SANDIA REPORT

SAND2002-1048
Unlimited Release
Printed April 2002

Risk Management Plan Sandia National Laboratories ASCI V&V Program

Ann L. Hodges, Gary K. Froehlich, Martin Pilch, David E. Peercy

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2002-1048
Unlimited Release
Printed April 2002

Risk Management Plan
Sandia National Laboratories
ASCI V&V Program

Ann L. Hodges and Gary K. Froehlich
Software & Information Engineering Department

Martin Pilch
V&UQ Processes Department

David E. Peercy
Software Quality Engineering Department

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-1137

October 22, 2001
Version 1.3

Abstract

This document describes a proactive plan for assessing and controlling sources of risk for the ASCI V&V program at Sandia National Laboratories. It offers a graded approach for identifying, analyzing, prioritizing, responding to, and monitoring risks.

Acknowledgements

The authors would like to thank the following individuals for their thoughtful input, comments, and discussion: Max Harcourt, Bob Paulsen, and Jack Jones.

Contents

Figures

Tables

1. Introduction

1.1. Background

Risk management is a key aspect of program management, and is integral to the traditional planning and tracking activities concerning cost, schedule, and performance. Risk management's objective is to increase the probability of success by controlling threats to program goals in a cost-effective manner. This objective is accomplished by providing an approach and environment for proactive decision making to assess, prioritize, and take steps to deal with risks. In addition, those who would be affected by the risk can use the information gathered during risk management to help build a case for getting support or the necessary resources to deal with the risk appropriately. Alternatively, risk management can allow programs to identify, and if necessary, eliminate high-risk activities.

An extensive search of the literature reveals that risk is commonly defined as *the possibility of experiencing an undesirable event*. An alternative definition, and the one used in this plan, views risk as *a combination of the likelihood of the event's occurrence and its impact*. Events with zero likelihood or that result in zero impact are not considered risk events, and thus are of no interest.[1] It is important to distinguish between an *event* and the *impact* of the event's occurrence. In this plan, the term "impact" will be restricted to effects on performance, cost, and/or schedule. Consider, for example, an event that leads to the departure of a key team member. While one impact of this event is the loss of a team member, the quantifiable impact, for purposes of risk management, is the effect of this person's departure on performance, cost, and schedule.

1.2. Purpose and Scope

The Department of Energy has undertaken the Stockpile Stewardship Program (SSP) to ensure confidence in the safety, performance, and reliability of the US nuclear stockpile. Collectively, the goals of safety, performance, and reliability are referred to as weapon surety. The Accelerated Strategic Computing Initiative (ASCI) provides the SSP with a capability to allow transition from purely test-based weapon surety to incorporation of simulation-based methods. This shift has resulted in an increased reliance on computational modeling and simulation to support the SSP. A formal, focused verification and validation (V&V) program therefore becomes essential for improving the confidence and credibility of these modeling and simulation activities.

To help ensure the successful attainment of confidence and credibility in ASCI modeling and simulation software, this plan specifies the strategy for planning, identifying, analyzing, prioritizing, responding to, monitoring, and controlling risks for the Sandia National Laboratories (SNL) ASCI V&V program. The stated intent is to better manage

[1] Opportunities can be viewed as risks for which the associated impact is favorable. Opportunity management focuses on possibilities to reduce costs, shorten schedule, or enhance performance.

activities that serve the programmatic customer (DOE/ASCI Headquarters), and SNL Defense Program (DP) stakeholders. The creation and implementation of a risk management plan for the (SNL) ASCI V&V program is in response to recommendations from a DOE-sponsored audit of the V&V program in FY00. This plan is also intended to meet the requirements of [qc1], [tbp000], and [tbp306].

A project should determine the applicable scope and level of rigor, then tailor the practices accordingly. In addition to a project's scope and rigor, tailoring should be commensurate with customer and programmatic needs. Thus, the activities described in this document may range in formality from code owners simply communicating risks with customers, all the way to the full rigor of a Risk Management Board and the use of an organizational risk database. *In any event, key benefits of this process, whatever the formality, are the early understanding and communication gained through application of the process itself.*

The practices and activities described in this document have been tailored to meet the needs of the (SNL) ASCI V&V program. The implementation of risk management described in this document is ongoing and evolutionary. As practices are discovered to be deficient, they will be enhanced. Similarly, as practices are found to be overly burdensome or superfluous, they will be simplified or eliminated.

1.3. Risk Management Principles

The following fundamental principles should be considered when performing risk management activities:

- *Risk is dependent upon the perspective of the risk agent.* A risk agent is someone who is affected by the risk. For example, in the Challenger tragedy, the risk to Morton-Thiokol, which involved losing a contract or possibly legal liability, was different than NASA's risk, which involved both losing the asset and damaging NASA's credibility. The crew's risks included loss of life. The challenge lies in reconciling these different perspectives, and negotiating a consistent, global understanding. Risk may also be time dependent; i.e., a risk agent takes on a risk for a limited period of time.
- *Risk management is proactive.* Risk management *is not* about assigning blame. Communication about risks needs to occur in a trusting, open environment.
- *Risk management is not free.* Risk management activities need to be considered in program management. Time for planning, identifying, analyzing, monitoring, and controlling risks needs to be allocated. People must be available, responsible, authorized, and trained to participate in risk management activities. Budget should be made available for projects to implement risk actions. The process must be defined and executed. And finally, budget, policy, and a risk-aware culture to support risk management must be provided. Because risk management activities mitigate or prevent future problems, the accrued cost savings are usually only realized in the future. However, the return on investment in preventing one major problem might offset the overall cost of risk management activities.

