State of California
Franchise Tax Board

EDR Risk Management Plan (MRD070)

FINAL Version 1.1

Revision 09.09.11

Document Information

Revision History

Version No.	Date	Summary of Changes	Revision Marks
0.1	08/16/2011	Working Draft submitted to the State.	No
1.0	08/29/2011	Final Walkthrough draft submitted to the State incorporating comments from Working Draft	No
1.1	09/06/11	Accepted minor tracked changes based on DRT review	No

Risk Management Plan Review

This document has been reviewed by the following people:

Name	Date
MRD070 Deliverable Review Team	09/06/2011
EDR Acceptance Board	09/08/2011

Table of Contents

1. INTRODUCTION

A risk is the possibility that a threat will cause the project to fail to meet one or more of its objectives. Risks are considered in project decisions, tradeoffs, planning, and day-to-day activities. Some risks rise from external influences, such as acts of nature and adverse actions by other individuals and organizations. Many risks, however, result from internal factors, such as invalid assumptions, poor design choices, or overly optimistic plans.

Risk Management is the process of anticipating, identifying, and defending against project risks. Its purpose is to ensure the likelihood of project success by recognizing and acting upon the identified risks.

This Risk Management Plan describes the process of Risk Management as it will apply to the Enterprise Data to Revenue (EDR) Project. This deliverable describes the detailed plan for risk identification, risk assessment, risk response, risk control, documentation, and reporting.

1.1. Purpose of the Document

The Risk Management Plan is used to define and communicate the approach to risk management by explaining process and procedural methods, the associated tools, the controls employed, and the communications with EDR Project team members. It is designed to provide the State and Solution Provider (SP) Teams with an understanding and guide to risk management for the EDR Project.

The essential concept of the Risk Management Plan is to document the approach to contain, reduce, and plan for risks and provide the capability to identify, analyze, and prioritize risks throughout all phases of the project. The process to manage risk is a continuous, ongoing function over the entire Systems Development Life Cycle (SDLC) as conditions and priorities on the EDR Project change. Mitigation actions are planned and initiated when specific triggers are activated.

1.2. Scope of the Document

This deliverable describes the processes and standards that are used to manage risks for the EDR project. The plan is used by the State and the SP to log, track, and manage risks and risk responses, and describes the tools to be used and references supporting documents (such as tool user manuals), as appropriate, to provide additional information.

The EDR Risk Management Methodology includes the following components:

- Risk Management Planning
- Risk Identification
- Risk Analysis
- Risk Response Planning
- Risk Tracking and Control
- Risk Resolution and Closure

The Risk Management Plan is used to manage and track Project-level risks. Organizational risks (for either the State or SP) will only be tracked using this plan if the risk has direct implications for the project. Risks involving legacy systems are tracked using this methodology if the risk is attributable to the EDR Project. Other legacy system risks are tracked using the legacy system management processes, as appropriate. In some cases, a similar risk may be tracked by both the EDR Project and the legacy system management team, each with different viewpoints.

1.3. Integration with Project Management Processes

To demonstrate integration with project management processes, Figure 1 demonstrates those processes that are tightly coupled and those that are more loosely integrated.

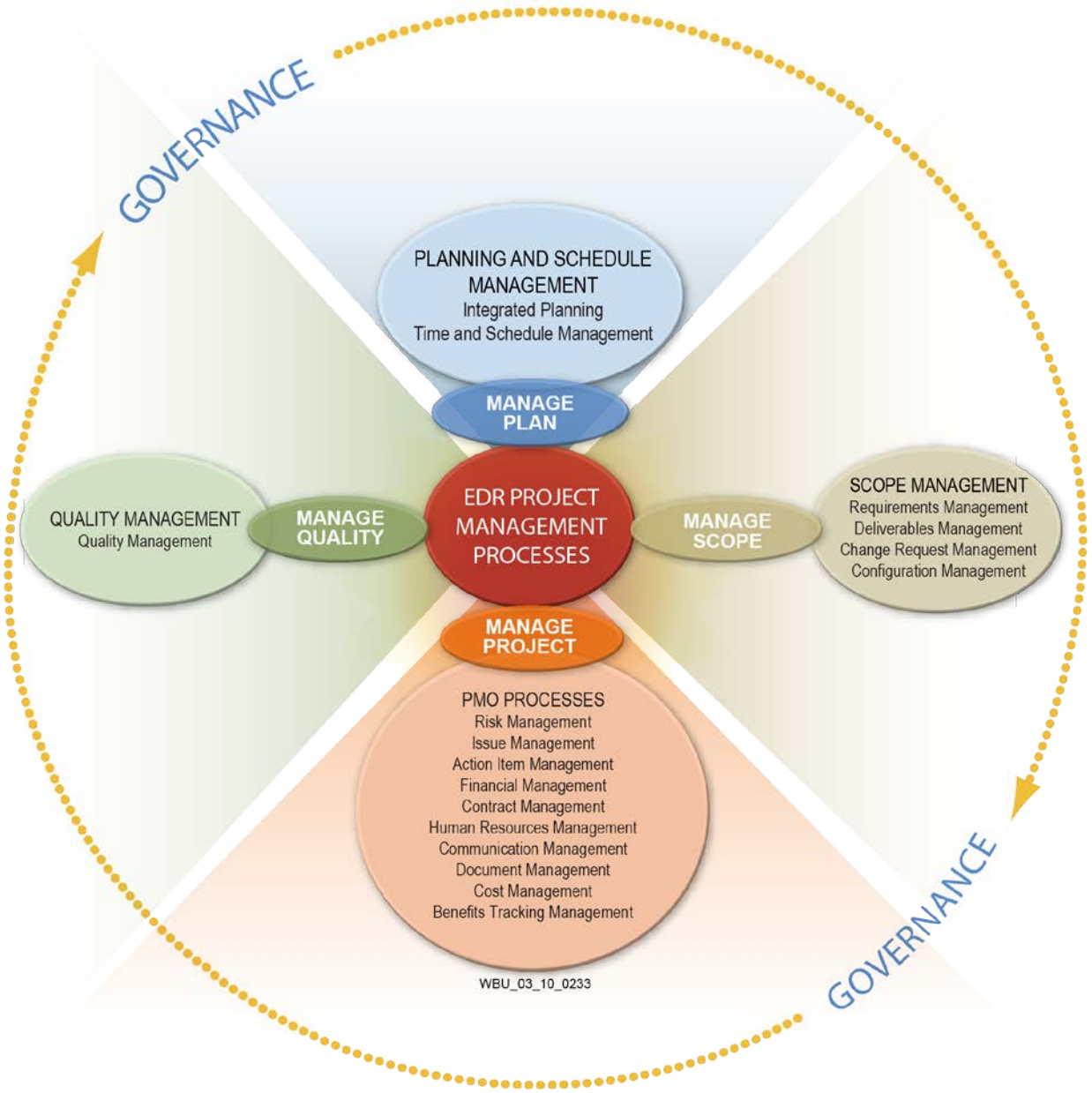

Figure 1. Integrated Project Management Processes

Risk Management is tightly coupled with Issue and Action Item Management since actions can become issues and conversely, if the potential event that was a risk comes to pass, the risk can become an issue and issues can become risks. It is also tightly coupled with the Communications Management process as the primary means of monitoring risk is through status meetings, particularly the team, group or discipline status meetings and the EDR Management Team Risks and Issues meetings attended by the State and SP EDR Project Directors, SP EDR Project Manager, SP EDR Phasing Manager, SP EDR Quality Manager, and State and SP EDR Discipline Managers.

The Risk Management process is coupled with the Scope Management and Change Request Management processes when risks are elevated to the Change Control Board for resolution and there is an associated change to scope, requirements, or deliverables. Risk Management can formally impact the integrated plans and associated Time and Schedule Management process which then impacts at a minimum, the release management process of Configuration Management through the release schedule. Quality Management is responsible for Risk Management oversight and measuring compliance with the project objectives and progress toward the objectives as they are impacted by the resolution or evaluation of risk.

1.4. Document Overview

The Risk Management Plan contains the following sections:

- Section 1: Introduction – This section contains the overview of Risk Management.
- Section 2: Risk Management Methodology – This section describes the approach for the management of risks.
- Section 3: Risk Management Tool – This section describes the tool used to document and track risks.
- Section 4: Risk Management Communications – This section describes the meetings, forms, reports and metrics that are used to monitor, track and manage risks on the project.
- Section 5: PASI – Roles and Responsibilities – This section presents the roles and responsibilities for Risk Management and provides a PASI (Primary, Approval, Supporting, Information) matrix.
- Appendix A: Risk Statement – This appendix contains the form for documenting the initial risk statement.
- Appendix B: Risk Response Plan (RRP) – This appendix contains the form for capturing the risk response strategy and planned actions. This form includes a Contingency Plan section.
- Appendix C: List of Risk Categories – This appendix contains the list of risk categories summarized from the California Technology Agency (TA) California Project Management Methodology (CA-PMM).
- Appendix D: Risk Tolerance Thresholds – This appendix contains the risk tolerance thresholds that will be used on the project.

1.4.1. Document Security Requirements

The Risk Management Plan is used by the EDR Project Team, which consists of the State and SP teams, and stakeholders. General document security and privacy considerations are to be followed in the control and release of this document. Refer to the *Document Management Plan (MRD001F)* for more information on document security and handling.

Individual risks, completed Risk Statement forms, and Risk Response Plans may be classified at higher security levels depending on the nature of the individual risk.

1.4.2. Maintenance of the Document

This plan is reviewed bi-annually in conjunction with the review of the EDR Project Management Plan (MRD001), and updated if necessary. Any updates result in a new version of the document which is made in accordance with the procedures described in the *EDR Document Management Plan (MRD001F)*.

1.5. Definitions

A master glossary and an acronym list are available in the EDR Project Repository. The following table contains definitions that are specific to the Risk Management Plan.

Table 1. Definitions

Term	Description
Decision Point	An actual concern or question at the team, group or discipline level that can be resolved within the team, group or discipline, and does not affect the overall project baselines, nor does it require coordination outside of the team, group or discipline.
Issue	An actual concern or question that, if not resolved, has an adverse impact on the project.
PIMRA	Project Implementation Management and Reporting Application (PIMRA) is the collaboration tool used to capture, report, and manage risks, issues, and action items.
Probability	A qualitative expression of the chances that a risk will occur.
Risk	A potential situation or event that will cause the project to fail to meet its success targets, or a potential opportunity which could result in a positive benefit to the project if action is taken. Risk involves uncertainties and factors that may not be completely within the control of the organization impacted by it. Requires active management and oversight throughout the life of the project. In this document, the term “risk” is used to address both positive risks (opportunities) and negative risks (threats). Positive risks can be thought of as a risk of a missed opportunity if the project does not respond to and manage the situation.

Term	Description
Risk Contingency Plan	The procedures to follow if a known potential risk occurs. Not all risks require a contingency plan. The contingency plan is included as a section of the Risk Response Plan.
Risk Event	A future occurrence of the risk; the potential event, expected to have a negative impact on the success of the project, if the event were to occur. Or, a positive effect that will occur if the project nurtures the opportunity.
Risk Exposure	The potential loss (or gain) presented to the project by a risk; a function of the probability (likelihood) that the risk will occur, and the magnitude of the impacts (consequences) of its occurrence, and the timeframe when action is required.
Risk Impact	A description of the anticipated consequences of a risk event occurring, in terms of impact to scope, schedule, cost, and quality.
Risk Management Process	A continuous process for systematically identifying, analyzing, treating, and monitoring risk throughout the lifecycle of the EDR Project.
Risk Mitigation	The act of taking steps to affect situational factors in order to lessen risk by lowering the probability of a risk occurrence or reducing its effect should the risk occur.
Risk Priority	A determination of the importance of the risk based upon: 1) the potential impact of the risk on the project, 2) the probability of occurrence, and 3) the risk timeframe. Often, the same as the risk exposure, except in cases where multiple risks have the same calculated exposure level.
Risk Register	The project repository for tracking all project risks.
Risk Response Plan (RRP)	The deliverable of the risk research and response effort performed by the Risk Owner. The RRP is documented within the Risk form in PIMRA. Not all risks require a RRP.
Risk Statement	The original document that identifies the major elements of the risk. The Risk Statement is attached to the Risk form in PIMRA.
Risk Status	The current condition of the risk, for instance: Identified, Closed, etc.
Risk Timeframe	The urgency with which risk management activities must be undertaken. The timeframe is based on the need to begin risk management work and varies based on the duration of the project.
Risk Transference	The ability to have another entity absorb some of the risk.

Term	Description
Risk Trigger Events	A threshold event that causes response actions to be initiated.
Watch Point	A potential situation or event at the team, group or discipline level that can be resolved within the team, group or discipline, and does not affect the overall project baselines, nor does it require coordination outside of the team, group or discipline.

1.6. Referenced Documents

The following documents are referenced in, or were used in the creation of the Risk Management Plan.

- IEEE 16326-2009 (ISO/IEC/IEEE (16326), Systems and Software Engineering – Life Cycle Processes – Project Management, Institute of Electrical and Electronics Engineers (IEEE), Dec 15 2009
- IEEE 1058-1998 (Revision and re-designation of IEEE Std 1058.1-1987, incorporating IEEE Std 1058-1998 and IEEE Std 1058a-1998). IEEE Standard for Software Project Management Plans. Sponsor: Software Engineering Standards Committee of the IEEE Computer Society. Approved 8 December 1998. Superseded by IEEE 16326-2009
- IEEE 1490-2003, Adoption of the PMI Standard A Guide to the Project Management Body of Knowledge – Description. Sponsor: Software Engineering Standards Committee of the IEEE Computer Society. Withdrawn Standard. Withdrawn Date: Jan 26, 2009
- A Guide to the Project Management Body of Knowledge Fourth Edition (PMBOK Guide). An American National Standards ANSI/PMI 99-001-2008
- Statewide Information Management Manual (SIMM), Section 17, California Project Management Methodology (CA-PMM), revised March 2011
- SIMM, Section 45, Information Technology Project Oversight Framework, revised April 2011
- State of California Franchise Tax Board, Enterprise Data to Revenue (EDR) Project, Project Management Plan, FTB FSR 08-05, Version 1.4, December 27, 2010
- State of California Franchise Tax Board, Enterprise Data to Revenue (EDR) Project, Franchise Tax Board Request for Proposal, RFP-FTB-0910-C001, September 29, 2010, Exhibit VI-B.1, Deliverable Item Description Project Management Plan
- State of California Contracting Agreement #C1100017 between FTB and CGI, including all attachments, dated July 1, 2011
- CGI Client Partnership Management Framework (CPMF), 2002 CGI Group Inc., Release no:11.0
- CGI Project Implementation Management and Reporting Application (PIMRA) Manual, updated TBD

- EDR Project Management Plan (MRD001), dated August 23, 2011, and Supporting Plans.
    - Change Request Management Plan (MRD001A)
    - Time and Schedule Management Plan (MRD001B)
    - Issue and Action Item Management Plan (MRD001E)
    - Document Management Plan (MRD001F)
- EDR Project Schedule (MRD002), dated August 5, 2011.
- EDR Quality Management Plan initially submitted with PMP (MRD001) followed by Quality Management Plan (MRD071), dated TBD.

