

---

---

# ABT Program Risk Management Plan

---

---

May, 2008

## Revision History

Version	Prepared by	Date	Reviewed by	Approved by	Note
Original v.1	Keith Pace - CIBER	May 16, 2008	Marjorie Mills	Manny Ovena	

# Table of Contents

1.0 Introduction.....	4
2.0 Methodology .....	4
2.1 Inputs .....	4
2.2 Risk Management Process .....	5
2.3 Outputs .....	5
2.4 Metrics.....	5
2.5 Risk Tracking Tools.....	6
2.6 Risk Management Process Flow.....	7
2.7 Risk Identification .....	8
2.7.1 Assign Responsibility .....	9
2.7.2 Risk Assessment .....	9
2.7.3 Develop Risk Response (step-down) Plan.....	9
2.7.4 Review Risk Responses.....	10
2.8 Manage Risks.....	10
2.8.1 Risk Response Plans.....	10
2.8.2 Monitor Identified Risks.....	11
2.8.3 Implement Risk Contingency Plans .....	11
2.8.4 Report Interim Status.....	11
2.8.5 Close the Risk .....	12
2.8.6 Perform Additional Risk Assessments .....	12
2.9 Close Risk Management.....	13
3.0 Roles and Responsibilities .....	13
Appendix A: Major Implementation Risk Categories .....	14
Appendix B: Risk Identification Questionnaire.....	15
Appendix C: Sample – Risk Response “Step-down” Plan Example .....	17
Appendix D: Sample – Risk Scoring Criteria.....	18
Appendix E: Sample Project Risk Profile for Status Reporting .....	19
Appendix F: Sample – Risk Tracking Log (part 1) .....	20

## 1.0 Introduction

---

The purpose of this document is to describe the process, tools and resources required to manage risks during the ABT implementation project. Additionally, we will identify the major risk categories and potential risks facing the ABT program.

Risk Management is the disciplined and structured approach of planning, identifying, analyzing, and controlling risks that may arise throughout the ABT program. A *risk* is an uncertain event or condition that, if it occurs, has a negative effect on the project. Identified risks can be planned for, monitored and proactively managed in order to reduce their potential impact and/or, in some cases, be completely removed. Unidentified risks, on the other hand, may cause a reactive situation that not only adversely impacts the project, but creates a distraction and disturbance that affects project performance. Risks are a certainty, but their affect on the project is dependent on our ability to manage them. Therefore, the primary objective of risk management is to reduce or remove the potential negative impact from the program.

Though opportunities are not specifically addressed in this risk management plan, opportunities should go through a similar identification, assessment and response planning process in order to realize some potential positive effects.

There is an important distinction between risks and issues; issues are existing conditions that must be dealt with, in a timely fashion, in order to maintain planned project performance. Issues are situations, actions, decisions or other elements that exist and must be addressed within a certain timeframe.

Proactive and disciplined risk assessment and response planning throughout the project life-cycle will minimize the potential threat of risks and reduce the amount of reactive fire-fighting that can consume project managers and team members if left unchecked. We plan to reduce the stress and effort caused by the onslaught of project risks (and issues) through thorough risk and issue management. Please refer to the ABT Issue Management Plan for details on issue management, which efforts are tightly managed and linked.

## 2.0 Methodology

---

### 2.1 Inputs

- King County and ABT Program risk management standards
- ABT Implementation Project Charter, Statement of Work and Detailed Implementation Plan (DIP)
- Schedule and Cost Plan
- Resource Plan

- Project Constraints
- Project Status Reports – Work results and other project records provide information about project performance and risks
- Change Requests – Changes may require new risk analysis and response plans
- Project Repositories – Records from previous ABT phases such as Lessons Learned and issues/risk logs are good references to identify risks because they describe problems and resolutions

## **2.2 Risk Management Process**

The risk management process follows these fundamental steps:

- Plan for risk management activities in the detailed implementation plan (DIP)
- Perform risk assessment in the planning phase of ABT implementation (and reassess throughout the ABT implementation)
- Assign responsibility for risks (Risk Manager and Risk Owner)
- Analyze and score the risk for severity/impact and probability (see Appendix D & E for risk scoring criteria and risk matrix)
- Develop a risk response plan (mitigation or contingency plan, otherwise known as a step-down plan to reduce or remove the risk) (see Appendix C for an example)
- Escalate risk response appropriately in the event an agreeable response is not found
- Monitor, report and update risks regularly (summarize critical risks in regular status reports)
- When an identified risk is realized, execute contingency/mitigation plan (possibly requires approval for change request)
- Close risks as appropriate
- Continue regular risk assessment to identify new risks

