



## Risk Management Plan

# E-Learning Management System Project IT073001

Version: 1.0      Revision Date: August 30, 2007

Approval of the Project Risk Management Plan indicates an understanding of the purpose and contents described in this document. By signing this document, each individual agrees with the contents of this document.

Approver Name	Title	Signature	Date
Usha Venkat	Client Services Manager	- Signed -	8/30/2007
William Mosher	Project Management Professional	- Signed -	8/30/2007

## Table of Contents

Section 1. Risk Management Approach.....	3
1.1 Overall Strategy .....	3
1.2 Roles Definition .....	3
Section 2. Risk Assessment .....	5
2.1 Risk Identification.....	5
2.1.1 Methods and Techniques .....	5
2.1.2 Project Risks .....	5
2.2 Risk Analysis .....	6
2.2.1 Methods and Techniques .....	6
2.2.2 Risk Analysis and Prioritization .....	6
2.3 Risk Response Actions .....	7
Section 3. Risk Monitoring and Control.....	11
3.1 Risk Tracking.....	11
3.2 Risk Reporting .....	11
3.3 Risk Status .....	11
Section 4. Glossary .....	12
Section 5. Revision History .....	13

## Section 1. Risk Management Approach

### 1.1 Overall Strategy

The overall strategy of risk management for the E-Learning Project shall be based on the principles of Risk Identification, Risk Analysis, Risk Response, and Risk Monitoring & Control. These four events will be accomplished iteratively at intervals throughout the life of the project. Brainstorming will be the primary method used to identify risks from project team members. This document is a living growing vehicle of project risk data. As risks are identified the tables in this document will increase to accept the additional information.

### 1.2 Roles Definition

The risk management activity matrix below displays the Risk Management Activity and each functional area. For these two main conditions, a status is depicted for the three following conditions; Joint/Shared responsibility, Primary/Lead responsibility, and Support/participating responsibility.

Risk Management Activity	Functional Manager	Project Management Professional	Project Administration Team Member	Project Technical Team Member
Develop and administer Risk Management Plan	P	J	-	-
Determine if Risk Management Plan is ready for approval	P	J	-	-
Identify Project risks	P	J	S	S
Approve and authorize use of Contingency Plans	P	J	-	-
Legend: J = Joint/Shared responsibility P = Primary/Lead responsibility S = Support/participate responsibility				

This Space Intentionally Left Blank

Risk Management Activity	Project Communication Strategy and Delivery Team Member	Project Teaching and Learning Team Member	Project Training and Support Team Member	Project Support Central Team Member
Develop and administer Risk Management Plan	-	-	-	-
Determine if Risk Management Plan is ready for approval	-	-	-	-
Identify Project risks	S	S	S	S
Approve and authorize use of Contingency Plans	-	-	-	-
<b>Legend:</b> J = Joint/Shared responsibility P = Primary/Lead responsibility S = Support/participate responsibility				

Risk Management Activity	Project Tracking and Reporting Team Member	-	-	-
Develop and administer Risk Management Plan	-	-	-	-
Determine if Risk Management Plan is ready for approval	-	-	-	-
Identify Project risks	S	S	S	S
Approve and authorize use of Contingency Plans	-	-	-	-
<b>Legend:</b> J = Joint/Shared responsibility P = Primary/Lead responsibility S = Support/participate responsibility				

## Section 2. Risk Assessment

### 2.1 Risk Identification

#### 2.1.1 Methods and Techniques

Risks are identified via many methods. First, Brainstorming will be the primary method. Project stakeholders with experience provide inputs based on lessons learned during past work assignments. Periodic reviews will be undertaken and risk will be identified during them.

Once identified, they will be logged into the table in section 2.1.2 below.

#### 2.1.2 Project Risks

The table below provides a visualization of each risk with its generic name, and description.