2. RISK MANAGEMENT METHODOLOGY

The Risk Management Methodology defines the processes used to identify, analyze, develop and prioritize risk response actions for risks that threaten the project's success. Risk management is the means by which such threats and opportunities are monitored and controlled. EDR's risk management approach is based on two essential principles:

- Early identification of project risk is required to contain and reduce risk.
- Proactive, ongoing risk mitigation and management is essential to project success.

EDR Project team members are responsible for the identification of risks. Regardless of where they are opened, risks must be quickly communicated to the appropriate decision makers, so that the risks are properly mitigated and managed. Prompt resolution is critical so that project activities underway are not delayed or otherwise negatively affected.

Project-level risks are managed through the methodology presented in this section. However, each team, group or discipline uses the same basic process to manage Watch Points, which are potential situations or events at the team, group or discipline level that can be resolved within the team, group or discipline, and does not affect the overall project baselines, nor does it require coordination outside of the team, group or discipline.

2.1. Process Overview

As depicted in Figure 2 below, the EDR Risk Management Process contains six components.

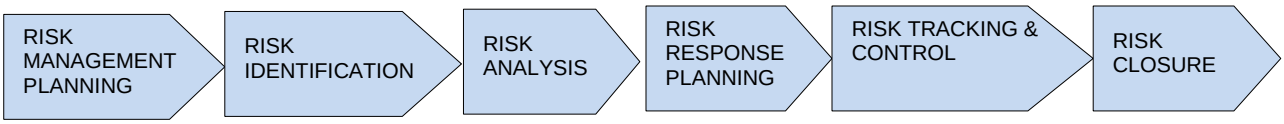

Figure 2. Risk Management Process

The components of the Risk Management Process are described below.

- Risk Management Planning – This component establishes the strategy for managing the project risks and implements the approach, process, methods, and tools.
- Risk Identification – This component gathers the initial set of project risks, and also establishes tolerance thresholds and channels for ongoing risk reporting as the project progresses. This component begins with the selection and briefing of staff to gather the initial risks from an interview process. This is a proactive process of identifying possible future occurrences that could have a negative impact on the cost, the schedule, or the project objectives. It also considers positive risks (opportunities) which may be leveraged to generate positive impacts or benefits. Risk identification includes periodic structured assessments to identify new risks, as well as ad hoc identification of risks from day-to-day activities by staff, managers, and stakeholders.

- Risk Analysis – This includes evaluation of individual risks using probability-impact scores, quantifying risks in terms of costs, time and performance, and evaluating risks based on overall exposure. The exposure is established during the process of quantifying a risk from the point of view of the probable effect, the probability of its occurrence, as well as the ability of the project to influence the risk. This is vital in prioritization of risks and establishing the risk response actions.
- Risk Response Planning – Risk response planning is the process of developing and implementing risk response strategies and plans to deal with the identified risks. This includes the assignment of risk owners, analysis using techniques such as root cause analysis, prioritizing the risks and selecting the risk response strategy as well as establishing risk mitigation actions based on urgency and manageability, and finally developing contingency plans, if warranted.
- Risk Tracking and Control – This is the process of reviewing each risk on a regular basis, assessing its current status, taking further actions as necessary including escalating the risk as needed, and reporting on the status of the risk and the status of those risks in development.
- Risk Resolution and Closure – This final component involves documenting the resolution of the risk, whether successfully prevented or not. The results of the risk response(s) are documented to record what actions were successful, and how to better respond in the event a similar risk arises in the future.

The six components of the Risk Management Process have a series of steps associated with them as depicted in Table 2 below.

Table 2. Risk Management Steps

Component	Section	Risk Management Step
Risk Management Planning	Section 2.1.1	This component involves the development of the Risk Management Plan (MRD070) which describes the Risk Management Steps below.
Risk Identification	Section 2.1.2	Step #1A: Conduct Initial Risk Assessment
		Step #1B: Conduct Periodic Risk Assessments
		Step #1C: Conduct Ongoing and Ad Hoc Risk Identification
Risk Analysis	Section 2.1.3	Step #2: Validate and Document Risk
		Step #3: Review Risk for Process Compliance
		Step #4: Enter Risk in Tool
		Step #5: Review and Prioritize Risk
		Step #6: Update Risk in Tool
		Step #7: Perform Risk Analysis
Risk Response Planning	Section 2.1.4	Step #8: Develop Risk Response Plan
		Step #9: Review and Approve Risk Response Plan
		Step #10: Update Risk in Tool
Risk Tracking and Control	Section 2.1.5	Step #11: Monitor and Report Risk Status
		Step #12: Execute Risk Response Plan
		Step #13: Monitor Effectiveness of Risk Response Plan
		Step #14: Update Risk Status and Actions in Tool

Component	Section	Risk Management Step
Risk Resolution and Closure	Section 2.1.6	Step #15: Close Risk in Tool

The management of risks is the responsibility of both the State EDR PMO and the SP EDR PMO with oversight from the State EDR Project Director and SP EDR Project Manager. The Project Team, consisting of the State and the SP, jointly manage and track risks to the project. The State and the SP record risk data in the same tool and have access to the same reports and metrics. A Risk Manager is assigned from each of the State and SP PMO teams who is responsible for managing and coordinating risks assigned to its organization. Though the State and SP PMO Teams own and facilitate the Risk Management process, the State and SP EDR Management Teams have the primary decision-making responsibility for EDR project risks. For more information on roles and responsibilities, refer to Section 5: PASI - Roles and Responsibilities.

The Risk Management Process Workflow is depicted in Figure 3 which is described in the rest of Section 2.1.

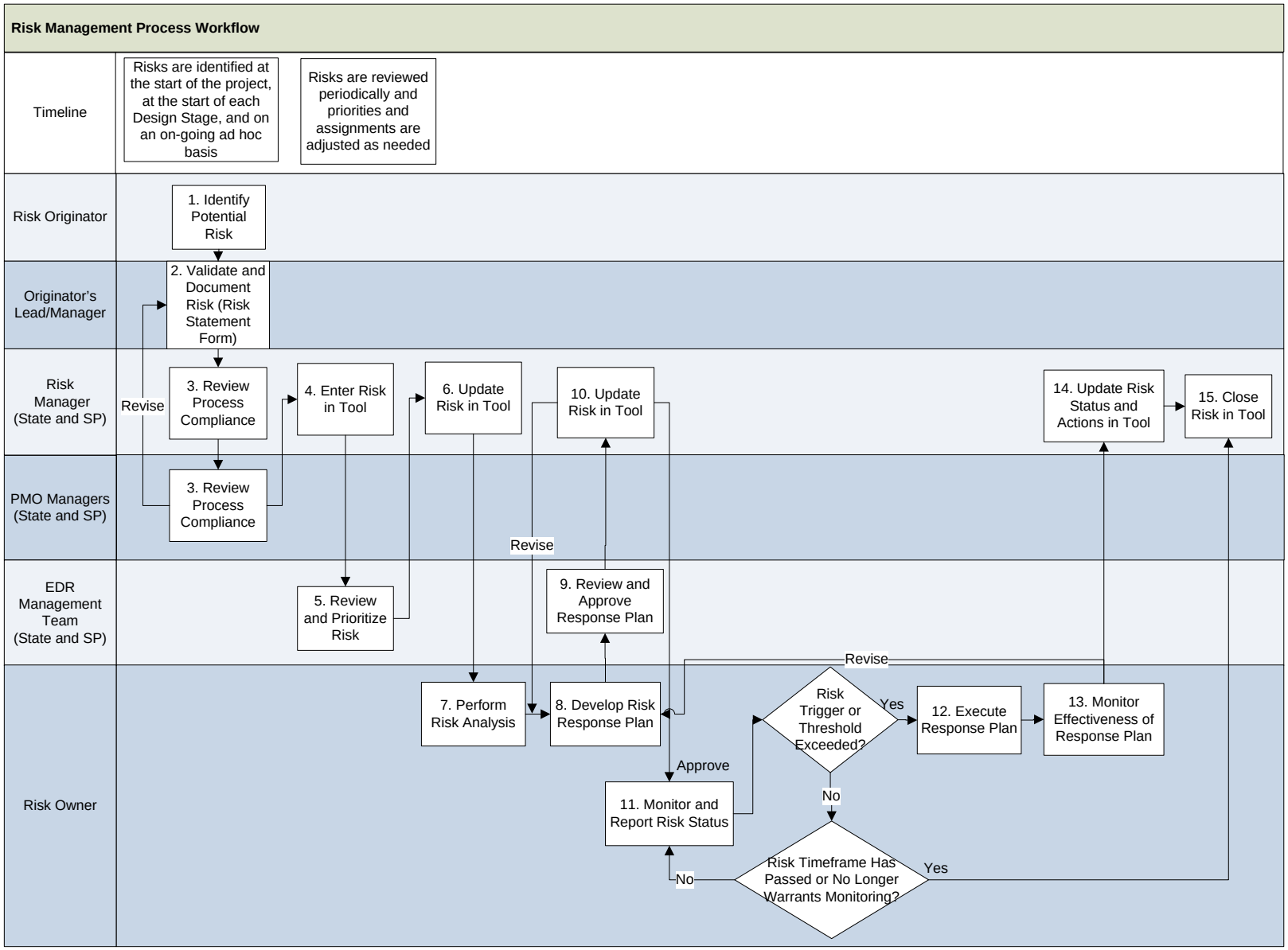

Figure 3. Risk Management Process Workflow

2.1.1. Risk Management Planning

Risks are non-trivial and capable of impacting the overall project objectives if not properly managed and given required management attention. A risk may become an issue after the event has occurred and its impact felt. Risks are assessed based on probability, timeframe, and impact to schedule, scope, budget and quality. The priority given to the risk and response actions are derived from the risk exposure level. For example, a high risk exposure level causes the risk to be given a high priority.

Risks are considered in project decisions, planning, and day-to-day activities. Some risks arise from external influences, such as acts of nature and adverse actions by other individuals and organizations. Most risks result from internal factors, such as invalid assumptions, inaccurate design choices, or overly optimistic plans. The approach is to find and mitigate or contain the risk as early in the process as possible.

Risk Management Planning involves the following activities:

- Develop the Risk Management Plan
- Implement the Risk Management Tool
- Assign Risk Management Roles
- Train Risk Management Staff and Project Staff

2.1.1.1 Develop the Risk Management Plan

The Risk Management Plan is developed and submitted by the SP as a contract deliverable (MRD070). The plan is referenced by the *Project Management Plan (MRD001)* and the risk processes are integrated into project management activities.

The plan is reviewed and accepted in accordance with the Deliverable Management Process for contract deliverables (contained in the State's *Contractual Obligations Management Plan*). Upon acceptance by the State, the processes and activities described by the plan are implemented. The accepted Risk Management Plan is stored in the EDR Project Repository. The plan is reviewed and updated by the SP as described in Section 1.4.2.

2.1.1.2 Implement the Risk Management Tool

The risk management tool for the project is the SP's Project Implementation Management and Reporting Application (PIMRA). The SP installs and configures the tool after contract start, and works with the State PMO to determine the appropriate users and reports. The SP's PIMRA administrator establishes the user accounts and access controls for both the State and the SP PMO and Leads and Managers. For more information on PIMRA, refer to Section 3: Risk Management Tool.

2.1.1.3 Assign Risk Management Roles

Each PMO team (the State and SP) has an assigned Risk Manager who is responsible for overseeing and coordinating the risk reporting for its organization. Each Risk Manager has at least one assigned backup to assist with the process. The Risk Managers work together to manage and coordinate the implementation of the Risk Management Plan. Refer to Section 5: PASI - Roles and Responsibilities for the specific responsibilities of the Risk Managers.

2.1.1.4 Train Risk Management Staff and Project Staff

Project staff receive an overview of risk management as part of the project orientation activities. This overview focuses on how to distinguish between risks, issues, action items, Watch Points, and Decision Points.

Training for Leads and Managers includes an overview of the process and the use of the forms and tools. The SP develops the training materials. The State and SP Risk Managers work together to schedule and deliver the session(s).

The training materials are located in the EDR Project Repository and available to project staff at any time.

2.1.2. Risk Identification

Risk identification is the process by which the perception of a potential problem or opportunity is documented in sufficient detail for effective assessment of the risk and subsequent management decisions on response actions.

During the initial phase of the EDR Project, risks are generally related to expectations concerning financial goals, qualitative goals, project schedule, or technology. A risk may originate as an issue that is left unresolved or that is resolved with a solution that causes another risk to the project. Another typical source of risk is an indication that the project is falling behind plan, such as tasks being completed late or key dependencies being missed.

Sources used to identify risks include project constraints and assumptions, schedule dependencies and resource allocations, risk identification workshops, change requests, stakeholder meetings, project reviews, team meetings, status reports, deliverable reviews, Independent Verification and Validation (IV&V) or Project Oversight reports, and Organizational Change Management (OCM) meetings with the end user.

Risks can be discovered at every level of the organization. Team members should be alert to recognize risks in the course of their daily work and should bring potential risks to the attention of their Lead/Manager as they discover them. Risks may also gain exposure at reviews with managers or executives, at meetings held with co-workers, or during interactions with stakeholders. Regardless of their source, team members should be encouraged to raise potential risks to their Lead/Manager for consideration. This is particularly the case for the EDR Project where there may be opportunities to increase productivity, benefits, or ease of use if the project can act on the opportunity early.

Risk Identification involves the following activities:

- Conduct Initial Risk Assessment
- Conduct Periodic Risk Assessments
- Conduct Ongoing and Ad Hoc Risk Identification

2.1.2.1 Step #1A: Conduct Initial Risk Assessment

Once the Risk Management Plan has been accepted, the State and SP Risk Managers plan the initial risk assessment activities. Working together to plan the appropriate number of focus group sessions, the Risk Managers identify and coordinate the participation of the appropriate SP and State staff in these focus group sessions.

The Risk Managers lead the initial risk identification sessions, focusing on the definition of project success so that participants come to a common understanding. The discussion then shifts to describing potential threats to success. This technique encourages workshop participants to match potential threats with the affected success measures, resulting in well-defined risk statements. The follow-on actions set forward during the initial risk workshop result in a set of risks that act as the foundation for further risk identification efforts. These risks are presented in the form of risk statements, with a description of the threat and the impact.

The Risk Managers document the results of the session in meeting minutes which are stored in the EDR Project Repository.