- *Multi-disciplinary teams are a crucial aspect of risk management* for proactive assessment and control of cost, schedule, performance, and producibility issues.
- *Once performance, schedule, and cost are negotiated and agreed upon, a context for risk management is established.* Performance, cost, and schedule only become new sources of risk if significant changes occur to any one of them, in which case the project must be replanned, and risks must be reassessed.

1.4. Configuration Management

The ASCI V&V Risk Management Plan (this document) will be placed in version control, and then published to the ASCI V&V Records Management System. The risk database (discussed in section 3) will also be version controlled. Issues concerning the risk management process, risk management plan, and supporting tools will be tracked in an issue tracking system.

2. Risk Management Process

The risk management models described in the literature share a common, basic approach. The activities are fundamentally the same, but partitioned into different phases. The model presented in this plan is based on those described in [pmbok], [cmmi], [epi], [gehmlich], [hall], [harcourtb], [jones], [mcconnell], [peercy], and [spc].

As shown in Figure 1, the risk management process is comprised of six steps that are iteratively conducted during the program's lifecycle. A summary of major activities for each step is shown below the box representing the step. Detailed descriptions for each step are contained in subsequent sections.

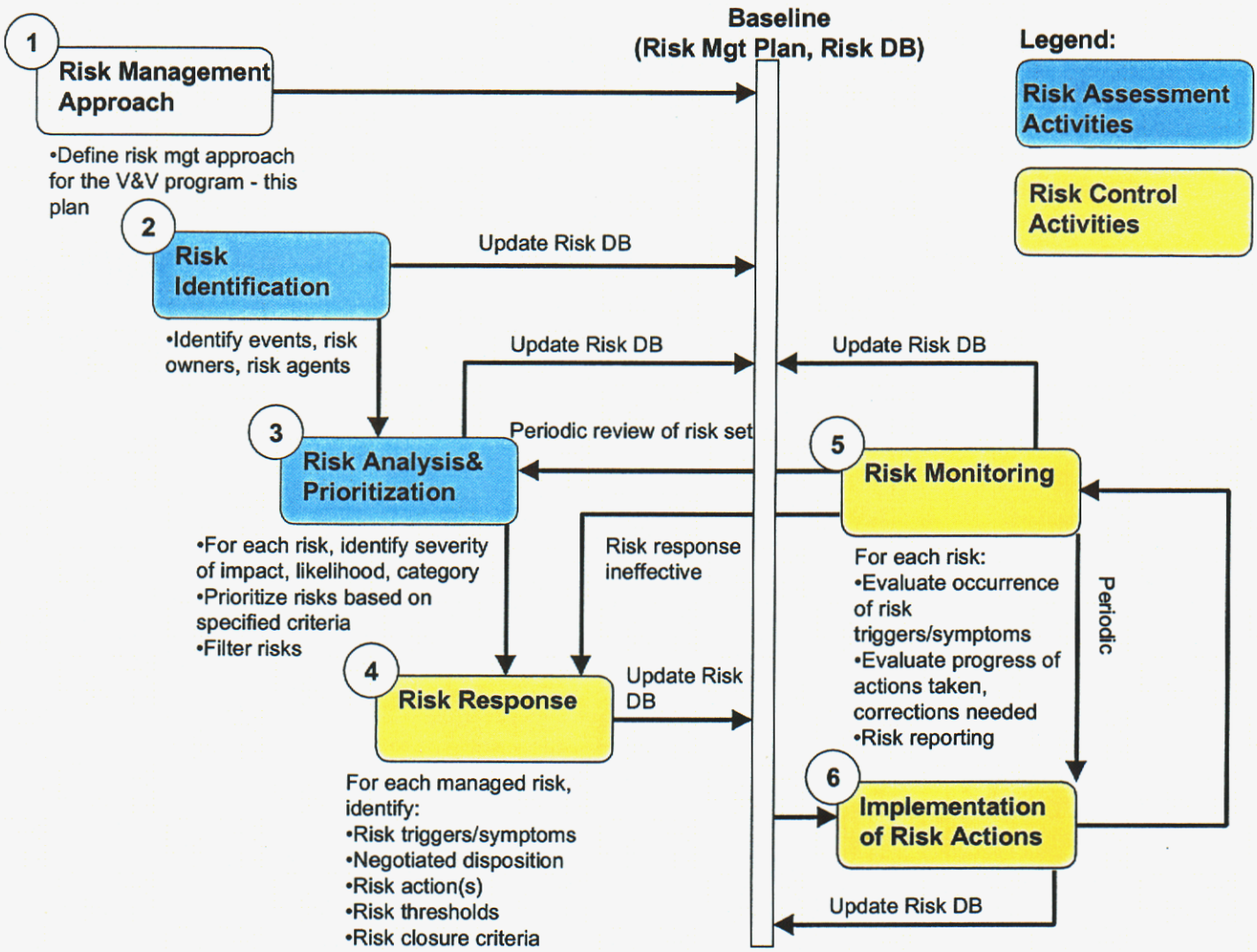

Figure 1. Risk Management Process

2.1. Risk Management Approach

What is the Risk Management Approach? - The approach to risk management involves identification of risk management requirements and stakeholders (driven and scoped by the V&V program objectives), specification of risk management processes and associated roles and responsibilities (including risk reporting and reviewing), definition of the risk database, and identification of training requirements. Risk management planning should be an integral part of program planning.

Output from this Step - This Risk Management Plan is the output of the Risk Management Approach.

How is the Risk Management Approach Developed? - The ASCI V&V program manager oversees the development of the risk management approach. The program manager has identified a small team (the authors of this plan) to define and document the risk management strategy. This team identified the objectives of the ASCI V&V program -- establishing confidence and credibility in ASCI modeling and simulation capabilities. Understanding these objectives limits the scope and thus the number of risks that need to be considered, since risks that do not affect the success of the program do not need to be given any further consideration. Given these objectives, the perspectives of stakeholders (groups who have an interest in the outcome of V&V and/or the V&V program) are considered during risk assessment and control steps. *The customer for the purpose of this V&V Risk Management Plan is DOE/ASCI HQ and the (SNL) ASCI V&V program, and the stakeholders include* the SNL Defense Program (DP) and weapons surety.

After the scope and risk management requirements are determined, the methodology to be used for risk assessment and control is identified. This includes determining organization of risks, scoring, risk response techniques, establishment of thresholds to help identify when risks need to be acted upon, tracking, and reporting techniques.

