Continuing Risk Management at NASA

The NASA Goddard Space Flight Center (GSFC) Software Assurance Technology Center (SATC) teaches a risk management process based on a course developed in collaboration with the Software Engineering Institute at Carnegie Mellon University. This risk management process has been taught to projects at all NASA Centers and is being successfully implemented on many projects. This paper will discuss the six primary functions of risk management and will give project managers the information they need to understand if risk management is to be effectively implemented on their projects at a cost they can afford.

Software risk management is important because it helps avoid disasters, rework, and overkill, but more importantly because it stimulates win-win situations. Software risk management objectives are to identify, address, and eliminate software risk items before they become threats to success or major sources of rework. In general, good project managers are also good risk managers. It makes good business sense for software development projects to incorporate risk management as part of project management.

NPG 7120.5A, the NASA guidebook for project managers, requires risk management applications and includes a section briefly discussing what should be included in a risk management plan [1]. The SEI-developed course on continuous risk management was first taught in January 1998[1] [2]. Since then, more than 300 students at NASA centers have attended the course.

There are a number of definitions and uses for the term *risk*, but there is no universally accepted definition. What all definitions have in common is agreement that risk has two characteristics:

uncertainty: An event may or may not happen.

loss: An event has unwanted consequences or losses.

Therefore, risk involves the likelihood that an undesirable event will occur, and the consequences can be severe. Risk management can:

- Identify and deal with potential problems before they *are* problems and before a crisis exists.
- .Focus on the project's objective and consciously look for things that may affect quality throughout the production process.
- Allow the early identification of potential problems (the proactive approach) and provide input into management decisions regarding resource allocation.
- Involve personnel at all levels of the project; focus their attention on a shared product vision, and provide a mechanism for achieving it.
- Increase the chances of project success.

NASA focuses on continuous risk management that can be applied to any development process: hardware, software, systems, etc. It provides a disciplined environment for proactive decision making to:

- Continually assess what could go wrong.
- Determine which risks are important.
- Implement strategies to deal with them.
- Assure measured effectiveness of implemented strategies.

Risk management must not be allowed to become shelfware. The process must be a part of regularly scheduled, periodic product management. It requires routinely identifying and managing risks throughout all phases of the project's life. The set of continuous risk management functions throughout a project's life cycle is the foundation for the application of continuous risk management. Each risk nominally goes through these functions sequentially, but the activity occurs continuously, concurrently, and iteratively. Risks are usually tracked in parallel while new risks are identified and analyzed, and the mitigation plan for one risk may yield another risk.

Continuous Risk Management Principle Functions

Identify

The purpose of identification is to consider risks before they become problems and to incorporate this information into the project management process. Anyone in a project can identify risks to the project. Each individual has particular knowledge about various parts of a project. Uncertainties and issues about the project are transformed into distinct (tangible) risks that can be described and measured.

During this function, all risks are written with the same, two-part format. The first part is the risk statement, written as a single statement concisely specifying the cause of the concern as well as its impact. The second part may contain additional supporting details in the form of a context.

A risk statement's aim is to be clear, concise, and sufficiently informative that the risk is easily understood. Risk statements in standard format must contain two parts: the condition and the consequence. The condition/consequence format provides a complete picture of the risk, which is critical during mitigation planning. It is read as follows:

given the ***<condition>*** *there is a possibility that* ***<consequence>*** *will occur*

The *condition* component focuses on what is currently causing concern; it must be something that is true or widely perceived to be true. This component provides useful information when determining how to mitigate a risk. The *consequence* component focuses on the risk's intermediate and long-term impact. Understanding the depth and breadth of the impact is useful in determining how much time, resources, and effort should be allocated to the mitigation effort. A well-formed risk statement usually has only one condition, but may have more than one consequence.

Risk statements should avoid abbreviations or acronyms that are not readily understood, sweeping generalizations, and irrelevant detail

Since the risk statement is to be concise, a context is added to provide enough additional information about the risk to ensure that the original intent of the risk can be understood by other personnel, particularly after time has passed. An effective context captures the what, when, where, how, and why of the risk by describing the circumstances, contributing factors, and related issues (background and additional information not in the risk statement).

A diagram of the complete risk statement and context are shown in Figure 1.