Establish Risk List and Risk Tolerance Thresholds

At the completion of the risk assessment sessions, the list of potential risks is consolidated and organized into a list of potential risks by risk category according to the risk categories from the CA-PMM (refer to Appendix C for the list of categories). The Risk Managers review and consolidate the potential risks that were identified, remove duplicates, and group related risks. The State and SP Risk Managers review the initial list of risks, verify the risk statements are clearly worded, and review initial probability, impact and timeframe values. The Risk Managers prepare the initial risk list for review with the EDR Management Team.

The list of risks is presented to the EDR Management Team for discussion and validation. The EDR Management Team reviews the risk exposure (calculated based on the probability, impact and timeframe), prioritizes the risks, and assigns Risk Owners to the risks for analysis. The risk analysis step is described in Step #2 (Section 2.1.3.1).

Next, the State and SP PMO Managers work with the EDR Management Team to establish the project's risk tolerance thresholds which define the project's tolerance for risk in key project areas. In establishing the risk tolerance thresholds, the EDR Management Team is reinforcing the project priorities and setting guidelines for managing risks.

Thresholds may be revisited at any time, and are reviewed during the periodic risk assessments (refer to Section 2.1.2.2) and effectiveness evaluated during the risk process evaluations (refer to Section 2.2). The Risk Managers document the risk tolerance thresholds which are included as Appendix D of the Risk Management Plan. The SP Risk Manager enters the initial list of risks into the Risk Tool, and the State and SP Risk Managers notify the appropriate Risk Owners of their assigned risks via email. The process continues as described in Section 2.1.2.3.

2.1.2.2 Step #1B: Conduct Periodic Risk Assessments

Within the first ninety days of each Design Stage, a risk assessment is conducted by the State and SP Risk Managers. The risk assessment provides an opportunity to review all open risks for continuing validity in the next Design Stage and to close risks whose timeframe has passed. The risk assessment includes a structured interview (especially for historically problematic areas caused by unanticipated or undocumented risks) to:

- Identify potential new risks based on the results of the current Design Stage and deliverables

- Identify potential new risks related to the upcoming Design Stage
- Identify potential new risks based on the overall status of the project's schedule, budget, resource levels, stakeholder input, and executive perspective
- Consider any potential opportunities which may be leveraged during the next Design Stage, such as increased benefits, improvements to productivity or ease of use, or organizational change management opportunities
- Evaluate the current risk tolerance thresholds and determine if changes or additions are needed

The periodic risk assessments include the EDR Management Team which assigns any newly identified risks for analysis and/or action.

The Risk Managers prepare the agenda materials for the risk assessment and schedule the meetings. The Risk Managers document the results of the session in meeting minutes which are stored in the EDR Project Repository.

2.1.2.3 Step #1C: Conduct Ongoing and Ad Hoc Risk Identification

Risks can arise at any time and team members should always consider risk identification as part of their project duties.

- The EDR Management Team may identify trends that are not visible to staff involved in the day-to-day work in a specific area. This feedback may come from executive stakeholder meetings or from managers during project or product reviews. Difficulties in meeting dependencies, resource commitments, or schedule milestones are yet another indicator of potential risks.
- Status reports and team meetings provide a more informal occasion for risk identification. These reports include status of current and late tasks, as well as a discussion of issues and risks facing the status reporter. This is the primary vehicle for most of the project staff to participate in the process of identifying risks.
- Status-at-a-Glance/Roadmap meetings allow the managers to review the status of project activities to ensure the project is progressing as planned. These meetings may identify risks due to late tasks, dependency impacts, or resource conflicts.
- Deliverable reviews and events may lead project staff to identify risks. Project staff should always review deliverables in the context of the whole solution and not just as a standalone document or activity. When applicable, deliverables should include a section to discuss risks associated with the deliverable or process described in the deliverable
- Change Control Board meetings are another opportunity to actively consider risks related to changes or increases in scope. Every change that is considered should be evaluated for the risks and opportunities it presents and the impacts to the project as a whole. The Change Request Management Process itself should be closely monitored for effectiveness and efficiency, since poor performance or a large number of changes being processed can increase risk for the project.
- The State's PMO considers risk in the context of contract performance by the SP, Project Management Support Contractor (PMSC) and Independent Verification and Validation. Deliverable reviews, project reviews, submitted work products, and general day-to-day participation in activities must be considered to ensure the

respective contract requirements are being met, the project's quality standards are being adhered to, and that the State is receiving value for its contract investment as defined by the contract. In addition, the State's PMO considers risk in the context of the project budget, alignment with internal and external initiatives, and other State policies and practices.

- Individuals and teams outside of the project may also have unique, broader perspectives on risks that may not be as obvious to people with a single-project focus. One way to encourage outside input is to invite Subject Matter Expert (SMEs) from outside the project to participate in project reviews and walkthroughs, as well as Organizational Change Management meetings. Another way is to involve end users in such exercises. Finally, the State's IV&V vendor may identify risks based on their experience with other similar projects or concurrent State initiatives.

Regardless of how the potential risks are identified, project team members should be encouraged to discuss any potential threats or opportunities with their Lead/Manager, and the Lead/Manager should seriously consider potential risks.

2.1.3. Risk Analysis

When a risk has been identified by a team member, the Lead/Manager discusses the risk with the team member and determines a course of action. If the risk is valid and determined to be a threat to or opportunity for the project, the Lead/Manager and the team member (as the Risk Originator) work together on an initial risk assessment, based on the information available. Risks are evaluated using qualitative methods (i.e., using probability and impacts to prioritize the risk). Where appropriate due to the type or severity of the risk, quantitative methods may be used to supplement the qualitative methods.

Project-level risks are managed through the processes defined below. Once a risk is classified as a Project-level risk, it is then submitted for tracking and management as described below. Project-level risks are those that involve both State and SP staff, cut across multiple disciplines, involve external project stakeholders, and involve Legacy Systems such that the risk specifically affects the EDR project.

Risk Analysis involves the following activities:

- Validate and Document Risk
- Review Risk for Process Compliance
- Enter Risk in Tool
- Review and Prioritize Risk
- Update Risk in Tool
- Perform Risk Analysis

2.1.3.1 Step #2: Validate and Document Risk

The Risk Originator and his/her Lead/Manager discuss the potential risk and determine if the risk is valid. A valid risk meets the following criteria:

- Describes a concern or opportunity for the project that is uncertain and does not have a definite answer or response (refer to the definition of a risk in Section 1.5);

- Describes a real situation that could occur on the project (i.e., is not theoretical or vague);
- Describes a situation that can be managed or influenced by the project or project stakeholders; and
- Is not already addressed by another risk or issue.

If the Risk Originator and Lead/Manager determine the risk to be valid, the Risk Originator's Lead/Manager then completes the Risk Statement Form (contained in Appendix A, and available in the EDR Project Repository). The form requires a description of the risk and the potential effects. The risk statement title should be stated in terms of "concern-likelihood-consequence", followed by a more in-depth discussion of the risk and rationale for the concern, as necessary. In addition, the Originator's Lead/Manager classifies the effects of the risk should it occur, including the probability, impact, and timeframe which leads to an assessment of risk exposure.

Probability Scale (Likelihood)

The Risk Originator and Lead/Manager estimate the probability of the risk occurring, according to the following definitions from the CA-PMM.

Table 3. Probability Scale

Value	Percentage of Probability	Description
1	Less than 20%	Unlikely
2	21 – 40%	Somewhat Likely
3	41 – 60%	Likely
4	61 – 80%	Very Likely
5	Greater than 80%	Most Likely

Impact Scale

The Risk Originator and Lead/Manager estimate the impact of the risk, assuming that it occurs, according to the following criteria from the CA-PMM.

Table 4. Impact Scale

Value	Degree of Impact
1	Less than 5% change to scope, schedule, budget or quality baselines[1]
2	5 – 10% change to scope, schedule, budget or quality baselines
3	11 – 15% change to scope, schedule, budget or quality baselines
4	16 – 24% change to scope, schedule, budget or quality baselines
5	25% or greater change to scope, schedule, budget or quality baselines

[1] The EDR Project baselines are identified in the EDR Scope Management Plan.

Note that if a risk has a positive effect (an opportunity), this value may be misleading. In these cases, the description and rationale in the risk statement should describe what impacts are positive and negative to clarify how this value should be interpreted. For instance, if there is an opportunity to reduce the duration of a set of tasks that equate to a 10% reduction in the schedule, the risk statement needs to clearly indicate this is a positive effect and not a negative effect (as the impact is usually interpreted).

Timing

The Risk Originator and Lead/Manager estimate when a risk response must occur, according to the following criteria from the CA-PMM.

Table 5. Timeframe

Value	Timeframe When Action Is Required
1	Within the next six months[2]
0.66	Six months to a year from now
0.33	More than a year from now

The probability, impact and timing are used to calculate the risk exposure when the data is entered into the Risk Tool.

2.1.3.2 Step #3: Review Risk for Process Compliance

The Originator's Lead/Manager submits the Risk Statement to the Risk Manager for his/her organization. State team members submit their Project-level risks to the State Risk Manager, and SP team members submit their Project-level risks to the SP Risk Manager.

The State and SP Risk Managers review the risks submitted to them by their organization's team members. The Risk Managers review the Risk Statement to ensure the risk is:

- Valid and timely
- Worded appropriately
- Correctly documented
- Does not duplicate an existing risk
- Does not inappropriately re-open an already closed risk
- Provides sufficient information required to create the risk in the Risk Tool

If the risk has not been submitted in accordance with the process or if the risk needs clarification, the Risk Managers work with the Originator's Lead/Manager to update the Risk Statement. If the PMO Managers determine that a Risk Statement is not valid, the Risk Manager notifies the Originator's Lead/Manager and advises him/her of the PMO Managers concerns or direction (for example, it may be an issue not a risk).

The SP and State PMOs discuss new risks and follow up on the status of existing risks and their risk response actions within their respective organizations. To support these discussions, the Risk Managers generate the risk reports from the Risk Tool.

[2] Both the Risk Statement From and Risk Response Plan Form indicate a fourth category of "immediately" to identify items requiring expedited response. Risks in this category will be assigned a value of 1.

2.1.3.3 Step #4: Enter Risk in Tool

The Risk Managers work with the Originator's Lead/Manager to obtain any needed clarification. The Risk Manager for each organization enters new risks in the Risk Tool with a status of "Identified". The Risk Tool uses the formulas in Section 3.1.6 of the CA-PMM, to calculate the risk exposure level for the newly entered risk. The Risk Manager stores the Risk Statement Form in the EDR Project Repository using the risk number as the file name.

The SP Risk Manager prepares a risk summary report for discussion at the EDR Management Team Risks and Issues meeting. The EDR Management Team may also requests these reports to prepare for the weekly meeting and familiarize themselves with any new risks in advance of the meeting.

2.1.3.4 Step #5: Review and Prioritize Risk

The EDR Management Team reviews new risks, high or medium exposure risks, critical or major priority risks, and risks with changes to status or action plans on a biweekly basis, and open risks on a bi-annual basis. As part of the review of the risk, the EDR Management Team considers:

- The ability of the project to manage the risk
- The risk exposure against the risk tolerance thresholds
- The risk exposure relative to other projects risks (priority)

The State Risk Manager presents risks raised by State team members, and the SP Risk Manager presents risks raised by SP team members.

Degree of Control

In considering the ability of the project to manage the risk, the EDR Management Team estimates the relative control that can be exerted on the probability of the risk occurring, and the project's ability to control the risk. Degree of control values are:

- Total direct control: The risk is completely within the control of the project. Examples include allocation of project resources or staffing.
- Moderate, 'hands-on' control: The risk may be controlled within the project but there are limits to the amount of control that may be exerted.
- Shared or partnered control: The risk incorporates elements that are both internal and external to the project. Examples include relationships with third-party vendors.
- Minimal realistic control: The project can exert some degree of control, but the majority of control resides outside of the project.
- No control: The project has little or no control over the risk. Examples include business disruption or regulatory changes.

In the case of minimal or no control, the best approach may be to escalate the risk to a higher level, if the risk has a high probability and/or high impact. Degree of control is a useful input to determine an appropriate risk response. Refer to Section 2.1.4.1 for an explanation of how the selection of a risk response strategy is related to the project's degree of control.

Security/Sensitivity

The EDR Management Team also considers the sensitivity of the risk. If the risk is determined to be sensitive or confidential in nature, the risk is marked as such in the Risk Tool and the associated documents and/or data are stored in a secured folder on the EDR Project Repository that is restricted to the EDR Management Team. In these cases, one of the PMO Managers is assigned as the Risk Owner and is responsible for analyzing, statusing and managing the risk. The EDR Management Team indicates if any other team members are authorized to view the risk and may dictate specific instructions on risk handling and dissemination.

Priority

The EDR Management Team assigns a priority to the risk, based on the potential impact to the project, the probability of occurrence, and the timing when action is needed. The priority focuses on when Risk Management action is required. Values are:

- Critical – Risk Management action required within one week
- Major – Risk Management action required within one month
- Minor – Risk Management action required within 90 days

The priority level is used to guide the allocation of time and resources to management of the risk. The priorities are reviewed at least bi-annually and adjusted based on the status of the risk/risk response actions, the risk timeframe, and the available resources.

Assign Risk Owner

If the risk requires further analysis and action, the EDR Management Team assigns a Risk Owner to work on further risk analysis and risk response planning. In some cases, the EDR Management Team may indicate a preferred risk response strategy or set of actions based on current knowledge of the risk. The Risk Owner should be an individual who has in-depth knowledge of the risk's project area (for example, a legacy system), discipline or influencing factors, and is not necessarily the Risk Originator. However, the Risk Owner should have the authority to make risk decisions and interact with key project stakeholders.

Escalated and External Risks

The EDR Management Team also evaluates whether the risk can be effectively managed and controlled at the EDR Management Team level. Due to the nature, timing, or impact of the risk, the EDR Management Team may determine that the risk would be more properly managed at a higher level, as determined by the project 's executive management governance structure. In these cases, the EDR Management Team assigns a Risk Owner at the appropriate level.

The risk may also be identified as External, meaning that it has impacts beyond the EDR Project or that assistance from an outside organization is required to respond to the risk. In these cases, the EDR Management Team assigns the risk to the State EDR PMO Manager for coordination and resolution with the external partner. The risk remains in the Risk Tool and continues to be tracked by the Risk Manager until successfully mitigated or closed.

2.1.3.5 Step #6: Update Risk in Tool

The Risk Manager of the respective organization then changes the status of the risk from “Identified” to “Assigned” and updates other fields as indicated by the EDR Management Team. The Risk Manager notifies the Risk Owner of his/her responsibilities via e-mail based on the EDR Management Team’s decisions.