2.2. Risk Assessment

2.2.1. Risk Identification

What is Risk Identification? - Risk identification is an iterative process for uncovering threats to the program goals. Risk events (i.e., events with non-zero likelihood and non-zero impact) must be identified and described understandably before they can be properly analyzed and ultimately managed. The list of identified risks should be periodically reviewed and updated as conditions change. This permits elimination of some former risks and facilitates discovery of new risks.

Outputs of Risk Identification - The risk database is populated with the identified, prioritized risks; for each risk, risk owners and risk agents are determined.

How is Risk Identification Performed? - One or more of these techniques can be used in risk identification.

- Information gathering techniques: Examples are shown below.
  - ASCI Quarterly Reports: Risks are currently identified and described in the "Issues and Concerns" section for each WBS element in the V&V program. This coverage helps to ensure that all facets of the program are considered. The V&V program manager further investigates any item contained in this quarterly report section.
  - ASCI V&V Plans, self-assessments, and Peer Review results: Project risk experts extract risks identified in any of these work products (e.g., the verification test suite might be examined for adequate code coverage, or the validation test suite might be examined for links to critical experiments). These risks can be linked to stockpile drivers through the phenomena identification and ranking tables (PIRT).

As prioritization of phenomenology has already been established, this could serve as an additional risk prioritization mechanism (refer to section 2.2.2).

- Assessments of SQE practices: Independent assessments of the ASCI Applications code team SQE Practices in accordance with the published versions of the [doesqe] and [snlsqe] serve as a way to identify risks at the code team, policy (published practices and guidelines), and programmatic levels.
- Brainstorming: A multi-disciplinary team of subject matter experts and stakeholders develops a list of risks.
- Interviewing: Key stakeholders, subject matter experts, and experienced managers are briefed on the program/project and provide risk sources based upon their backgrounds and perspectives.
- Delphi technique: The subject matter experts and stakeholders provide anonymous input via a questionnaire designed to generate risk ideas. The responses can then be distributed to these same experts for further comment. Facilitated consensus can be reached after several such rounds of comments.
- Strengths, weaknesses, opportunities, and threats (SWOT) analysis: The team performs this analysis to enrich the breadth and depth of considered risks.

- Risk taxonomy: The risk taxonomy is used as a checklist for identifying common sources of risk events. Figure 2 depicts the risk taxonomy for the V&V program.
- Risk checklists: Compilations of common risks for similar activities are consulted for applicability to this program. (For example, see [jones].)

As a further activity of Risk Identification, the risk owner(s) and risk agent(s) are identified for each risk. (Risk owners have responsibility for the risk; risk agents are anyone affected by the risk.)

Each risk is described using a common format in the risk database. Refer to section 3 for further details on this format. The attributes contained in this database are further refined during subsequent risk management steps.

