Understanding Risk Management

Software Technology Support Center

The U.S. Air Force's Software Technology Support Center offers an updated and condensed version of the "Guidelines for Successful Acquisition and Management of Software-Intensive Systems" (GSAM) on its Web site <www.stsc.hill.af.mil/resources/tech_docs>. This article is taken from Chapter 5 "Risk Management" of the GSAM (Version 4.0). We are pleased that all editions have been so well received and that many individuals and programs have worked hard to implement the principles contained therein. The latest edition provides a usable desk reference that gives a brief but effective overview of important software acquisition and development topics, provides checklists for rapid self-inspection, and provides pointers to additional information on the topics covered.

Risk is a product of the uncertainty of future events and is a part of all activity. It is a fact of life. We tend to stay away from situations that involve high risk to things we hold dear. When we cannot avoid risk, we look for ways to reduce it or its impact upon our lives. Yet even with careful planning and preparation, risks cannot be completely eliminated because they cannot all be identified beforehand. Even so, risk is essential to progress.

The opportunity to succeed also carries the opportunity to fail. It is necessary to learn to balance the possible negative consequences of risk with the potential benefits of its associated opportunity [1]. Risk may be defined as the possibility to suffer damage or loss. The possibility is characterized by three factors [1]:

1. The probability or likelihood that loss or damage will occur.
2. The expected time of occurrence.
3. The magnitude of the negative impact that can result from its occurrence.

The seriousness of a risk can be determined by multiplying the probability of the event actually occurring by the potential negative impact to the cost, schedule, or performance of the project:

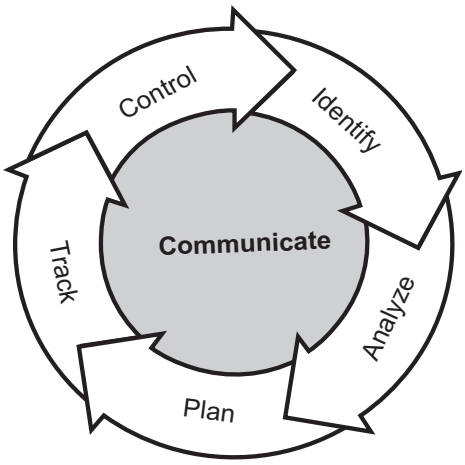
Risk Severity = Probability of Occurrence x Potential Negative Impact

Thus, risks where probability of occurrence is high and potential impact is very low, or vice versa, are not considered as serious as risks where both probability of occurrence and potential impact are medium to high.

Project managers recognize and accept the fact that risk is inherent in any project. They also recognize that there are two ways of dealing with risk. One, risk management, is proactive and carefully analyzes future project events and past projects to identify potential risks. Once risks are identified, they are dealt with by taking measures to reduce their probability or to reduce their impact. The alternative to risk management is crisis management. It is a reactive and resource-intensive process, with available options constrained or restricted by events [1].

Effective risk management requires establishing and following a rigorous process. It involves the entire project team, as well as requiring help from outside experts in critical risk areas (e.g., technology, manufacturing, logistics, etc.). Because risks will be found in all areas of the project and will often be interrelated, risk management should include hardware, software, integration issues, and the human element [2].

Figure 1: *Software Engineering Institute's Risk Management Paradigm [3]*



Process Description

Various paradigms are used by different organizations to coordinate their risk management activities. A commonly used approach is shown in Figure 1. While there are variations in the different paradigms, certain characteristics are universally required for the program to be successful [2]:

- The risk management process is planned and structured.
- The risk process is integrated with the acquisition process.
- Developers, users, procurers, and all other stakeholders work together closely to implement the risk process.
- Risk management is an ongoing process with continual monitoring and reassessment.
- A set of success criteria is defined for all cost, schedule, and performance elements of the project.
- Metrics are defined and used to monitor effectiveness of risk management strategies.
- An effective test and evaluation program is planned and followed.
- All aspects of the risk management program are formally documented.
- Communication and feedback are an integral part of all risk management activities.