2.1.3.6 Step #7: Perform Risk Analysis

The primary objective of risk analysis is to better understand and document the nature, the likelihood, and the consequences of the risk. Different approaches to risk analysis apply under different circumstances, since risks may vary significantly. By performing risk analysis, the Risk Owner expands the risk-related data past the initial risk assessment to guide the selection of an appropriate risk response. The Risk Owner is the individual responsible for performing and coordinating the analysis, but other staff and SMEs may assist with the analysis and development of the Risk Response Plan.

As a first activity in Risk Analysis, the Risk Owner verifies the initial assessment of impact, probability, timeframe, and degree of control. If the initial assessment proves incorrect, the Risk Owner notifies the Risk Manager for his/her organization so that the revised assessment may be reviewed at the next EDR Management Team Risks and Issues meeting.

Root Cause Analysis

The Risk Owner performs a root cause analysis of the risk to determine the underlying conditions that could lead to the risk. The general approach is a stepwise refinement of the risk statement to consider why and how different factors contribute to cause the risk. Example questions used in the root cause analysis are:

- Why would this event happen?
- What would cause this?
- What existing conditions permit this?

This analysis further refines the definition of the original risk into more detailed, specific statements, potentially resulting in the identification of additional, related risks. In addition, the root cause projection identifies opportunities for corrective actions and potential responses that may be used to eliminate the risk.

Other analysis techniques may be used, as needed, to determine the factors influencing the risk and the options for monitoring and control. Typical techniques include decision analysis (decision trees), cause and effect analysis (fish-bone diagrams), risk factor checklists, risk relationship mapping, or use of Pareto diagrams. The Risk Owner determines which analysis techniques to use based on his/her judgment and consultation with his/her Lead/Manager and the Risk Manager, as needed. In some cases, the EDR Management Team may indicate certain techniques to be used based on past experience or the specific risk characteristics.

Identifying Risk Indicators and Risk Triggers

The Risk Owner then identifies risk indicators that provide insight into the status of the risk. These indicators should be relevant to the risk, easy to collect, and/or easily derived or calculated.

Finally, the Risk Owner identifies risk triggers. These risk triggers provide thresholds for the risk indicators that specify when an action (such as implementing a mitigation or contingency plan) may need to be taken. Risk triggers should provide early warning and adequate time to take appropriate action and should not initiate actions unnecessarily.

2.1.4. Risk Response Planning

Once the cause of the risk is understood, the Risk Owner then formulates a Risk Response Plan (RRP) to address the risk, unless the EDR Management Team indicated a response plan is not necessary (for example, for low probability risks). The plan describes the steps to be taken in the event the risk indicators reveal that risk probability is increasing or in the event of actual risk occurrence.

The Risk Owner is responsible for documenting actual risk responses, measurements, and the RRP, as well as determining when these plans and strategies need to be initiated. The Risk Owner may conduct further risk analysis (such as forecasts of potential cost or schedule results) to validate the risk assumptions or to evaluate potential risk response actions.

Risk Response Planning involves the following steps:

- Develop Risk Response Plan
- Review and Approve Risk Response Plan
- Update Risk in Tool

2.1.4.1 Step #8: Develop Risk Response Plan

The Risk Owner develops the RRP based on the results of the root cause analysis and the priority of the risk. The risk response plan must include the following:

- A description of the risk to be addressed
- The risk response strategy
- Specific monitoring criteria and methods to collect the data
- How and when the risk response action(s) will be initiated
- How and when (frequency) the risk response action(s) will be tracked
- The desired effect and how to tell if the response actions are working
- What will cause the response actions to cease

The Risk Owner is responsible for developing the RRP, but may consult with other project staff and SMEs to develop the plan and strategy. This is particularly true for risks involving technical concerns, where the Risk Owner may consult with appropriate technical SMEs for assistance. The Risk Owner must consider the effects to the schedule, project cost and benefits, resources, and quality when developing the plan.

Determine Risk Response Strategy

Risk response strategies attempt to reduce the negative impact of the occurrence of a risk (or increase the potential for an opportunity) and usually consist of one of the following, as guided by the risk tolerance thresholds:

- Risk Avoidance – Risk avoidance generally entails changing the project schedule or solution approach to eliminate the risk or condition.

- Risk Transfer – If the project has little or no control over the risk, transferring may be appropriate. It is important to note that transferring the risk simply gives another party responsibility for its management; it does not eliminate the risk.
- Risk Mitigation – Risk mitigation involves identifying actions for reducing the effects of the risk. Risk mitigation seeks to reduce the probability and/or consequences of a risk event to an acceptable threshold.
- Risk Acceptance – The project may choose to accept the risk if the predicted probability and impact are considered acceptable when compared to the cost of risk response alternatives, or if the risk is unlikely to be affected by any mitigation activities. In some cases, a contingency plan still may be prepared to address the risk in the event it does occur.

It is important to determine the appropriate strategy first, then to design the risk response to implement that strategy. There are several factors to consider when choosing the right strategy, including the type and nature of the risk, determining whether it is amenable to reduction or control, the severity of the impact, available resources, and cost-effectiveness.

Avoidance strategies are considered first. Transfer is investigated next, though the potential for this option is often limited. The next choice is Mitigation, leaving Acceptance as a last resort for risks that cannot be addressed by any other strategy. Once a risk response strategy is selected, the other strategies should be kept in mind in the event the original risk strategy fails or project conditions change. In some cases, a tiered or multi-step strategy may be developed based on how well the original strategy does or does not reduce the risk.

Depending on the nature, severity, and timing of a particular risk, the Risk Owner may decide that it is also necessary to create a contingency plan.

Risk Avoidance Responses

Risk avoidance is appropriate in situations where the project has no direct control over the risk or when it is the most cost-effective means to deal with the risk. The Risk Owner can apply two types of responses to achieve a risk avoidance strategy—direct and indirect.

A direct response is suitable for risks that arise from uncertainty or ambiguity. In this situation, the risk response action is to eliminate the cause of the uncertainty. The following are examples of risk actions that lead to eliminating ambiguity:

- Clarifying requirements
- Defining objectives
- Improving communication
- Conducting prototyping

Indirect avoidance responses include completing the affected activity in a different manner, so that the threat is eliminated or reduced as much as possible. Early in the project, strategic decisions can be made, such as building redundancy into the project design, to avoid risky elements. Indirect avoidance responses become less effective as

the project progresses, since the ability to affect project scope and planning is diminished.

When considering risk avoidance, the Risk Owner must consider the following:

- Does the project have the authority and ability to avoid the risk?
- What are the cost, schedule and resource impacts of avoiding the risk?
- Are there staff with the appropriate skills available to implement the risk avoidance strategy?
- Are there scope, quality or organizational impacts to the risk avoidance strategy?
- What is the probability the risk avoidance strategy will be successful?
- Will this avoidance strategy avert the risk, or simply delay the risk until later in the project?
- Is the effort (cost, schedule, resources) required to avoid the risk worth the desired result?
- What other risks are created by choosing the avoidance strategy?

Risk Transfer Responses

Risk transfer is appropriate when the project has little or no control over the risk. Risk transference moves the responsibility for management of the risk to the party best positioned to analyze and respond to the risk, based on their expertise and level of authority.

If a risk is to be transferred, it is critical that the recipients of the transferred risk have the means to manage the risk allocated to them. This includes having the responsibility, authority, resources, and knowledge to own the transferred risks. Without this, the project remains exposed to an open, uncontrolled risk.

When considering this strategy, the Risk Owner must consider the following:

- What level of the organization would need to manage this risk?
- What is the likelihood that the organization would accept responsibility for the risk?
- Does the organization have the resources and skills to manage the risk?
- How will the project know if the organization's risk response actions were effective?
- What would be the effect on the project if the organization failed to manage the risk?

In many cases, the project still needs to monitor the transferred risk to determine if the transference strategy is having the desired effect on the project. A Risk Owner from the project should be assigned to coordinate the monitoring of the RRP results with the Risk Owner in the other organization.

Risk Mitigation Responses

Risk mitigation, the most common response to an identified risk, is the process of reducing the size of the risk exposure. This can be performed by either reducing the likelihood of the risk occurring, reducing the potential impact of the risk, or both.

A proactive approach of reducing the likelihood of the risk occurring is preferred over a curative approach. Taking early action to protect against the worst effects of the risk can make the risk more reasonable to accept.

Risk mitigation is specific to an individual risk since it addresses both the cause of the risk and its effects on project objectives. The mitigation strategy may involve modifications to the project approaches, the project schedule or procedures, staffing profiles, or other aspects of the project.

The Risk Owner must evaluate the mitigation cost and compare it to the cost of bearing the original risk. If the mitigation cost outweighs the cost impact of the risk, then an alternative response should be found.

A risk mitigation plan contains the following information:

- Mitigation plan objective
- Early warning signs (indicators) that the mitigation plan is needed
- Thresholds and values (triggers) that cause the mitigation plan to be put into effect
- Approval necessary to implement the mitigation plan (if any)
- Indicator values that will be used to monitor the effectiveness of the mitigation activities
- Indicator values that signal when the risk mitigations have been effective (and mitigation actions may cease)
- Thresholds and values (triggers) that signal a need to execute a contingency plan (if appropriate)
- Owner for the mitigation plan
- Specific actions to be taken, due dates and ownership/assignments
- Any impacts to cost or schedule or resources
- Criteria for escalation to management (if appropriate)

Risk Acceptance Responses

Risk acceptance is the remaining option if avoidance, transfer, and mitigation strategies are not appropriate. Risk acceptance involves planning for ways to deal with the risk event if it occurs, rather than trying to influence its probability or impact. In particular, risk acceptance is useful in situations where any response is not cost-effective compared to bearing the cost impact of the risk occurrence, such as low impact, low probability risks (which are neither very likely nor very critical). If the risk can be recognized and accepted, the response can either be passive with no action to be taken, or active by adoption of a response in the case of the risk event occurring. The most typical risk acceptance response is contingency planning.

When considering risk acceptance, the Risk Owner must consider the following criteria:

- What are the cost, schedule and resource impacts of accepting the risk (i.e., doing nothing right now)?
- What are the cost, schedule and resource impacts if the risk does occur?
- Are there scope, quality or organizational impacts if the risk occurs?
- Would the risk occurrence be a one-time event, or would the risk event be a recurring problem throughout the project?

- Is the effort (cost, schedule, resources) required to address the risk if it occurs commensurate with the probability and impact levels (as currently understood)?
- What other risks are created by choosing the acceptance strategy?

Risk Escalation

If the root cause analysis indicates the risk cannot be influenced by the project team, the risk is escalated to the management level that has the authority to influence the risk.

The escalation levels are as follows:

- EDR Management Team - Risks that exceed the risk tolerance thresholds are escalated to the EDR Management Team for resolution and management.
- EDR Steering Committee – Risks that cannot be influenced and managed at the EDR Management Team level are escalated to the Steering Committee.

Generally, high exposure risks and external risks are discussed at the Steering Committee meetings. For risks that are escalated, the Risk Manager continues to manage and track the risk in the Risk Tool, and the risk is included in the agenda items for the appropriate Committee meeting. If more frequent monitoring is needed, the State PMO Manager coordinates with the appropriate Committee member to monitor and track the risk.

When considering risk escalation, the Risk Owner must consider the following:

- Does the project have the authority and ability to avoid the risk?
- What specific activities are required of the executives? Is it feasible for them to perform the activities?
- How much lead-time is needed for the executives to influence the risk and is sufficient lead-time available?
- How could the project determine if the escalated risk response actions were effective?
- Are there organizational change impacts to the risk escalation strategy?
- Is the effort (cost, schedule, resources) required to avoid the risk worth the desired result?
- What other risks are created by choosing the escalation strategy?

Develop Contingency Plan

The purpose of contingency planning is to define the actions that are taken if a risk consequence occurs, or if the impact of a risk is greater than expected. A risk contingency plan contains the following information:

- Contingency plan objective
- Early warning signs (indicators) that the contingency plan is needed
- Thresholds and values (triggers) that cause the contingency plan to be put into effect
- Indicator values that will be used to monitor the effectiveness of the contingency activities

- Indicator values that signal when the contingency activities have been effective (and the activities may cease)
- Approval necessary to implement the contingency plan (if any)
- Owner for the contingency plan
- Specific actions to be taken, due dates and ownership/assignments
- Any impacts to cost, schedule or resources
- Criteria for escalation to management (if appropriate)

Not every risk on the project requires a contingency plan, but it is important to have the details of the contingency plan mapped out in advance of a risk occurrence in case the risk response strategy fails to meet expectations. The contingency plan is the last defense against the risk. Additionally, the plan can prevent subsequent effects on other areas of the project and help to restore control. Generally, contingency plans are required for high or medium exposure risks, critical and major priority risks, and risks with an impact estimated at 25% or greater change to schedule, scope, budget or quality.

2.1.4.2 Step #9: Review and Approve Risk Response Plan

Once the Risk Owner completes work on the risk response strategies and plan, he/she notifies the Risk Manager of the respective organization, via e-mail, that the RRP is ready for review. The Risk Manager adds the RRP to the agenda for the next EDR Management Team Risks and Issues meeting.

The Risk Manager for each organization generates materials for newly developed RRPs in preparation for the biweekly EDR Management Team Risks and Issues meeting. The Risk Managers present the RRPs to the EDR Management Team for discussion.

The EDR Management Team is responsible for reviewing the risk response plans for:

- Completeness
- Feasibility of the actions
- Ability to monitor the triggers and effectiveness
- Reasonableness of the plan in context of the risk impact, probability of occurrence, and timeframe
- Availability of resources with the necessary skill sets to perform the risk response actions

The RRP must include specific, feasible tasks, due dates, and indicate the responsible party for the action. In some cases, the responsible party may be the EDR Management Team.

The EDR Management Team determines if the RRPs are appropriate and may make changes to the risk response actions. The EDR Management Team also considers the resource commitment needed for the RRP and, if necessary, identifies additional resources (beyond the Risk Owner) to perform the necessary actions should the need arise. If the risk response does not appear sufficient to reduce the risk exposure, the EDR Management Team may request that a contingency plan be developed to supplement the response plan. If the plan is incomplete or does not meet the criteria

above, the Risk Manager returns the plan to the Risk Owner for refinement or correction.

2.1.4.3 Step #10: Update Risk in Tool

If the proposed RRP is approved, the Risk Manager changes the status of the risk in the Risk Tool. If revisions are required, the Risk Manager works with the Risk Owner to revise the plan, as needed. The Risk Manager updates the risk information in the Risk Tool to indicate the strategy being applied (Avoid, Transfer, Mitigate, Accept) and summarizes the triggers and monitoring criteria. If necessary, the Risk Owner revises the RRP, updates the version in the EDR Project Repository, and notifies the Risk Manager that the RRP has been updated.

If additional resources are required to initiate the RRP, the PMO Managers work with the Risk Owner and appropriate other managers to coordinate when and how the resources are notified and the actions for which they are responsible.