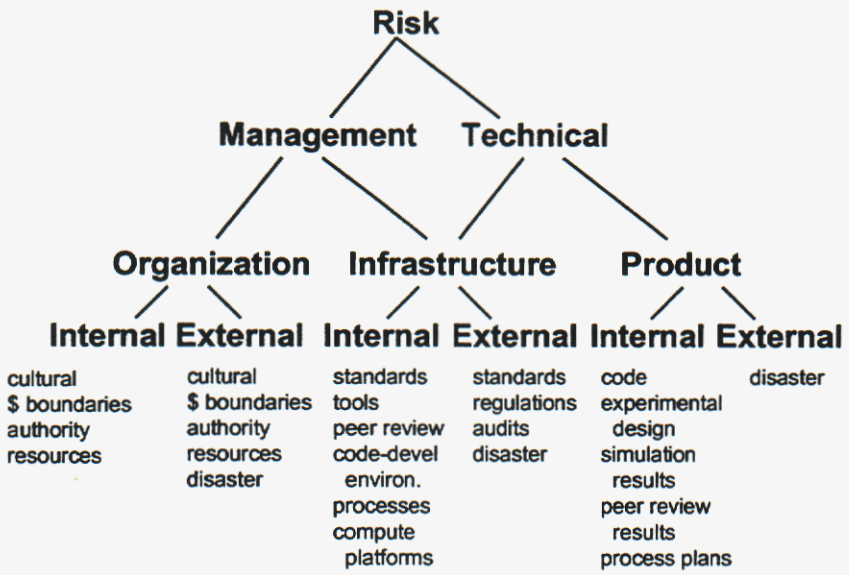

Figure 2. Risk Taxonomy

2.2.2. Risk Analysis and Prioritization

What are Risk Analysis and Prioritization? - Risk analysis is the process of determining the impact and likelihood of the identified risk events. This step starts the conversion of risk data into decision-making information. For each risk, the category (or categories) is determined, and the likelihood of the risk event and the severity of the impact are scored. This information is entered into the risk database. The risks are then prioritized in descending order, using a combination of each risk's severity and likelihood scores. (Note that a ranking might simply be *assigned* to a risk, independent of its severity and likelihood scores, based on expert judgement, risk tolerance, culture, or programmatic need). *Note that since prioritization only requires a ranking, precise values for mathematical probability or for impact (cost, schedule, performance) are* ***not needed****. Any scoring system that is consistent with the* ***beliefs*** *of the risk agents regarding their subjective, qualitative sense of likelihood and severity of impact is adequate for this ranking.* (This scoring system should be monotonic, and the weight of zero impact or zero likelihood should be preserved).

Outputs of Risk Analysis and Prioritization – The output is a prioritized list of risks, with an associated decision to manage, watch, or accept. A "parking lot" list of the risks that will not be actively managed may also be produced.

How are Risk Analysis and Prioritization Performed? – Risk attributes provide a framework for identifying and organizing risks by category, impact, and likelihood. Consistently applying attributes and analysis criteria, and consistently scoring risk likelihood and severity levels, allows risks to have common semantics and to receive the

appropriate level of attention. This consistency allows prioritization even among dissimilar risks that might have the same likelihood and severity levels. For each risk, the values for the following attributes are determined and entered in the risk database.

- Severity of impact – Quantitative scores for each level of severity are shown in the table below.

Relative Score	Performance Factor	Cost Factor	Schedule Factor
0	No impact. Program/activity goals fully met.	No impact to budget.	No impact to schedule.
1	Program/activity goals not fully met, customer satisfied with work products.	Customer able and willing to accommodate budget impact.	Customer able and willing to accommodate schedule impact.
2	Program/activity goals not fully met, customer dissatisfied with work products.	Customer must go to great lengths to accommodate budget impact.	Customer must go to great lengths to accommodate schedule impact.
3	Program/activity goals not met, customer rejects work products.	Customer unable and unwilling to accommodate budget impact.	Customer unable and unwilling to accommodate schedule impact.

Table 1. Risk Impact Severity Levels

- Likelihood of occurrence – As with the severity levels, quantitative scores for likelihood are shown in the table below. For most risks, there is no historical knowledge base; consequently, it makes no sense to talk in terms of probabilities or frequency of events. For such common circumstances, the risk analyst must think in terms of subjective degrees of belief. Note that the likelihood *scores* do not represent a linear increase in likelihood (as shown in the example likelihood column), thus accommodating a range of experiences from common to extremely rare.

Relative Score	Example Likelihood	Likelihood Factor (Belief)
0	$\sim 10^{-3}$	Extremely unlikely or impossible -- outside the realm of experience, can be ruled out.
1	$\sim 10^{-2}$	Highly unlikely -- outside the realm of common experience, but cannot be ruled out.
2	$\sim 10^{-1}$	Reasonably likely -- within the realm of experience.
3	~1	Highly likely -- within the realm of common experience, or assumed for regulatory/programmatic reasons.

Table 2. Risk Likelihood Levels

- Risk priority and response category – The purpose of prioritization is to identify the most important risks to focus on (those that will have the greatest impact to the program). A risk-priority score (with 1 as the highest and 9 as the lowest) is established by combining the severity score (ordinate) and the likelihood score (abscissa) into an ordered pair, as shown in Figure 3. In addition, prioritized risks are grouped as shown in Figure 3, and assigned to a response category (accept, watch, or manage). The result of this filtering step is one of the following:
  1. For risks in the "manage" response category, the risk response steps (next section) are followed.
  2. For risks in the "watch" response category, these risks are moved to a "parking lot" list rather than being actively managed. The risk management team reviews the risk parking lot, and risks are added or moved to the set of managed risks as appropriate. Otherwise, risks in the parking lot are not considered in subsequent steps.
  3. For risks in the "accept" response category, these are risks for which no action will be taken.