## **2.3 Outputs**

- PMRx or other risk tracking log
- Status report summary of critical risks (ongoing)
- Project change requests (*as necessary*)

## **2.4 Metrics**

The principle metrics to be used to measure and improve the quality of this process are:

- A Risk tracking log exists for the project
- Number of risks identified for the project
- Number of risks with effective mitigation or contingency plans and related risk score/exposure
- Number of risks with ineffective mitigation or contingency plans and related risk score/exposure
- Number of risks that were prevented
- Number of risks that occurred

## ***2.5 Risk Tracking Tools***

CIBER recommends the use of the PMRx tool to log and track project risks and the use of risk assessment templates (using MS Excel) to capture the necessary risk details.

See risk tracking templates and scoring criteria in Appendix C, D & E.

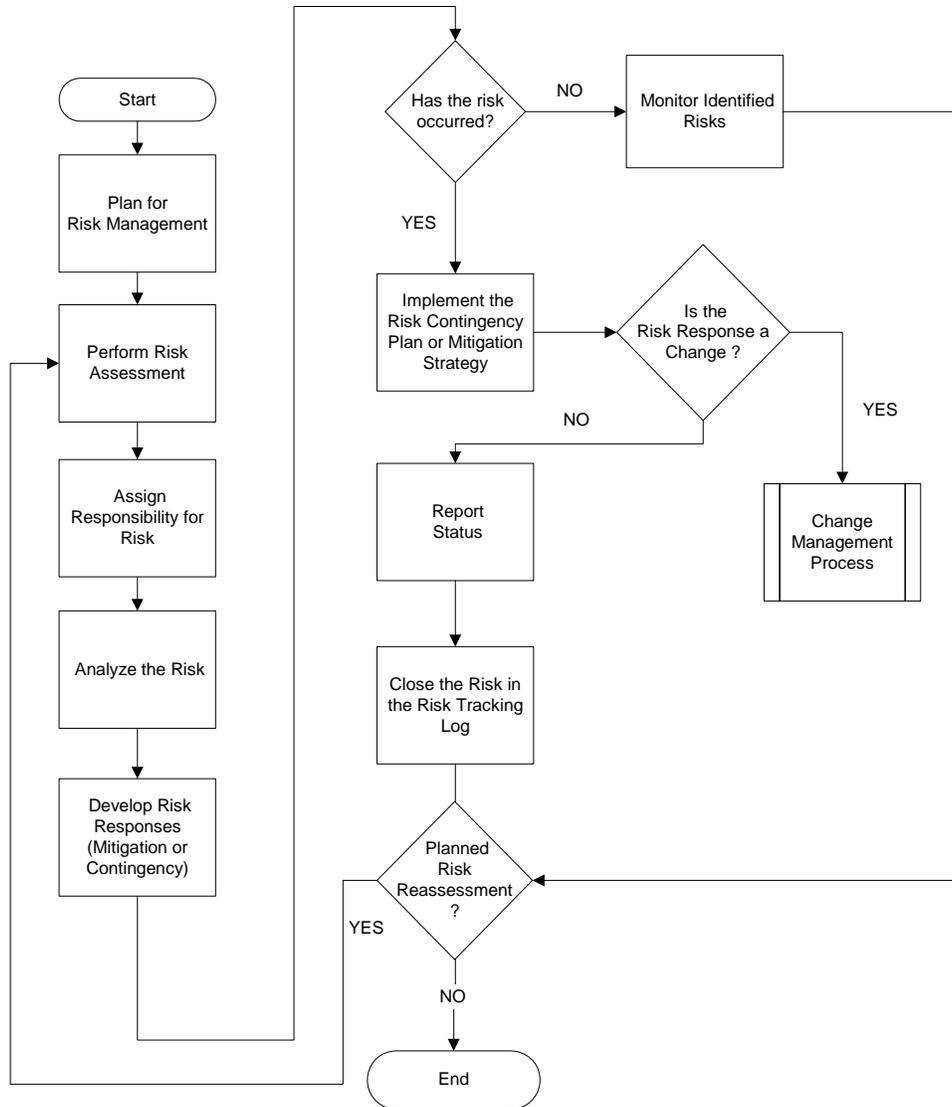
**Appendix C** is an example of a risk response plan (or step-down plan). This shows the risk id, brief description of the risk, the risk score (severity x probability), brief description of the contingency plan and details of the step-down plan by actionable items with estimated completion dates (ECD).

