



OAKS Risk Management Plan

Prepared

for

The State of Ohio

OAKS Project

Prepared By

Accenture

September 26, 2005

This page intentionally left blank

Document Information

Edition Information:	Type of Document:	Project Plan – Risk
	Status of Document:	<i>Final</i>
	Effective Date:	<i>9/26/2005</i>
	Document File Name:	<i>PM129 OAKS Risk Management Plan.doc</i>
	Document File Location:	<i>In BI Designer at: OAKS\Cabinets\Project Management\Working Deliverables\Deliverable 9</i>
Document Control:	Title of Document:	<i>OAKS Risk Management Plan</i>
	Program Name:	<i>OAKS</i>
	Originator:	<i>Andrew W. Gordon</i>
Contact Information:	Author:	<i>Andrew W. Gordon</i>
	Phone:	<i>614-387-3001</i>
	E-mail Address:	<i>Andrew.gordon@oaks.state.oh.us</i>

Record of Review and Changes

Person	Date	Version	Description of Change
Andrew Gordon	8/5/2005	1.0	Document Created
Andrew Gordon	9/9/2005	1.1	Incorporated updates from Shirley Whaley
Andrew Gordon	9/22/2005	1.2	Incorporated updates resulting from official state review

Embedded Deliverable Tracking Form:

1. Keep this embedded form updated as the deliverable winds its way through the deliverable process.
2. This form is to be updated every time this deliverable is submitted for a review (peer review, management review, quality team lead review, etc.)
3. To update this form, double click on the embedded file below, make your updates, click the save button, then close the file.



"Document
Deliverable Tracking

Table of Contents

1	INTRODUCTION	1
1.1	DOCUMENT OVERVIEW	1
1.2	SCOPE	1
1.3	OBJECTIVES.....	1
1.4	GUIDING PRINCIPLES.....	2
1.5	RESPONSIBILITY FOR THE PLAN	2
1.6	PLAN AND/OR PROCESS DEPENDENCIES	2
1.7	REFERENCED DOCUMENTS.....	2
2	PROCESS RESPONSIBILITY – ROLES AND RESPONSIBILITIES.....	2
2.1	RISK MANAGER/DATABASE ADMINISTRATOR	3
2.2	RISK ORIGINATOR	3
2.3	RISK OWNER.....	4
2.4	RISK POINT OF CONTACT.....	4
2.5	PROJECT TEAM LEADS	4
2.6	EXECUTIVE PROGRAM MANAGERS.....	5
2.7	OAKS PROJECT TEAM MEMBERS	5
2.8	BUSINESS AND TECHNICAL ADVISORY GROUP.....	5
2.9	OAKS PROGRAM MANAGEMENT OFFICE (PMO)	6
2.10	RISK MANAGEMENT WORKING GROUP.....	6
3	RISK MANAGEMENT PROCESS	7
3.1	RISK MANAGEMENT OVERVIEW.....	9
3.1.1	<i>Risk Initial Planning and Identification.....</i>	<i>9</i>
3.1.2	<i>Continual Risk Identification.....</i>	<i>10</i>
3.1.3	<i>Risk Assessment and Categorization of Risks.....</i>	<i>11</i>
3.1.4	<i>Risk Data.....</i>	<i>12</i>
3.1.5	<i>Process Steps</i>	<i>16</i>
3.2	RISK ESCALATION PROCEDURES	24
3.3	RISK MANAGEMENT WORKING GROUP MEETINGS (QUARTERLY OR AS NEEDED)	24
3.4	RISK MEETING AND REPORTING PROCESSES (WEEKLY AND DAILY)	25
3.5	RISK MEETING REPORT	26
3.6	RISK MAILING LIST	26
4	RISK MANAGEMENT TOOL	26
4.1	RISK SECTION OF BI DESIGNER AVAILABLE TO ALL OAKS TEAM MEMBERS	26
4.2	USING THE RISK ENTRY FORM TO CREATE NEW RISKS	26
4.3	VIEWING RISKS	27
4.4	UPDATING RISKS.....	27
5	OAKS RISK MANAGEMENT METRICS	27
6	RISK IDENTIFICATION QUESTIONNAIRE	27

Table of Figures

Figure 1 - Risk Management Overview..... 3
 Figure 2 - Risk Management Process..... 7
 Figure 3 - Risk Assessment Color Matrix..... 8
 Figure 4 - Risk Initial Evaluation and Planning 9
 Figure 5 - Risk Rating 17
 Figure 6 - Risk Response and Control 20
 Figure 7 - Risk Mitigation Approval Matrixes 22

Table of Tables

Table 1 - Risk Data Captured in Risk Management Tool..... 12
 Table 2 - Standard Risk Notices and Reports..... 25



1 Introduction

1.1 Document Overview

The OAKS Risk Management Plan (RMP) is a living document providing the OAKS Program a method for managing risks to ensure program success. A risk is defined as any concern that could impact the ability of the OAKS Program to meet its schedule, and cost objectives. Risk has two components:

- The probability of failing to achieve a particular outcome
- The consequences of failing to meet that outcome

Risks are measured in terms of severity as determined by probability of occurring and affecting the program. Unlike issues (which are problems involving a significant choice between two or more alternative for an event that is happening now), risks relate to events that could occur and may affect the program's schedule, or cost objectives.

The risk management process will enable the OAKS Program to create strategies that effectively address potential barriers to program success. The risk management process involves identifying, assessing, mitigating, and managing the program's risks. Actions taken to address risk may lead to decisions that affect reporting or the development of the business capability or affect the management of the program. The RMP serves as a guide to all team members in managing program-wide and Integrated Project Team (IPT)-level risks.

1.2 Scope

Risk management is executed at all levels within the program and IPT. The risk management process ensures that risks are mitigated at the appropriate level and communicated as appropriate. This plan provides guidance on managing all levels of risks. These processes are implemented within the individual teams and IPTs that comprise the program.

1.3 Objectives

Successful management of the OAKS Program requires informed, proactive, and timely management of risks. The specific objectives of the OAKS RMP and approach are listed below:

- Ensure critical risks impacting schedule, cost, and/or performance are identified to communicate, escalate, and mitigate risks in a timely manner.
- Ensure the probability and impact of risks is reduced to an acceptable level through an effective mitigation process.
- Focus attention on key risks affecting the program versus individual teams or IPTs.
- Provide risk information for milestone decisions.
- Produce meaningful information that allows program management to focus efforts on the "right" risks (e.g., very high and high probability or impact) with an effective coordination of effort to mitigate the risk.
- Ensure that appropriate stakeholders are informed and, if applicable, participate in the mitigation.



- Ensure that the stakeholders understand the implication of accepting certain risks and are comfortable with accepting these risks.
- Provide an audit trail of discussions and mitigation of program risks.

1.4 Guiding Principles

To be successful, the principles listed below guide the use and implementation of the risk management process:

- The risk management process emphasis will be placed on effectiveness and simplicity.
- A single owner will be assigned responsibility for each risk even if several people work to mitigate it.
- Effort and communication will be focused on the most severe risks.
- Realistic due dates for mitigation steps will be set to meet these dates.
- Risks will be mitigated at the appropriate organizational level (e.g., program, IPT).
- Risk owners will evaluate the initial risk severity and impact levels of risks they are assigned.
- Planned risk mitigation history and actual mitigation of each risk will be documented. This documentation can serve as key input to root cause analysis, key learning, metrics, and risk analysis.

1.5 Responsibility For the Plan

The RMP was prepared by the OAKS Risk Management Leads, who are also responsible for updating it with any significant changes, and making sure that all project members adhere to all risk management processes. The risk management plan will be updated at least once per quarter and submitted to the client for reviews at that time.

1.6 Plan and/or Process Dependencies

The information contained in the OAKS Risk Management Plan both affects, and is affected by the following project plans and processes.

- Project Plans (OAKS Work Plan)
- WBS
- Project Measurement Plan

1.7 Referenced Documents

- OAKS Quality Management Plan
- OAKS Risk Owners Guide

2 Process Responsibility – Roles and Responsibilities

An overview of the risk management process is depicted in figure 1. Key roles and responsibilities are then defined in the following sections.

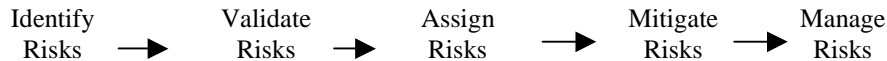


Figure 1 - Risk Management Overview

2.1 Risk Manager/Database Administrator

To maintain the integrity of the risk database, the risk database administrator will be responsible for entering and updating data into the database, as well as doing regular maintenance to the Risk Management tool. Regular maintenance includes:

- Updating field values as they become available
- Ranking the risks on a regular basis
- Validate that risk mitigation steps include the corresponding decrease to probability and/or impact
- Report when required contingency plans are missing
- Report when risk milestones are not entered into the OAKS Work Breakdown Structure (WBS)
- Validate that risks have been closed in accordance with risk closure guidelines

These individuals are also responsible for creating reports for the team lead project status meetings, setting schedules for the Risk Management (RM) Working Group meetings, and producing custom reports as required. The Risk Database Administrators are Shirley Whaley (Shirley.Whaley@oaks.state.oh.us) and Andrew Gordon (Andrew.Gordon@oaks.state.oh.us). The risk managers are also responsible for:

- Writing and maintaining the Risk Management Plan
- Defining and implementing the risk management process
- Train all OAKS team members on the risk management process
- Maintain and update the risk section of the BI Designer web page
- Hold quarterly (or as needed) risk working group workshops

2.2 Risk Originator

The Risk Originator is any person in the OAKS Program who identifies an OAKS Program risk. The Risk Originator will submit the risk to his or her risk administrator by filling out the new risk entry form located on the risk section of the BI Designer website (OAKS\Cabinets\Project Management\Risk Management\Risk Job Aids\OAKS Risk Entry Form.xls). Members of the following groups may recommend new risks:

- OAKS PMO
- OAKS State Team Members
- OAKS Contractor Team Members (Lead contractor and subs)

Specific responsibilities of the risk originator include the following:



- Identify any significant risk to the OAKS Program
- Enter the risk, including initial severity assessment, into the risk entry form
- Clarify risk information for the Risk Management (RM) Working Group, as requested
- After initial risk entry, communicate significant newly discovered information regarding the risk to the RM Working Group or Project Team Leads, as necessary

2.3 Risk Owner

The Risk Owner is the person to whom the responsibility for mitigating the risk is assigned. Risk Owners should be the people who will be most affected if the risk occurs (becomes realized). The Risk Owner has the following responsibilities:

- Create a risk mitigation plan, as required and a contingency plan, as directed, in the event the risk occurs
- Update risk information, as necessary
- Ensure the risk is being mitigated
- Execute the Contingency Plan, as required
- Recommend risk closure to the appropriate group
- Present risk status as required

2.4 Risk Point of Contact

A Risk POC has responsibility for answering risk-related questions his or her team members may have about the Risk Management Process, along with compiling recommendations for the risk management working group meetings. The OAKS POCs are as follows:

- OAKS State Risk Manager – Shirley Whaley
- OAKS Accenture Risk Manager – Andrew Gordon

2.5 Project Team Leads

The Project Team Leads have overall responsibility for the risk management process. Each Project Team Lead will be responsible for all risks that fall within his or her release. Basic responsibilities of Project Team Leads include:

- Discuss risk status during weekly project status meetings
- Ensuring no risk mitigation steps are past due
- Validating new risks
- Establishing initial priority, owner, and target due dates
- Approving initial risk mitigation plans
- Reviewing and updating Risk Owners, as necessary
- Approving risk mitigation plan updates
- Reviewing probability, impact, impact date, and completeness of risks, as necessary
- Approving changes on impact date, new probability, new impact, etc.
- Retiring risks
- Reviewing status of risks



- Re-opening retired risks
- Ensuring contingency plans are executed for appropriate realized risks
- Ensure that Risk Owner's update their risk information prior to Risk Workshops
- Identifying risks for escalation to the OAKS Executive Leadership (EL).
- Note: Risks that get escalated to the EL are risks that are categorized as Very High risks and have major problems that the Project Team Leads, RM Working Group, and OAKS management are not capable of resolving; these risks can include:
 - Problems that involve outside parties essential to the problem and/or solution
 - Risks where the solution requires significant changes to baseline costs and/or schedule
- Ensuring all risks that fall within their Release are being managed
- Representing their Release and ensure that key risk owners attend Risk Working Group Meetings
- Working with Integrated Project Teams (IPTs), subject matter experts, and EL to mitigate risks

2.6 Executive Program Managers

The executive program managers are also referred to as the Executive Leadership (EL) and include:

- OAKS Executive Program Manager
- OAKS Deputy Program Manager
- Accenture Program Manager
- Accenture Deputy Program Manager

The responsibilities of the OAKS EL in the risk management process include the following:

- Assisting in cross-organization and controversial risk mitigation
- Supporting mitigation implementation as necessary

2.7 OAKS Project Team Members

The OAKS project team members have been assigned to the OAKS project on a full time basis and responsibilities would include the following:

- Perform any risk management tasks as assigned by the Team Leads
- Identify risks in a facilitated risk evaluation, as assigned by Team Leads
- Identify new risks to the Team Leads, as soon as each risk is perceived
- Review the Risk Management Plan for correctness and adequacy, as well as, provide feedback for improvement

2.8 Business and Technical Advisory Group

The Business and Technical Advisory Group members include EL, project managers, team leads, IPT leads, and part time module business owners, and responsibilities would include the following:



- Maintain awareness of risks and their potential impact
- Provide assistance and support to the Team Leads
- Identify risks & their impacts

2.9 OAKS Program Management Office (PMO)

Risks will be communicated to the PMO through the weekly status meeting. Slides will be created that identify new risks, summarize red risks, and summarize all risks (by color). The OAKS PMO responsibilities in the risk management process include the following:

- Assisting in cross-organization and controversial risk mitigation
- Supporting mitigation implementation as necessary
- Identifying risks for escalation to the Business Owners Advisory (BOA) Group

2.10 Risk Management Working Group

The RM Working Group's schedule will be dependent on the Program Management review of the OAKS Program or on an as-needed basis. The Group should meet quarterly (or as needed) and its goal is to bring together all people who are involved in the risk process and discuss strategy, evaluate existing risks, and create new risks. Basic responsibilities of the RM Working Group include:

- Beginning risk identification by holding initial Risk Brainstorming session.
- Acting as liaison to stakeholder groups regarding:
 - Risk Identification
 - Risk Analysis
 - Assigning Risk Mitigation and Contingency Planning Actions
 - Monitoring status of assigned actions
- Communicating status to risk originators, risk owners, and risk stakeholders
- Identifying new risks
- Reopening retired risks
- Establishing severity of risks and define target dates
- Establishing owner of risk and confirm target dates
- Reviewing status, severity, owner, and completeness of risks
- Approving changes on impact date, new probability, new impact, etc.
- Identifying risks for escalation to the EL
 - Note: Risks that get escalated to the EL are risks that are categorized as Very High risks and have major problems which the Project Team Leads, RM Working Group, and OAKS management are not capable of resolving; these risks can include:
 - Problems that involve outside parties which are essential to the problem and/or solution
 - Risks where the solution requires significant changes to baseline costs and/or schedule
 - Working with IPTs, subject matter experts, and EL to facilitate solutions to risks.

Recommended members of the RM Working Group includes:

- OAKS Risk Managers



- Risk Originator, as required
- Risk Owner, as required

3 Risk Management Process

This section describes the risk management process from risk identification to risk completion. The risk management process is a continuous cycle performed initially during program planning and thereafter following identification of new risks. New risks may arise from a variety of sources:

- Risks previously missed or unforeseen
- Risks arising from an approved change request, where cost, schedule, or scope may be amended, impacting the critical path
- Risks arising from major issues
- Risks arising from the investigation of current risks
- Risks arising from the outcome or consequence of a separate risk occurrence

Figure 2 depicts the high level risk management process steps in direct relation to the risk management overview shown in Figure 1. Subsequent sections detail each process step, describe the data elements tracked for each risk, the escalation procedure, the current RM Working Group meeting schedule, and an overview of the feedback and reporting process is provided.

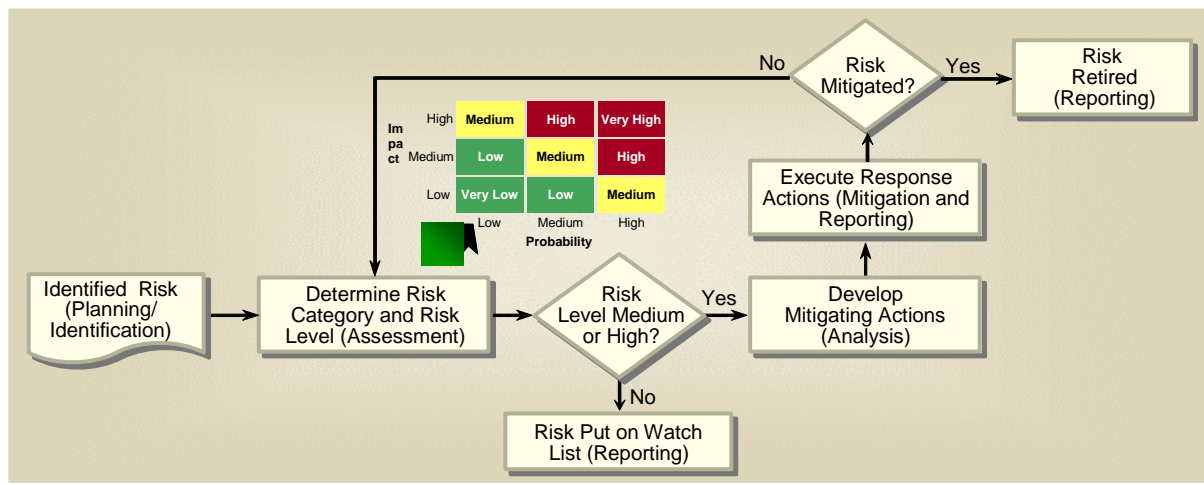


Figure 2 - Risk Management Process

Difference Between Risks and Issues

An *Issue* refers to a problem involving a significant choice between two or more alternatives for an event that is happening now. *Risk* describes situations that could occur. If it does occur, it would have a significant impact on the project. Issues are handled separately. For information on issue management, please refer to the Issues Management Plan. The two major variables used in classifying a risk are 1) probability of the risk occurring and 2) the impact or



consequence if that risk occurs. The two variables are combined to assess the risk as shown in Figure 2.

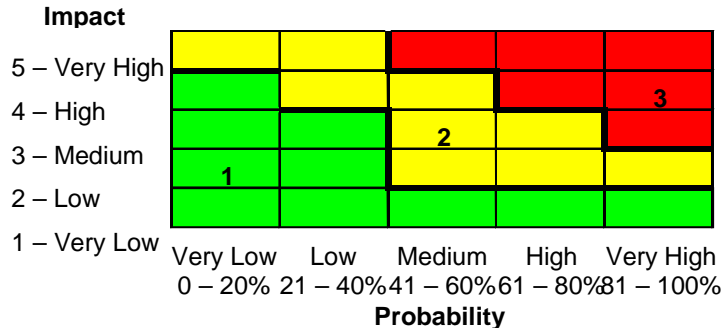


Figure 3 - Risk Assessment Color Matrix

Risks that fall into area 1 (green) can be categorized as ‘Low’ and should be monitored. Risks that fall into area 2 (yellow) can be categorized, as ‘Medium’ and a mitigation plan should be prepared for implementation in case the risk increases in probability or impact. Risks that fall into area 3 (red) are categorized as ‘High’ and active steps should be taken to prevent them (create mitigation and contingency plan).



