Risk/Issue Management Plan

Centralized Revenue Opportunity System

California State
Board of Equalization

November 2014

Version 2.0

This page intentionally left blank

Date Submitted for Review: 10/04/2014			
Formal Review My signature below indicates I have reviewed this document:			
Role	**Reviewer Name**	**Signature**	**Date Reviewed**
Project Director	Eric Steen		11/5/14

Revision Log:

Version Number	Version Date	Revision Author	Summary of Major Changes Made
0.01	2/15/12	Kim Brain	Initial Draft.
0.02	10/6/14	Kim Brain	Revised to CROS standard format and to address issue management process.

Document Review Cycle

This document is reviewed annually and as needed throughout the Project's lifecycle. The goal of the review is to verify the relevance of the Plan to the business needs of the CROS Project and update the Plan accordingly.

Table of Contents

1. Overview

1.1 Purpose

The purpose of this document is to define the process, roles, and tools CROS will use to manage project risks and issues.

1.2 Scope

The scope of the Risk and Issue Management Plan is the identification and tracking to resolution issues and risks that could have an impact on the success of the CROS project. The procedures in this document will be used by the CROS team to identify, evaluate and manage risks and issues within the project. The project will use a single repository to record and track project issues and risks.

The project defines a risk as an issue that has not occurred or the trigger is at least 6 months in the future. An issue will be triggered within six months or is a risk that has been triggered.

The following steps describe the Risk/Issue Management process:

- **Identify –** recognize and discover risks/issues; assign an owner
- **Assign Owner** – the person for resolving the issue or responsibility for mitigating the risk
- **Analyze –** process risk/issue data into decision-making information
- **Plan Risk/Issue Response** – translate risk/issue information into decisions and response actions (mitigations)
- **Execute Risk/Issue Response** – execute decisions and mitigation plans
- **Track and Monitor** – monitor risk/issue indicators and mitigation actions; correct for deviations from planned actions
- **Communicate** – share information and solicit feedback on all risk/issue management activities with project stakeholders; escalate issues and risks based upon exposure and impact to project

2. Roles and Responsibilities

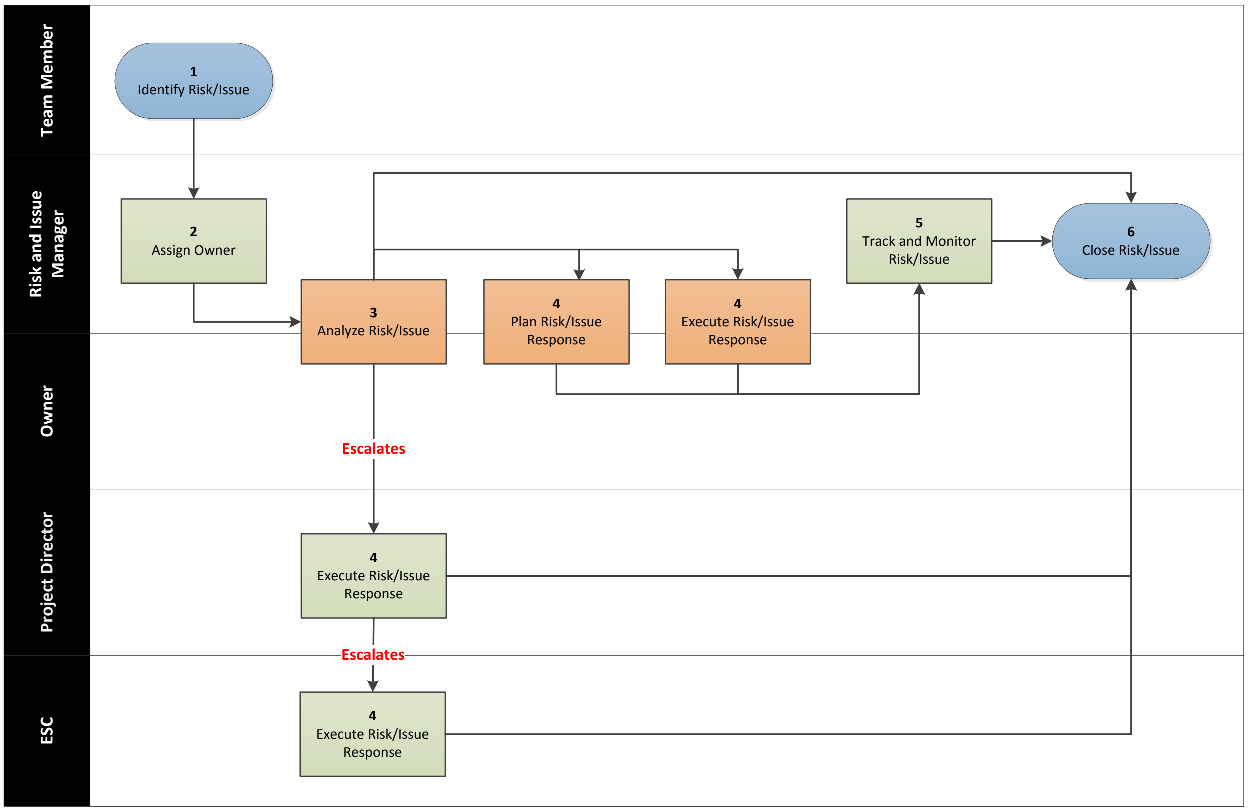
The following table defines the risk management roles and responsibilities for the CROS project.