**Appendix D** is an example of the risk scoring criteria for assessing severity scores.

**Appendix E** is a chart summarizes all open risk items by risk id, risk score, risk description and mitigation status.

These 3 templates are meant to work together in assessing risk scores, developing/managing the risk response/step-down plan and reporting on status.

## 2.6 Risk Management Process Flow



## 2.7 Risk Identification

Initial risk identification will be performed during the ABT implementation planning phase and will be reassessed throughout the ABT implementation as risk characteristics may change or new risks may arise. Consider the categories listed in *Appendix A: Major Implementation Risk Categories* while identifying potential risks.

Risk identification techniques include:

- Conduct interviews, brainstorming sessions and/or questionnaires with ABT project stakeholders and project team. (See Appendix B for sample questionnaire).
- Conduct interviews/discussions with subject matter and/or technical experts.
- Review lists drawn from industry experience.
- Review project schedule performance, status reports, issue logs, test results and other project artifacts.
- Review lessons learned and issues/risk logs from similar or related projects.

**Note: It is every team member's responsibility to identify and log risks.**

Upon identification, risks must contain the following information (logged in PMRx Risk Log and Excel risk template):

Data	Description
• Risk Number	Non-repeating, sequential number used to identify the risk.
• Risk Identifier	The name of the person who identified the risk.
• Date Opened	The date the risk was identified.
• Title	A short (~ ten-word or less) descriptive label used to identify the risk.
• Risk Description	A clear explanation of the risk with enough detail to understand the problem and potential consequences. This should be described as <b>“if risk event occurs, then the consequence will be this...”</b>
• Status	Current standing of a request (e.g., Open, Closed or Pending).

See Appendix C: Sample Risk Identification and Response Template

## 2.7.1 Assign Responsibility

Assign an ABT team member to each risk, as the *Risk Owner*. This person will be responsible for researching and developing a risk response (step-down) plan for. Though multiple people may be involved in performing the research and developing the response plans, the Risk Owner will be accountable for ensuring a plan is established – and invoked if the risk occurs – and to maintain current status of the risk for status reporting.

Upon assignment, risks must be updated with the following information (logged in PMRx Risk Log and Excel risk template):

Data	Description
• Risk Owner	The name of the team member responsible for assessing, monitoring and managing the risk and the risk mitigation.

## 2.7.2 Risk Assessment

The Risk Owner is responsible for the analysis of assigned risks to understand its impact(s) and probability of occurring, and developing a risk response (or step-down) plan with actions and due dates. The owner may be sufficiently experienced to perform the analysis or may need to assemble a team with the experience required to perform the analysis effort.

The Risk Owner must analyze, quantify, and document the risk score based on severity and probability as described in the *Risk Scoring Criteria* table found in Appendix C. Risk mitigation can only be as effective as the assessment and response planning. Therefore discipline and assertiveness should be taken in assessing risks and risk responses.

## 2.7.3 Develop Risk Response (step-down) Plan

The Risk Owner must develop and document a risk response for each risk that meets the definition of “critical”, which is a calculated risk score greater than 12 (e.g. probability of 4, severity of 3, (4x3) equals 12). *Please see Appendix E for an example of a risk scoring matrix.*

Throughout the course of a project the probability and severity of a risk event may change (actually it is expected to change *downward*, based on the execution of the step-down plan) and whenever a risk crosses the criteria thresholds of a critical risk (score of 12), a risk response must be established or re-established.

Upon developing a risk response (step-down) plan, risks must be updated with the following information (logged in PMRx Risk Log and Excel risk template):

Data	Description
<ul style="list-style-type: none"> <li>Risk Description</li> </ul>	Stated as <b><i>“if risk event occurs, then the consequence will be this...”</i></b>
<ul style="list-style-type: none"> <li>Mitigation Plan</li> </ul>	A plan to reduce (or step down) the probability or severity of the risk occurring, with specific activities, ownership assignment and due date.
<ul style="list-style-type: none"> <li>Trigger Date</li> </ul>	The trigger date that activates the contingency plan.
<ul style="list-style-type: none"> <li>Contingency Plan</li> </ul>	The contingency action to be taken if the risk occurs or upon reaching the trigger date without an adequate risk mitigation.

See Appendix C: Sample Risk Identification and Response Template

## 2.7.4 Review Risk Responses

Review risks and risk responses weekly or bi-weekly, particularly for critical risks. When a reviewer finds a response inadequate or inappropriate, the reviewer will notify the Risk Owner who will address the review findings and redevelop and resubmit the response.

