrence
Extent of Demonstration	Full-scale, integrated technology has been demonstrated previously	Has been demonstrated but design changes, tests in relevant environments required	Significant design changes required in order to achieve required/desired results
Existence of Capability	Capability exists in known products; requires integration into new system	Capability exists, but not at performance levels required for new system	Capability does not currently exist

Also see Technology Readiness Levels matrix in Chapter 2