If the response is to transfer the risk, the Risk Manager notifies the new Risk Owner of the risk via email and works with the new Risk Owner to ensure the risk is monitored and an RRP is developed by the new Risk Owner.

If appropriate, the Risk Owner works with the Schedule Analyst from the appropriate organization to update the project schedule to include any new or modified tasks, dependencies or resources as a result of the approved RRP. The schedule is updated using the process described in the *EDR Time and Schedule Management Plan (MRD001B)*. If the approved risk strategy has spawned other risks, issues, changes or action items, the Risk Owner is responsible for initiating these other items in accordance with the appropriate project management process.

2.1.5. Risk Tracking and Control

After a risk response strategy has been selected and an RRP has been approved, the Risk Owner begins monitoring the task according to the RRP. In some cases this involves immediate implementation of risk response actions, while in other cases risk response actions may not occur until a specific trigger is reached. If the RRP is not triggered until later, the Risk Owner monitors the risk until the early warning signs indicate the response plan must be implemented (at which point the schedule will be updated if appropriate), or until the timeframe for the risk occurrence has expired.

If it becomes necessary to implement the risk response actions, the Risk Owner has the primary responsibility for performing and coordinating the actions, as well as monitoring whether the actions are having the desired effect. The Risk Owner is responsible for coordinating how risk response activities are implemented and integrated with existing project plans and associated management processes and activities. Additionally, Risk Owners will coordinate the process to manage appropriate work products under appropriate levels of configuration management. If the desired effect is not being achieved, the Risk Owner may work with the Risk Manager to update the RRP and obtain approval for the change in approach from the EDR Management Team. In certain circumstances, it may be necessary to escalate the risk to the EDR Management Team (or higher) if a risk appears imminent. The risk response actions continue until:

- The risk is successfully eliminated

- The risk's exposure (probability or impact) drops to an acceptable level
- The risk occurs and becomes an issue or is accepted

Risk Tracking and Control involves the following activities:

- Monitor and Report Risk Status
- Execute Risk Response Plan
- Monitor Effectiveness of Risk Response Plan
- Update Risk Status and Actions in Tool

2.1.5.1 Step #11: Monitor and Report Risk Status

Risks are monitored to determine whether a risk trigger or threshold is exceeded, whether the risk timeframe has passed, and whether the risk no longer warrants monitoring.

Risks are monitored on an ongoing basis as long as the risk trigger or threshold is not exceeded, the risk timeframe has not passed, and the risk warrants monitoring. If a risk trigger or threshold is exceeded, the risk response plan is executed. If a risk trigger or threshold has not been exceeded and if the risk timeframe has passed or the risk no longer warrants monitoring, the risk is closed.

Risks are monitored at two levels:

- Risk Owner Monitoring: Individual risks are monitored by the assigned Risk Owners.
- Management Monitoring: The EDR Management Team monitors the overall risk profile of the project and adjusts assignments and direction, as necessary, to ensure project risks are managed.

2.1.5.2 Risk Owner Monitoring of Assigned Risk

Once the RRP is approved, the Risk Owner begins monitoring the risk indicators. The Risk Owner is responsible for monitoring the risk indicators as required by the approved RRP, and recording the results of monitoring in the RRP. If there are changes to the risk status or if a trigger is reached, the Risk Owner notifies the Risk Manager who updates the status in the Risk Tool.

At least monthly or as directed by the approved RRP, the Risk Owner reviews the risk to determine if the risk is still a valid risk or if the circumstances contributing to the risk no longer exist. The Risk Owner includes the rationale and current status of indicator/trigger values in the updates. If the Risk Owner believes the risk is no longer a threat or if the opportunity has passed, the Risk Manager should be notified and the risk will be considered at the next EDR Management Team Risks and Issues meeting.

2.1.5.3 Management Monitoring of Assigned Risks

New risks, high or medium exposure risks, critical or major priority risks, and risks with changes to status or action plans are monitored and discussed at the EDR Management Team Risks and Issues meetings. The status of the risk and the effectiveness of the response plan actions are reviewed including:

- Is the risk still valid?

- Has the nature of the risk changed?
- Has the timeframe for the risk changed?
- Are the risk triggers still appropriate?
- Is the response plan having the desired effect to probability and/or impact?
- Does the severity of the risk still warrant monitoring?
- Are there sufficient resources being applied to the risk?
- Can the risk still be influenced at this level or should it be escalated?

Any changes or recommendations are noted in the meeting minutes. The Risk Manager updates the Risk Tool based on the meeting minutes and notifies the Risk Owner of any changes.

2.1.5.4 Step #12: Execute Risk Response Plan

When a mitigation or contingency plan trigger is reached, the Risk Owner notifies the Risk Manager who updates the Risk Tool to indicate the response plan has been activated. The Risk Owner works with the Schedule Analyst for their organization to add tasks to the project schedule, if appropriate, and notifies other team members and their Lead/Manager of their risk response assignments, as appropriate.

The Risk Owner then proceeds to execute the actions from the approved RRP. The Risk Owner is responsible for ensuring the risk actions are performed by the assignee in accordance with the defined due dates, and reporting the status and results of the actions as directed by the approved RRP. The Risk Owner is responsible for ensuring the risk response tasks in the project schedule are statused and updated appropriately.

2.1.5.5 Step #13: Monitor Effectiveness of Risk Response Plan

The Risk Owner coordinates the risk response actions and monitors whether the response is having the desired effect using the indicator values described in the RRP. The Risk Owner notifies the Risk Manager of the status and effectiveness as directed in the approved RRP and, if there are changes in status, the Risk Manager updates the Risk Tool with the status. The monitoring and response actions continue according to the plan, until either the desired state has been reached, the trigger for escalation or closure has been reached, or the risk conditions have changed sufficiently that a new response must be developed.

The Risk Manager updates the Risk Tool with the status of the response actions which are reviewed at the EDR Management Team Risks and Issues meeting. Changes in overall risk status (probability, impact) are presented to the EDR Management Team.

Update Risk Response Plan

There are several instances where a revised RRP may be needed, including:

- The RRP is not having the desired effect
- The RRP has exceeded a indicator/trigger and the contingency plan or escalation is needed
- The risk has changed due to other circumstances and the current RRP is no longer applicable (such as an assumption that was proved wrong or a change in influencing factors)

If the Risk Owner or Risk Manager determines the need to update the RRP, then the current plan is retired and a revised RRP is created. The revised RRP must indicate the reason for the revision and what problem the new RRP is trying to address. The revised RRP must be reviewed and approved as described in Section 2.1.4.2, and the revised RRP is stored in the EDR Project Repository as a new version. The Risk Owner works with the Schedule Analyst for their organization to add or revise risk response tasks in the Project Schedule, as appropriate. The Risk Owner also notifies team members and their Leads/Managers of any changes to assignments resulting from the revised RRP.

Escalate Imminent Risks

For high exposure risks, the Risk Owner notifies the Risk Managers and PMO Managers when the risk occurrence is imminent or has occurred. The SP PMO Manager notifies the EDR Management Team and, if appropriate, additional resources may be assigned to execute the contingency plan or additional risk response actions. If necessary, the Risk Owner updates the RRP based on direction from the EDR Management Team.

During the process of monitoring risks, the Risk Owner must consider whether he/she is able to influence the risk and execute the RRP as approved. If the Risk Owner can no longer influence the risk, the risk should be escalated to the appropriate level that can influence the risk. The Risk Owner escalates the risk to the Risk Manager with an indication of the severity of the situation. The Risk Manager works with the PMO Managers to escalate the risk to the appropriate level of management. Depending on the severity of the risk, escalation may be immediate or may occur at the next management meeting.

Some typical reasons for escalating risks from the monitoring stage are:

- A high exposure risk is imminent or has occurred despite any response actions
- The mitigation/contingency plans are having no effect on the risk exposure (probability and impact)
- The risk's exposure is increasing
- The resources required to perform the risk response actions are unavailable or unable to perform the approved actions
- The nature of the risk has changed and the risk can no longer be influenced by the EDR Management Team
- The EDR Management Team requested the risk to be escalated when certain indicators/triggers have been reached (according to the approved RRP)

The State EDR Project Director determines which high exposure risks should be presented at the Management Performance Reviews or at the EDR Steering Committee meetings.

2.1.5.6 Step #14: Update Risk Status and Actions in Tool

Throughout the risk monitoring process, the Risk Manager updates the status of the risk and the RRP actions in the Risk Tool based on updates from the Risk Owner. The State Risk Manager tracks and updates the Tool for State Risk Owners and the SP Risk Manager tracks and updates the Tool for SP Risk Owners.

2.1.6. Risk Resolution and Closure

Eventually, the risk is closed and the results of the risk response are documented to assist with managing future risks.

Risk Resolution and Closure involves the following activity:

- Close Risk in Tool

2.1.6.1 Step #15: Close Risk in Tool

A risk is closed when one of the following occurs:

- The risk was successfully mitigated, avoided or transferred and the consequences were eliminated
- The risk's impact and/or probability has been reduced to an acceptable level
- The timeframe for the risk has passed and the risk is no longer likely or valid
- The risk has occurred and has become an issue or has been accepted
- The risk circumstances have changed and this risk is being closed in favor of a new risk or issue

When this occurs, the Risk Owner updates the RRP to indicate the results of the risk response actions and forwards the information to the Risk Manager for their organization. The Risk Manager updates the information in the Risk Tool to close the risk and notifies the PMO Managers of the risk closure request. The PMO Managers review the risk for closure and if appropriate, direct the Risk Manager to close the risk.

If the PMO Managers disagree with the risk closure, the Risk Owner is notified to continue the current risk response actions. The Risk Managers discuss the risk at the next EDR Management Team Risks and Issues meeting. The Risk Manager of the appropriate organization notifies the Risk Owner of the EDR Management Team decision. The Risk Manager updates the Risk Tool with the decision based on the meeting minutes. The Risk Owner works with the Schedule Analyst for their organization to update any risk response tasks in the Project Schedule, as necessary. If necessary, the Risk Owner generates an issue, change request or new risk using the appropriate project management process, indicating the item is being opened as a result of the closure of this risk.

Conduct Risk Result Evaluation

If the risk response was not successful, the EDR Management Team may direct the Risk Owner to perform an analysis to determine why the response was not effective and what contributed to the failure. The purpose of the analysis is to determine how to address the risk in the future should it or a similar risk occur. The Risk Owner reviews the original root cause analysis and conducts a new analysis to determine the source of the failure. Some of the reasons may include:

- Inaccurate assumptions
- Incomplete information or more complex problem than originally understood
- Wrong or misleading indicators/triggers or data sources for monitoring
- Improper timing of response actions (too soon or too late)

- Insufficient resources to implement the response actions
- Attempting to manage the risk at the wrong level

The Risk Owner documents the results of the analysis in the RRP. A synopsis of the analysis is entered into the Risk Tool by the Risk Manager for historical purposes. The RRP is stored in the EDR Project Repository as a new version, along with any supporting documentation for the analysis. Any lessons learned that are applicable to the risk process or general management is submitted to the SP Quality Team's lessons learned database.

2.2. Monitor Risk Process Effectiveness

The Risk Managers work with the PMO Managers and SP Quality Manager to monitor the effectiveness of the Risk Management Process. The Risk Managers and PMO Managers review the risks in the Risk Tool bi-annually to ensure areas of the project are submitting risks appropriately. The team considers, for instance:

- Is the process being followed?
- Are potential risks reviewed with Leads/Managers and validated appropriately before being entered into the Risk Tool?
- Are the risk tolerance thresholds being applied correctly and consistently?
- Is the process, as documented in the plan, accurate or are there other activities or dependencies that were not considered?
- Is the necessary data being captured and is it complete and accurate?
- Is the risk process documentation (i.e., risk forms, risk response plans) being completed appropriately and in accordance with the instructions (e.g., no blank fields)?
- Are status updates being made on schedule and are the updates clearly described?
- Are the risk reports useful and easy to read?
- Are the risk metrics meaningful and useful?
- Are the participants able to keep up with the workload?
- Are certain activities taking a long time to complete?
- Does the tool need to be corrected or improved to streamline the process?
- How can the risk process be made more effective or less cumbersome (process improvements)?

The team reviews the results and discusses how to implement corrections or improvements. The SP Risk Manager updates the Risk Management Plan, associated forms, the Risk Tool, and/or risk training materials to incorporate corrections or improvements. The revised versions are stored in the EDR Project Repository, and the PMO Managers announce any changes to project staff via email. If appropriate, training sessions may be held using the revised training materials and/or may be held for certain project areas which appear to need refresher training.

2.3. Procedures

The Risk Management Procedures are summarized in Table 6.

Table 6: Risk Management Procedures

Step	Role	Timeframe	Description	Tool/Template	Output
1a. Conduct Initial Risk Assessment	State and SP Risk Managers	After Risk Management Plan is Approved	Conduct interviews or focus groups to identify early project risks	• None	• Initial Risk List
1b. Conduct Periodic Risk Assessments	State and SP Risk Manager	At the start of each Design Stage	Review current risks for continuing validity, identify new risks for the Design Stage, and adjust thresholds, as needed	• Risk List	• Updated Risk List • Updated Risk Thresholds, if necessary
1c. Conduct Ongoing and Ad Hoc Risk Identification	EDR Team Members	Daily	Identify potential risks/opportunities as part of day-to-day activities based on the definition of a risk in the Risk Management Plan	• Risk Statement Form	• Draft Risk Statement Form
2. Validate and Document Risk	Originator's Lead/Manager	As needed	Define nature of risk and document details	• Risk Statement Form	• Completed Risk Statement Form

Step	Role	Timeframe	Description	Tool/Template	Output
3. Review for Process Compliance	State and SP Risk Managers and PMO Managers	Biweekly	Verify risk is complete and valid	• Risk Statement Form	• Agenda item for EDR Management Team Risks and Issues meeting • Comments/ Revisions to Risk Statement
4. Enter Risk in Tool	State and SP Risk Managers	2 to 3 State business days after Risks and Issues Meeting	Enter Risk Statements into Risk Tool	• Risk Tool	• Risk number from Risk Tool
5. Review and Prioritize Risk	EDR Management Team	Biweekly	Review and prioritize new risks, assign Risk Owners, determine priority	• Risk List	• Assigned Risk Owners • Risk Priorities • Comments/ revisions to Risk Statements
6. Update Risk in Tool	State and SP Risk Managers	2 to 3 State business days after Risks and Issues Meeting	Update Risk Tool, notify Risk Owners of assignments	• Risk Tool • MS Outlook	• Update Risks in Tool • Email to Risk Owners
7. Perform Risk Analysis	Risk Owner	According to time frame and priorities assigned by EDR Management Team	Review risk documentation and conduct an analysis of risk drivers and influencing factors	• Various	• Various

Step	Role	Timeframe	Description	Tool/Template	Output
8. Develop Risk Response Plan	Risk Owner	Upon completion of risk analysis	Determine risk strategy, and, if appropriate, develop mitigation and/or contingency plan	• Risk Response Plan	• Completed Risk Response Plan
9. Review and Approve Risk Response Plan	EDR Management Team	Biweekly	Review and approve Risk Response Plan, verify/assign resources	• Risk List	• Approval of Risk Response Plan • Updates or corrections to Risk Response Plan • Additional assignments as necessary
10. Update Risk in Tool	State and SP Risk Managers	2 to 3 State business days after Risks and Issues Meeting	Update Risk Tool with management decisions and assignments	• Risk Tool • MS Outlook	• Update Risks in Tool • Email to Risk Owners and additional Assignees, if appropriate
11. Monitor and Report Risk Status	Risk Owner	As indicated in the approved Risk Response Plan	Monitor risk indicators and triggers, report status to Risk Manager	• None	• Status updates to Risk Managers

Step	Role	Timeframe	Description	Tool/Template	Output
12. Execute Risk Response Plan	Risk Owner	As indicated in the approved Risk Response Plan	Execute response actions in accordance with the approved plan	• None	• Notification to Risk Manager
13. Monitor Effectiveness of Risk Response Plan	Risk Owner	As indicated in the approved Risk Response Plan	Report status of risk response actions and risk indicators	• None	• Status updates to Risk Manager
14. Update Risk Status and Actions in Tool	State and SP Risk Managers	As indicated in the approved Risk Response Plan	Enter status updates in Risk Tool	• Risk Tool	• Updated Risk Tool
15. Close Risk in Tool	State and SP Risk Managers	2 to 3 State business days following Risks and Issues meeting	Confirm with EDR Management Team that risk is ready for closure, close risk in Risk Tool, evaluate results of risk strategy and response actions	• Risk Tool	• Updated Risk Tool • Analysis of Risk Result

3. RISK MANAGEMENT TOOL

The EDR Project uses the SP's PIMRA tool for tracking and managing risks. The SP PMO manages PIMRA which includes risk tracking, monitoring, and reporting functionality.