An example is shown in Figure 2. One condition and two consequences are the risk statement. The context explains

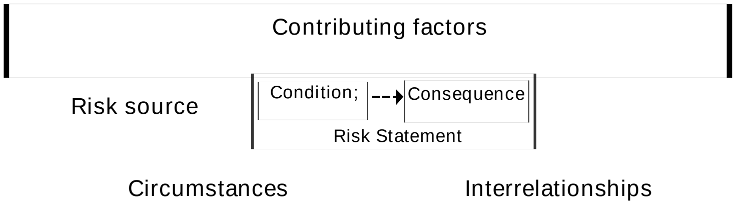

Figure 1. *Risk Statement and Context*

Risk statement: This is the first time that the software staff will use OOD; the staff may have a lower-than-expected productivity rate and schedules may slip because of the associated learning curve.

Context: Object-oriented development is a very different approach that requires special training. There will be a learning curve until the staff is up to speed. The time and resources must be built in for this or the schedule and budget will overrun.

Figure 2. *Example of Risk Statement and Context*

why this is a risk, and supplies additional information for someone unfamiliar with this risk.

Risk identification depends heavily on both open communication and a forward-looking view to encourage all personnel to bring forward new risks and plan beyond their immediate problems. Although individual contributions play a role in risk management, teamwork improves the chances of identifying new risks. It allows personnel to combine their knowledge and understanding of the project.

Analyze

The purpose of analysis is to convert data into decision-making information. Analysis is a process of examining the risks in detail to determine the extent of the risks, how they interrelate, and which ones are the most important. Analyzing risks has three basic activities: evaluating their attributes (impact, probability, and time frame), classifying, and prioritizing or ranking them.

Evaluating—The first step provides better understanding of the risk by qualifying the expected impact, probability, and time frame. This involves establishing values for:

Impact: the loss or negative affect on the project should the risk occur

Probability: the likelihood
the risk will occur

Time frame: the period when action must be taken in order to mitigate the risk

Figure 3 shows sample values used to evaluate a risk's attributes.

Classifying—The next step is to classify risks. There are several ways to classify or group risks. The ultimate purpose of classification is to understand the nature of the risks facing the project and to group any related risks to build more cost-effective mitigation plans. The process of clarifying risks may reveal that two or more risks are equivalent—the statements of risk and context indicate that the subject of these risks is the same. Equivalent risks are duplicate statements of the same risk and should be combined into one.

Prioritize—The final step in the analysis function is to prioritize the risks. The purpose is to sort through a large number of risks and determine which are more important—the few vital risks—and to separate the risks to be dealt with first when allocating resources. This involves partitioning risks or groups of risks based on the *vital few* sense and ranking risks or sets of risks based on consistently applying an established set of criteria. No project has unlimited resources with which to mitigate risks. It is essential to determine consistently and efficiently which are more important and then to focus those limited resources on mitigating risks.

Conditions and priorities will change during a project, and this natural evolution can affect the important risks to a project. *Risk analysis must be a continual process.* Analysis requires open communication so that prioritization and evaluation are accomplished using all known information. A forward-looking view enables personnel to consider long-range impact.

Plan

Planning is the function of deciding what, if anything, should be done about a risk or set of related risks. Decisions and mitigation strategies are developed based on current knowledge of project risks. The purpose of plan is to:

- Make sure the consequences and sources of risk are known.
- Develop effective plans.
- Plan efficiently (only as much as needed or is of benefit).
- Produce the correct set of actions over time that minimize the cost and schedule impacts of risks while maximizing opportunity and value.
- Plan important risks first

There are four options to consider when planning for risks:

1. Research: establish a plan to research the risk(s).
2. Accept: decide to *accept* the risk(s), and document the rationale behind the decision.
3. Watch: monitor risk conditions for any indications of change in probability or impact (tracking metrics must be established and documented).
4. Mitigate: allocate resources and assign actions in order to reduce the probability or potential impact of risks. This can range from simple tasking to sweeping activities:
    - Action Items: a series of discrete tasks to mitigate risk.
    - Task Plan: formal, well-documented and larger in scope.

