Line

Risk Management Plan

Version 1.0

Refer to the Software Engineering Risk Management Framework for additional information: [http://www.sei.cmu.edu/reports/10tr017.pdf](https://webmail.noblis.org/exchweb/bin/redir.asp?URL=http://www.sei.cmu.edu/reports/10tr017.pdf)

**Revision History**

| **Date** | **Rev** | **Author** | **Description** |
| --- | --- | --- | --- |
| **MM/DD/YY** | 1 |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1. Introduction 4](#_Toc278356857)

[2. Risk Plan Stakeholders 4](#_Toc278356858)

[3. Project Risk Roles and Responsibilities 5](#_Toc278356859)

[4. Project Risk Management Process Overview 8](#_Toc278356860)

[5. Recommended Risk Tracking 16](#_Toc278356861)

[6. Project Risk Management Checklist 17](#_Toc278356862)

[7. Best Practices for Risk Management Process Items 19](#_Toc278356863)

[7.1. Identify and Classify Risk 19](#_Toc278356864)

[7.2. Risk Classification 20](#_Toc278356865)

[7.3. Analyze Risk 21](#_Toc278356870)

[7.4. Determine Approach to Identified Risk 22](#_Toc278356871)

[7.5. Track Risk 23](#_Toc278356872)

[7.6. Mitigate Risk 23](#_Toc278356873)

[7.7. Escalation Process 24](#_Toc278356879)

[8. Suggested Risk Reporting 24](#_Toc278356880)

[Appendix: SMA Medicaid Information Technology Architecture (MITA) Risks 26](#_Toc278356881)

**List of Tables**

[Table 1: Project Risk Management Roles and Responsibilities 5](#_Toc289696158)

[Table 2: Project Risk Management Process Overview 9](#_Toc289696159)

[Table 3: Project Risk Management Checklist 18](#_Toc289696160)

[Table 4: Likelihood of Occurrence Values 22](#_Toc289696161)

[Table 5: Occurrence Severity 23](#_Toc289696162)

[Table 6: Risk Levels 23](#_Toc289696163)

[Table 7: Recommended Risk Reports 25](#_Toc289696164)

[Table 8: Operations Management Business Processes Impact Levels 29](#_Toc289696165)

[Table 9: Program Management Business Processes Impact Levels 31](#_Toc289696166)

[Table 10: Provider Management Business Processes Impact Levels 32](#_Toc289696167)

[Table 11: Contractor Management Business Processes Impact Levels 32](#_Toc289696168)

[Table 12: Member Management Business Processes Impact Levels 34](#_Toc289696169)

# Introduction

The Risk Management Plan is a document created to begin the risk management process in any ICD-10 project or the overall ICD-10 program. This document is created by Program Management and addresses the following:

* Who is the Risk Coordinator for the Project[[1]](#footnote-1) or Program[[2]](#footnote-2)?
* What are the elements of the Risk Management Process?
* Which tools will be used in managing the risks?

All SMA project team members, Executive Sponsor and stakeholders should be familiar with the content of this document so that the Risk Management Plan can be executed efficiently and effectively.

A risk is defined as a threat that, if not mitigated or avoided, may cause negative business outcomes (e.g., incorrect payment). Risk Management is the recognition, assessment and control of uncertainties that may result in schedule delays, cost overruns, performance problems, adverse environmental impacts of other undesired consequences.

The objectives of risk management are:

* To focus attention on minimizing exposure to possible events that threatens accomplishment of the objectives of the SMA ICD-10 Implementation Program.
* To provide a systematic approach for:
  + Identifying, classifying, assessing and managing risks
  + Developing proactive plans and approaches that avoid or mitigate risks
  + Rapidly implementing contingency plans based on timely identification of risk occurrence
  + Monitoring and reporting progress in reducing risk

Additionally the appendix contains the Medicaid Information Technology Architecture (MITA) Risk Assessment based on version 2 of the MITA framework.

# Risk Management Plan Stakeholders

When changes are made to this plan, the following stakeholders are advised:

1. Program Leadership
2. Workgroup[[3]](#footnote-3) Leads

# Project Risk Management Roles and Responsibilities

The Risk Management Process identifies five fundamental roles: Risk Identifier, Risk Coordinator, Risk Owner, Workgroup Leads, and PMO Risk Coordinator. Table 1 below describes each role and associated responsibilities.