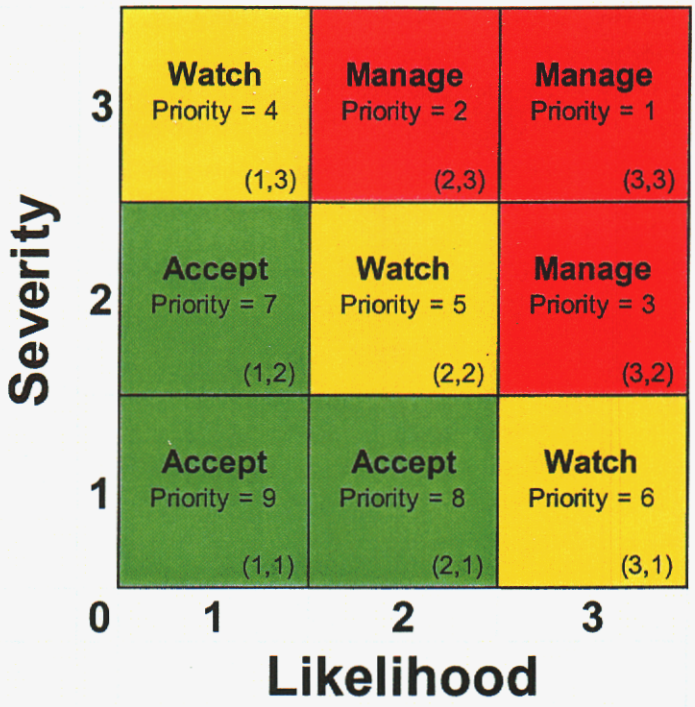

Figure 3. Risk Priority Scores

- Risk source category – The risk taxonomy in Figure 2 contains a list of categories of common sources of risk events. Select one or more of these source categories as appropriate for the risk. Generally, there are more management risks at the beginning of a project, with technical risks being more common later.

2.3. Risk Control

2.3.1. Risk Response

What is Risk Response? - The risk response step involves planning for options that will facilitate opportunities and reduce threats to the program's goals. Given a prioritized and filtered set of risks, the risk disposition strategy for each managed risk is determined, risk actions are developed, the triggers (or symptoms) that indicate the impending threat of a risk event are identified, and associated thresholds that indicate when a risk becomes unacceptable are specified. For a given risk, response planning should be commensurate with the level of the threat. Additionally, several risks may share a common cause, which could represent an opportunity to control multiple risks with one response.

Outputs of Risk Response – The disposition strategy, actions, triggers, and thresholds for each managed risk are outputs from this step. The risk management database is updated appropriately.

How is Risk Response Planning Performed? – The following elements are identified and entered in the risk database. Start at the highest priority risks. Note that the WBS is a

useful tool for providing a framework for planning by providing a high-level notion of tasks, schedule, and interdependencies between tasks.

- Risk disposition strategy - Initially determine the risk disposition strategy. For a given risk, the most effective strategy is chosen. Alternative strategies are shown below, and are adapted from [gehmlich], [harcourtb], [cmmi], and [pmbok].
  - Avoid: Change the project plan (e.g., project scope or requirements) in order to *eliminate* the risk condition and thus protect the program goals from being affected.
  - Mitigate: Take active steps to lower the likelihood of occurrence or the severity of the risk.
  - Transfer: Shift the risk impact and/or ownership to another party.
  - Accept: Acknowledge and assume the risk, and determine that no action will be taken. This is an appropriate strategy for low priority risks. Risks that have this disposition strategy may be moved to the risk parking lot list.
- For each risk that is using a disposition strategy other than acceptance:
  - Risk actions - develop one or more actions to mitigate the risk. Risk actions may already be identified in the ASCI quarterly reporting process, and these should be incorporated into the overall set of risk actions. For each action, develop a cost-benefit estimate, responsibilities, and a high-level schedule.
  - Risk triggers - Identify indicators or warning signs that a risk is about to occur or has occurred. For example, not meeting intermediate milestones is a trigger for a schedule slip.
  - Thresholds - Determine the level of one or more attributes of a trigger that, if exceeded, indicates the associated action should be taken.

2.3.2. Risk Monitoring

What is Risk Monitoring? - Successful risk monitoring provides information that aids effective decision-making prior to the occurrence of a risk. This is accomplished by collecting timely, accurate, and relevant information, and presenting that information in a concise and intelligible way to the appropriate recipients. If a problem does occur, monitoring helps determine whether risk responses have been executed and are progressing as planned. The effectiveness of response actions, changes in the severity of the impact, and changes in the likelihood of occurrence are also monitored.