3.1 Risk Management Overview

3.1.1 Risk Initial Planning and Identification

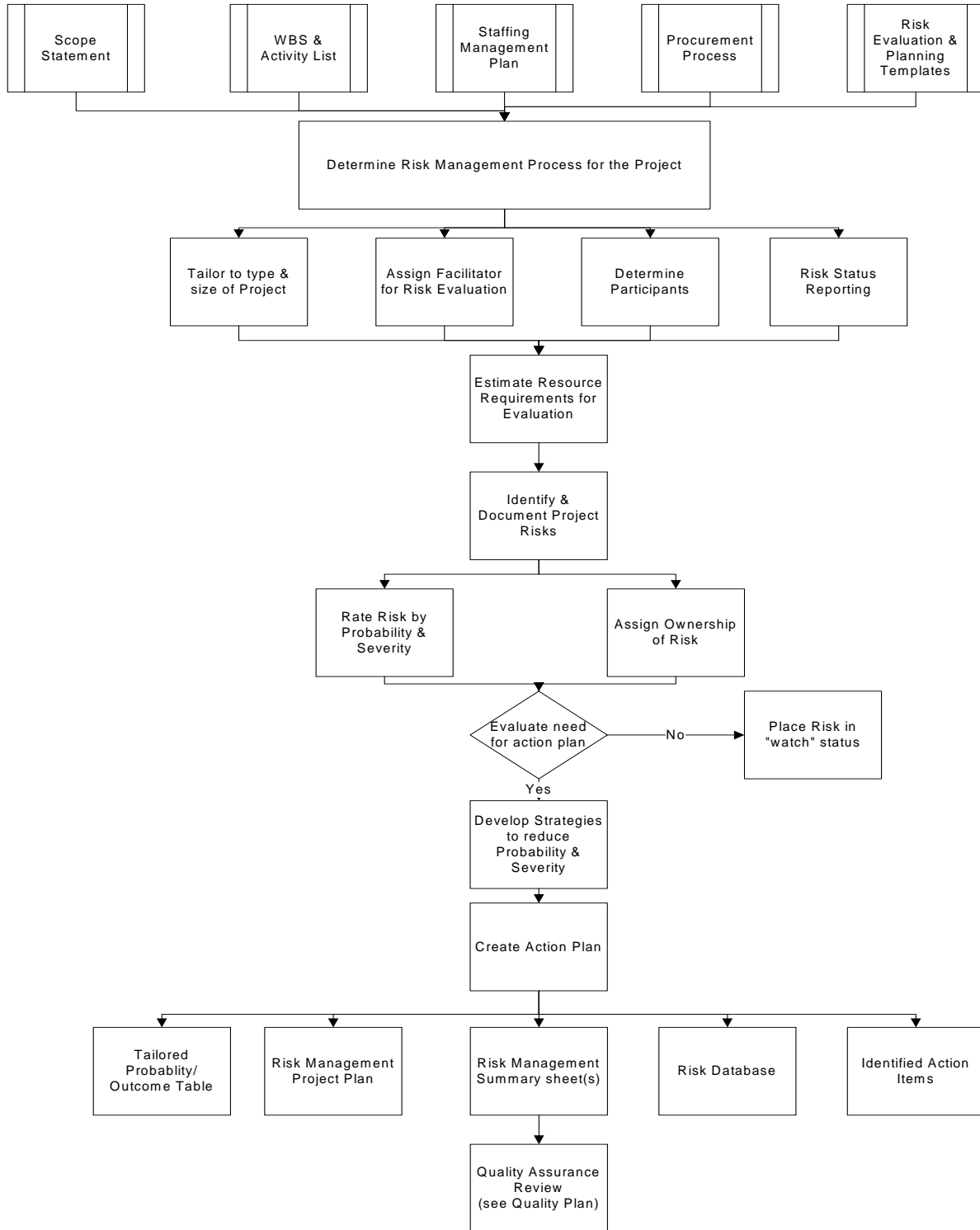


Figure 4 - Risk Initial Evaluation and Planning



Figure 4 outlines the detailed flow of initial risk evaluation and planning. During the startup of the Risk Management Process, existing risks must be identified quickly to begin timely mitigation. Three alternatives to identify existing risks initially are:

- Risk Workshops
- Risk POCs working within their groups to identify risks
- Combination of Risk Workshop and Risk POC Group meetings

The selected approach is the combination.

3.1.1.1 Risk Workshops

A Risk Workshop is a brainstorming session used to identify initial risks. The meeting participants are the members of the entire RM Working Group and representatives from OAKS Program stakeholders. RM Working Group members discuss and identify potential and/or existing risks. At the workshop's end, a list is compiled of all the initial risks and then entered into the Risk Management tool.

3.1.1.2 Risk POC Groups

Another method of first identifying risks is to have both the Risk POCs gather risks from within their respective teams, consolidate them, and submit them to the RM Working Teams. The Risk POCs will compile a composite risk list and enter them into the Risk Management tool.

3.1.1.3 Combination: Risk Workshops and Risk POC Groups

All OAKS team members are expected to identify risks and communicate them to their OAKS Risk POC for both initial and ongoing risks gathering efforts. The representatives of each OAKS stakeholder group will participate in the Risk gathering workshop. The OAKS RM Working Group, with program management's approval, will determine and recommend these Teams. The selected approach to determining initial risks is to have a combination of a Risk Workshop and Risk POC Group meetings. First, the Risk POCs gather risks from within their own teams. That list is then consolidated and taken to the Risk Workshop. The POCs then participate in a one-time Risk Workshop, starting with their Teams' consolidated risk lists. During the risk workshop a final list of risks will be produced and submitted to the Risk Administrator for entry into the Risk Management tool. With this "combination" approach, a greater number of people have input into determining the initial risks. Also, the Risk Workshop is much shorter and much more efficient.

3.1.2 Continual Risk Identification

Once initial risks are identified, an ongoing process for timely capture and management of risks will be established in several ways:

- The Project Team Leads will hold regular meetings where risks will be constantly submitted and reviewed.



- A risk entry form (Excel spreadsheet) will be available for users to enter data. This form is located on BI Designer at *OAKS\Cabinets\Project Management\Risk Management\Risk Job Aids*. The data will be sent via e-mail to the Risk Administrator where they will then be entered into the Risk Management tool.

3.1.3 Risk Assessment and Categorization of Risks

Risk categorization is achieved by defining characteristic sources of risks. These sources describe the generic areas where specific risks are likely to occur, and formalize the categorization initially performed during Risk Management Planning. Risks can be assessed into five categories: cost, schedule, technological, and external.

3.1.3.1 Cost

Cost-based risks outline the non-achievement of the financial benefits of the project detailed in the project objectives or key success factors (such as the Cost Performance Index (CPI)). Typical cost risks include external contractor overspend, additional costs in changing/solving design, or application project problems.

3.1.3.2 Schedule

Schedule-based risks focus on the non-achievement of the project's products or benefits within the specified time frame. Typical schedule-based risks arise from extensions from scope changes, resource unavailability, market opportunities missed, and additional schedule extensions from solving those risks outlined in 'Cost' above.

3.1.3.3 Technological

Technology-based risks consider the non-achievement of the application specifications and benefits expected. Typical risks include new/non-standard platform technology, integration problems with existing other systems, migration problems, performance expectations not achieved, environment complexity and functionality, and system operability.

3.1.3.4 External

External-based risks consider the 'environmental' factors largely outside of the control of the Project Management, which can directly/indirectly affect the successful delivery of the Project. Typically, risks arising from legislative regulations, legal requirements, communication to the State, lack of market sophistication, and the strategic direction and priority conflicts of a controlling body, are profiled under this category.

The Cost and Schedule risk sources are known as the risk 'indicators', as they are often the most tangible measure of overall progress towards Project objectives or goals. The Technological, and External risk sources are referred to as risk 'drivers', as these are the sources of all Project risks, which additionally drive the Cost and Schedule risks.

The recognition that the management of the sources of Technological, and External risk is inter-related to the management of Cost and Schedule risks is an important link in effectively responding and reporting risk-reducing activities.



3.1.4 Risk Data

Data necessary to create and track the risk in the Risk Management tool is identified in the table below. The data fields are defined along with the list of values, if applicable. This data maps directly to the fields in the risk management tool, Risk Radar (see Section 4).

Table 1 - Risk Data Captured in Risk Management Tool

FIELD NAME	DEFINITION	LIST OF VALUES	
Risk Title	Identifies the title of the risk.	Unique for each risk.	
Risk ID	Uniquely identifies each risk.	001, 002, etc. This number is assigned by the Risk Management tool.	
Rank	Shows the rank of the risk based on Impact Date, Probability, and Severity	Integer value (1, 2, 3, etc.)	
Risk Statement/Description	Description of what the risk consists of	Unique for each risk.	
Date Identified	The date the risk was identified and entered into the risk tracking system	Date risk was identified.	
Status	Indicates risk's position in the Risk Management process.	<u>Status Name</u>	<u>Definition</u>
		New	A newly identified risk.
		Assigned	A risk that has been assigned an owner and is waiting for necessary data (mitigation plan, etc.).
		Mitigated	This status means that the risk has been successfully mitigated (resolved). At this point, the risk probability and/or impact should be lowered so that the risk color code is Green.