Role	Responsibilities
Steering Committee	• Work with the Director as needed to resolve issues that cannot be resolved by the Project Sponsors • Work with the Director as needed as mitigate department-wide and external stakeholder risks • Evaluate risks and recommend risk mitigation strategies • Prepare for contingencies and communicate contingency actions
Project Sponsors	• Work with the Director as needed to resolve issues • Work with the Director as needed as mitigate department-wide and external stakeholder risks • Evaluate risks and recommend risk mitigation strategies • Prepare for contingencies and communicate contingency actions
Project Director	• Ensure accountability of all roles in the risk and issue management process • Provide resources and support for the development and implementation of the risk and issue management process • Authorize execution of the contingency plan • Escalate issues that cannot be resolved at the project level to the Project Sponsors • Escalate high level risks that cannot be controlled at the project level to the Project Sponsors • Work with the Steering Committee as needed to mitigate department-wide and external stakeholder risks
Project Manager(s)	• Validate newly identified risks • Coordinate risk response activities within the project, such as risk mitigation plan and contingency plans • Act to resolve issues escalated to the Project Management team • Escalate issues that cannot be resolved at the Project Management team level to the Director • Escalate high level risk that cannot be controlled at the project team level to the Director
Risk/Issue Manager	• Ensure that risks and issues are identified and properly assessed • Ensure new risk and issue updates are captured on the Risk Log • Conduct a weekly review of the project risks and issues • Report project progress and risk status to all project team members, executive sponsors, and Steering Committee • Escalate risks and issues to the Project Director
Risk/Issue Source	• Identify potential risk or issue and informs the Risk Manager immediately as new risks or issues are discovered

Role	Responsibilities
Risk/Issue Owner	• Assess new risks or issues as they are assigned • Conduct a root cause analysis of the risk to assist in understanding the source of risk • Actively monitor assigned risks • Advise the Risk/Issue Manager on the effectiveness of risk mitigation strategies • Develop new mitigation strategies or modifies old ones if the current strategy works poorly or if further mitigation is necessary • Provide risk updates to the Risk/Issue Manager as requested

3. Risk and Issue Management

The diagram below shows the steps the project follows to identify, analyze, mitigate or resolve, and track risks/issues.



Process Step	Participants	Inputs	Outputs
Identify Risk/Issue	• PMO • Source (team member, stakeholder, etc) • Assignee	• Information about the problem • Project artifacts	• Defined risk/issue
Assign Owner	• Risk/Issue Manager	• Team members • Risk/Issue identifier information (team, source, impact, etc.)	• Assigned risk/issue
Analyze Risk/Issue	• Risk/Issue Manager • Owner • Management Team	• Impact • Project schedule • Trigger	• Classified and prioritized risk/issue

Process Step	Participants	Inputs	Outputs
Plan Risk/Issue Response	• Owner • Risk/Issue Manager • Management Team	• Risk/issue classification and priority	• Defined response plan
Execute Risk/Issue Response	• Owner • Management Team	• Risk/issue response plan • Escalation criteria	• Mitigated risk/issue • Resolved/defused issue
Track and Monitor Risk/Issue	• Owner • Risk/Issue Manager	• Risk/issue action date • Priority • Action plans	• Updated risk/issue data • Risk/issue updates communicated
Close Risk/Issue	• Risk/Issue Manager	• Issue resolved • Risk mitigation info	• Risk/issue status changed • Risk/issue status communicated

3.1 Identify Risk and Issue

Risk/issue identification occurs on an ongoing basis. Risks and issues will be items on CROS project meeting agendas and status reports. This section describes the activities that occur when a potential risk/issue is identified or discovered.