While your risk management approach should be tailored to your project needs, it should incorporate these fundamental characteristics. The process is iterative and should have all the components shown in Figure 2. Note that while planning appears as the first step, there is a feedback loop from the monitoring activity that allows planning and the other activities to be redone or controlled by actual results, providing continual updates to the risk management strategy. In essence, the process is a standard approach to problem solving:

1. Plan or define the problem-solving process.
2. Define the problem.
3. Work out solutions for those problems.
4. Track the progress and success of the solutions.

The following sections expand upon the risk management approach.

Planning

Risk planning includes developing and documenting a structured, proactive, and comprehensive strategy to deal with risk. Key to this activity is establishing methods and procedures to do the following:

1. Establish an organization to take part in the risk management process.
2. Identify and analyze risks.
3. Develop risk-handling plans.
4. Monitor or track risk areas.
5. Assign resources to deal with risks.

A generic sample risk management plan can be found in Appendix B of the "Risk Management Guide for DoD Acquisition" [4].

Assessment

Risk assessment involves two primary activities: risk identification and risk analysis. Risk identification is actually begun early in the planning phase and continues throughout the life of the project. The following methods are often used to identify possible risks [1]:

- Brainstorming.
- Evaluations or inputs from project stakeholders.
- Periodic reviews of project data.
- Questionnaires based on taxonomy, the classification of product areas and disciplines.
- Interviews based on taxonomy.
- Analysis of the Work Breakdown Structure.
- Analysis of historical data.

When identifying a risk it is essential to do so in a clear and concise statement. It should include three components [1]:

1. **Condition:** A sentence or phrase briefly describing the situation or circumstance that may have caused concern, anxiety, or uncertainty.
2. **Consequence:** A sentence describing the key negative outcomes that may result from the condition.
3. **Context:** Additional information about the risk to ensure others can understand its nature, especially after the passage of time.

Table 1 is an example of a risk statement [1].

The other half of assessment is risk analysis. This is the process of examining each risk to refine the risk description, isolate the cause, quantify the probability of occurrence, and determine the nature and impact of possible effects. The result of this process is a list of risks rated and prioritized according to their probability of occurrence, severity of impact, and relationship to other risk areas [2].

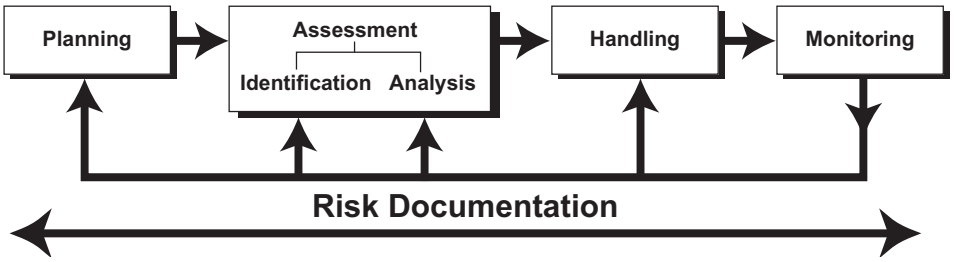


Figure 2: *Risk Management Process Example*

Condition	End users submit requirements changes even though we are in the design phase and the requirements have been baselined.
Consequence	Changes could extend system design cycle and reduce available coding time.
Probability and Impact	80%. $2 million.
Mitigation Actions	Who, what, and when?

Table 1: *Risk Statement Example*

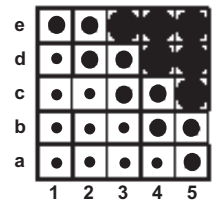
Once risks have been defined, and probability of occurrence and consequences assigned, the risk can be rated as to its severity. This facilitates prioritizing risks and deciding what level of resources to devote to each risk. Figure 3 depicts an assessment model using risk probability and consequence levels in a matrix to determine a level of risk severity. In addition to an overall method of risk rating, the model also gives good examples of probability levels and types and levels of consequences. The ratings given in the assessment guide matrix are suggested minimum ratings. It may be necessary to adjust the moderate and high thresholds to better coincide with the type of project.