Attribute	Value	Description
Probability	Very Likely (H) Probable (M) Improbable (L)	High chance of this risk occurring, thus becoming a problem > 70% Risk like this may turn into a problem once in a while {30% < x < 70%} Not much chance this will become a problem {0% < x < 30%}
Impact	Catastrophic (H)	Loss of system; unrecoverable failure of system operations; major damage to system; schedule slip causing launch date to be missed; cost overrun greater than 50% of budget
	Critical (M)	Minor system damage to system with recoverable operational capacity; cost overrun exceeding 10% (but less than 50% of planned cost)
	Marginal (L)	Minor system damage to project; recoverable loss of operational capacity; internal schedule slip that does not impact launch date cost overrun less than 10% of planned cost
Timeframe	Near-term (N) Mid-term (M) Far-term (F)	Within 30 days 1 to 4 months from now more than 4 months from now *NOTE: refers to when action must be taken*

Figure 3. *Sample Attribute Values*

Dealing with risk is a continuous process of determining what to do with new concerns as they are identified and efficiently utilizing project resources. An integrated approach to management is needed to ensure mitigation actions do not conflict with project or team plans and goals. A shared product vision and global perspective are needed to create mitigation actions on the macro-level to benefit the project, customer, and organization. The focus of risk planning is to be forward-looking, to prevent risks from becoming problems. Teamwork and open communication enhance the planning process by increasing the amount of knowledge and expertise applied to the development of mitigating actions.

Track

Tracking is the process by which risk status data are acquired, compiled, and reported. The purpose is to collect accurate, timely, and relevant risk information, and to present it in a clear and easily understood manner to the appropriate group of people. Tracking is done by those responsible for monitoring *watched* or *mitigated* risks. Tracking status information becomes critical to performing the next function in the continuous risk management paradigm, i.e. control. Supporting information, such as schedule and budget variances, critical path changes, and project/performance indicators can be used as triggers, thresholds, and risk- or plan-specific measures where appropriate.

When a mitigation plan has been developed for a risk or risk set, both the mitigation plan and the risk attributes are tracked. Tracking the mitigation plan, or even a list of action items, will indicate whether the plan is being executed correctly and/or on schedule. Tracking any changes in the risk attributes will indicate whether the mitigation plan is reducing the impact or probability of the risk. Tracking risk attributes gives an indication of the effectiveness of the mitigation plan.

Program and risk metrics provide decision makers with information needed for making effective decisions. Normally, program metrics are used to assess the cost and schedule of a program as well as the performance and quality of a product. Risk metrics are used to measure a risk's attributes and assess the progress of a mitigation plan. They can also be used to help identify new risks. For example, a program metric might look at the rate of module completion. If this indicates that the rate of completion is lower than expected, then a schedule risk should be identified.

Open communication regarding risk and mitigation status stimulates the project and risk management process. Tracking is a continuous process—current information about a risk status should be conveyed regularly to the rest of the project. Risk metrics provide decision makers with information needed for effective decisions.

Control

The purpose of the control function is to make informed, timely, and effective decisions regarding risks and their mitigation plans. It is the process that takes in tracking status information and decides what to do based on the reported data. Controlling risks involves analyzing status reports, deciding how to proceed, and implementing the decisions.

Decision makers need to know when or whether there is a significant change in risk attributes, and the effectiveness of mitigation plans within the context of project needs and constraints. The goal is to obtain clear understanding of the current status of each risk and mitigation plan relative to the project in order to make decisions based on that understanding. Tracking data is used to ensure that project risks continue to be managed effectively and to determine how to proceed with project risks. Options include:

Replan: A new or modified plan is required when the threshold value has been exceeded, analysis of the indicators shows that the action plan is not working, or an unexpected adverse trend is discovered.

Close the risk: A closed risk is one that no longer exists or is no longer cost-effective to track as a risk. This occurs when the probability or impact falls below a defined threshold, or the risk has become a problem and is tracked.

Invoke a contingency plan: A contingency plan is invoked when a trigger has been exceeded or other related action needs to be taken.

Continue tracking and executing the current plan: No additional action is taken when analysis of the tracking data indicates that all is going as expected or project personnel decide to continue tracking the risk or mitigation plan as before.

Open communication is important for effective feedback and decision making, a critical aspect of control. Risk control is also enhanced through integrated management; combining it with routine project management activities enables comprehensive project decision making.

Communication, Documentation

The purpose of communicating and documenting is for all personnel to understand the project's risks and mitigation alternatives as well as risk data to make effective choices within the constraints of the project. Communication and documentation are essential to the success of all other functions within the paradigm and are critical for managing risks.

Identify: In risk identification, risk statements are communicated.

Analyze: In analysis, project personnel communicate information about impact, probability, and time frame attributes. Risk classification involves grouping risk information communicated by individuals.

Plan: Action plans are developed and communicated to project personnel.

Track: Reports designed to communicate data to decision-makers are compiled.