- a. ABT and System Integrator Program/Project Managers will review and approve all risk responses.
- b. Risk Owners will review risks and risk responses.
- c. Regular status reports will summarize critical risks and risk responses. (See Appendix E for example)

## 2.8 Manage Risks

This activity defines the tasks to be performed throughout the project life cycle. It is ultimately the Project Manager’s responsibility to ensure risks are indentified, assessed, planned, monitored and controlled and to manage new risks as they arise. The Risk Manager will be responsible for the daily or weekly assigned activities in managing risks.

### 2.8.1 Risk Response Plans

Risk responses (mitigations/step-down plans) are planned, proactive actions designed to mitigate (reduce or eliminate) the probability and/or severity of a risk; for example, to establish an additional testing cycle for a critical module if test results are not satisfactorily met by a certain date, of course, having done everything possible to date to accomplish the desired testing results. As such, risk response plans must be planned and managed just like tasks in the master project plan. These responses are called step-down plans as they are intended to “step-down” the probability and/or severity of the risk. Include all tasks necessary to execute the appropriate response/mitigation for each risk and include necessary details in master project plan to schedule, assign resources and monitor these tasks. The same disciplined behavior in managing the risk step-down (response) plans should be taken as in managing the master project plan.

### 2.8.2 Monitor Identified Risks

The Project Manager, Risk Manager and Risk Owner must monitor identified risks, step-down plans and triggers to determine if action is required, such as invoking the contingency plan. Regularly reviews, usually during scheduled status meeting, of identified risks to ensure risk details, scores and step-down plans continue to be accurate, current and complete. Critical risks must be reported in regular status report with summary level information regarding their status and response effectiveness. (See Appendix E for an example.)

### 2.8.3 Implement Risk Contingency Plans

When a Risk is triggered – e.g. as indicated by its trigger event– activate the Risk Contingency Plan and enter the following data into the Risk Log:

Data	Description
<ul style="list-style-type: none"> <li>Date Risk Occurred</li> </ul>	The date the risk actually occurred.
<ul style="list-style-type: none"> <li>Actual Impact</li> </ul>	The actual ramifications (positive or negative) to the project, due to the risk occurring, specified in terms of effort (hours), schedule (days) and budget (dollars).

Note: Implementing Contingency Plans may result in Change Requests. Follow the Project Change Management Process defined for the project to implement a change.

### 2.8.4 Report Interim Status

It is important to have a current, complete and accurate record of the status of each risk; particularly critical risks. The status must include revised information of all applicable items collected in the PMRx Risk Log or Excel risk tracking spreadsheet. The Project Manager or Risk Manager must perform the following activities in tracking and reporting risks.

- a) Discuss/update the status of risks regularly at ABT project team/management meetings.
- b) Update the status of risks on a regular basis to capture a complete and current information trail of the risk's life-cycle.
- c) As mentioned previously, report all critical risks in status report.

(See Appendix E: Sample – Status Report Risk Summary)

### 2.8.5 Close the Risk

A Risk is considered closed when:

- a. The probability of the risk event occurring falls to 0%, or
- b. The risk event has occurred and the impact to the project has been removed.

When a Risk is closed, document the following information for each Risk:

Data	Description
<ul style="list-style-type: none"> <li>• Resolution</li> </ul>	A written description detailing the outcome of the implemented solution. Make sure to include any deviations from the expected impact documented during the analysis of the risk (e.g. the risk never occurred—so no impact).
<ul style="list-style-type: none"> <li>• Closed By</li> </ul>	The person, usually the Project Manager or Risk Manager, who closes the risk.
<ul style="list-style-type: none"> <li>• Date Closed</li> </ul>	The date the risk is officially closed.

### 2.8.6 Perform Additional Risk Assessments

The Project Manager or Risk Manager must periodically reassess the risks of the project.

## 2.9 Close Risk Management

At the completion of the project, ensure documentation regarding the risk management life-cycle has been captured. Risks that are no longer relevant, based upon project closure, are updated to a status of “Closed” with a full explanation of the resolution. Risks that are still relevant, but will not be addressed during a later phase of the project, must be given to the appropriate project/risk manager so they can be managed later.

## 3.0 Roles and Responsibilities

---

The following table lists the Roles and Responsibilities for Risk Management.