Outputs of Risk Monitoring – Newly identified risks, closed risks, feedback on efficiency of risk actions, potentially updated risk actions, severity of impact, likelihood of occurrence, and risk responses are outputs from this step. The risk management database is updated appropriately.

How is Risk Monitoring Performed? – The risk owners are responsible for monitoring all of the managed risks under their purview. One approach is to review (e.g., at project meetings) the top ten identified risks. Rollups of status reports are examined at periodic

internal technical and management reviews.[2] Risk status is reported in the SNL ASCI quarterly reports, or on an emergency/as-needed basis. High priority risks may be discussed in external reviews.

The following presents the steps to be taken for the set of managed risks:

- For those risk events that have *not yet taken place*, the risk owner determines *whether a trigger condition (symptom) has occurred*[3] and *whether the associated threshold has been exceeded*. If both conditions are true, then
  - For those risks that have an "avoid" risk-disposition strategy, the risk-avoidance actions have been unsuccessful, and the "Risk Response" step will first have to be revisited.
  - The "Implementation of Risk Actions" step is executed.
- For those risks events that *have already occurred* and *risk actions have been implemented*, then
  - The risk owner evaluates the effectiveness of the actions based upon related cost, schedule, and performance information. The risk event's impact and likelihood may be greater than expected, and thus the risk action is not sufficient to address the risk. Using this evaluation, the risk owner determines whether modifications are needed. If current actions are deemed adequate, those actions continue; otherwise, the "Risk Response" step is repeated, and updates are made to the associated fields in the risk database. It may be necessary to obtain appropriate management review in cases where the adjustments affect cost, schedule, or performance of a WBS element.
  - For risks that have been adequately handled to completion, as determined from the associated closure criteria, those risks are closed and no longer actively managed.

During the monitoring process, previously unidentified risks may emerge. In this case, the risk management process is followed for each new risk, starting at the "Risk Identification" step.

Figure 4 gives a pictorial representation of monitoring a hypothetical risk using the risk priority scores. In this example, the hypothetical risk had a risk priority score of 2. This is depicted on the left with a circle. Following implementation of risk actions to reduce severity (described in the next section), a reassessment of the hypothetical risk shows a new risk priority score of 5, as depicted on the right. In this example, the risk is moved from "managed" to the "parking lot" set of risks. This figure visually demonstrates the effectiveness of these hypothetical risk actions.

---

[2] An interim postmortem, conducted after a major milestone, can be another monitoring point for a project or program.

[3] Earned value analysis may be useful for monitoring overarching project performance, and can indicate deviations of cost and schedule targets. When a project's earned value differs significantly from the project baseline, updated risk identification and analysis should be undertaken. Technical performance measurement is another useful approach for determining whether technical achievements deviate from planned accomplishments.

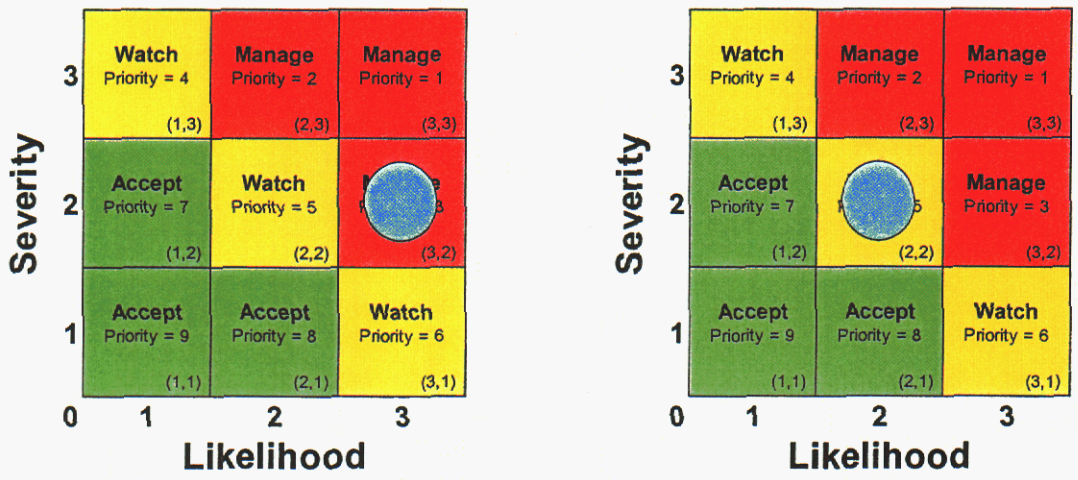

Figure 4. An Example of Risk Monitoring Using the Risk Priority Scores

2.3.3. Implementation of Risk Actions

What is Implementation of Risk Actions? - Identified risk actions are executed as specified in the associated risk description. Refer to section 3.

Outputs of Implementation of Risk Actions – Outputs from this step include updated schedules, implemented risk actions, and associated outputs of these risk actions. The risk management database is updated appropriately.

How is Implementation of Risk Actions Performed? – The risk owner is responsible for assuring that risk actions are started as specified in the risk action plan. The action with the most favorable cost-benefit to the program is implemented. The risk owner notifies the risk agent and the affected project leaders about the need to implement risk action(s), and has associated milestones added to appropriate program or project schedules to direct initiation and monitoring of the actions.