3.1. Description of the Tool

PIMRA is a web-accessible, collaborative application that provides modules for:

- Risk/Watch Point Management Module - Supports overall Project-level risk management as well as specific team, group and discipline Watch Points
- Issue/Action Item Management Module - Tracks the Project-level issues and action items
- Decision Point Management Module - Tracks the Decision Points put forward by the team, group, and discipline

PIMRA is pre-configured with a set of elements recommended to track and manage project risks. Following project start-up, the PMO Teams review the risk elements and the tool will be re-configured, as necessary, to meet EDR Project-specific needs. Table 7 provides a list of the basic elements recommended to manage risks when recording the risk in PIMRA. PIMRA will also capture appropriate data elements related to both the Risk Statement and Risk Response Planning forms.

Table 7. PIMRA Data Elements for Risk Management

Field	Description
Risk ID	A unique identifier used to reference the risk
Risk Title	The title appears on risk reports and should be brief but convey the risk threat/opportunity, preferably as "concern – likelihood – consequence" format
Date Identified	The date the risk was identified
Originator Name	The name of the individual who originally identified the risk
Risk Description	The description should contain detail sufficient to assess the risk impact and provide project stakeholders with an understanding of the risk
Risk Category	The risk categories are summarized from the California Technology Agency (TA) California Project Management Methodology (CA-PMM)
Timeframe for Action	This element indicates when a risk response must be performed in order to be effective. The value is used in the calculation of Risk Exposure Level.
Impact	This element is used to describe the impact to the project should the risk occur. Areas of the project that should be assessed relative to the risk include baselined requirements, scope, resources, budget, schedule, quality, and external agencies. The value is used in the calculation of Risk Exposure Level.

Field	Description
Probability	Probability is a quantitative or qualitative expression of the chances that a risk will occur. The value is used in the calculation of the Risk Exposure Level.
Risk Exposure Level	This is a calculated field. Exposure Level = Timeframe for Action times Impact times Probability. Reflects the risk level, showing how management of the risk is progressing. There are three levels indicating risk threat – Low (green, level 1-9), Medium (yellow, level 10-15) and high (red, level 16-25). The risk level is reviewed by the Risk Manager on a biweekly basis based on input from the Risk Owner following the biweekly EDR Management Team Risks and Issues meeting.
Risk Owner	The Risk Owner is assigned to a new risk by the EDR Management Team. The owner is responsible for managing aspects of the risk, including development of monitoring strategies and contingency plans. The owner may or may not be the originator of the risk, but should have the authority to make risk decisions and interact with key project stakeholders.
Date Assigned	Reflects the date that the Risk Owner was identified and assigned to the risk
Primary Risk Area	Describes the primary risk area (in terms of schedule, cost, scope or quality) that would be primarily affected by the risk
Project Discipline	Relates to the project disciplines/swimlanes such as Application Development, Business/Implementation, and Testing. The Risk Manager and/or PMO Manager determine which specific discipline is related to the risk.
Priority	Indicates how quickly action must be taken on the risk: Critical – Risk Management action required within one week Major – Risk Management action required within one month Minor – Risk Management action required within 90 days
Risk Response Type	Identifies the strategy (accept, avoid, mitigate, transfer) to be used to attempt to reduce the negative impact of the occurrence of a risk (or increase the potential for an opportunity)
Risk Response Description	Details the strategy (accept, avoid, mitigate, transfer) to be used to attempt to reduce the negative impact of the occurrence of a risk (or increase the potential for an opportunity)

Field	Description
Trigger	A trigger is an event that can be reasonably forecasted to signal that the risk is likely to occur. An example could be pending legislation that is in progress that will modify program policy which will in turn affect the EDR functional requirements. The trigger in this case is approval of such legislation.
Risk Status	The risk status element is maintained by the Risk Manager. The status is "Identified" upon the addition of a new risk, then "Assigned" once a Risk Owner has been identified by the EDR Management Team. In the event of risk mitigation or resolution, the status is changed to "Closed."
Date Closed	Records the date that the risk was closed. The Risk Manager closes the risk based upon instructions from the EDR Management Team and the Risk Owner. Closure criteria are noted in the PM Actions element on the Risk Page.

3.2. Features of the Tool

To assist with managing and tracking risks, PIMRA provides the following features:

- Management of risk data – PIMRA provides screens to create, modify and delete a risk, subject to appropriate access controls.
- Search functionality – PIMRA provides the ability to search the risk list based on multiple criteria, including key word.
- Convert risk to an issue – PIMRA allows users to convert the risk to an issue in the Issue Module.

3.3. User Accounts and Access Levels

The SP PMO is responsible for the security and administration of the tool. Initial users of the tool will be Leads and Managers. After the tool is installed at the project site, the State and SP will confirm the necessary users and access levels.

3.4. Risk Management Standards and Conventions

Risk naming conventions are as follows:

- R-NNNNN-Title – Numbering convention for Risk Statements. The "NNNNN" represents the number of the risk that is assigned sequentially by the State and SP Risk Managers and the "Title" is the title of the risk as it appears in the Risk Statement which should follow the Concern-Likelihood-Consequence format. The title may be summarized if necessary.
- RRP-NNNNN-Title – Numbering convention for Risk Response Plans. The "NNNNN" represents the associated risk number.

- Once a risk has been submitted to the Risk Manager, the risk is given a number and is reflected in the Risk Register.
- Risk numbers are unique and not re-assigned.

4. RISK MANAGEMENT COMMUNICATIONS

Risks are communicated to management through reports presented at management meetings. EDR project staff can access and print the reports directly from the EDR Project Repository.

The Risk Managers periodically scan through open risks looking for items that are outstanding past their targeted due dates.

The continuous documentation of risks should occur from the beginning until the end of the project. The Risk Managers are responsible for validating that regular updates to the risk documentation in PIMRA are occurring. If the documentation is not current, the Risk Manager from the appropriate organization monitors the process and coordinates with the appropriate Risk Owner.

4.1. Risk Forms

The following are the forms used by the Risk Management Process.

- Risk Statement Form – The Risk Statement form will be used to document the initial risk statement. Refer to Appendix A.
- Risk Response Plan – This Risk Response Plan will be used to capture the risk response strategy and planned actions. Refer to Appendix B.

4.2. Risk Reports

The following section summarizes the risk reports used to monitor and manage the risk process. These reports are generated and tracked in the Risk Tool unless otherwise noted. Reports and forms, as well as risk statements and RRPs/status updates, are saved in the EDR Project Repository for historical purposes.

Open risks are discussed at the EDR Management Team Risks and Issues meeting bi-annually. New risks, high or medium exposure risks, critical or major priority risks, and risks with changes to status or action plans are discussed biweekly at the EDR Management Team Risks and Issues meeting.

The risk register report contains the list of the risks currently being managed by the project. The report will be statused and available biweekly for discussion at the biweekly Risks and Issues meeting. The risk level is a calculated field based on the probability, impact and timeframe of the risk, with possible values between 1 and 25 (1 is low, 25 is high). Fields contained in the Risk Register include:

- Risk ID
- Date Identified
- Originator Name
- Risk Title
- Risk Description
- Risk Category
- Timeframe for Action
- Impact

- Probability
- Risk Exposure Level
- Risk Owner
- Risk Response Type
- Risk Response Description
- Risk Status
- Date Closed

Risk trend reports summarize the current state of risks in the Risk Tool. This set of on-demand reports allows the user to select a date range and type of report (summary or detail) to select. The trend reports include:

- Number of open and closed risks by risk priority
- Number of open and closed risks by project area/discipline
- Number of risks submitted by project area/discipline
- Number of risks by status
- Number of risks by risk category
- Number of risks where the risk priority has been reduced compared to previous month's risk priority
- Number of risk response plans with actions behind schedule
- Risks with the highest risk priorities
- Risks identified by month
- Aging report for open risks

4.3. Metrics

The Risk Tool allows for the collection of various risk management metrics to gauge the effectiveness of the Risk Management Process which can then be used to communicate the status of the risk profile and identify opportunities for process improvement. The metrics include:

- Number of new risks identified – Indicates the effectives of risk identification and may act as a trigger for remedial risk and/or planning action.
- Number and/or percentage of risks reduced in probability/impact – Indicates the effectiveness of the RRPs over time.
- Number and/or percentage of risks requiring contingency plans – Acts as an overall indicator of the severity of risks facing the project.
- Number and/or percentage of risk events occurring – Provides the opportunity to use this data for purposes of continuous improvement of risk identification and risk response planning.

Additional metrics may be added during the life of the project to help diagnose process problems or to implement process improvements.

4.4. Meetings and Reviews

At the start of the project, risk assessment sessions will be held to develop the initial list of project risks, as described in Section 2.1.2.1. In addition, periodic risk assessments are conducted as described in Section 2.1.2.2.

The status of Project-level risks is discussed at:

- EDR Management Team Risks and Issues Meetings
- EDR Steering Committee Meetings (for critical or escalated risks)
- EDR Management Performance Reviews (MPRs)

Risks are also a standard topic at team, group and discipline meetings.

The SP Risk Manager is responsible for developing the meeting agendas for the Biweekly EDR Management Team Risks and Issues Meetings. The State Risk Manager is responsible for scheduling the appropriate conference rooms. The State and SP Risk Managers work together to identify the participants for the meetings, and take turns in creating meeting minutes for the EDR Management Team Risks and Issue Meeting.

4.5. General Communications

Risk status and identification will be a standard topic at team, group, and discipline meetings. Leads/Managers discuss applicable risks with their team members to ensure areas of the project are aware of the mitigation/contingency actions to assist with monitoring for unintended consequences or other early warning signs.

Meeting minutes also may contain information on risk identification and RRP status updates or coordination needs for RRPs. Meeting minutes and agendas are stored in the EDR Project Repository in the respective team, group, and discipline folders. In particular, the minutes from the following meetings contain an agenda item for considering and discussing risks to the project:

- EDR Management Team Joint Schedule Meetings
- EDR Steering Committee Meetings (for critical or escalated risks)
- EDR Management Performance Reviews

Upon approval of the Risk Management Plan (and supporting templates), the documents are stored in the EDR Project Repository. The Risk Management Plan and supporting templates are available to project team members via the EDR Project Repository, subject to appropriate user access restrictions.

5. PASI – ROLES AND RESPONSIBILITIES

This section describes the participants in the Risk Management Process and their responsibilities.

5.1. Management of the Process

Though the State and SP PMO Teams own and facilitate the Risk Management process, the EDR Management Teams have the primary decision-making responsibility for EDR project risks. Items are escalated to the EDR Steering Committee, as needed, if the EDR Management Team cannot reach a decision or if the necessary actions exceed the Team's authority level. The Risk Managers are responsible for the day-to-day implementation, management and tracking of the Risk Management Process.

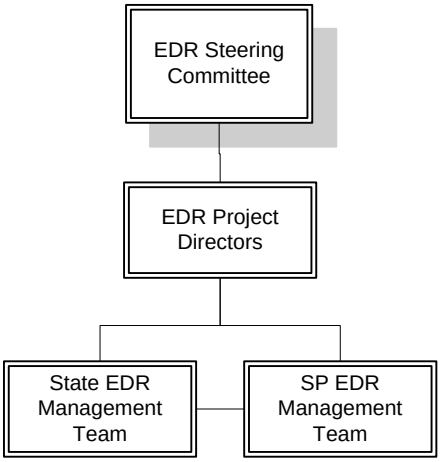

Figure 4. Management of the Risk Management Process

5.2. Roles and Responsibilities

The Risk Management Plan is executed jointly by the State and SP Teams. Each team has a Risk Manager who is responsible for coordinating updates and assignments for its organization. The Risk Managers work together to report status and to ensure that risk activities and analyses involve both organizations, as appropriate.

Table 8 below summarizes the roles and responsibilities for the participants in the Risk Management Process. The PASI matrix in the next section indicates the level of participation in each step of the Risk Management Process.