Ohio Administrative Knowledge System

OAKS —————> Transforming the Way Ohio Does Business

FIELD NAME	DEFINITION	LIST OF VALUES		
		Retired	The completed risk no longer has impact, has been fully mitigated, or has occurred and the contingency plan has been successfully executed. Tracking of the risk is no longer required and the issue is archived by the risk-tracking tool.	
		Monitor	The risk is being watched in anticipation of certain events or activities that might trigger the need to execute risk mitigation, or retire/closing of the risk.	
		Realized	This represents a risk that has been realized and has become an issue that is being tracked in the issues tracking database.	
Critical Path	This specifies that the risk involve an activity that is on the project's critical path.	Check Box (check/uncheck)		
Impact Time Frame	The period when the risk is expected to have impact.	<u>Date</u>		<u>Definition</u>
		Beginning Impact Date	Earliest assessed date the risk may begin to have impact.	
		Ending Impact Date	Latest assessed date the risk may have impact.	
Probability of Occurrence	Indicates the probability of the risk occurring.	<u>Probability</u>		<u>Definition</u>
		Very High	81-99%	Data or judgment indicates very high likelihood of occurrence.
		High	61-80%	Data or judgment indicates high likelihood of occurrence.
		Medium	41-60%	Data or judgment indicates moderate likelihood of occurrence.
		Low	21-40%	Data or judgment indicates small likelihood of occurrence.
		Very Low	1-20%	Data or judgment indicates very small likelihood of occurrence.



Ohio Administrative Knowledge System

OAKS —————> Transforming the Way Ohio Does Business

FIELD NAME	DEFINITION	LIST OF VALUES		
Impact (specified for Cost, Schedule, Technical, and Other)	Indicates the estimate of the impact, should the risk occur.	<u>Impact</u>		
		Severity Level	Level	Definition
		Very High	5	Cost – Increased cost > 10% and/or Schedule – > 25% increase in overall schedule, cannot achieve goal.
		High	4	Cost – Increased cost between 7-10% and/or Schedule – Major increase in overall schedule, critical path affected.
		Medium	3	Cost – Increased cost between 5-7% and/or Schedule – Increase in team schedule affects ability to meet major milestones
		Low	2	Cost – Low cost impact, < 5% and/or Schedule – Additional resources required, but overall schedule not affected.
		Very Low	1	Cost – No/Minimal cost impact and/or Schedule – No/Minimal schedule impact
Program Areas	Indicates the OAKS Project Release in which the risk would have the earliest impact.	Releases		Definition
		Program Wide		Risks that would affect all OAKS releases
		Change Management		Risks that affect Change Management
		Financials 1		Risks that affect Financials 1
		Financials 2a		Risks that affect Financials 2a
		Financials 2b		Risks that affect Financials 2b
		HCM 1		Risks that affect HCM 1
		HCM 2		Risks that affect HCM 2
Technology		Risks that affect the planned technological infrastructure of OAKS		



Ohio Administrative Knowledge System

OAKS —————> Transforming the Way Ohio Does Business

FIELD NAME	DEFINITION	LIST OF VALUES	
Affected Phase	This specifies the software lifecycle phase the risk might affect	Valid values for include: <ul style="list-style-type: none"> • Requirements Analysis • Functional Design • Technical Design • Build/Configure • Testing • Deployment • Sustainment 	
Responsible Person	This specifies the risk owner	The name of the Risk Owner	
Risk Area	This specifies the programmatic areas affected by the risk	Valid values include: <ul style="list-style-type: none"> • Data • Deployment • Integration • Management • Methodology • Performance • Requirements • Resources • Security • Testing 	
Control	This specifies is this risk is internal or external (on the assumption that OAKS leadership has no control over external risks)	Valid values include <ul style="list-style-type: none"> • External • Internal • Internal/External 	
Risk Mitigation Description	This describes the plan to mitigate the risk.	Risk mitigation text.	
Risk Mitigation Step	There are no limits to the number of steps for a mitigation plan. Each step has the following fields:	Step Number	Mitigation step number
		Risk Description	Mitigation step description
		Person	Person responsible for executing the mitigation step
		Due Date	Due date for mitigation step
		Complete	Check box indicating step is complete
Contingency Plan	This specifies what to do in case the risk is realized	Contingency plan description.	



FIELD NAME	DEFINITION	LIST OF VALUES	
History Event Log	This is a history log used to track all updates made to the risk from risk identification to closure	Date	Date the update to the risk was made
		Person	The person who made the update to the risk. This field should be limited to only the risk administrators who have sole read/write access to the risk database
		Event	A description of the updates made to the risk record

3.1.5 Process Steps

This section describes each step in the risk management process as depicted in Figure 2.

3.1.5.1 Identify and Submit Risk

The Risk Originator identifies and submits a new risk using the Risk Entry form, which can be obtained from BI Designer. Note: Every risk identified is automatically identified as a "New" risk. The risk remains in its "New" status until the RM Working Group or a Project Team Lead evaluates and modifies the risk. Once the risk has been approved as a valid risk, its status is changed from "New" to "Assigned."

3.1.5.2 Risk Assessment

The Risk Originator is responsible for the initial risk assessment. The Project Team Lead or RM Working Group will work with the Risk Originator, as necessary, to assist in the completion of the risk entry form. After the risk is entered into Risk Radar, the appropriate party will evaluate the assessment of the initial values entered and will make necessary adjustments to the assessment. The risk assessment activity includes filling in the following data elements, and using the values listed in Table 1 as appropriate:

- Title
- Description
- Probability
- Impact
- Status (defaults to New)
- Earliest Impact Date
- Latest Impact Date
- Source Person
- Point of Contact
- Program Areas
- Affected Phase
- Risk Category



- Control
- Risk Source

In assessing the risk, the Risk Originator first assesses the Probability of Occurrence using Figure 5 as a reference. The Risk Originator assesses the Severity of Impact in each of the three impact areas noted in Table 1.

Once the Risk Originator determines the initial Probability of Occurrence and the Severity of Impact, the Risk tool will calculate the overall Risk Exposure Level. Then the Risk Exposure Level will fall into one of the following three Risk Rating categories:

- **Green** for Low/Very Low level risks
- **Yellow** for Medium level risks
- **Red** for Very High/High level risks

The Risk Rating is determined as depicted in the following two tables:

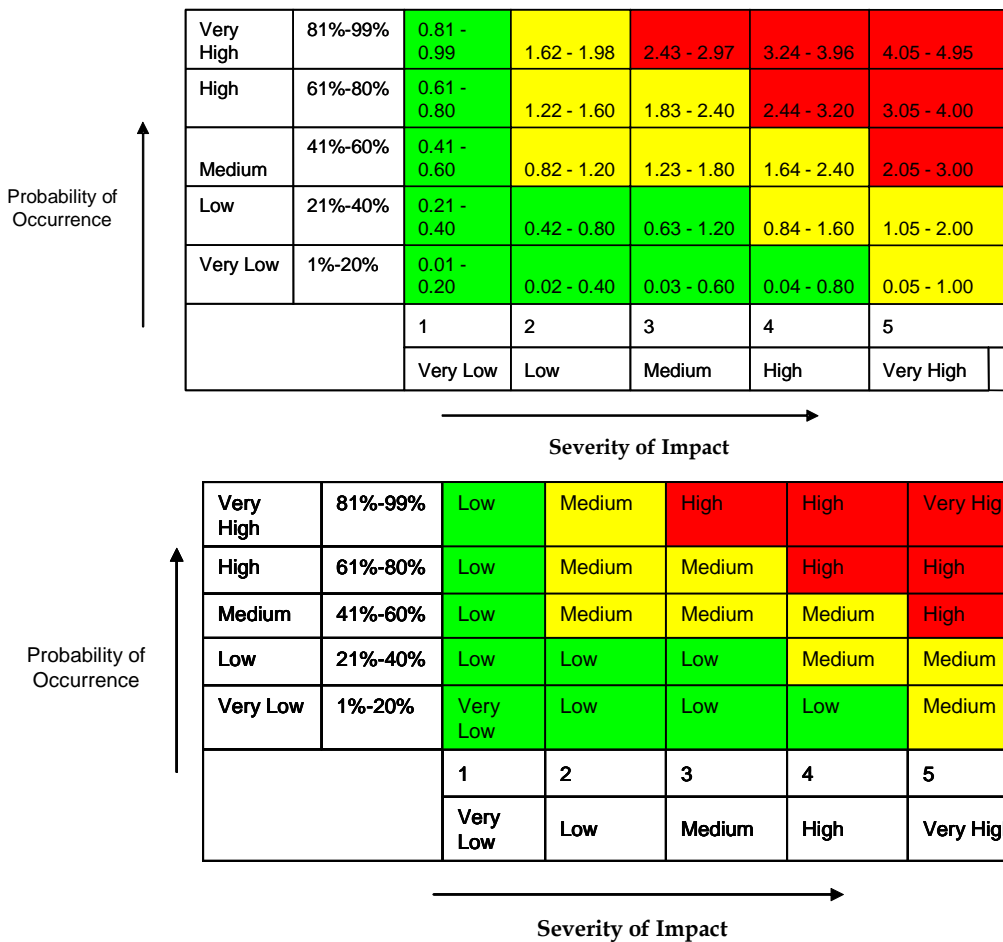


Figure 5 - Risk Rating



For example, a risk has been identified and assessed with a Probability of Occurrence of "medium" and a Severity of Impact of "high." The overall Risk Severity Level is "medium." Using this same example to show how the Risk Exposure Level is calculated, Risk Exposure uses Probability of Occurrence and Severity of Impact to compute the overall impact of the risk. The Risk Exposure Level also is used to rank risks in the risk management tool. For example, the Probability of Occurrence is 60% and the Severity of Impact is Level 4. The following formula is applied:

$$\text{Risk Exposure Level} = \text{Prob. Of Occurrence} * \text{Severity of Impact}$$

The Probability of Occurrence "60%" and the Severity of Impact "4" are multiplied making the overall Risk Exposure Level of "2.4" ($4 * 0.60 = 2.4$). Figure 5 shows that a risk with a Risk Exposure level of 2.4 falls approximately in the Yellow Risk Rating category.