Control: The decisions made during control must be communicated and recorded to project personnel.

For effective risk management, an organization must have open communication and formal documentation. Communicating risk information is often difficult because the concept of risk comprises two subjects that people do not normally deal well with: probability and negative consequences.

Not only continuous risk management, but the project as a whole is in jeopardy when the environment is not based on open communication. No one has better insight into risks than project personnel, and management needs their input. Experienced managers know that the free flow of information can make or break any project. Open communication requires:

- Encouraging free-flowing information

at and between all project levels.

- Enabling formal, informal, and impromptu communication.
- Using consensus-based processes that value the individual voice, bringing unique knowledge and insight to identifying and managing risks.

NASA Risk Management Course

Risk is a daily reality on all projects, and continuous risk management should become just as routine. It should be ongoing and comfortable, and neither imposed nor forgotten. Like any good habit, it should seamlessly fit into the daily work. During the course taught at NASA, various tools and methods are demonstrated that will work for any project. The key is to adhere to the principles, perform the functions, and adapt the practice to fit the project's needs. Continuous risk management is not one-size-fits-all. To be effective, tailoring is needed. Tailoring occurs when organizations adapt the processes, and select methods and tools which best fit their project management practice and their organizational culture. Following the principles of continuous risk management is the key to successful tailoring.

With this in mind, the Continuous Risk Management course for NASA was tailored to two days. The first day was lecture, covering all material with some exercises applying methods and tools. This is an intense day, as there is a lot of information to absorb. The second day is devoted to a project workshop. In most classes, personnel from one or two projects attend the lecture, then split up for the workshop (Classes are limited to 20 students.) The workshop is done in small groups. Periodically, these groups come together to review what each group has chosen to work on. Depending on the audience, there are two possible workshops, one for management, and the other for the implementation team.

The workshop for management starts by compiling the project information needed for the risk management plan. This starts with getting the functional organizational chart, identifying key meetings where risk management activities should take place, and identifying key personnel. The methods and tools to be used are then selected, and the criteria for the attributes probability, impact, and time frame are defined. This usually takes two to three hours. A shortened version of the implementation workshop described below is then applied.

The implementation workshop starts by identifying risks to the project based on everyone's knowledge. Phrases are used, with brainstorming, to compile a list of more than 20 potential risks. It is stressed that if it is a problem now, it is not a risk. From this list five risks are identified as those the group feels it can do something about and would like to work on. The risks are written using the correct format of condition and consequence as shown in Figure 1. The risk context is discussed but not written. Using these five risks and the attribute definitions from management, the risks are classified and prioritized. A mitigation plan for the top risk is developed, data for tracking is identified, and presentation formats discussed. Depending on time, two or three risks are processed through this cycle so that the attendees not only feel comfortable with the process, they have some risks specific to their project that they can start working on. Based on course feedback, it seems the workshop is the key to the training's success.

When a class is not made up of people from the same project, either the group is told to make up a project based on common experience, or it uses a project with which many are familiar. The second option is encouraged so real work is accomplished, although it only benefits a few attendees.

After completion of the course, students should:

- Understand the concepts and principles of continuous risk management and how to apply them.
- Possess basic risk management skills for each function of the risk management paradigm.
- Be able to use key methods and tools.
- Be able to tailor CRM to a project or organization.

Implementation

Three steps should be considered when implementing risk management. First, project risk management should be structured. The training itself is not important, it is what the training does for the project. The training helps the project to see how a formal process can be used to manage risks, but more importantly facilitate communication and initial brainstorming among project personnel.

Second, the project should adopt tools that project members are familiar with to aid in tracking risks and communication of risk status. The key is to use tools that members know how to use, and that they will use.

Lastly, the risk management process needs to be integrated into the normal project management process. Risk management must become the normal way of doing project business. This ensures that, rather than a separate process requiring extra overhead, risk management is ingrained. This leads to a cost-effective implementation within the project.

Conclusion

Most project managers agree that risk management works, but the difficulty lies in actual implementation, even when it is required. The risk management plan is often hastily written and then thrown in a corner to gather dust. In addition to the course, NASA has established a web site, http://satc.gsfc.nasa.gov/crm, that contains sample risk management plans and a schedule of classes. Much time is spent discussing with managers the benefits of taking a formal training course, the cost of which is more than recovered by a project when team members all work toward common goals in a coordinated manner.◆

References

1. *Continuous Risk Management Guidebook,* CMU, SEI, 1996
2. *NASA Procedures and Guidelines* 7120.5A, section 4.2.