Role/Resource	Responsibilities
ABT/SI Program Manager	<ul style="list-style-type: none"><li>• Responsible for overall Risk Management.</li><li>• Responsible for risk escalation resolution.</li><li>• Responsible to execute risk contingency and resolve potential changes to scope, cost and/or schedule.</li></ul>
ABT/SI Project Manager	<ul style="list-style-type: none"><li>• Responsible for coordinating participation from the appropriate personnel regarding risk identification, assessment and response strategies.</li><li>• Responsible to monitor and maintain risks and risk responses.</li><li>• Responsible to escalate risks and risk responses.</li></ul>
ABT/SI Risk Manager	<ul style="list-style-type: none"><li>• Responsible for risk management administrative functions as designated by the Project Manager.</li></ul>
ABT/SI Risk Owner	<ul style="list-style-type: none"><li>• Responsible for assessing risks, providing responses and monitoring risks.</li></ul>
ABT/SI Project Leads & Team Members	<ul style="list-style-type: none"><li>• Responsible for identifying, analyzing and responding to risks.</li></ul>

## Appendix A: Major Implementation Risk Categories

A. Implementation	B. Development Environment	C. Program Constraints
<b>A1. Requirement</b> <ul style="list-style-type: none"> <li>a. Stability</li> <li>b. Completeness</li> <li>c. Clarity</li> <li>d. Validity</li> <li>e. Feasibility</li> <li>f. Precedent</li> <li>g. Scale</li> </ul>	<b>B1. Development Process</b> <ul style="list-style-type: none"> <li>a. Formality</li> <li>b. Suitability</li> <li>c. Process Control</li> <li>d. Familiarity</li> <li>e. Product Control</li> </ul>	<b>C1. Resources</b> <ul style="list-style-type: none"> <li>a. Schedule</li> <li>b. Staff</li> <li>c. Budget</li> <li>d. Facilities</li> <li>e. Hardware/Software</li> </ul>
<b>A2. Design</b> <ul style="list-style-type: none"> <li>a. Functionality</li> <li>b. Difficulty</li> <li>c. Interfaces</li> <li>d. Performance</li> <li>e. Testability</li> <li>f. Hardware Constraints</li> <li>g. Non-Developmental Software</li> </ul>	<b>B2. Development System</b> <ul style="list-style-type: none"> <li>a. Capacity</li> <li>b. Suitability</li> <li>c. Usability</li> <li>d. Familiarity</li> <li>e. Reliability</li> <li>f. System Support</li> <li>g. Deliverability</li> </ul>	<b>C2. Contract</b> <ul style="list-style-type: none"> <li>a. Type of Contract</li> <li>b. Restrictions</li> <li>c. Dependencies</li> </ul>
<b>A3. Code and Unit Test</b> <ul style="list-style-type: none"> <li>a. Feasibility</li> <li>b. Testing</li> <li>c. Coding/Implementation</li> </ul>	<b>B3. Management Process</b> <ul style="list-style-type: none"> <li>a. Planning</li> <li>b. Project Organization</li> <li>c. Management Experience</li> <li>d. Program Interfaces</li> </ul>	<b>C3. Program Interfaces</b> <ul style="list-style-type: none"> <li>a. Customer</li> <li>b. Associate Contractors</li> <li>c. Subcontractors</li> <li>d. Prime Contractor</li> <li>e. Management</li> <li>f. Vendors</li> <li>g. Politics</li> </ul>
<b>A4. Integration and Test</b> <ul style="list-style-type: none"> <li>a. Environment</li> <li>b. Product</li> <li>c. System</li> </ul>	<b>B4. Management Methods</b> <ul style="list-style-type: none"> <li>a. Monitoring</li> <li>b. Personnel Management</li> <li>c. Quality Assurance</li> <li>d. Configuration Management</li> </ul>	<b>C4. Organizational Change Management</b> <ul style="list-style-type: none"> <li>a. Sponsorship, commitment and support</li> <li>b. Organizational resistance</li> <li>c. Organizational readiness (ability to change)</li> </ul>
<b>A5. Engineering Specialties</b> <ul style="list-style-type: none"> <li>a. Maintainability</li> <li>b. Reliability</li> <li>c. Safety</li> <li>d. Security</li> <li>e. Human Factors</li> <li>f. Specifications</li> </ul>	<b>B5. Work Environment</b> <ul style="list-style-type: none"> <li>a. Quality Attitude</li> <li>b. Cooperation</li> <li>c. Communication</li> <li>d. Morale</li> </ul>	

## Appendix B: Risk Identification Questionnaire

---

### Implementation

*Risks to the project that may arise due to the nature of the product being implemented.*