Note that the conversion from Risk Exposure Level to Risk Rating is not an exact process; some cells in Figure 5 have the same value but are given a different Assessment (different color). For instance, using Figure 5, the risk exposure value of 2.4 can be located in the "Yellow/Medium Risk Rating" and the "Red/High Risk Rating"; it depends on the value of the Probability of Occurrence.

Risk Ratings are used to determine what actions must be executed. Generally, three actions will be taken, as determined by each risk's Risk Rating:

- If the Risk Rating is **Green** (Very Low/Low level risks), the risk should be monitored and maintained in the risk watch list; for Green Risks, mitigation plans are not required;
- If the Risk Rating is **Yellow** (Medium level risks), the risk requires a Risk Mitigation Plan with implications that the mitigation actions will be able to complete the tasks within current costs and schedule constraints. It should be documented how each mitigation step will affect the risks probability and impact (a successful mitigation should reduce risk exposure).
- If the Risk Rating is **Red** (High/Very High level risks), the risk requires a Risk Mitigation Plan (Document how each mitigation step will affect the risk's probability and impact [a successful mitigation should reduce risk exposure]) and also a Contingency Plan because there is a higher probability that the mitigation actions will not be sufficient enough to maintain cost and schedule constraints, and therefore a Contingency Plan is required.

Milestones

Risk Milestones are the trigger points or "drop dead" dates when a Contingency Plan execution is triggered unless the risk has been successfully mitigated. The trigger points must be incorporated in the WBS so they can be tracked. All of the risks containing a Risk Rating of Red potentially have risk milestones. The client and the RM Working Group will work together to determine which risks in the Red Risk Rating category will have risk milestones.



Once the Risk Originator identifies and assesses the risk, the Project Team Lead or RM Working Group evaluates the risk to ensure it fits the RMP definition of a risk. If the risk does not meet the risk definition or duplicates another risk, the RM Working Group deletes it and notifies the Risk Originator. If the risk is judged valid, but the analysis is incomplete, the Project Team Lead or RM Working group will work with the Risk Originator and others to complete the analysis and recommendations. Should the Project Team Lead or RM Working Group have any questions or need further clarification, they will contact the Risk Originator to obtain the necessary information.

3.1.5.3 Evaluate Risk

The Project Team Lead or RM Working Group recommends a Risk Owner and, as appropriate, works with that person to set a risk mitigation plan due date, contingency plan due date, and a risk milestone date. Upon approval, the Project Team Lead or RM Working Group changes the risk status to the appropriate open status and notifies the Risk Owner of actions required. The Risk Owner will then validate the risk analysis and develop any required Mitigation and Contingency plans.

Should the assigned Risk Owner disagree with the ownership assignment or the Project Team Lead or RM Working Group risk analysis, the Risk Owner will inform the appropriate parties and provide justification for this conclusion and recommended changes to the risk analysis and ownership assignment as appropriate. Should the Risk Owner have any questions or need further clarification, the Risk Owner will work with the Risk Originator and the Project Team Lead or RM Working Group to obtain needed information. The Risk Owner will update the risk information by sending an e-mail to a Risk Administrator with the necessary updates. If the Risk Owner needs help developing a Risk Mitigation or Contingency Plan, the Risk Owner can use the "Risk Owner Guide" for reference which can also be obtained through the Risk section of the BI Designer Website, the Risk Administrators, and/or a RM Working Group POC; or he or she can contact the Risk Administrators and/or a RM Working Group POC for further assistance. After updates have been made, the Risk Entry Form should be e-mailed to a Risk Administrator.

Risk Response and Control

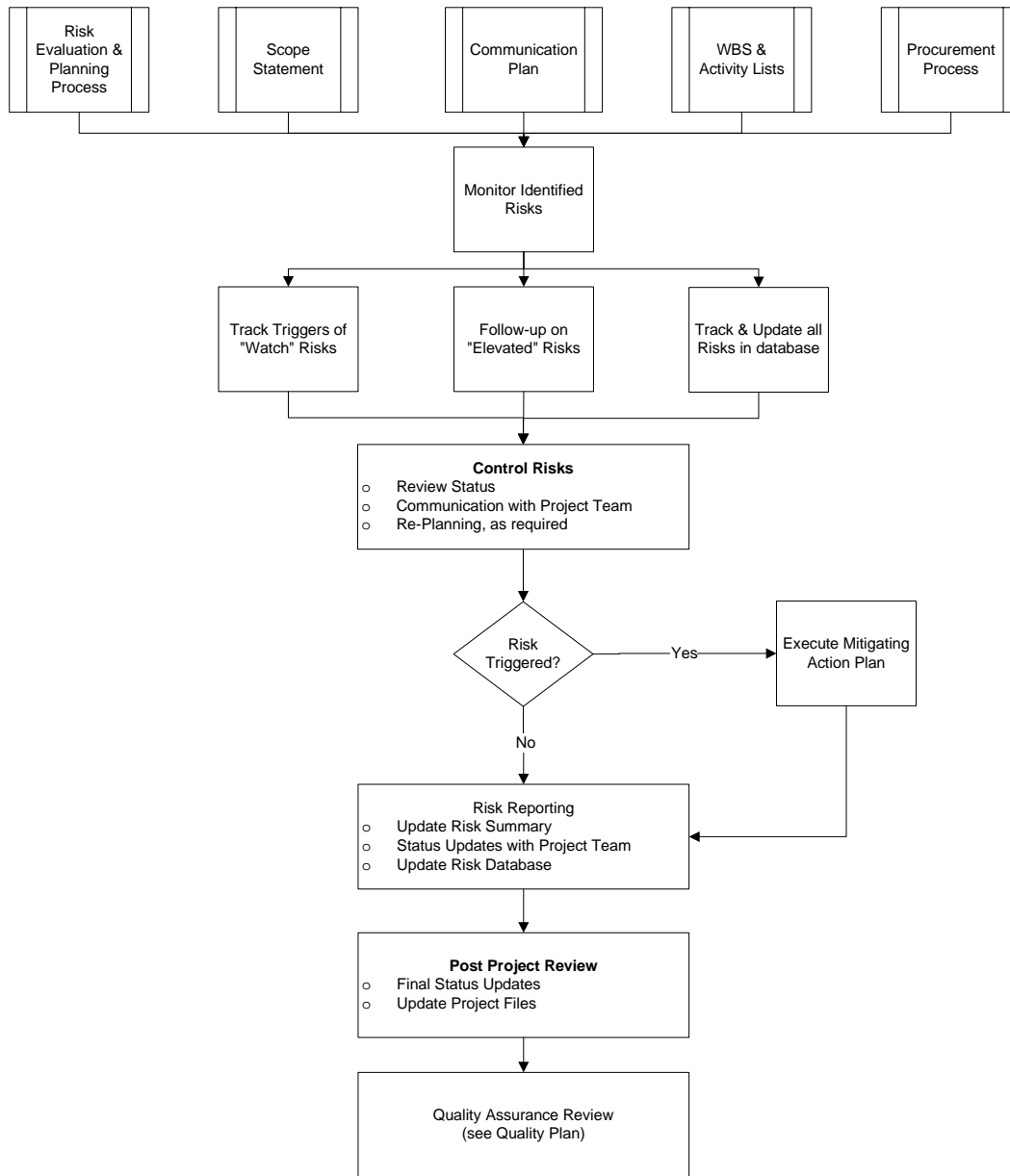


Figure 6 - Risk Response and Control

Figure 6 depicts the typical flow of activities for risk response and control. The initial steps in the Risk Analysis Process consider the analysis of detailed risk responses to those risks which:

- May occur soonest in the development lifecycle, irrespective of probability
- Are high impact, high level of probability

This is intended to cover any short-term exposure first, before considering overall project risk reduction. Overall, project risk response analysis covers five characteristic responses:



Avoidance

Avoidance-based responses are employed at any point in the development lifecycle where future-planning work is performed. Typically, most risk avoidance occurs during the project definition and planning phases of a project, where objectives, scope, key success factors, work breakdown, and project outputs or deliverables are defined. An example of risk avoidance is the use of a stable, established technical solution in preference to an untried, or complex new technology. However, risk avoidance solutions may limit the ability to achieve high-level project objectives, by unnecessarily constraining a desirable solution.

Transfer

Transfer-based responses target the party who are best placed to analyze and implement the response to the risk, based on their expertise, experience, and suitability. Typical transfer responses include the sub-contracting to external suppliers who are able to reduce the overall risk exposure.

Control

Control-based responses occur at all points throughout the development lifecycle, and are typically the most common response. They identify an action or product that becomes part of the development effort, and which are monitored and reported as part of the regular performance analysis and progress reporting of the project.

Acceptance/Assumption of Risk

These describe the factors that may directly affect the success of the project, but are outside of the sphere of influence of the Project Management, and can therefore only be 'accepted'. In addition, acceptance of risks as a response may be based on the cost-ineffectiveness of any available response or solution. An example: acceptance response could be created from a legislative or legal risk, over which no control could be leveraged.

Investigation/Research

Investigation-based responses do not define any mitigation for reducing an individual risk. They are responses to risks where no clear solution is identified, and further research is required. However, investigative responses will not be ignored, as they immediately and directly lead to a greater aggregated project risk. This is because the probability quantifier for each risk includes the effect of the applied response, for which there is none, and the level of control quantifier indicates the level of influence to apply that response, which is low.

3.1.5.4 Develop Mitigating Actions

Once the Risk Owner has agreed to ownership and the Risk Mitigation Plan has been approved, the Risk Owner is responsible for timely risk mitigation. The Risk Mitigation Plan will provide the action items (with due dates) needed to mitigate the risk successfully. The Risk Owner will involve all parties affected by the risk and will provide mitigation progress reports on a regular basis.