3.1.1 Define Risk/Issue Attributes

When a new risk/issue is discovered, a few identifying attributes will be gathered and documented in the risk log.

Risk/Issue Attribute	Description
Title	A brief sentence or phrase that summarizes the risk/issue.
Risk/Issue	Indicates whether the item is a risk or issue. Risk – has not occurred; at least 6 months or more until the trigger. Issue – is within 3 months of the trigger or the risk has occurred.
Creation Date	The date the risk/issue was identified.
Source	Defines who identified the risk/issue or during what meeting the risk/issue was identified.

Risk/Issue Attribute	Description
Category	A logical classification of the risk/issue. CROS uses the following categories: a. Data Cleansing b. Governance c. Infrastructure d. Procurement e. Project Management f. RFP g. SharePoint
Description	An explanation of the issue or risk event, consequence to the project, or negative impact on a project objective.
Affected Areas	Describes the impact to the CROS project scope, schedule, cost, quality, revenue, etc. because of the issue or if the risk occurs.
Severity	Describes how quickly and intense the impact to the project will be because of the issue or will be if the risk is triggered.
Status	Defines the state of the risk/issue.

3.1.2 Assign Owner

Once a risk or issue has been identified and submitted to the Risk/Issue Manager, an owner will be assigned. The owner is the person responsible for conducting analysis on the risk or issue and providing feedback on mitigation strategies, contingency plans, and action plans. In general, the Risk/Issue Manager assigns the owner, but may consult with the Project Director to assign an owner or especially if the owner is outside the CROS project such as the Executive Director or a Sponsor.

4. Analyze Risk/Issue

The objective of risk/issue analysis is to develop more specific information to aid decision-making and the mitigation and resolution process. Analysis involves risk/issue classification and prioritization, providing recommendations for mitigating, measuring, and tracking risk/issue information. The PMO is responsible for working with the owner and other stakeholders as needed to complete and document the analysis of the risk/issue.

4.1.1 Analysis Attributes

The following table defines the attributes collected during risk/issue analysis.

Risk/Issue Attribute	Description
Probability (risk only)	The likelihood a risk event will occur.
Impact	The affect the issue/risk event will have on the CROS project.
Exposure (risk only)	Based upon the probability and impact, risk exposure defines how vulnerable the project will be if the event occurred.
Mitigation Strategy	Options and actions that will lessen the threat to the project because of the issue or if the risk event occurs.
Contingency Plan	A course of action to take if the risk event has been triggered or if the issue cannot be resolved.
Trigger	An event that will cause the risk to occur which will result in the execution of the contingency plan. It is also the event that created the issue.

4.1.1.1 Probability Assessment

This attribute is defined for risks only. The risk probability is the likelihood the risk event will occur. The following probability table will be used to rate the probability to ensure consistency in calculating the risk assessment:

Probability	Probability Definition
10%	Remote
30%	Unlikely
50%	Likely
70%	Highly Likely
90%	Nearly Certain

4.1.1.2 Impact Assessment

The impact assessment describes the resulting effect on the project because of the issue or should the risk event occur. The impact could affect cost, schedule and/or performance. The impact should be chosen based on the effect that most impacts the risk or issue as noted in the table.

Impact Rating	Scope	Cost Effect	Schedule Effect	Quality/Performance
1	Affects a non-critical area with minimal impact to operations	<1%	Possible slip of non-critical activities	Possible reduction in performance
2	Affects non-critical area with some impact to operations; alternative solution is available	2-4%	No milestone slips, work-around required	Minor reduction in performance
3	Affects critical areas of scope are but alternative solution is available	5-7%	Minor slip of milestone	Moderate performance degradation
4	Affects a critical area and there is no alterative solution	8-10%	Major slip of milestone	Serious performance degradation
5	Stops processing in a critical area and there is no workaround; unacceptable to the client	>10%	Unacceptable slip of milestone	Unacceptable performance degradation

4.1.1.3 Risk Exposure

Risk exposure is used to classify risks only. Exposure is calculated by multiplying the probability of occurrence by the impact assessment rating. The exposure level is the degree to which the risk, if triggered, makes the project cost, schedule, or resources vulnerable to impact.

The following exposure table plots and assigns a value for exposure based upon the probability and impact ratings.