Table 8: Risk Management Process Roles and Responsibilities

Project Role	Responsibilities
EDR Steering Committee	• Participate in risk identification • Review escalated risks and provide direction for resolution • Approve risk mitigation strategies, as appropriate • Coordinate risk responses for external risks, as needed

Project Role	Responsibilities
EDR Management Team	• Assume overall decision-making responsibility for Risk Management activities within the EDR project • Review and approve Risk Response and Contingency Plans • Authorize execution of Risk Response and Contingency Plans, as appropriate • Determine whether to escalate risks to the EDR Steering Committee • Escalate at appropriate points to the EDR Steering Committee • Identify and direct external or cross-project risks for monitoring by the Risk Management Process • Participate, as needed, in meetings on the Risk Management Process • Promote risk awareness within the project team as a whole • Work with team members to identify, validate and communicate potential risks to the project • Participate in risk identification • Prioritize risks and resources assigned for risk response actions • Actively monitor Project-level risks, based on prioritized selection subsequent to probability/impact analysis • Approve ownership of Project-level risks • Review and monitor the Risk Register • Actively monitor and resolve risks for which they are assigned ownership.
State and SP PMO Managers	• Review the initial risk list and make initial assignments • Review new risks and RRPs for completeness and process compliance prior to submitting the risks to the EDR Management Team
State PMO Manager	• Coordinate risks involving external stakeholder participation
SP Risk Manager	• Conduct risk management training • Lead the initial risk identification sessions with assistance from the SP PMO Manager and develop the initial risk list from the sessions • Enter the initial risks into the Risk Tool • Lead periodic risk assessments to identify new Design Stage-specific risks

Project Role	Responsibilities
State and SP Risk Managers	• Schedule and conduct risk management training for project staff as part of project orientation • Plan and schedule the initial risk identification sessions • Enter Risk Statement Forms to the Risk Tool • Notify Risk Owners and communicate assignments and expectations • Maintain Risk Register • Maintain Risk Management Plan and processes • Chair the EDR Management Team Risks and Issues Meetings • Facilitate the identification of risks that may impact the project • Identify process improvement opportunities and implement them as consensus dictates • Confirm that Project-level risks are appropriately logged into the Risk Register • Review Project-level risks so that there are no duplicates • Confirm that a Risk Owner is assigned to each Project-level risk • Confirm that each Project-level risk is assessed for probability of occurrence and potential impact on the project • Confirm there is an appropriate risk response with clearly defined actions for prioritized Project-level risks, and that the risk responses are properly implemented • Recommend to the EDR Management Team which risks they should review • Regularly review the Project-level risks and associated data in the Risk Register to validate that it is complete and up to date, and notify owners if updates are needed • Report on Project-level risks and their status to interested parties
Originator's Lead/Manager	• Validate potential risks/opportunities identified by their team members • Document the risk and initial assessment on the Risk Statement Form • Notify the Risk Manager that the risk is ready to be communicated and included in the Risk Register

Project Role	Responsibilities
Risk Originator	• Identify a risk to (or opportunity for) the EDR Project in accordance with the EDR Risk Management Process • Communicate newly identified risks to their Lead/Manager or PM designee (the supervisor who has been defined by their project manager to review new risks), if they are not at the Project Management level of the organization • At the direction of their Lead/Manager, further define the risk, and make the initial assessment of the impact and probability
Risk Owner	• Conduct further risk analysis to validate and refine the initial risk assessment and support the development of appropriate risk responses • Coordinate participation of SMEs and technical resources in the analysis and development of risk response strategies and action plans • Formulate and implement risk response strategies, measurements, and risk response actions for risks assigned to them • Monitor the risk indicators/triggers in accordance with the approved RRP to determine when and if risk response actions are needed • Document the status of indicators/triggers and risk response actions in accordance with the approved RRP • Update and modify RRPs, as necessary, as time progresses and/or project conditions change • Assign responsibility for risk response actions and monitor progress of those actions • Validate that the completion of risk response actions is entered into the Risk Register • Notify the Risk Manager if the RRP needs revision, if a risk is imminent or occurring, or if the risk should be escalated • Recommend risk closure of Project-level risks to the Risk Managers at the appropriate time

5.3. PASI Matrix

The Risk Management Process roles and responsibilities are documented in Table 9.

Table 9. Risk Management Plan PASI Matrix

Activity	Role/Person								
	EDR Steering Committee	EDR Management Team	State PMO Manager	SP PMO Manager	State Risk Manager	SP Risk Manager	Originator's Lead/Manager	Risk Originator	Risk Owner
1a Conduct Initial Risk Assessment	I	A	S	S	P	P		S	
1b Conduct Periodic Risk Assessments	I	A	S	S	P	P		S	
1c Conduct ongoing and Ad Hoc Risk Identification	I	A	S	S	S	S		P	
2 Validate and Document Risk					S	S	P	S	
3 Review for Process Compliance			A	A	P*	P*	S	I	
4 Enter Risk in Tool					P*	P*	S	I	
5 Review and Prioritize Risk		A	S	S	P*	P*	S	I	
6 Update Risk in Tool					P*	P*	S	I	I
7 Perform Risk Analysis					S	S	S	S	P
8 Develop Risk Response Plan					S	S	S	S	P
9 Review and Approve Risk Response Plans	I	A	S	S	P*	P*	I	I	S
10 Update Risk in Tool					P*	P*	I	I	S
11 Monitor and Report Risk Status		I	I	I	S	S	I	I	P
12 Execute Risk Response Plan		I	I	I	S	S	I	I	P

Activity	Role/Person								
13 Monitor Effectiveness of Risk Response Plan		I	I	I	S	S	I	I	P
14 Update Risk Status and Actions in Tool					P*	P*	I	I	S
15 Close Risk in Tool	I	A	S	S	P*	P*	I	I	S
P = Primary; A = Approval Authority; S = Supporting Responsibility; I = Information Only									

*The State Risk Manager leads the activities for the risks assigned to State team members; the SP Risk Manager leads the activities for risks assigned to SP team members.

APPENDIX A – RISK STATEMENT

This appendix contains the Risk Statement template and sample.

Appendix A.1 – Risk Statement Template

	Risk Statement
Complete the section below, review with Lead/Manager, and submit to Risk Manager	
Risk ID #	*<Completed by Risk Manager>*
Risk Title	
Date Identified	
Originator Name	

Category: *(Select one or more)*

☐ **Audit and Control Needs**	☐ **Human Resource: Skills, Availability**	☐ **Requirements Management**
☐ **Budget/Revenue**	☐ **Infrastructure**	☐ **Schedule**
☐ **Client/Server Architecture**	☐ **Legislation**	☐ **Sponsorship Commitment**
☐ **Customer Sophistication**	☐ **Litigation**	☐ **Structure of Installed Systems**
☐ **Design and Implementation**	☐ **Management Processes**	☐ **Supplier/Vendor Capability/Capacity**
☐ **Development Environment**	☐ **Other Projects**	☐ **System Architecture**
☐ **External Environment**	☐ **Paradigm Shift**	☐ **Technology**
☐ **Facilities**	☐ **Regulations**	☐ **Turnover**

Probability *(In regards to project scope, schedule, cost and quality)*	**Impact** *(In regards to project scope, schedule, cost and quality)*	**Timeframe** *(Impact timeframe of the potential risk)*
☐ **1- < 20%**	☐ **1- less than 5%**	☐ **Immediately**
☐ **2- 21-40%**	☐ **2- 5-10%**	☐ **Within the next 6 months**
☐ **3- 41-60%**	☐ **3- 11-15%**	☐ **Six months to a year from now**
☐ **4- 61-80%**	☐ **4- 16-24%**	☐ **Over a year from now**
☐ **5- >80%**	☐ **5- 25% or greater**	

Risk Description
<A detailed description of the risk. Describe the risk in a way that makes it clear why it is a problem by identifying both the threat and the targets at risk. Identify the implications to the project if the risk is not controlled successfully.>
Additional Information
<Threat> *<Targets Affected>* *<Early Warning Signs>*

MRD(s) Affected (if known)	*<Identify the deliverable to which the risk pertains>*
Closure Criteria	*<Identify the requirements for closing the risk>*
Date Accepted	*<Completed by Risk Manager>*
Assigned To/Risk Owner	*<Completed by Risk Manager>*

Instructions

1) Complete form (If necessary, separate attachments may be utilized. The section where the attachment is utilized should refer to the file name and file location of the attachment.)
2) Review with Lead or Manager
3) Submit to the Risk Manager from your organization (i.e., State or SP)

Description of Risk Categories

- **Audit and Control Needs** – What is the probability that the audit and review procedures discover defects that will cause problems or delays in the project?
- **Budget/Revenue** – What is the probability that the amount of money allocated to complete the project will be inadequate to complete the project on site with the complete scope that meets quality expectations? What is the probability that the projected revenue and benefits targets for the project will not be achieved?
- **Client/Server Architecture** – What is the probability that the complex of hardware and software (servers, client PCs, printers, drivers, et al) needed to support the project will cause problems or delays during the development or implementation of the project?
- **Customer Sophistication** – What is the probability that the customers' lack of understanding or lack of ability to use the product or service will cause problems or delays to the project?
- **Design and Implementation** – What is the probability the design and/or implementation challenges of this project will cause problems or delays?
- **Development Environment** – What is the probability that the environment in which the project will be developed will cause problems or delays?
- **External Environment** – What is the probability that individuals or entities external to the organization will cause problems or delays?
- **Facilities** – What is the probability that the facilities (buildings, rooms, storage areas, office space, phones, parking lots, electrical, plumbing, etc.) required by the project will not be available, usable, or adequate thereby causing problems and/or delays to the project?
- **Human Resource: Skills, Availability** – What is the probability that there will not be enough qualified, skilled people available to complete the effort involved in the project?
- **Infrastructure** – What is the probability that the existing infrastructure into which the project will be delivered will cause problems or delays?
- **Legislation** – What is the probability that pending legislation will cause delays, extra effort, or cancellation of the project if passed?
- **Litigation** – What is the probability that lawsuits will cause problems or delays in the project?
- **Management Processes** – What is the probability that current management processes (approvals, decisions, hiring, etc.) will cause problems or delays in the project?
- **Other Projects** – What is the probability that other projects planned or in progress could cause problems or delays in this project by consuming available resources or by causing changes in the fundamental design of the project?
- **Paradigm Shift** - What is the probability that the level of change in the work model due to this project will cause problems or delays in the project due to resistance from stakeholders?
- **Regulations** - What is the probability that any regulatory process in motion will cause problems or delays in the project?
- **Requirements Management** - What is the probability that the collection and management of the project's requirements will cause problems or delays in the project?
- **Schedule** – What is the probability that the time allocated to complete the project will cause problems or delays?

- **Sponsorship Commitment** - What is the probability that the sponsor of the project will lose interest or be unable to provide sufficient direction and support?
- **Structure of Installed Systems** - What is the probability that the systems that currently exist in the project environment will cause extra effort, problems or delays in the project?
- **Supplier/Vendor Capability/Capacity** - What is the probability that the vendors or suppliers involved in this project do not possess the capacity and capability to provide adequate service and support?
- **System Architecture** - What is the probability that the system architecture (operating system, system interfaces, databases, programming languages, et al) is not sound and stable thereby causing problems or delays in the project?
- **Technology** - What is the probability that the appropriate technology will not be available to complete the project? What is the probability that the available technology will not be stable?
- **Turnover** - What is the probability that the rate of replacement of team members on the project will cause problems or delays in the project?

Appendix A.2 – Risk Statement Sample

	**Risk Statement**
Complete the section below, review with Lead/Manager, and submit to Risk Manager	
Risk ID #	*R-00032*
Risk Title	*Cost Reasonableness Consultant Contract May Not Be Completed in Time to Support Change Request Analysis*
Date Identified	*07-15-2011*
Originator Name	*Kim Garcia*

Category: *(Select one or more)*

☐ **Audit and Control Needs**	☐ **Human Resource: Skills, Availability**	☐ **Requirements Management**
☒ **Budget/Revenue**	☐ **Infrastructure**	☐ **Schedule**
☐ **Client/Server Architecture**	☐ **Legislation**	☐ **Sponsorship Commitment**
☐ **Customer Sophistication**	☐ **Litigation**	☐ **Structure of Installed Systems**
☐ **Design and Implementation**	☐ **Management Processes**	☐ **Supplier/Vendor Capability/Capacity**
☐ **Development Environment**	☐ **Other Projects**	☐ **System Architecture**
☐ **External Environment**	☐ **Paradigm Shift**	☐ **Technology**
☐ **Facilities**	☐ **Regulations**	☐ **Turnover**

Probability *(In regards to project scope, schedule, cost and quality)*	**Impact** *(In regards to project scope, schedule, cost and quality)*	**Timeframe** *(Impact timeframe of the potential risk)*
☐ **1- < 20%**	☐ **1- less than 5%**	☐ **Immediately**
☐ **2- 21-40%**	☐ **2- 5-10%**	☒ **Within the next 6 months**
☒ **3- 41-60%**	☒ **3- 11-15%**	☐ **Six months to a year from now**
☐ **4- 61-80%**	☐ **4- 16-24%**	☐ **Over a year from now**
☐ **5- >80%**	☐ **5- 25% or greater**	

Risk Description

Currently, the State does not have the services of a Cost Reasonableness Consultant to support change request analysis. If a Cost Reasonableness Consultant contract is not completed in time to support change request analysis, then change requests could be delayed which may negatively impact the project schedule and/or quality.

Additional Information

Early Warning Sign – Preliminary change request discussions

MRD(s) Affected (if known)	*None*
Closure Criteria	*Implemented Cost Analysis Process*
Date Accepted	*<Completed by Risk Manager>*
Assigned To/Risk Owner	*<Completed by Risk Manager>*

APPENDIX B – RISK RESPONSE PLAN (RRP)

This appendix contains the Risk Response Plan template and sample.