Developing and Documenting a Risk Mitigation or Contingency Plan

A successful mitigation plan includes all the necessary steps (in sequential order) needed to reduce the risks exposure. The sequential plan contains those steps that when completed in the order given will successfully mitigate or eliminate the risk. Each step requires a corresponding decrease in probability and/or impact. When the Risk Owner completes this plan, he or she should e-mail it to the Risk Administrator who can include it in the appropriate reports to be approved by the appropriate party (in most cases, the Project Team Lead at the regular Release meetings).

- At a minimum, every Risk Mitigation or Contingency Plan contains steps that will successfully mitigate the risk to a lower severity level by the risk's targeted due date. When completed, these steps should be sent to the Risk Administrator to ensure the database is updated.

Should the Risk Owner need help in formulating the Risk Mitigation or Contingency Plan, the Risk Owner should read the "Risk Owner Guide," on the risk section of BI Designer website (OAKS\Cabinets\Project Management\Risk Management\Risk Job Aids).

Obtain Approval For a Risk Mitigation or Contingency Plan

Risk mitigation plans are required for risks with Yellow or Red Risk Ratings. However, risk mitigation and contingency plans may be developed for Green Risks as desired. The final Risk Mitigation step for the Risk Owner is to obtain approval of the Risk Mitigation Plan. When the Risk Owner documents the Risk Mitigation or Contingency Plan, the Project Team Lead or RM Working Group reviews the plan. Should the Project Team Lead or RM Working Group have any questions or need further clarification, they will contact the Risk Owner. At the next Release Meeting or RM Working Group Meeting, the plan is reviewed and approved or denied. Figure 5 illustrates the decision-making authority for each risk profile. The OAKS EL approves mitigation plans regarding Very High severity level risks. The Project Team Leads or RM Working Group approves mitigation plans involving High and Medium severity level risks.

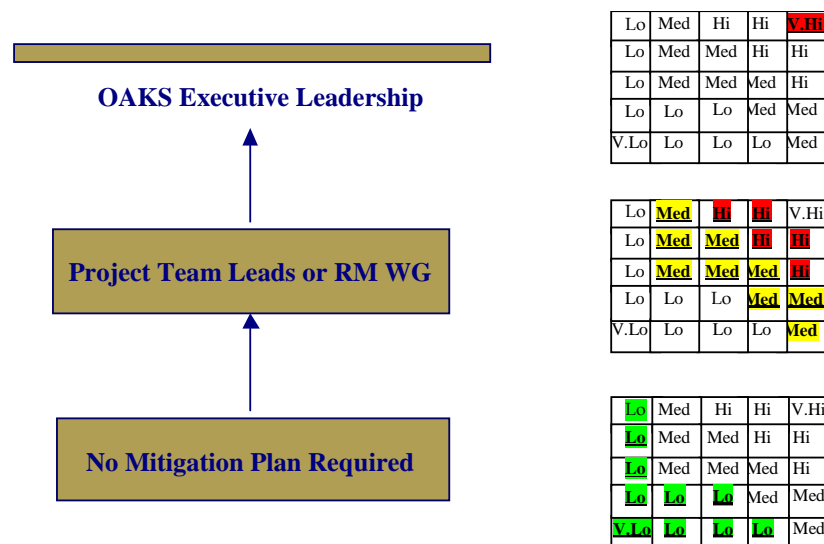


Figure 7 - Risk Mitigation Approval Matrixes



Performing The Risk Mitigation and Contingency Actions

Upon approval of the risk mitigation or contingency plan, the Risk Owner begins the risk mitigation or contingency actions (if the entry criteria have been met). If the Risk Owner cannot execute the risk mitigation or contingency plan, he or she should contact the Project Team Lead immediately and give the reason for not resolving the risk. The Project Team Lead may do the following:

- Work with the Risk Owner to enable execution of the plan
- Notify project manager of the reason the plan cannot be executed
- Recommend re-assignment of the risk to another Risk Owner who is capable of resolving the risk

The Risk Owner provides status updates as they occur to the Project Team Lead and before the RM Working Group Meetings. The updates include:

- Any research of alternatives or background
- Any mitigation or contingency schedule slippage
- Adequate detail to describe the results where mitigation has been achieved or contingency plans have been completed
- When the risk has a recommended mitigation and indicates the risk is Ready-to-Complete for RM Working Group review
- Updated Mitigation Plans
- Recommended changes in status as appropriate

When the Risk Owner has mitigated the risk or completed contingency actions, the Risk Owner informs the Project Team Lead and recommends that the risk either be retired or remain open but be put on a watch list until a date specified in the future.

3.1.5.5 Complete Risk

When all steps in a risk mitigation plan are complete, steps need to be taken to re-evaluate the risk. If the impact date has passed (risk has occurred and been realized), the Project Team Lead must evaluate it and he or she must notify the Risk Radar Administrator if the Risk has in fact been realized, needs to be retired, or both. Provided that the risk is Green or Yellow at the time of realization, the risk can be retired at the Release or Risk Management Working Group meetings without any additional actions. If the risk is a Red Risk and becomes realized, this fact usually will trigger the Contingency Plan.

The criteria for determining if a risk is complete:

- The risk has been completely mitigated
- The risk has occurred and the contingency plan has been successfully executed
- The impact period for the risk has passed and the RM Working Group, with the agreement of the decision authority for the appropriate risk severity level, determines that the risk is no longer valid



If the Project Team Lead or RM Working Group decides the risk mitigation is not satisfactory, the risk remains open and the Risk Owner must re-apply mitigation to the risk. This process includes reviewing the mitigation strategies/techniques and the Risk Mitigation Plan to determine what additional steps must be taken to mitigate the risk to its targeted severity level.

Once a risk is completed but remains open, the risk remains in the "Monitoring" status until a later date at which time the status will be reassessed. This status does not mean the risk is "closed," "not applicable anymore," "unimportant," or "inactive." Rather, it means the risk is still valid and could still affect program cost or schedule.

In the event a mitigated risk has been retired but is later reassessed as a valid risk, any Team Lead or RM Working Group participant can recommend the risk be re-opened at the next meeting. Once the risk is re-opened, it will be treated as all other risks and will require a new mitigation plan depending on color.

3.2 Risk Escalation Procedures

Escalation decisions can be made at the Project Lead level and higher to escalate decisions to the PMO or EL. Risks with Very High severity levels are elevated to the OAKS BOA Group through the Weekly Status Meeting. Additionally, the Project Team Leads and RM Working Group escalate to the EL, through the PMO, those issues determined to need cross-organization involvement, are controversial, or require OAKS EL decisions.

3.3 Risk Management Working Group Meetings (Quarterly or as needed)

The RM Working Group meetings are conducted on a quarterly basis, and are facilitated by the State or Contractor Risk Manager. Meeting schedules may vary with the need for them. The OAKS RM Working Group roles are considered part-time roles. For meeting attendees unable to attend in person, a dial-up telephone number will be available. Regular meeting attendees include:

- OAKS Risk Managers
- Risk Originator, as required
- Risk Owner, as required

During the RM Working Group meeting, the Group will discuss all the new and past due risks. New or modified Mitigation and Contingency plans will be reviewed for concurrence. The risk originators will provide or present (as requested) new risks to the RM Working Group and provide necessary details. The risk owners will provide updates for all other risks, either in person or through the appropriate Risk POC. Any additional action items or updates to their status will be communicated to the action item owner. Upon completion of the meeting, the RM Working Group will generate a Risk Report to be provided to OAKS management with updated metrics and what changes occurred during the meeting.

In addition to the RM Working Group meeting, the Risk Managers will brief the OAKS Program Manager on a regular basis, as determined by the Program Manager.



3.4 Risk Meeting and Reporting Processes (Weekly and Daily)

The Risk Database Administrators generate standard reports as part of the day-to-day risk management process. Risks (and issues) are discussed in the project's team lead weekly meetings. In preparation for these meetings, the Risk Administrators prepare a Risk Watch List (see Table 3) listing the risks for review (i.e., new, past-due, mitigation steps past due). After such meetings, the Project Team Leads notifies the Risk Administrators of the results of the meetings (i.e., status of new risks submitted, new risk assignments, etc.) so that he or she can make the appropriate updates to the risk database. These reports, RM Work Group meeting minutes, and risk listings will be placed in the BI Designer risk folders for accessibility. A summary of standard notices and reports is listed below.

These reports are an initial draft of recommended risk reports. This list is subject to change based on the project team leads, and project managers risk reporting requirements.

REPORT	SENDER	AUDIENCE	TIMING
New Risks	Risk Radar Administrator	All	Once a week by Risk Administrator, and as needed by team members.
Risks Past Due	Risk Radar Administrator	All	Once a week by Risk Administrator, and as needed by team members.
Detailed Reports (or all risks) Sorted by ID	Risk Radar Administrator	All	Once a week by Risk Administrator, and as needed by team members.
Short Term Risks (Risks coming due in the next 30 days)	Risk Radar Administrator	All	Once a week by Risk Administrator, and as needed by team members.
Detailed Report (For all risks) sorted by owner	Risk Radar Administrator	All	Once a week by Risk Administrator, and as needed by team members.
Detailed Report (For all risks) sorted by Rank	Risk Radar Administrator	All	Once a week by Risk Administrator, and as needed by team members.
Risk Mitigation Steps Past Due	Risk Radar Administrator	All	Once a week by Risk Administrator, and as needed by team members.
Mid Term Risks (risks coming due in the next 31 – 90 days)	Risk Radar Administrator	All	Once a week by Risk Administrator, and as needed by team members.

Table 2 - Standard Risk Notices and Reports



3.5 Risk Meeting Report

Within two business days of the meeting, the RM Working Group publishes via email, a Risk Meeting report summarizing all action items taking place at the RM Working Group meeting.