Risk	Risk Description
Lack of support personnel is a risk to the project	The current level of support personnel is so low that the dropped call rate is so high that it will have a negative impact on the project. The negative impact of the dropped call rate is a risk to the adoption of the project.
Multiple tasked system administrators is a risk to the project	Current system administrators are working full time on multiple systems. Bringing this new system on board only add more load to people currently assigned full time to other systems.
The technically complex environment is a risk to the project	The load balanced server environment is technical complex. The technical approach has components that are new to ACCD infrastructure. Integration and ongoing operation will require a steep learning curve.
Training of users is a risk to the project	Large numbers of individuals will require training within relatively short periods of time.
The aggressive schedule is a risk to the project	The schedule is directly related to the master schedule (e.g., Fall 07, Spring 08). Installing the system and teaching users must be accomplished in time to satisfy the master schedule. Tasks are closely coupled and a delay in accomplishing one relatively minor task could force delays to the entire

	project
Loss of Personnel is a risk to the project	The losses of knowledgeable personnel could significantly impact the project schedule. Project will require personnel responsible for configuration, installation, and maintenance of key components
Late Delivery is a risk to the project	Late delivery of key components (i.e., SAN) could impact delivery schedule

## 2.2 Risk Analysis

### 2.2.1 Methods and Techniques

Risks analysis will be accomplished using two scales. Both scales shall use a range from 1 to 10.

Value	Rating
2	Very Low
4	Low
6	Moderate
8	High
10	Very High

The first scale will rate the risk probability of happening. The second scale will rate the impact to the project if it does happen. Each risk will have a number from 1 to 10 for the risk event and a number from 1 to 10 for the consequences. These two numbers will be multiplied by each other. The risk will be ranked or prioritized from the highest number (100) to the lowest (1).

Range		Rating
From	To	
1	8	Very Low
9	24	Low
25	48	Moderate
49	80	High
81	100	Very High

### 2.2.2 Risk Analysis and Prioritization

The table below provides a high level view of the analysis and prioritization of each risk. The table provides the risk name, ranking, probability of occurrence, impact or consequence, numerical ranking of the event, numerical ranking of the consequence, and the total numerical ranking for each risk.

Risk Name	Rank	Risk Statement		Probability (P), Impact (I), Severity (P x I)		
		Event	Consequence	P	I	(P x I)
Lack of support personnel	1	Very High	Very High	10	10	100
Multiple Tasked System Administrators	2	Very High	Very High	10	10	100
Technically complex environment	3	High	High	7	7	49
Training of users	4	Moderate	High	6	7	42
Aggressive schedule	5	Moderate	Moderate	6	6	36
Loss of Personnel	6	Low	High	3	7	21
Late Delivery	7	Very Low	High	2	7	14

### 2.3 Risk Response Actions

Below is a list of tables that describe the risk event, risk description, date initiated, assignment, response action, response description and date closed.

Risk Event	Lack of support personnel
Risk Description	The current level of support personnel is so low that the dropped call rate is so high that it will have a negative impact on the project. The negative impact of the dropped call rate is a risk to the adoption of the project.
Date Initiated	July 09, 2007
Assigned To	Usha Venkat
Risk Response Action	Avoidance
Response Description	It has been proposed to outsource support to allow improved support and allow for our support team to jump start their learning curve
Date Closed	To be determined

Risk Event	Multiple tasked system administrators
Risk Description	Current system administrators are working full time on multiple systems. Bringing this new system on board only add more load to people currently assigned full time to other systems.
Date Initiated	July 09, 2007
Assigned To	Usha Venkat
Risk Response Action	Avoidance
Response Description	It is proposed to provide alternate hosting for the initial period of performance to insure 100% operational time. If our system goes down while we are learning how to operate/maintain the system the back-up hosting center will come on-line and support the users while we bring our system back up. It is further proposed to hire additional system administration support to alleviate this risk.
Date Closed	To be determined

Risk Event	Technically complex environment
Risk Description	The load balanced server environment is technical complex. The technical approach has components that are new to ACCD infrastructure. Integration and ongoing operation will require a steep learning curve.
Date Initiated	July 09, 2007
Assigned To	Usha Venkat
Risk Response Action	Avoidance
Response Description	It is proposed to provide an alternate hosting for the initial period of performance to insure 100% operational time. If our system goes down while we are learning how to operate/maintain the system the back-up hosting center will come on-line and support the users while we bring our system back up.
Date Closed	To be determined