Note

1. Some material is based on reference No. 1.

About the Authors

Linda H. Rosenberg manages the Software Assurance Technology Center at Goddard Space Flight Center, NASA. The SATC primary responsibilities are in the areas of metrics, assurance tools and techniques, risk management, and outreach programs. Although she oversees all work areas, Rosenberg's area of expertise is metrics. The emphasis of her work with project managers is metrics application to evaluate quality of development products. She holds a bachelor's degree in mathematics and a master's and a doctorate degree in computer science.

Al Gallo manages the Software Assurance Technology Center at NASA's Goddard Space Flight Center. He has more than 15 years experience in software systems engineering and quality assurance. As one of the SATC's lead trainers of continuous risk management, he has provided training and consulting throughout NASA. Gallo holds bachelor's degrees in pure mathematics and computer science as well as a master's degree in technical management from the Johns Hopkins University, Baltimore, Md.

Ted Hammer is the Associate Chief of the Systems Safety and Reliability Office at the NASA Goddard Space Flight Center. His duties entail overall management responsibility for the continuous risk management and SATC activities of the office. The SATC is the GSFC center of excellence for applied research in software assurance tools and methods. Hammer has more than 22 years experience in software development and assurance, and holds a bachelor's degree in electrical engineering from the University of Maryland. He is a member of the American Society for Quality.

Frank Parolek is the SATC Senior Risk Management Coordinator at NASA's Goddard Space Flight Center. He is responsible for providing continuous risk management (CRM) training and other risk management consulting at all NASA sites. He also coordinates the CRM Train the Trainers program and has provided training to the FAA, Army, and other organizations external to NASA. Parolek earned a bachelor's degree in liberal arts from Regents College and an advanced Russian Linguist Certificate from Defense Language Institute/ Foreign Language Center.

Contact the authors of this article at http://satc.gsfc.nasa.gov/personnel/index.html

Call for Articles

If your experience or research has produced information that could be useful to others, CROSSTALK will get the word out. We welcome articles on all software-related topics, but are especially interested in several high-interest areas. Drawing from reader survey data, we will highlight your most requested article topics as themes for future issues. In future issues of *CROSSTALK*, we will place a special, yet nonexclusive, focus on:

Personal Software Process and Team Software Process
July 2000
Submission deadline: March 1

Object-Oriented Technology
August 2000
Submission deadline: April 3

Software Acquisition
September 2000
Submission deadline: May 4

We will accept article submissions on all software-related topics at any time; issues will not focus exclusively on the featured theme.

Please follow the *Guidelines for CROSSTALK Authors*, available on the Internet at http://www.stsc.hill.af.mil. Send submissions to:

Ogden ALC/TISE
ATTN: Heather Winward
7278 Fourth St.
Hill AFB, Utah 84056-5205

You may e-mail articles to features@stsc1.hill.af.mil. or call 801-775-5555 DSN 775-5555.

Letters to the Editor

✎I would like to compliment Norm Brown on his paper published October 1999, *High-Leverage Best Practices—What Hot Companies are Doing to Stay Ahead and How DoD Programs Can Benefit.* Could you follow it up with a paper describing and listing the 16 critical software practices?

I think this would be a big help to those industry and government people who develop and maintain software.

Dr. L.G. Egan
Software Certification Institute

Editor's Note

Please see our October issue on best practices, in which Jane T. Lochner of the Navy addresses the "16 Critical Software Practices for Performance-Based Management." Thank you for writing.

✎May I suggest another entry to *Influential Men and Women of Software?* (*CROSSTALK,* December 1999)

The women who programmed ENIAC were given the task of programming the first modern electronic computer. Most of what we now consider good programming was invented by these "amateurs," including notions of subroutines and software development process.

We who make our living programming computers owe a debt to the creativity of these unknown women, a tribute to whom may be found in a recent exhibit at the Smithsonian (American History) in Washington, D.C.

Joe Iaquinto

Talk to CROSSTALK

We welcome reader comments regarding CROSSTALK articles or matters pertaining to software engineering. Please send your comments and Letters to the Editor to crosstalk.staff@hill.af.mil or mail to

OO-ALC/TISE
Attn: CROSSTALK staff
7278 Fourth St.
Hill AFB, Utah 84056-5205

Please limit letters to less than 250 words. Include your name, phone number, and