3.6 Risk Mailing List

The OAKS Program Risk Administrators maintains an e-mail distribution list used to mail risk reports to the individuals applicable for each release. The mailing list is located at: *OAKS\Cabinets\Project Management\Risks\Risk Mailing List*.

4 Risk Management Tool

The Risk management tool is Risk Radar Version 2.0.2. Risk Radar is developed and maintained by Integrated Computer Engineering Inc (http://www.iceincusa.com/products_tolls.htm). It is a customized risk management system built using Microsoft Access with proprietary VBA code running in the background. Risk Radar was selected because it is built by project managers for project managers for one purpose only: effective risk management.

Risk Radar comes fully loaded out of the box with pre-configured canned reports and queries. However, since the Risk Radar data model is available to users, we have the ability to customize existing reports, or create new ones. Additionally, the data managed in Risk Radar can be readily exported to other Microsoft applications, such as Excel, or Word, allowing for maximum flexibility regarding how we can use data stored in Risk Radar.

Since the Risk Radar database is a Microsoft Access file, it will be managed under configuration control in BI Designer. Only the OAKS Risk Administrators will have Write access to the Risk Radar Database in BI Designer (this means, only the administrators will be able to check out and update the Risk Radar database). Everyone else will be able to browse the database, or download/export a copy to his or her desktop for local use.

4.1 Risk Section of BI Designer Available to All OAKS Team Members

While the Risk Radar is the primary repository for the Risk data, the risk management folder is available for all risk reports and risk related resources, including a read-only copy of the Risk Radar database. The path to the risk section of BI Designer is *OAKS\Cabinets\Project Management\Risk Management*. This website allows all the team members to submit risks as well as review risk information. The Risk Administrators regularly reviews and updates data on this website, by publishing new reports and posting the latest version of the Risk Radar for read-only access.

4.2 Using The Risk Entry Form to Create New Risks

The risk entry form allows users to enter the risk data into a spreadsheet. They must then email the spreadsheet to a Risk Database Administrator to be entered into the Risk database. The Risk Entry Form can be found on the Risk Management Section of BI Designer. New risks must first be validated before they are active in the system. Please consult with your co-workers or



supervisor before submitting a new risk request. Furthermore, new risks are reviewed in weekly and daily status meetings. Be sure your immediate reporting official is aware of the new risks so that he or she can discuss the risk when it is brought up at the status meeting. Or, if you routinely attend such status meetings, be prepared to discuss your rationale for creating the new risk.

4.3 Viewing Risks

Risks can be viewed on the Risk section of the BI Designer website, by downloading the appropriate risk report. Only the Risk Administrators will have Read/Write access to risk information. Everyone else will have read-only access, and can create their own reports by running queries using the Risk Radar Database.

4.4 Updating Risks

In order to update risk information, risk owners should simply e-mail a risk administrator with the required update information, since only Risk Administrators can update the Risk Radar database.

5 OAKS Risk Management Metrics

Reference the OAKS Program Project Measurement Plan in BI Designer for risk measurement information: *OAKS\Cabinets\Project Management\QualityMetrics\Project Measurement Plan*.

6 Risk Identification Questionnaire

The following list of questions can be used to help identify project risks.

Risk Area of Concern		Risk Questions	Y/N
PROJECT MANAGEMENT	MANAGEMENT APPROACH	Is the project managed according to the plan?	
		Do people routinely get pulled away to fight fires?	
		Is re-planning (change control) done when disruptions occur?	
		Are people at all levels included in planning their own work?	
		Are there contingency plans for known risks?	
		Is there a mechanism in place to determine when to activate the contingencies?	
		Are long-term issues being adequately addressed?	
		Are project members at all levels aware of their status versus plan?	
		Do people feel it is important to keep to the plan?	
		Does management feel it's important to keep to the plan?	
		Does management consult with people before making decisions that affect their work?	
		Is the quality assurance function adequately staffed on this project?	
		Do you have defined mechanisms for assuring quality?	



Ohio Administrative Knowledge System

OAKS —————> Transforming the Way Ohio Does Business

		Do all areas and phases have quality procedures?	
		Are people used to working with quality procedures?	
		Do you have an adequate configuration management system?	
		Is the configuration management function adequately staffed?	
		Is coordination required with an installed system?	
		Does the configuration management system synchronize your work with site changes?	
	ROLES/SKILLS	Is the project organization effective?	
		Do we have adequate support from Executive Sponsors and Executive Advisory Committee?	
		Do we have adequate support from the Governor's Office?	
		Do people understand their own and others' roles in the project?	
		Do people know who has authority for what?	
		Does the project have experienced managers or leads?	
		Do people get trained in the skills required for this project?	
		Is this part of the project plan?	
		Do people get assigned to the project who do not match the experience profile for your work area?	
		Is it easy for project members at all levels to get management action?	
		Are there any areas in which the required technical skills are lacking (e.g., software engineering and requirements analysis methods, programming languages, integration and test methods, reliability, maintainability, availability, human factors, configuration management)?	
		RESOURCES	Do you have adequate personnel to staff the project?
	Is the staffing stable?		
	Do you have access to the right people when you need them?		
	Does the staff have previous project experience?		
	Have the project members implemented systems of this type?		
	Is the program reliant on a few key people?		
	Is there a problem with getting people cleared (security)?		
	Is there any problem keeping the people you need?		
		Is the team geographically dispersed?	
PROJECT MANAGEMENT	SCHEDULE	Will resources be unavailable during certain times (tax season, Christmas & other holidays and end of fiscal year, etc.)?	
		Could work delays / stoppage occur due to program's impact to union workforce (i.e., changing of job duties)?	
		Are the development facilities adequate?	
		Has the schedule been stable?	
		Is the schedule realistic?	
		Is the estimation method based on historical data?	
		Has the method worked well in the past?	
		Is there anything for which adequate schedule was not planned (e.g., analysis and studies, quality assurance, training, maintenance courses and training, equipment, deliverable development system)?	
		Are there external dependencies which are likely to impact the schedule?	
	CO ST		Is the budget stable?



Ohio Administrative Knowledge System

OAKS —————> Transforming the Way Ohio Does Business

		Is the budget based on a realistic estimate?	
		Is the estimation method based on historical data?	
		Has the method worked well in the past?	
		Have features or functions been deleted as part of a design-to-cost effort?	
		Is there anything for which adequate budget was not allocated (e.g., analysis and studies, quality assurance, training, maintenance courses and training, equipment, deliverable development system)?	
		Do budget changes accompany requirement changes?	
		Is this a standard part of the change control process?	
	COMMUNICATION	Does management communicate problems up and down the line?	
		Are conflicts / issues documented and resolved in a timely manner?	
		Does management involve appropriate project members in meetings (e.g. Technical Leaders, Developers, Analysts)?	
		Does management work to ensure that all factions are represented in decisions regarding functionality and operation?	
		Are there periodic structured status reports?	
		Do people get a response to their status reports?	
		Does appropriate information get reported to the right organizational levels?	
		Do you track progress versus plan?	
		Does project management communicate problems to senior management?	
		Does management present a realistic picture to senior management?	
		Does management have a clear picture of what is going on?	
ENGAGEMENT MANAGEMENT	CONTRACT	Does the type of contract you have (e.g., time & materials, cost plus award, fixed priced, etc.) present any problems?	
		Is the contract burdensome in any aspect of the project (e.g., statement of work, specifications, contract sections, excessive client oversight)?	
		Is the required documentation burdensome (e.g., excessive amount, long approval cycle)?	
		Are there any problems with data rights (e.g., packages, developmental software, non-developmental items)?	
		Are there external dependencies on external products or services that may affect the product, budget or schedule (e.g., associate consulting firms, prime contractor, subcontractor, vendors or suppliers, client furnished resources)?	
ENGAGEMENT MANAGEMENT	CULTURE	Are all staff levels oriented toward quality procedures (process improvement)?	
		Does schedule get in the way of quality?	
		Do people work cooperatively across functional boundaries?	
		Do people work effectively toward common goals?	
		Is management intervention sometimes required to get people working together?	
		Is there good communication among the members of the program (e.g., managers, Tech Leads, Developers, Testers, Configuration management, quality assurance)?	



Ohio Administrative Knowledge System

OAKS —————> Transforming the Way Ohio Does Business

		Are the managers receptive to communication from project staff?	
		Do you feel free to ask your managers for help?	
		Does management tend to micro-manage?	
		Are members of the program able to raise risks without having a solution in hand?	
		Do the project members get timely notification of events that may affect their work?	
		Is notification informal?	
		Is morale on the project good?	
		Are you aware of the main contributors to low morale?	
	POLITICS	Are politics affecting the project (e.g., agency, subcontractors, prime contractors, vendors)?	
		Are politics affecting the State's support of the project?	
		Are politics affecting technical decisions?	
		Are politics affecting project communications?	
		Is adequate support available for the project?	
		Are politics affecting issue escalation?	
		Are politics affecting business decisions?	
		Is it good politics to present an optimistic picture to the State or senior management?	
	STATE	Is the State approval cycle timely (e.g., documentation, change proposals, project reviews, formal reviews)?	
		Do you ever proceed before receiving State approval?	
		Is this project dependent upon completion of other State projects?	
		Is the State fractured in their support of the project?	
		Does the State understand software?	
		Does the State interfere with process or people?	
		Does management work with the State to reach mutually agreeable decisions in a timely manner (e.g., requirements understanding, test criteria, schedule adjustments, interfaces)?	
		Are your mechanisms for reaching agreement with the State (e.g., working groups, technical interchange meetings, etc.) effective?	
		Are all State factions involved in reaching agreements?	
		Is it a formally defined process?	
		Is there any problem with getting schedules or interface data from user agencies?	
	Are they accurate?		
INTERFACES	USE SUBS	Are there any ambiguities in subcontractor task definitions?	
		Is the subcontractor status reporting and monitoring procedure consistent with the rest of the project team?	
		Is the subcontractor administration and technical management done by a separate organization?	
		Are you highly dependent on subcontractor expertise in any areas?	
		Is subcontractor knowledge being transferred to the State?	
		Is there any problem with getting schedules or interface data from subcontractors?	