Appendix B.1 – Risk Response Plan Template

Risk Response Plan (RRP)

SECTION 1 – RISK STATEMENT SUMMARY

<This section mirrors the original Risk Statement. The Risk Owner should update this section as necessary.>

Risk ID #	*<Completed by Risk Manager>*
Risk Title	*<Completed by Risk Manager>*
Date Identified	*<Completed by Risk Manager>*
Date Assigned	*<Completed by Risk Manager>*
Originator Name	*<Completed by Risk Manager>*
Risk Owner Name	*<Completed by Risk Manager>*

Category: *(Select one or more)*

☐ **Audit and Control Needs**	☐ **Human Resource: Skills, Availability**	☐ **Requirements Management**
☐ **Budget/Revenue**	☐ **Infrastructure**	☐ **Schedule**
☐ **Client/Server Architecture**	☐ **Legislation**	☐ **Sponsorship Commitment**
☐ **Customer Sophistication**	☐ **Litigation**	☐ **Structure of Installed Systems**
☐ **Design and Implementation**	☐ **Management Processes**	☐ **Supplier/Vendor Capability/Capacity**
☐ **Development Environment**	☐ **Other Projects**	☐ **System Architecture**
☐ **External Environment**	☐ **Paradigm Shift**	☐ **Technology**
☐ **Facilities**	☐ **Regulations**	☐ **Turnover**

Probability *(In regards to project scope, schedule, cost and quality)*	**Impact** *(In regards to project scope, schedule, cost and quality)*	**Timeframe** *(Impact timeframe of the potential risk)*
☐ **1- < 20%**	☐ **1- less than 5%**	☐ **Immediately**
☐ **2- 21-40%**	☐ **2- 5-10%**	☐ **Within the next 6 months**
☐ **3- 41-60%**	☐ **3- 11-15%**	☐ **Six months to a year from now**
☐ **4- 61-80%**	☐ **4- 16-24%**	☐ **Over a year from now**
☐ **5- >80%**	☐ **5- 25% or greater**	

Risk Description

<A detailed description of the risk. Describe the risk in a way that makes it clear why it is a problem by identifying both the threat and the targets at risk. Identify the implications to the project if the risk is not controlled successfully. Utilize format of "concern – likelihood - consequence".>

Additional Information

<Threat>
<Targets Affected>
<Early Warning Signs>

MRD(s) Affected	*<Identify the deliverable to which the risk pertains>*
Closure Criteria	*<Identify the requirements for closing the risk>*

SECTION 2 – RISK RESPONSE *<Complete the section below, review with Lead/Manager, and submit to Risk Manager.>*		
Risk Response Type *(Select one of the following)* ☐ **Avoid** ☐ **Transfer** ☐ **Mitigate** ☐ **Accept**	**Priority** *(Identify when action is required)* ☐ **Critical** – Within 1 week ☐ **Major** – Within 1 month ☐ **Minor** – Within 90 days	**Degree of Control** *(Select one)* ☐ **Internal** – Within the control of EDR ☐ **External** – Outside of the control of EDR

Impacted Project Discipline(s) *<Document the discipline(s) that would be primarily affected and the impact to those discipline(s)>*

Risk Response Description *<Describe the risk response and rationale based on the Risk Response Type (accept, avoid, mitigate, transfer.>*
<If applicable, describe the impact on the WBS Item(s), MRD(s), and Critical Path (include Task IDs)> *<If risk is outside the control of EDR, identify which group(s) external to EDR should be involved.>*

#	**Response Action Steps** *<Identify specific action steps for the risk response>*	**Responsible Party**	**Due Date**	**Status**

Contingency Plan Description *<Required for High/Medium Exposure Risks, High Impact Risks (>25%), and Critical/Major Priority Risks>*
< State what event would cause the contingency plan to be implemented as the risk becomes an issue.> *<Describe the overall approach to the contingency plan. >*

#	**Contingency Plan Action Steps** *<Identify specific action steps for the contingency plan>*	**Responsible Party**	**Due Date**	**Status**

Revision History *<Document updates and changes in the risk response and/or contingency plan >*	**Revision Date**
<Describe what changed and why>	

Risk Result *(Select one)*	☐ **Risk Occurred** ☐ **Risk Transferred**	☐ **Risk Mitigated** ☐ **Risk Retired**
Risk Closure Approved by	*<Completed by Risk Manager>*	
Risk Closure Date	*<Completed by Risk Manager>*	

Instructions

1) Update Section 1 Risk Statement Summary. Review all fields to confirm that the Risk Statement is accurate and update accordingly.
2) Complete Section 2 Risk Response. Only if necessary, separate attachments may be utilized. The section where the attachment is utilized should refer to the file name and file location of the attachment.
3) Review with Lead or Manager
4) Submit to the Risk Manager from your organization (i.e., State or SP)

Project Disciplines

The project disciplines correspond to the following:

- Application Development
- Business/Implementation
- Data
- Discovery
- Governance
- Infrastructure and Organization
- Legacy Systems
- Organizational Change
- Production Operations
- Project Management
- Technical Architecture
- Technical Operations
- Testing

Description of Risk Categories

- **Audit and Control Needs** – What is the probability that the audit and review procedures discover defects that will cause problems or delays in the project?
- **Budget/Revenue** – What is the probability that the amount of money allocated to complete the project will be inadequate to complete the project on site with the complete scope that meets quality expectations? What is the probability that the projected revenue and benefits targets for the project will not be achieved?
- **Client/Server Architecture** – What is the probability that the complex of hardware and software (servers, client PCs, printers, drivers, et al) needed to support the project will cause problems or delays during the development or implementation of the project?
- **Customer Sophistication** – What is the probability that the customers' lack of understanding or lack of ability to use the product or service will cause problems or delays to the project?
- **Design and Implementation** – What is the probability the design and/or implementation challenges of this project will cause problems or delays?
- **Development Environment** – What is the probability that the environment in which the project will be developed will cause problems or delays?
- **External Environment** – What is the probability that individuals or entities external to the organization will cause problems or delays?
- **Facilities** – What is the probability that the facilities (buildings, rooms, storage areas, office space, phones, parking lots, electrical, plumbing, etc.) required by the project will not be available, usable, or adequate thereby causing problems and/or delays to the project?
- **Human Resource: Skills, Availability** – What is the probability that there will not be enough qualified, skilled people available to complete the effort involved in the project?
- **Infrastructure** – What is the probability that the existing infrastructure into which the project will be delivered will cause problems or delays?
- **Legislation** – What is the probability that pending legislation will cause delays, extra effort, or cancellation of the project if passed?
- **Litigation** – What is the probability that lawsuits will cause problems or delays in the project?
- **Management Processes** – What is the probability that current management processes (approvals, decisions, hiring, etc.) will cause problems or delays in the project?

- **Other Projects** – What is the probability that other projects planned or in progress could cause problems or delays in this project by consuming available resources or by causing changes in the fundamental design of the project?
- **Paradigm Shift** - What is the probability that the level of change in the work model due to this project will cause problems or delays in the project due to resistance from stakeholders?
- **Regulations** - What is the probability that any regulatory process in motion will cause problems or delays in the project?
- **Requirements Management** - What is the probability that the collection and management of the project's requirements will cause problems or delays in the project?
- **Schedule** – What is the probability that the time allocated to complete the project will cause problems or delays?
- **Sponsorship Commitment** - What is the probability that the sponsor of the project will lose interest or be unable to provide sufficient direction and support?
- **Structure of Installed Systems** - What is the probability that the systems that currently exist in the project environment will cause extra effort, problems or delays in the project?
- **Supplier/Vendor Capability/Capacity** - What is the probability that the vendors or suppliers involved in this project do not possess the capacity and capability to provide adequate service and support?
- **System Architecture** - What is the probability that the system architecture (operating system, system interfaces, databases, programming languages, et al) is not sound and stable thereby causing problems or delays in the project?
- **Technology** - What is the probability that the appropriate technology will not be available to complete the project? What is the probability that the available technology will not be stable?
- **Turnover** - What is the probability that the rate of replacement of team members on the project will cause problems or delays in the project?

Description of Risk Response Types

- **Avoid** – Risk avoidance generally entails changing the project schedule or solution approach to eliminate the risk or condition.
- **Transfer** – If the project has little or no control over the risk, transferring may be appropriate. It is important to note that transferring the risk simply gives another party responsibility for its management; it does not eliminate the risk.
- **Mitigate** – Risk mitigation involves identifying actions for reducing the effects of the risk. Risk mitigation seeks to reduce the probability and/or consequences of a risk event to an acceptable threshold.
- **Accept** – The project may choose to accept the risk if the predicted probability and impact are considered acceptable when compared to the cost of risk response alternatives, or if the risk is unlikely to be affected by any mitigation activities. In some cases, a contingency plan still may be prepared to address the risk in the event it does occur.

Appendix B.2 – Risk Response Plan Sample

Risk Response Plan (RRP)

SECTION 1 – RISK STATEMENT SUMMARY

<This section mirrors the original Risk Statement. The Risk Owner should update this section as necessary.>

Risk ID #	*R-00032*
Risk Title	*Cost Reasonableness Consultant Contract May Not Be Completed in Time to Support Change Request Analysis*
Date Identified	*07-15-2011*
Date Assigned	*07-15-2011*
Originator Name	*Kim Garcia*
Risk Owner Name	*Kim Garcia*

Category: *(Select one or more)*

☐ **Audit and Control Needs**	☐ **Human Resource: Skills, Availability**	☐ **Requirements Management**
☒ **Budget/Revenue**	☐ **Infrastructure**	☐ **Schedule**
☐ **Client/Server Architecture**	☐ **Legislation**	☐ **Sponsorship Commitment**
☐ **Customer Sophistication**	☐ **Litigation**	☐ **Structure of Installed Systems**
☐ **Design and Implementation**	☐ **Management Processes**	☐ **Supplier/Vendor Capability/Capacity**
☐ **Development Environment**	☐ **Other Projects**	☐ **System Architecture**
☐ **External Environment**	☐ **Paradigm Shift**	☐ **Technology**
☐ **Facilities**	☐ **Regulations**	☐ **Turnover**

Probability *(In regards to project scope, schedule, cost and quality)*	**Impact** *(In regards to project scope, schedule, cost and quality)*	**Timeframe** *(Impact timeframe of the potential risk)*
☐ **1- < 20%**	☒ **1- less than 5%**	☐ **Immediately**
☐ **2- 21-40%**	☐ **2- 5-10%**	☒ **Within the next 6 months**
☐ **3- 41-60%**	☐ **3- 11-15%**	☐ **Six months to a year from now**
☐ **4- 61-80%**	☐ **4- 16-24%**	☐ **Over a year from now**
☒ **5- >80%**	☐ **5- 25% or greater**	

Risk Description

Currently, the State does not have the services of a Cost Reasonableness Consultant to support change request analysis. If a Cost Reasonableness Consultant contract is not completed in time to support change request analysis, then change requests could be delayed which may negatively impact the project schedule and/or quality.

Additional Information

Early Warning Sign – Preliminary change request discussions

MRD(s) Affected	*None*
Closure Criteria	*Implemented Cost Analysis Process*

SECTION 2 – RISK RESPONSE

<Complete the section below, review with Lead/Manager, and submit to Risk Manager.>

Risk Response Type *(Select one of the following)*	**Priority** *(Identify when action is required)*	**Degree of Control** *(Select one)*
☐ **Avoid** ☐ **Transfer** ☒ **Mitigate** ☐ **Accept**	☐ **Critical** – Within 1 week ☒ **Major** – Within 1 month ☐ **Minor** – Within 90 days	☒ **Internal** – Within the control of EDR ☐ **External** – Outside of the control of EDR

Impacted Project Discipline(s)

<Document the discipline(s) that would be primarily affected and the impact to those discipline(s)>

All – Throughout any project, any project discipline may require a necessary change request

Risk Response Description

<Describe the risk response and rationale based on the Risk Response Type (accept, avoid, mitigate, transfer.>

Immediately begin working with Procurement Division and DGS to escalate contract, or search for financial experts within FTB

#	**Response Action Steps** *<Identify specific action steps for the risk response>*	**Responsible Party**	**Due Date**	**Status**
1	*Work with Procurement Division and DGS to escalate contract*	*Kim Garcia*	*08/15/11*	
2	*Search for financial experts within FTB*	*Kim Garcia*	*08/15/11*	

Contingency Plan Description

<Required for High/Medium Exposure Risks, High Impact Risks (>25%), and Critical/Major Priority Risks>

Preliminary discussion of a necessary change request

#	**Contingency Plan Action Steps** *<Identify specific action steps for the contingency plan>*	**Responsible Party**	**Due Date**	**Status**
1	*Escalate the procurement of the contract or secure an financial expert within FTB*	*Kim Garcia*	*Within 1 week of Trigger*	

Revision History *<Document updates and changes in the risk response and/or contingency plan >*	**Revision Date**
Created RRP	*7/15/11*

Risk Result *(Select one)*	☐ **Risk Occurred** ☐ **Risk Transferred**	☐ **Risk Mitigated** ☐ **Risk Retired**
Risk Closure Approved by	*<Completed by Risk Manager>*	
Risk Closure Date	*<Completed by Risk Manager>*	

APPENDIX C – LIST OF RISK CATEGORIES

The following are the categories that are used to group and manage risks for the project. This list is taken from the CA-PMM Toolkit.

- Audit and Control Needs – What is the probability that the audit and review procedures discover defects that will cause problems or delays in the project?
- Budget/Revenue – What is the probability that the amount of money allocated to complete the project will be inadequate to complete the project on site with the complete scope that meets quality expectations? What is the probability that the projected revenue and benefits targets for the project will not be achieved?
- Client/Server Architecture – What is the probability that the complex of hardware and software (servers, client PCs, printers, drivers, et al) needed to support the project will cause problems or delays during the development or implementation of the project?
- Customer Sophistication – What is the probability that the customers' lack of understanding or lack of ability to use the product or service will cause problems or delays to the project?
- Design and Implementation – What is the probability the design and/or implementation challenges of this project will cause problems or delays?
- Development Environment – What is the probability that the environment in which the project will be developed will cause problems or delays?
- External Environment – What is the probability that individuals or entities external to the organization will cause problems or delays?
- Facilities – What is the probability that the facilities (buildings, rooms, storage areas, office space, phones, parking lots, electrical, plumbing, etc.) required by the project will not be available, usable, or adequate thereby causing problems and/or delays to the project?
- Human Resource: Skills, Availability – What is the probability that there will not be enough qualified, skilled people available to complete the effort involved in the project?
- Infrastructure – What is the probability that the existing infrastructure into which the project will be delivered will cause problems or delays?
- Legislation – What is the probability that pending legislation will cause delays, extra effort, or cancellation of the project if passed?
- Litigation – What is the probability that lawsuits will cause problems or delays in the project?
- Management Processes – What is the probability that current management processes (approvals, decisions, hiring, etc.) will cause problems or delays in the project?
- Other Projects – What is the probability that other projects planned or in progress could cause problems or delays in this project by consuming available resources or by causing changes in the fundamental design of the project?

- Paradigm Shift - What is the probability that the level of change in the work model due to this project will cause problems or delays in the project due to resistance from stakeholders?
- Regulations - What is the probability that any regulatory process in motion will cause problems or delays in the project?
- Requirements Management - What is the probability that the collection and management of the project's requirements will cause problems or delays in the project?
- Schedule – What is the probability that the time allocated to complete the project will cause problems or delays?
- Sponsorship Commitment - What is the probability that the sponsor of the project will lose interest or be unable to provide sufficient direction and support?
- Structure of Installed Systems - What is the probability that the systems that currently exist in the project environment will cause extra effort, problems or delays in the project?
- Supplier/Vendor Capability/Capacity - What is the probability that the vendors or suppliers involved in this project do not possess the capacity and capability to provide adequate service and support?
- System Architecture - What is the probability that the system architecture (operating system, system interfaces, databases, programming languages, et al) is not sound and stable thereby causing problems or delays in the project?
- Technology - What is the probability that the appropriate technology will not be available to complete the project? What is the probability that the available technology will not be stable?
- Turnover - What is the probability that the rate of replacement of team members on the project will cause problems or delays in the project?

APPENDIX D – RISK TOLERANCE THRESHOLDS

This appendix contains the risk tolerance thresholds that are used as guidelines to manage risks on the EDR Project.

Generally, contingency plans are required for high or medium exposure risks, critical and major priority risks, and risks with an impact estimated at 25% or greater change to schedule, scope, budget or quality.

Subsequent to the acceptance of the Risk Management Plan and the initial risk assessment, the State and SP PMO Managers will work with the EDR Management Team to establish the project's risk tolerance thresholds which define the project's tolerance for risk in key project areas.

This appendix will be updated accordingly at that time.