Risk Event	Training of users
Risk Description	Large numbers of individuals will require training within relatively short periods of time.
Date Initiated	July 09, 2007
Assigned To	Usha Venkat
Risk Response Action	Mitigate
Response Description	The vendor has been contracted to train our trainers and the initial group of Fall 07 faculty. In addition to this support, we plan on purchasing course ware for web based instruction. From this material we plan on developing tailored course material for all follow-on training. College Instructional Innovation Centers will support training activities.
Date Closed	To be determined

Risk Event	Aggressive schedule
Risk Description	The schedule is directly related to the master schedule (e.g., Fall 07, Spring 08). Installing the system and teaching users must be accomplished in time to satisfy the master schedule. Tasks are closely coupled and a delay in accomplishing one relatively minor task could force delays to the entire project
Date Initiated	July 09, 2007
Assigned To	Usha Venkat
Risk Response Action	Acceptance
Response Description	We are unable to change the master calendar. Proper planning will help prevent negative repercussions related to not meeting the aggressive schedule.
Date Closed	To be determined

Risk Event	Loss of Personnel
Risk Description	The losses of knowledgeable personnel could significantly impact the project schedule. Project will require personnel responsible for configuration, installation, and maintenance of key components
Date Initiated	July 09, 2007
Assigned To	Usha Venkat
Risk Response Action	Mitigate
Response Description	We will mitigate the potential of loss of personnel by having backup team members in case of loss of primary or key personnel. Having backup hosting will assist in personnel retention.
Date Closed	To be determined

Risk Event	Late Delivery
Risk Description	Late delivery of key components (i.e., SAN) could impact delivery schedule
Date Initiated	July 09, 2007
Assigned To	Usha Venkat
Risk Response Action	Mitigate
Response Description	Late delivery of the SAN could cause the project to miss the fall 07 delivery of the system. Close monitoring of purchase and delivery of material will mitigate this condition.
Date Closed	To be determined

Risk Event	
Risk Description	
Date Initiated	
Assigned To	
Risk Response Action	
Response Description	
Date Closed	

Risk Event	
Risk Description	
Date Initiated	
Assigned To	
Risk Response Action	
Response Description	
Date Closed	

Risk Event	
Risk Description	
Date Initiated	
Assigned To	
Risk Response Action	
Response Description	
Date Closed	

## **Section 3. Risk Monitoring and Control**

### ***3.1 Risk Tracking***

The team will meet frequently and discuss status. The functional manager will facilitate these meetings. The team members will report status. During these meetings time will be set aside to discuss individual risk status. The functional manager and team members will have the opportunity to articulate concerns related to risk response actions.

### ***3.2 Risk Reporting***

This document is the primary vehicle to record risk and their mitigation activities. It is a living document that grows with each additional risk identified, analyzed, and mitigated. This document will also be posted on the web within the Secure Wireless Campuses Project area. The project status report will be used to visualize risk activity.

### ***3.3 Risk Status***

Again, the team will have regular status meetings. The functional manager will facilitate these meetings. The team members will report status. During these meetings time will be set aside to discuss individual risk status. The functional manager and team members will have the opportunity to articulate concerns related to risk response actions.

## Section 4. Glossary

The following terms have been used within this document:

<b>Term</b>	<b>Definition</b>
ACCD	Alamo Community College District
SAN	In computing, a storage area network (SAN) is an architecture to attach remote computer storage devices such as disk arrays, tape libraries and optical jukeboxes to servers. In such a way to the operating system, the devices appear as locally attached devices.

## Section 5. Revision History

The following document changes have been identified:

<b>Version</b>	<b>Date</b>	<b>Name</b>	<b>Description</b>
0.1	Nov 14, 2006	W Mosher	Initial Template Release
0.2	Mar 06, 2007	W Mosher	ACCD to Alamo Community Colleges
0.3	Jul 20, 2007	W Mosher	Initial Draft Risk Management Plan
1.0	Aug 30, 2007	W Mosher	Initial Risk Management Plan