Ohio Administrative Knowledge System

OAKS —————> Transforming the Way Ohio Does Business

	ARE A SUB	Are your task definitions from the Prime ambiguous?		
		Do you interface with two separate prime organizations for administration and technical management?		
		Are you highly dependent on the Prime for expertise in any areas?		
		Is there a problem with getting schedules or interface data from the Prime?		
	VENDORS	Are you relying on vendors for deliveries of critical components (e.g., compilers, hardware, packages)?		
		Are vendors used in a critical path task?		
		Is the performance of the vendors currently poor?		
		Are multiple vendors supporting the project?		
		Are multiple vendors used on the project?		
		Is the contract clear on that point?		
	REQUIREMENTS	SCOPE	Are relevant vendor contracts in place for the duration of the project?	
			Do you have solutions for all of the requirements?	
			Are the requirements stable?	
			Is there an effect on the system or project (e.g., quality, functionality, schedule, integration, design, testing)?	
			Are the external (human and system) interfaces changing?	
Are the interfaces defined, documented, and baselined?				
Are there any "To Be Determined"s in the specifications / scope statement?				
Are there requirements (scope / deliverables) you know should be in the specifications (scope statement) but aren't?				
Will you be able to get these requirements (scope / deliverables) into the project?				
Does the State have unwritten requirements / expectations?				
Is there a way to capture these requirements / expectations?				
Are the external (human and system) interfaces completely defined?				
Are you able to understand the requirements (scope / deliverables) as written?				
Are the ambiguities being resolved satisfactorily?				
Are there problems with interpretation?				
Are there any requirements that may not specify what the State really wants?				
Is this being resolved satisfactorily?				
Do you and the State understand the same thing by the requirements (scope / deliverables)?				
Is there a process by which to determine this?				
Are you validating the requirements (e.g., by prototyping, analysis or simulation)?				
Are there any requirements that are technically difficult to implement?				
Were feasibility studies done for the requirements?				
Are you confident in the assumptions made in the studies?				
Are there any state-of-the-art requirements (e.g., technologies, methods, languages, hardware, communications)?				



Ohio Administrative Knowledge System

OAKS —————> Transforming the Way Ohio Does Business

		Are there any technologies, methods, languages, hardware or communications that are new to you?	
		Is there a plan for acquiring knowledge in these areas?	
		Is the project size a concern?	
		Is the project complexity a concern?	
		Does the size require a larger organization than usual for Accenture?	
		Is this a mission critical system?	
DEVELOPMENT METHODOLOGY	DEVELOPMENT PROCESS	Will the implementation be difficult to understand or maintain?	
		Is there more than one development model being used (waterfall, incremental, evolutionary)?	
		Is coordination between them a problem?	
		Are there formal, controlled plans for all development activities (e.g., requirements analysis, design, code, integration & test, installation, quality assurance, configuration management, etc.)?	
		Do the plans specify the process well?	
		Are developers familiar with the plans?	
		Is the development process adequate for this product?	
		Is the development process supported by a compatible set of procedures, methods and tools?	
		Does everyone follow the development process?	
		Can you measure whether the development process is meeting productivity and quality goals?	
		Is there adequate coordination among distributed development sites?	
		Is there a parallel cutover period with the existing system?	
		Are people comfortable with the development process?	
		CHANGE CONTROL	Is there a requirements traceability mechanism that tracks requirements from the source specification through test cases?
	Is the traceability mechanism used in evaluating requirement (scope) change impact analyses?		
	Is there a formal change control process?		
	Does it cover all changes to baselined requirements, design, code, and documentation?		
	Are changes at any level mapped up to the system level and down through the test level?		
	Is there adequate analysis when new requirements are added to the system?		
	Are the external interfaces changing without adequate notification, coordination, or formal change procedures?		
	Do you have a way to track interfaces?		
	Is there a change control process for internal interfaces?		
	Is a formal change control process currently used?		
DEVELOPMENT ENVIRONMENT	Are there enough workstations and processing capacity for all staff?		
	Is there sufficient capacity for overlapping phases, such as coding, integration and test?		



Ohio Administrative Knowledge System

OAKS —————> Transforming the Way Ohio Does Business

		Does the development system support all aspects of the project (e.g., requirements analysis, performance analysis, design, coding, test, documentation, configuration management, management tracking, requirements traceability)?	
		Do people find the development system easy to use?	
		Is there good documentation of the development system?	
		Have people used these tools and methods before?	
		Is the system considered reliable (e.g., compiler, development tools, hardware)?	
		Are the people trained in the use of the development tools?	
		Do you have access to experts in use of the system?	
		Do the vendors respond to problems rapidly?	
		Are you delivering the development system to the State?	
		Have adequate budget, schedule, and resources been allocated for this deliverable?	
		Is the development computer the same as the target computer?	
		Are there compiler differences between the development and target computer?	
DEVELOPMENT METHODOLOGY	DESIGN	Are there any specified algorithms that may not satisfy the requirements?	
		Will development of database be difficult to match physical design?	
		Are any of the algorithms or designs marginal with respect to meeting requirements?	
		Do you determine the feasibility of algorithms and designs (e.g., using prototyping, modeling, analysis or simulation)?	
		Does any of the design depend on unrealistic assumptions?	
		Does any of the design depend on optimistic assumptions?	
		Are there any requirements or functions that are difficult to design?	
		Will the complexity of functions or databases be a factor?	
		Are the internal interfaces well defined (software-to-software and software to hardware)?	
		Is there a process for defining internal interfaces?	
		Are there any problems with performance (e.g., throughput; scheduling asynchronous real-time events; real-time response; recovery timelines; response time; database response, contention or access)?	
		Has a performance analysis been done?	
		Do you have a high level of confidence in the analysis?	
		Do you have a model to track performance through design and implementation?	
		Does the architecture, design or code create any maintenance difficulties?	
		Are the maintenance people involved early in the design?	
		Is the product documentation adequate for maintenance by an outside organization?	
		Are reliability requirements allocated to the software?	
Are availability requirements allocated to the software?			
Are recovery timelines any problems?			



Ohio Administrative Knowledge System

OAKS —————> Transforming the Way Ohio Does Business

		Are the design specifications adequate to implement the system (e.g., internal interfaces)?		
		Does the hardware limit your ability to meet any requirements (e.g., architecture, memory capacity, throughput, real-time response, response time, recovery timelines, database performance, functionality, reliability, availability)?		
		Are there any parts of the product implementation not completely defined by the design specification?		
		Are the selected algorithms and designs easy to implement?		
		Does the design include features to aid testing?		
	CODING	Have coding standards been documented and communicated?		
		Has the State / end-user signed off on the coding specifications?		
		Are the design specifications in sufficient detail to write the code?		
		Is the design changing while coding is being done?		
		Are there system constraints that makes the code difficult to write (timing, memory, external storage)?		
		Is the language suitable for producing software on this project?		
		Are there multiple languages used on the project?		
	DEVELOPMENT METHODOLOGY	PACKAGES & REUSE	Is there interface compatibility between the code produced by the different compilers?	
			Are there problems with software used in the project but not developed on the project?	
			Are you reusing or re-engineering software not developed on the project?	
Do you foresee any problems (e.g., documentation, performance, functionality, timely delivery, customization)?				
Are there any problems with using packages such as:				
insufficient documentation to determine interfaces, size or performance				
poor performance				
requires a large share of memory or database storage				
difficult to interface with application software				
not thoroughly tested				
not bug free				
not maintained adequately				
slow vendor response				
Do you foresee any problem with integrating packaged software updates or revisions?				
For testing, will vendor data be accepted in verification of requirements allocated to the packaged products?				
Has sufficient system integration been specified for integration testing of packaged products?				
Has adequate time been allocated for system integration and test?				
Are all contractors part of the integration test team?				
Will the product be integrated into an existing system?				
Have you made plans to guarantee that the package will work correctly when integrated?				



Ohio Administrative Knowledge System

OAKS —————> Transforming the Way Ohio Does Business

		Will system integration occur on State site?		
TESTING		Do the testers get involved in analyzing requirements?		
		Do you begin unit testing before you verify code with respect to the design?		
		Has sufficient unit testing been specified?		
		Is there sufficient time to perform all the unit testing you think should be done?		
		Will compromises be made regarding unit testing if there are schedule problems?		
		Will there be sufficient hardware to do adequate integration and testing?		
		Is there any problem with developing realistic scenarios and test data to demonstrate any requirements (e.g., specified data traffic, real-time response, asynchronous event handling, multi-user interaction)?		
		Is there UAT performed by the end-user without input from IT?		
		Are you able to verify performance in your facility?		
		Does hardware and software instrumentation facilitate testing (e.g., line sniffers, etc.)?		
		Is it sufficient for all testing?		
		Will the target hardware be available for testing when needed?		
		Have acceptance criteria been agreed to for all requirements?		
		Is there a formal agreement?		
		Are there any requirements that will be difficult to test?		
DEVELOPMENT METHODOLOGY		Has sufficient product integration been specified?		
		Has adequate time been allocated for product integration and test?		
	PROTOTYPES		If prototyping, is it a throw-away prototype?	
			Are you doing evolutionary development?	
			Are you experienced in this type of development?	
			Are interim versions deliverable?	
			Does this complicate change control?	
			Are the software requirements specifications adequate to design the system?	
			Are the hardware specifications adequate to design and implement the system?	
			Are the external interface requirements specified?	
			Are the test specifications adequate to fully test the system?	
			Is the integration environment adequate?	
			Is the software going to be easy to test?	