Exposure Values

Probability					
90%	0.9	1.8	2.7	3.6	4.5
70%	0.7	1.4	2.1	2.8	3.5
50%	0.5	1.0	1.5	2.0	2.5
30%	0.3	0.6	0.9	1.2	1.5
10%	0.1	0.2	0.3	0.4	0.5
	1	2	3	4	5

Impact

4.1.1.4 Risk Severity

The prioritization of risks for risk response planning, however, cannot simply use risk exposure ranking. For example, consideration must be given to the timeframe for each risk. More emphasis is generally required on risks with a "near" timeframe of occurrence rather than those with a "far" timeframe. Other subjective factors may be involved depending on the particular risk. A technique to identify the most critical and impactful risks is to define the risk severity.

Risk severity is determined from the exposure and time frame ratings, and is used to prioritize the risk. Risks with a "High" severity has the highest priority for risk response activity and escalation, followed by "Medium" and then "Low" severity risks.

4.1.1.4.1 Risk Exposure Timeframe

Typically a risk is tied directly to one or more project milestones. Some risks may not be tied to project milestones, but may be tied to events outside of the project; or the risk may occur anytime during the project. The timeframe defines the earliest and latest date the risk can occur. Because the risk exposure timeframe may be contingent on project milestones, the exposure timeframe will change as the schedule changes.

The severity rating for each risk is the intersection of that risk's exposure and time frame, as presented in the following table:

Risk Severity

Exposure Timeframe			
One to three months	Medium	**High**	**High**
Three to six months	Low	Medium	**High**
Six months to one year	Low	Low	Medium
	0 to 1.5	**1.5 to 3.0**	**3.0 to 4.5**

Exposure Rating

The level of the risk based on its position within the matrix, in conjunction with expert judgment related to the timeframe of the risk and other subjective factors, is used by the Risk Manager to determine whether or not a Risk Response Plan will be developed for the risk. If the risk/issue has an impact to project scope, budget, quality, or schedule, a change request may be generated. Please refer to the Change Management Plan for change request process. Risks with high and medium severity will normally have a contingency plan.

4.2 Escalate Risk/Issue

New issues will be communicated immediately to the Project Director. All new risks or updates to risks/issues are communicated to the Project Management team at the weekly Director or PM Sync meetings. Within the CROS project, risks/issues will be recorded, tracked and resolved on a specific team (Program Area Readiness, Procurement, Data Readiness, Interfaces, etc). The following section defines the escalation path within the project.

Project Team Level

- Team level issues are reported immediately to the Team Lead and the Risk/Issue Manager;
- Team level risks are reported to the Team Lead who will log them in the risk/issue log;
- Team Leads and Risk/Issue Manager plan how to address;
- Team members will review and evaluate team issues, risks and risk mitigation strategies during weekly/monthly meetings and on an as-needed basis through email, memo, and verbal communication.

Business/Technical/Project Managers and Director Level

- Risks assigned a high severity or new issues will be reported immediately by the Risk/Issue Manager to the Project Director;
- Risks/issues are monitored weekly by the Risk/Issue Manager and issues and risks that have been triggered are reviewed weekly at the PM Sync until they are resolved;
- Project Manager updates the Project Sponsors and Steering Committee via status reports;
- Risks assigned a high severity will be reported by the Project Director to the Project Sponsor(s) and Steering Committee;
- If the risk has an impact to project scope, budget, quality, or schedule, a change request may be generated.

Executive Level

- Based upon criteria identified in the Governance Plan, some risks/issues get escalated to the Sponsors and the Executive Steering Committee.
    - The Project Director escalates unresolvable risks categorized as high-impact to the Sponsors
    - The Sponsors escalate unresolved BOE policy conflicts and unresolved conflicts between project objectives and organizational goals to the Executive Steering Committee

- The Executive Steering Committee escalate unresolved BOE policy conflicts and unresolved conflicts between project objectives and organizational goals to the Executive Director
- The Executive Director escalates significant policy issues (e.g., conflicts with the CPPM and audit manual) to the Board Members

5. Plan Risk/Issue Response

A response plan will be developed for medium to high priority risks and for issues if there are known strategies for resolution. Generally, actions taken will be documented for issues/risks.

Risk/issue response planning is comprised of three general strategies:

- **Risk/issue reduction** – identifies ways to minimize or eliminate project risks/issues.
- **Risk/issue acceptance** – risks/issues are accepted as is or after mitigation steps have been taken.
- **Risk/issue contingency planning** – put in place for accepted risks/issues and identifies an agreed upon set of actions that will be taken to mitigate risk/issues.

The risk/issue owner working with the Risk/Issue manager updates the risk log with the risk response strategy and planned completion dates for each response action.

5.1.1 Risk Reduction Strategies

The risk owner working with the Risk/Issue Manager is responsible for developing the risk reduction plan by developing options and determining actions to lessen threats to the project.