2.4. Roles and Responsibilities

The following roles and their corresponding responsibilities comprise the risk management team. Note that *an individual may perform more than one role*, depending on the size and complexity of the program.

2.4.1. Program Manager

The Program Manager has overarching responsibility for the projects comprising the program, and provides resources (i.e. funding, personnel, and tools) for the risk management activities. The Program Manager also serves as a point of contact for customers and other managerial components. Additionally, the Program Manager is responsible for both internal and external V&V program risks.

2.4.2. Risk Management Board

The Risk Management Board helps assure that risk assessment and control activities are administered in a consistent fashion. For programmatic risks, the Board consists of the ASCI V&V Program Manager, the applicable DP/surety stakeholder, and a V&V process representative. This multi-disciplinary team collectively provides a strategic perspective on risk management issues.

2.4.3. Risk Owner

A risk owner is an individual assigned to a risk. For programmatic risks, it is the (SNL) ASCI V&V Program Manager. For individual tasks, the risk owner is the applicable task PI. It is the owner's responsibility to help define the risk's attributes (severity score, likelihood score, category, risk response, risk priority score, etc.), to facilitate any changes required to address a risk, and to track a risk's status.

3. Risk Database

The risk database is a repository for the identified risks and related information. The database supports gathering, analyzing, tracking, and reporting of data collected during the risk management process described in section 2. This database, which is available to the risk management team, is crucial in enhancing the effectiveness of risk management. This database forms the foundation of a risk "lessons learned" repository. The database is implemented as an Excel worksheet, and is available in the ASCI V&V Records Management System.

The attributes necessary to support risk assessment and control activities are shown in Table 3. The risk attributes are populated and refined during the applicable risk management steps, as described in section 2. Each attribute is listed with its associated description, the risk management step where modification occurs, and the role responsible for modification. The required attributes are denoted by a "+" before the attribute name.

Attribute Name	Description	Step Where Modified	Responsible Role
Unique ID	A unique identifier for the risk record.	Risk Identification	Program Manager
+Risk Name	Title of the risk.	Risk Identification	Program Manager
+Risk Description	Summary description of the risk. This should be described in no more than one or two sentences.	Risk Identification	Program Manager
+Risk Owner	Name of the person responsible for the risk.	Risk Identification	Program Manager
+Risk Agent	Person who is affected by the risk.	Risk Identification	Program Manager
Risk Source Category	Type of risk. One of the elements identified in the risk taxonomy depicted in	Risk Analysis & Prioritization	Risk Owner

Attribute Name	Description	Step Where Modified	Responsible Role
	Figure 2.		
WBS Elements Affected	Lists which WBS elements are affected by the risk.	Risk Analysis & Prioritization	Risk Owner
+Likelihood Score	Numerical ranking of likelihood of occurrence. Refer to the "Relative Score" column in Table 2.	Risk Analysis & Prioritization	Risk Owner
+Severity Score	Numerical ranking of the severity of impact. Refer to the values in the "Relative Score" column in Table 1.	Risk Analysis & Prioritization	Risk Owner
+Risk-Priority Score	Numerical ranking of the risk.	Risk Analysis & Prioritization	Risk Owner
+Risk Response Category	Category associated with risk-priority score (manage, watch, or accept).	Risk Analysis & Prioritization	Risk Owner
+Risk Disposition	Identifies approach for dealing with the risk. Refer to the values in section 2.3.1.	Risk Response	Risk Owner
+Risk Action(s)	Discusses plans for how risks will be dealt with.	Risk Response	Risk Owner
Risk Closure Criteria	Identifies criteria for determining whether actions for dealing with a risk have been completed.	Risk Response	Risk Owner
+Risk Trigger(s)	Symptoms that indicate that a risk may occur. For each symptom, include the threshold that indicates the risk has occurred.	Risk Response	Risk Owner
+Status of Risk Actions	Discussion of how risk actions are progressing.	Risk Monitoring	Risk Owner
+Date Action was Initiated	Date that the risk action was started.	Implementation of Risk Actions	Risk Owner
+Closure Date	Date when risk action was completed.	Risk Monitoring	Risk Owner
Closure Rationale	Reason for closure.	Risk Monitoring	Risk Owner
+Last Monitoring Date	Date that the risk was last monitored.	Risk Monitoring	Risk Owner
+Comments	Comments not covered in other attributes; e.g., rationale for likelihood and severity scores; lessons learned.	Risk Identification, Risk Analysis & Prioritization, Risk Response, Risk	RMB, Risk Owner

Attribute Name	Description	Step Where Modified	Responsible Role
		Monitoring, Implementation of Risk Actions	

Table 3. Risk Database Schema

4. Risk Management Metrics

There are two main categories of risk management metrics: *results metrics* and *process metrics*. Recommended metrics are listed below for each category. Note that the information necessary for reporting these metrics is already in the risk database.