Figure 3: *Defense Acquisition University Assessment Model [4]*

PROBABILITY

Level	Likelihood Risk Will Happen
a	Minimal/Remote
b	Small/Unlikely
c	Probable/Likely
d	Large/Highly Likely
e	Significant/Near Certainty

ASSESSMENT GUIDE



RISK IMPACT RATING

●	**HIGH:** Significant impact on cost, schedule, and performance. Significant action required. High priority management attention required.
●	**MODERATE:** Some impact. Special action may be required. Additional management attention may be needed.
●	**LOW:** Minimum impact. Normal oversight needed to ensure risk remains low.

CONSEQUENCE

Level	Technical Performance	Schedule	Cost	Impact on Other Teams
1	Minimal or No Impact	Minimal or No Impact	Minimal or None	None
2	Acceptable With Some Reduction in Margin	Additional Resources Required – Able to Meet Need Dates	< 5%	Some
3	Acceptable With Significant Reduction in Margin	Minor Slip in Key Milestone – Not Able to meet Need Dates	5% - 7%	Moderate
4	Acceptable – No Remaining Margin	Minor Slip in Key Milestone or Critical Path Impacted	7% - 10%	Major
5	Unacceptable	Cannot Achieve Key Team of Major Project Milestone	> 10%	Unacceptable

Figure 4: *Risk Handling Process*

Handling

Risk handling is the process that identifies, evaluates, selects, and implements options for mitigating risks, as shown in Figure 4. Two approaches are used in handling risk. The first is to employ options that reduce the risk itself. This usually involves a change in current conditions to lessen the probability of occurrence. The second approach, often employed where risk probability is high, is to use options that reduce the negative impact to the project if the risk condition should occur. Improving jet engine maintenance and inspection procedures to reduce the risk of in-flight engine failure is an example of the first approach. Providing a parachute for the pilot, to reduce loss if the risk condition should occur, is an example of the second approach.

Monitoring

Risk monitoring is the process of continually tracking risks and the effectiveness of risk handling options to ensure risk conditions do not get out of control. This is done by knowing the baseline risk management plans, understanding the risks and risk handling options, establishing meaningful metrics, and evaluating project performance against the established metrics, plans, and expected results throughout the acquisition process. Continual monitoring also enables new risks to be identified if they become apparent over time. Monitoring further reveals the interrelationships between various risks [2].

The monitoring process provides feedback into all other activities to improve the ongoing, iterative risk management process for the current and future projects.

Documentation

Risk documentation is absolutely essential for the current, as well as future, projects. It consists of recording, maintaining, and reporting risk management plans, assessments, and handling information. It also includes recording the results of risk management activities, providing a knowledge base for better risk management in later stages of the project and in other projects [2]. Documentation should include – as a minimum – the following information:

- Risk management plans.
- Project metrics to be used for risk management.
- Identified risks and their descriptions.
- The probability, severity of impact, and prioritization of all known risks.
- Description of risk handling options selected for implementation.
- Project performance assessment results, including deviations from the baseline plans.
- Records of all changes to the above documentation, including newly identified risks, plan changes, etc.

Risk Management Checklist

This checklist is provided to assist you in risk management. If you answer no to any of these questions, you should examine the situation carefully for the possibility of greater risks to the project. This is only a cursory checklist for such an important subject. Please see [5, 6] for more detailed checklists.