- A.1 Requirements**—Are there risks that may arise from product requirements? Examples: stability, completeness, clarity, validity, feasibility, precedent, scale, etc.
- A.2 Design**—Are there risks that may arise from the design the project has chosen to meet its requirements? Examples: functionality; difficulty; interfaces; performance; testability; hardware constraints; non-developmental software.
- A.3 Code & Unit Test**—Are there risks that may arise from the way the project is choosing to subdivide the design and construct the pieces? Examples: feasibility; testing; coding; implementation.
- A.4 Integration & Test**—Are there Risks that may arise from the way the project is choosing to bring the pieces together and prove that they work as a whole? Examples: Hardware and software support facilities; integration of the parts of the product; integration with the larger system
- A.5 Engineering Specialties**—Are there Risks that may arise from special attributes of the product, such as maintainability, reliability, safety, security, human factors, etc.?
- A.99 (Other)**—Are there other Risks that may arise from the product itself, but are not covered by the above categories?

### Process (Development Environment)

*Risks to the project that may arise due to the way you are developing the product.*

- B.1 Development Process**—Are there Risks that may arise from the process the project has chosen to develop the product? Examples: formality; suitability; process control; familiarity; product control.
- B.2 Development System**—Are there Risks that may arise from the hardware and software tools the project has chosen for controlling and facilitating its development process? Examples: capacity; suitability; usability; familiarity; reliability; system support; deliverability.
- B.3 Management System**—Are there Risks that may arise from the way project budget or schedule is planned, monitored or controlled, or the project's structure, or its handling of internal and external organization interfaces?
- B.4 Management Methods**—Are there Risks that may arise from the way the development or program personnel are managed, in areas such as status monitoring, personnel management, quality assurance, or configuration management?
- B.5 Work Environment**—Are there Risks that may arise from the general environment or the larger organization to which the project belongs, such as quality attitude,

cooperation, communication, or morale?

**B.99 (Other)**—Are there other Risks that may arise from the way the project is going about its development, but not covered by the above categories?

### **Constraints (Program Constraints)**

*Risks to the project that may arise due to sources outside the project's control.*

**C.1 Resources**—Are there Risks that may arise from resources the project needs but that are outside its control to obtain or maintain? Examples: schedule; staff; budget; facilities.

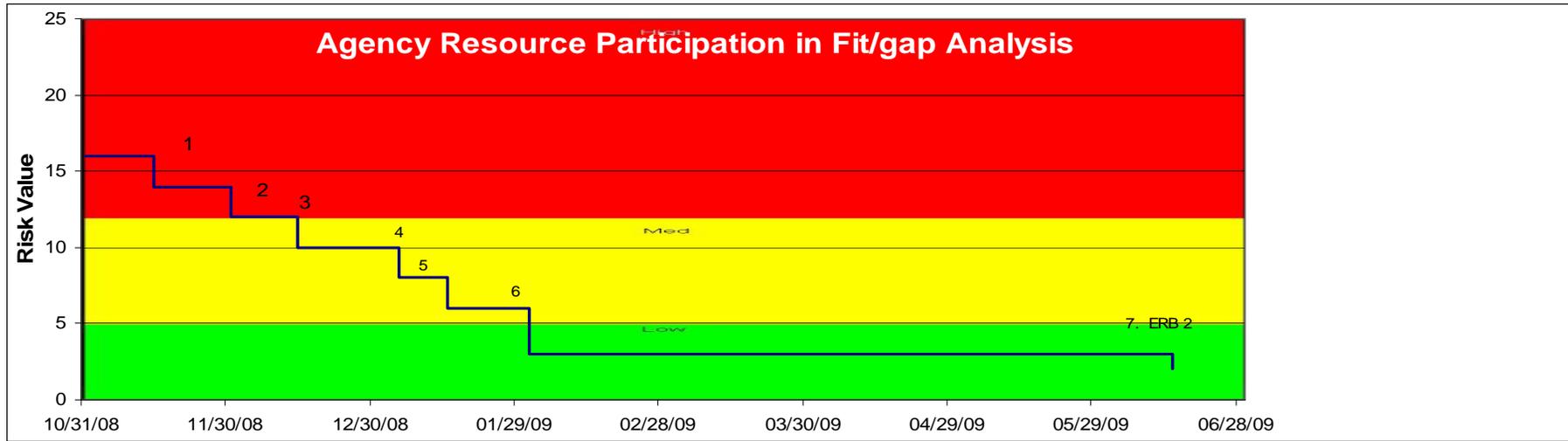
**C.2 Contract**—Are there Risks that may arise from the [already legally binding] contract? Example areas include the contract's type, restrictions, or dependencies.