Risk reduction strategies are generally one or a combination of the following:

- **Mitigate –**reduced the probability and/or impact of an issue or a risk event to an acceptable threshold.
- **Avoid** – involves changing the project plan to eliminate the threat posed by the adverse risk/issue.
- **Transfer** – requires shifting the negative impact of a threat along with the ownership of the response to a third party. Transferring the risk/issue simply gives another party responsibility for its management.

5.1.2 Risk/Issue Acceptance Strategies

Risks/issues are typically accepted when a reduction plan has not eliminated the risk or if it is deemed too expensive to attempt reduction. Contingency reserves may be established for these risks/issues including amounts of time, money or resources. Accepted risks are monitored and if the risk event happens, the project team deals with it when it occurs. Risk/Issue Manager will escalate to Project Director risks that require contingency resources.

5.1.3 Risk/Issue Contingency Planning Strategies

It may be appropriate for risks that have been accepted and/or have a high severity, to have an agreed plan of action which is called a contingency plan. A risk trigger is an event that has caused the risk to occur which will result in the execution of the contingency plan. If execution of the contingency plan requires significant funds, a reserve may be set aside for the contingency.

5.1.4. Actions Taken

Actions taken to solve an issue or mitigate a risk are recorded in the Risk/Issue log.

6. Execute Risk/Issue Response

When a risk/issue response is executed, the mitigation/resolution actions are put into effect. Changes in risks/issues are recorded in the log by the Risk/Issue Manager. The CROS Director will approve the execution of mitigation and contingency plans.

Based upon criteria, risks/issues may be escalated to the Project Director, Sponsors, or Executive Steering Committee.

7. Track and Monitor Risk/Issue

Tracking and monitoring risks/issues insures that all steps of the Risk/Issue Management process are being followed and, as a result, risks are being mitigated and contingency plans are followed as necessary. Risk tracking and control involves the oversight and tracking of risk mitigation and contingency action plan execution, reassessment of risks, and recording risk information changes.

7.1 Risk/Issue Management Log

The Risk/Issue Management Log is used to track risks and issues. The log is a SharePoint list and is posted on the PMO site. There is a separate risk/issue log posted on the project administration site where issues/risks that are more sensitive in nature are posted and not for public consumption. The two logs record and track the same meta data about a risk/issue and the processes for identifying, analyzing, and tracking, resolving risks/issues are the same.

The following table defines the columns in the Risk/Issue Management Log.

Column	Description
Risk/Issue	Indicates whether the item is a risk or issue. Risk – has not occurred; at least 6 months or more until the trigger. Issue – is within 3 months of the trigger or the risk has occurred.
ID No	Sequential number.
Description	An explanation of the issue or risk event, consequence to the project, or negative impact on a project objective.
Date Created	Date the risk/issue was identified.
Source	Who or what meeting identified the risk/issue.
Category	A logical classification of the risk/issue. CROS will use the following categories: a. Data Cleansing b. Governance c. Infrastructure d. Procurement e. Project Management f. RFP g. SharePoint
Description	A few sentences that defines the risk/issue.
Affected Areas	The areas that will be impacted by the issue or if the risk is triggered.
Trigger	The condition/event that will cause the response to be invoked and the date it is likely to occur.
Trigger Date	The date in the CROS project schedule it is projected the condition event will occur.
Action Date	The date the CROS project management team needs to take action to resolve the issue or if action was not already to mitigate risk.

Column	Description
Probability (risk only)	The likelihood the risk event will occur.
Impact	Scope, schedule, cost, quality.
Exposure (risk only)	The risk exposure level is the degree to which the risk, if triggered, makes the project cost, schedule, or resources vulnerable to impact.
Severity	How quickly and intense the impact to the project because of the issue or will be if the risk is triggered.
Owner	The person responsible for resolving the issue or mitigating the risk.
Status	The state of the risk/issue.
Actions Taken	A list of actions taken to minimize/reduce/resolve the risk or issue.
Mitigation strategy (risk only)	Actions that will be executed/taken to reduce the probability and/or impact of an adverse risk event to an acceptable threshold.
Contingency plan (risk only)	The actions that will be taken if the risk is triggered and mitigation strategies have been unsuccessful or the project accepts the risk.

Appendix A – Referenced Documents and Terms

A.1 Referenced Documents

The following documents are referenced in the plan:

Document/Version	SharePoint Location
CROS Governance Plan, v1.0	*CROS PMO/Project Management/Plans*

A.2 Definitions of Acronyms and Terms

Term/Acronym	Definition