- ❑ Do you have a comprehensive, planned, and documented approach to risk management?
- ❑ Are all major areas/disciplines represented on your risk management team?
- ❑ Is the project manager experienced with similar projects?
- ❑ Do the stakeholders support disciplined development methods that incorporate adequate planning, requirements analysis, design, and testing?
- ❑ Is the project manager dedicated to this project, and not dividing his or her time among other efforts?
- ❑ Are you implementing a proven development methodology?
- ❑ Are requirements well defined, understandable, and stable?
- ❑ Do you have an effective requirements change process in place, and do you use it?
- ❑ Does your project plan call for tracking/tracing requirements through all phases of the project?
- ❑ Are you implementing proven technology?
- ❑ Are suppliers stable, and do you have multiple sources for hardware and equipment?
- ❑ Are all procurement items needed for your development effort short lead-time items (no long-lead items)?
- ❑ Are all external and internal interfaces for the system well defined?
- ❑ Are all project positions appropriately staffed with qualified, motivated personnel?
- ❑ Are the developers trained and experienced in their respective development disciplines (i.e., systems engineering, software engineering, language, platform, tools, etc.)?
- ❑ Are developers experienced or familiar with the technology and the development environment?
- ❑ Are key personnel stable and likely to remain in their positions throughout the project?
- ❑ Is project funding stable and secure?
- ❑ Are all costs associated with the project known?
- ❑ Are development tools and equipment used for the project state-of-the-art, dependable, and available in sufficient quantity, and are the developers familiar with the development tools?
- ❑ Are the schedule estimates free of unknowns?
- ❑ Is the schedule realistic to support an acceptable level of risk?
- ❑ Is the project free of special environmental constraints or requirements?
- ❑ Is your testing approach feasible and appropriate for the components and system?
- ❑ Have acceptance criteria been established for all requirements and agreed to by all stakeholders?
- ❑ Will there be sufficient equipment to do adequate integration and testing?
- ❑ Has sufficient time been scheduled for system integration and testing?
- ❑ Can software be tested without complex testing or special test equipment?
- ❑ Is a single group in one location developing the system?
- ❑ Are subcontractors reliable and proven?
- ❑ Is all project work being done by groups over which you have control?
- ❑ Are development and support teams all collocated at one site?
- ❑ Is the project team accustomed to working on an effort of this size (neither bigger nor smaller)?

Summary

Project managers recognize and accept the fact that risk is inherent in any project. The most successful project managers choose to deal proactively with risk. They carefully analyze future project events and past projects to identify potential risks. Once risks are identified, managers take steps to reduce their probability or reduce the impact associated with them by establishing and following a

rigorous process, which involves the entire project team as well as outside experts. Risk management should include hardware, software, integration issues, and the human element. A risk management process includes planning, assessment, handling, monitoring, and documentation. Risk is a product of the uncertainty of future events and is a part of all activity. Learning to balance its possible negative consequences with its potential benefits is the key to successful risk management.◆

References

1. Software Technology Support Center. "Life Cycle Software Project Management." Project Initiation. Hill Air Force Base, UT, 9 Oct. 2001.
2. Department of Defense. "Risk Management Guide for DoD Acquisition." Washington, D.C.: DoD Feb. 2001: Chap. 2 <www.dsmc.dsm.mil/pubs/gdbks/risk_management.htm>.
3. Higuera, Ron, and Yacov Haimes. "Software Risk Management." Pittsburgh, PA: Software Engineering Institute, 28 June 1996 <www.sei.cmu.edu/publications/documents/96.reports/96.tr.012.html>.
4. Department of Defense. "Risk Management Guide for DoD Acquisition." Washington, D.C.: DoD, Feb. 2001: Appendix B <www.dsmc.dsm.mil/pubs/gdbks/risk_management.htm>.
5. Arizona State University. "Question List for Software Risk Identification in the Classroom." <www.eas.asu.edu/~riskmgmt/qlist.html>.
6. Department of Energy. Risk Assessment Questionnaire. <http://cio.doe.gov/sqse/pm_risk.htm>.

About the Author

The **Software Technology Support Center** (STSC) produced the "Guidelines for Successful Acquisition and Management of Software-Intensive Systems." Visit the STSC Web site at <www.stsc.hill.af.mil/resources/tech_docs> to access all 17 chapters of this document. The STSC is dedicated to helping the Air Force and other U.S. government organizations improve their capability to buy and build software better. The STSC provides hands-on assistance in adopting effective technologies for software-intensive systems. The STSC helps organizations identify, evaluate, and adopt technologies that improve software product quality, production efficiency, and predictability. Technology is used in its broadest sense to include processes, methods, techniques, and tools that enhance human capability. The STSC offers consulting services for software process improvement, software technology adoption, and software technology evaluation, including the Capability Maturity Model® Integration, software acquisition, project management, risk management, cost and schedule estimation, configuration management, software measurement, and more.

Software Technology Support Center
6022 Fir AVE BLDG 1238
Hill AFB, UT 84056-5820
Phone: (801) 586-0154
DSN: 586-0154
E-mail: stsc.consulting@hill.af.mil