**C.3 Program Interfaces**—Are there Risks that may arise from outside interfaces which the project cannot reasonably expect to control? Examples: customer; associate contractors; subcontractors; prime contractor; management; vendors; politics.

**C4. Organizational Change Management**—Are there Risks that may arise from limited sponsorship, commitment or support, resistance to change and/or the readiness or ability to change. Example areas include senior management and project stakeholder sponsorship, team commitment, political acceptance, general nature of accepting change.

**C.99 (Other)**—Are there other Risks that may arise from factors outside project control, but not covered by the above categories?

## Appendix C: Sample – Risk Response “Step-down” Plan Example



<b>Risk Score</b>	<b>16</b>		Contingency Plan: Plan for additional fit/gap sessions and add one month to project.				
			Risk Owner: Steven Vowles				
	<b>Risk Mitigation Plan</b>	Trigger Date	06/01/2009	<b>ECD</b>	<b>Target Value</b>	<b>Actual Date</b>	<b>Actual Value</b>
<b>Risk Description/#</b>	<b>ABT108</b>	0	Risk Open Date and Baseline Risk Level	11/1/2008	16		16
If agencies are not able to provide resources to contribute to the fit/gap workshops between 02/09 and 06/09, then we will likely miss key requirements and related configurations in the initial test prototype and require 1 month of rework.	1	1	Build support at ABT/County leadership for required resource commitments	11/15/2008	14		16
	2	2	Determine County resource needs by department and by skill set	12/1/2008	12		15
	3	3	Schedule County resources for Feb - April workshops	12/15/2008	10		10
	4	4	Schedule County resources for May - July workshops	1/5/2009	8		
	5	5	Confirm County resources for Feb - April	1/15/2009	6		
	6	6	Follow up with actual counts in May - July	2/1/2009	3		
	7	7	Follow up at end of workshops	6/15/2009	2		
	8	8					
	9	9					
<b>Risk Scoring</b>	<b>NOTE: Risk Score is Probability x Severity (4x4=16)</b>						
<b>Probability</b>	<b>4</b>						
<b>Severity</b>	<b>4</b>						
Cost	4	\$	731k				
Schedule	4		1 mo				
Technical	2						
Success	2						

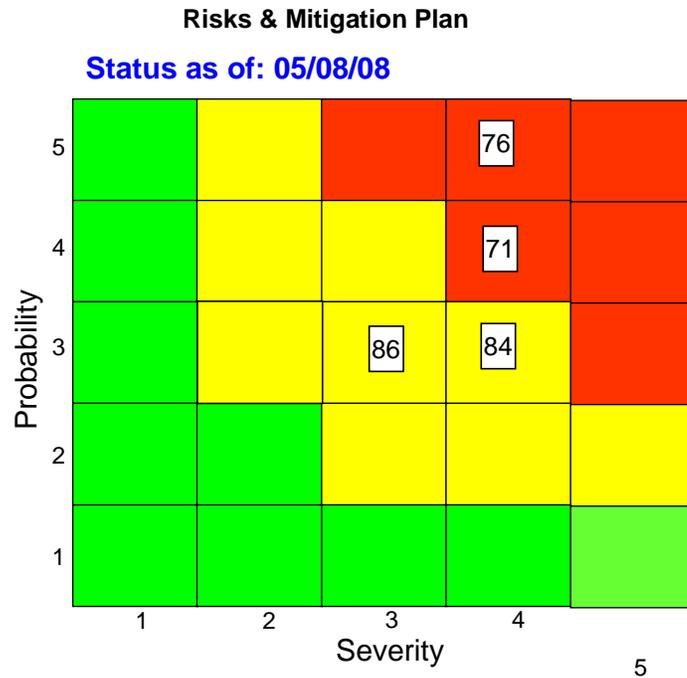
## Appendix D: Sample – Risk Scoring Criteria