- Results metrics
  - total number of identified risks (this gives some indication of the complexity and difficulty of the program)
  - number of risks per source category (e.g., management/infrastructure/internal, technical/product/internal, etc. -- this gives some notion of the program manager's span of control over risks)
  - the trend demonstrated by each risk's response category and disposition category history (this gives some indication of the risk management program's effectiveness)
- Process metrics
  - number of risks per response category (e.g., manage, watch, accept -- this gives an indication of the effectiveness of the risk assessment activities)
  - number of risks per disposition category (e.g., avoid, mitigate, etc. -- this gives an indication of how seriously risk management is treated in the program)

Appendix A Bibliography

[pmbok] 2000 Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 2000 edition, Newtown Square, PA 2000.

A Short Report on Risk Management, http://members.ozemail.com.au/~spain/meeting_reports/Risk_report.html.

[cmmi] Carnegie Mellon Software Engineering Institute. *CMMI for Systems Engineering/Software Engineering,* version 1.02, Pittsburgh, PA, November 2000.

[doeo4141a] *DOE O 414.1A – Quality Assurance*, United States Department of Energy, National Nuclear Security Administration, September 19, 1999. http://prp.lanl.gov:8686/.

[doeo4xx] *DOE O 4xx - Certification of the Nuclear Weapons Stockpile*, draft, Department of Energy, National Nuclear Security Administration, January 2001.

[doesqe] *ASCI Software Quality Engineering: Goals, Principles, and Guidelines*, DOE/DP/ASC-SQE-2000-FDRFT-VERS2, February 2001.

[epi] *Engineering Process Improvement Risk Management Guide*, EPI 100-21 version 1.0, Lockheed Martin Corp., December 10, 1999.

[gehmlich] Gehmlich, D. L., *W80-2/3 Life Extension Project Risk Management Program Plan for Sandia National Laboratories*, Sandia National Laboratories, draft, 3/2001.

[hall] Hall, E. M. *Managing Risk - Methods for Software Systems Development*, SEI Series in Software Engineering, Addison-Wesley 1997.

[harcourta] Harcourt II, M. M. Personal communication between Max Harcourt, Gary Froehlich, and Ann Hodges, September 28, 2001.

[harcourtb] Harcourt II, M. M. *W76-1 Life Extension Project Risk Management Program Plan*, revision B, March 21, 2001.

[jones] Jones, Capers. *Assessment and Control of Software Risks*, Yourdon Press, Prentice Hall, Upper Saddle River, NJ 1994.

[mcconnell] McConnell, Steve. *Rapid Development.* Microsoft Press, Redmond, WA 1996.

[tbp-ecp] *Nuclear Weapons Complex Technical Business Practice - Engineering Certification Process*, Department of Energy, draft 2, November 28, 2000.

[peercy] Peercy, D. E.; Chapin, N. *Interview with David E. Peercy*, Software Maintenance: Research and Practice, vol. 9, 177-200 1997.

[rosenberg] Rosenberg, L. H; Hammer, T.; Gallo, A. *Continuous Risk Management at NASA*, http://satc.gsfc.nasa.gov/support/ASM_FEB99/crm_at_nasa.html

[snlsqe] *Sandia National Laboratories ASCI Site-Specific Software Quality Engineering Practices*, version 1.00, September 2001.

[qc1] QC-1 – DOE/AL, *Quality Criteria (QC-1)*. Revision 9. February 5, 1998. http://prp.lanl.gov:8686/.

[sei] Carnegie Mellon Software Engineering Institute, *Risk Management Overview*, http://www.sei.cmu.edu/programs/sepm/risk/risk.mgmt.overview.html.

[spc] Software Productivity Consortium, *Risk Management Plan - Template.*

[sqas] DOE Quality Managers Software Quality Assurance Subcommittee, Software Risk Management - A Practical Guide, SQAS21.01.00 - 1999, 2000.

[stsc] STSC's home page: http://www.stsc.hill.af.mil/.

[tbp000] *TBP-000 – NWC Technical Business Practice, Program Management*. Issue E. May 4, 2001. http://prp.lanl.gov:8686/

[tpb306] *TBP-306 – NWC Technical Business Practice, Software Product Processes*. Issue B. July 15, 1999. http://prp.lanl.gov:8686/

DISTRIBUTION:

1	MS	0139	S. E. Lott, 9905
1		0139	R. K. Thomas, 9904
1		0429	J. S. Rottler, 2100
1		0453	H. J. Abeyta, 2101
1		0482	R. A. Paulsen, 2109
5		0638	D. E. Peercy, 12316
1		0819	T. G. Trucano, 9211
1		0824	J. L. Moya, 9130
1		0824	A. C. Ratzel, 9110
5		0828	M. Pilch, 9133
1		0835	J. M. McGlaun, 9140
1		0841	T. C. Bickel, 9100
1		0847	H.S. Morgan, 9120
5		1137	G. K. Froehlich, 6536
5		1137	A. L. .Hodges, 6536
1		9019	Central Technical Files, 8945-1
2		0899	Technical Library, 9616
1		0612	Review & Approval Desk, 9612 For DOE/OSTI