Probability	1 >0-20 %	2 >20-40%	3 >40-60%	4 >60-80%	5 >80-100%
Severity	1	2	3	4	5
<b>COST</b>	Potential loss less than 1% of budget or up to [\$200,000]	Budget overrun of effected activities of 1 to 5% or cost impacts greater than [\$50,000 and up to \$200,000]	Budget overrun of effected activities of 5% or cost impacts greater than [\$200,000 and up to \$2 million]	Budget overrun of effected activities of greater than 5% or cost impacts between \$[2 to 10] million.	Budget overrun exceeds contingency or cost impacts greater than \$[10] million.
<b>SCHEDULE</b>	No impact on milestones. Existing schedule margin (slack) may be consumed.	No impact on critical path milestones. Up to [5] working day delay to non-critical path.	Up to [10] working day impact on critical path, out of sequence work required to prevent impact to plan. Up to 1 month delay to non-critical path milestone	Up to [20] working day impact on critical path, out of sequence work required to prevent impact to plan. Greater than 1 month delay to non-critical path milestone	Greater than [1] day impact to plan, or greater than [20] day impact to critical path
<b>TECHNICAL</b>	Requirements are satisfied but less than 10% of the margin band remains. No impact to design.	Minimum Performance impact. Requirements are met but with zero margins using standard methodologies. No impact to design.	Moderate Performance Impact. Zero margins can be shown using non-standard methodologies. Design change may be required but no change to hardware configuration.	Significant Performance impact. Negative margins exist but can be resolved by utilizing contingency. Minor design change may be required with a minor change to the hardware or software configuration.	High Performance impact: No remaining margin is available under any condition. Potential impacts to program success. Significant redesign or re-qualification may be required.
<b>PROGRAM SUCCESS</b>	Problem affects non-critical systems.	The problem shows minimal affects to systems and/or ABT program, though not noticeable.	The problem shows moderate affects to systems and/or ABT program, noticeable to leadership.	The problem shows significant affects to systems and/or ABT program, requiring political damage control.	The problem shows serious affects to the systems and/or ABT program, with potential for ABT program failure.

**Note: We will determine specific dollar and schedule risk criteria amounts at the beginning of the ABT Risk Assessment.**

## Appendix E: Sample Project Risk Profile for Status Reporting

# Project Risk Profile



### Risk Levels

<ul style="list-style-type: none"> <li><span style="color: red;">■</span> High</li> <li><span style="color: yellow;">■</span> Medium</li> <li><span style="color: green;">■</span> Low</li> </ul>	<ul style="list-style-type: none"> <li>Major disruption of the plan</li> <li>Some disruption in the plan</li> <li>Little or no disruption to plan</li> </ul>
---	--

### Risk Items:

- 76 – Phase 2 resource conflicts (new risk)
- 84 – Transfer knowledge to O&M Organization. (new risk)
- 86 – Timing to load FICO Delta historical data (prior 4x3)
- 71 – Data conversions (prior 4x3)

### Mitigation Status:

- 76 – Assessing options for risk mitigations due 2/15/08
- 84 – O&M to on-board additional resources and train by 2/28
- 86 – Managing step-down plan
- 71 – Managing recovery plan & monitor progress daily

**Note: This chart is an example of a risk profile. The blocks represented by numbers 71, 76, 84 and 86 are sample risk ids, and the “Risk Item” is the general description of the risk and, the “Mitigation Status” is the general description of the current mitigation.**

## Appendix F: Sample – Risk Tracking Log (part 1)

 <b>King County</b> <b>ABT PROGRAM</b> <small>Accountable Business Transformation</small>										
<b>ABT Program</b> <b>Risk Tracking Log</b>										
Risk Number	Opened By	Date Opened	Title	Risk Factor	Status	Owner	Impact (\$, Hrs, Schedule)	Severity	Probability	Trigger Event/Date
1	S. Vowles	8/27/2008	Team members assigned part-time.	Must be able to accomplish the setup in minimal time, but with part-time resources.	Open	K. Pace	\$50,000 240 Hrs 30 Days	4	5	Missed Milestone 11/30/08
2	S. Vowles	8/31/2008	Unable to meet all requirements.	Multiple requirements with conflicting needs that may pose a threat to accomplishing a complete migration.	Open	K. Pace	\$10,000 50 Hrs 5.5 Days	3	3	Missed Milestone 11/30/08

## Appendix F: Sample – Risk Tracking Log (part 2)

 <b>ABT Program</b> <b>Risk Tracking Log (continued from first page with additional columns)</b>										
Risk Number	Opened By	Mitigation Plan	Contingency Plan	Date Risk Occurred	Actual Impact	Status Entered By (Date)	Status Comments	Resolution	Date Closed	Closed By
1	S. Vowles	Acquire more full-time help.	Reset stakeholder expectations and revise the schedule.							
2	S. Vowles	Acquire more full-time help.	Redefine the requirements and/or reset stakeholder expectations and revise the schedule.							