Table 1: Project Risk Management Roles and Responsibilities

| **Role** | **Description** | **Responsibilities** |
| --- | --- | --- |
| **Risk Identifier** | Anyone who identifies, documents, and submits a risk. In addition, they assist in mitigating and resolving the risk. | * Identifies Risk * Documents Risk * Submits Risk   Also within SMA ICD-10 Implementation:   * Discusses upcoming risks and risk mitigation techniques during project meetings. * Monitors and identifies risk occurrence. * Develops contingent risk responses.   Implements risk response actions based on risk occurrence. |
| **Risk Coordinator** | The person who is responsible for facilitating the risk management process for a given project. | * Researches, clarifies, consolidates, and prioritizes risks. * Assigns the Risk Owner. * Monitors, escalates, and reports on the Risk(s) and related Plan(s). * Closes Risks.   Additional SMA ICD-10 Implementation Responsibilities:   * Develops and maintains the project Risk Management Plan as part of the overall risk management effort. * Develops and maintains the risk tracking process as part of the overall risk management process. * Incorporates risk mitigation/avoidance approaches into the Risk Management Plan.   Asserts a Quality role by working with all project managers during weekly meetings to address risk identification and management, implementation, and effectiveness on projects. |
| **Risk Owner** | The person who is ultimately responsible for assessing and managing an assigned risk and related plan to completion. Also provides overall direction and oversight. | * Assesses/Validates Risk Severity and Probability. * Develops, gains approval, implements, and administers Risk Elimination, Contingency, and Risk Mitigation plans. |
| **Workgroup Lead** | Workgroups can be comprised of internal SMA resources and external contractor or vendor SMEs (as needed). Workgroups can be especially useful in:   * Addressing recommended actions and raising issues and risks to leadership; * Facilitating communications across MITA business areas to limit duplication of work effort spanning multiple MITA business areas; and * Reaching beyond the SMA, fostering communication with other SMAs or focus groups implementing ICD-10. | * Develops, implements, and manages the Risk Management Plan. * Provides sign-off where requested / appropriate. |
| **Program Manager Risk Manager** | ICD-10 Implementation Project Management responsible for monitoring Risks. | * Audits project risks to ensure updates are being completed on a timely basis. * Escalates risks to Program Directors. * Has the ability to close issues and risks. * Tracks and Monitors risks. * Runs and post weekly reports for the ICD-10 Project Team Meeting. Reviews open risks that are escalated to program directors at the ICD-10 Project Team Meeting. * Responsible for identifying, documenting, submitting, and facilitating the risk management process for program level risks working in conjunction with program level directors. |

# Project Risk Management Process Overview

Refer to Table 2 for a high level process description and key activities. The table identifies the following:

**ID:**  Represents the process step in Risk Management

**Activity Title:** Process Step

**Description:** Detailed description of the process step.

**Task:**  “Checklist’ that the Project Manager can use to evaluate steps in the risk management process.

**Template/Tool:** Suggested tool required to support activity/process step.

Table 2: Project Risk Management Process Overview

| **ID** | **Activity Title** | **Description** | **Task** | **Template/Tool** |
| --- | --- | --- | --- | --- |
| **1** | Develop, Implement and Manage Risk Management Plan | The Risk Management Plan identifies the Risk Coordinator and the tool(s) the project/program will use to assist in the Risk Management process. | **🞎** Develop, Implement, and Manage a Risk Management Plan | A Risk Management Plan template in word format has been developed. |
| **2** | Identify Potential Risk | Any individual can identify a potential risk to a given project or program. This individual, risk identifier, could be part a project team member, an internal or external stakeholder, Business Leadership, or anybody else, who has the knowledge to identify a pertinent risk. | **🞎** Identify Potential Risks | None |
| **3** | Submit Potential Risk | The Risk Identifier passes on the potential risk to the Risk Coordinator by documenting the potential risk in the tool(s) specified in the Risk Management Plan (Risk Tracker, Word templates, etc.). The Issues Management Process could also submit potential risks. | **🞎** Submit the Potential Risk electronically | Risk Tracking Tool, Word templates etc. Tool should track the following: |
| **4** | Research, Clarify, Consolidate, and Prioritize Risks | One of the primary roles of the Risk Coordinator is to review potential risks that are submitted. The Risk Coordinator may need to confer with other individuals to understand the risk and may choose to reword the submitted risk and consolidate the submitted risk with another risk. The other fields in the Risk Summary Template are updated as appropriate including the impact areas. | * Do you understand the risk? * Do you need to reword or consolidate the risk? * Any additional research required? * What is the initial Probability and Impact of the risk? * Update Risk Summary Template as appropriate | Risk Tracking Tool, Word templates etc. |
| **5** | Close Risk? | Risk Coordinator determines if the potential risk that was submitted should be rejected based on their analysis. A risk should not be closed outright without deliberation or review. Two possible reasons for closing a risk include: 1. if it is not a risk, perhaps an issue or 2. If it is a duplicate risk. | * Should the risk be closed? | Risk Tracking Tool, Word templates, etc. Tool should capture and identify if a risk is closed by selecting the state “Closed”. Document the reason for closing in “Resolution.” |
| **6a** | Assign Risk Owner | Once the Risk Coordinator is satisfied with the statement of a given risk and its initial Risk Magnitude, the individual assigns a Risk Owner. The Risk Owner should ideally be the individual who is best suited to own the risk and if such an owner cannot be determined, the Risk Coordinator can identify an owner from the pool of resources assigned to the project or program. | * Assign a Risk Owner – Who is the best person to manage this risk? | Risk Tracking Tool, Word templates etc. Tool should capture Risk Owner in the “Delegate To” field. |
| **6b** | Close Risk? | This activity is used by the Risk Coordinator to close a risk. This activity removes that particular submitted risk from the list of risks that the Risk Coordinator has to manage. | * Update the tool to reject or close a given risk | Risk Tracking Tool, Word templates, etc. Tool should capture Risk Owner in the “Delegate To” field. |
| **7** | Assess / Validate Risk Severity and Probability | One of the very first activities that a Risk Owner takes is to validate the Probability and Impact of the assigned risk and then modifies these ratings to change the Risk Magnitude as appropriate. The other fields in the Risk Summary Template are updated as appropriate including the impact areas. | * Is the risk clearly stated? * Is the risk valid? * What is the impact of the risk? Modify Impact, if applicable. * What is the probability of occurrence? Modify Probability, if applicable. * Update Risk Summary Template as appropriate. | Tool should capture Risk Owner in the “Delegate To” field. |
| **8** | Close Risk? | The Risk Owner determines if the Risk can be eliminated by taking specific actions. | * Can this risk be eliminated by taking some action(s)? | Risk Tracking Tool, Word templates, etc. |
| **9** | Risk Magnitude yellow or red (See above Sample Risk Management Plan & the Form Help File)? | The Risk Owner determines if the Risk Magnitude is yellow or red. If the Risk Magnitude is yellow or red, then both a Risk Mitigation Plan and a Contingency Plan have to be developed. If the Risk Score is green, a Contingency plan has to be developed. | * Determine if the Risk Score is yellow or red | Decision box, no specific tool required |
| **10** | Develop Risk Elimination Plan | Risk Elimination Plan is a plan of action and activities designed to eliminate the possibility of a risk from occurring. Risk elimination simply removes the specific risk associated with the project. The Risk Owner develops a Risk Elimination Plan as it has been determined that the specific risk can be eliminated. | * Develop Risk Elimination Plan | Risk Tracking Tool, Word templates, etc. Log the plan under “History” |
| **10b** | Develop Risk Mitigation Plan | A Risk Mitigation Plan is a plan of action and activities executed ahead of time to either reduce the probability of occurrence of the risk and/or its severity of impact. It is also defined as a plan of action to reduce the probability and/or consequences of an adverse risk event to an acceptable threshold. The Risk Owner develops a Risk Mitigation Plan if the risk cannot be eliminated and the Risk Magnitude is yellow or red. | * Develop Risk Mitigation Plan | Risk Tracking Tool, Word templates, etc. Log the plan under “History” |
| **10c** | Develop Contingency Plan | The Contingency Plan is a plan of action and activities that addresses recognized risks that may arise during the course of a project. This plan identifies alternative strategies to be used to ensure a project’s success, if a specified risk event occurs. The Risk Owner has to develop a Contingency Plan if the risk cannot be eliminated regardless of the Risk Magnitude. One of the major sections within the Contingency Plan document is the identification of the trigger(s) that would cause the risk to occur. | * Develop Contingency Plan | Risk Tracking Tool, Word templates, etc. Log the plan under “History”. |
| **11** | Risk Elimination Plan Approval Process | The Risk Owner is responsible for using the project management approval process or any other appropriate approval process to get the Risk Elimination Plan approved. The Approval Process should be the same process as that established when documenting the governance structure of the project or program. The risk needs to be approved at the escalation level. | * Seek approval of the Risk Elimination Plan using the appropriate process | None required for the approval process. |
| **12** | Plan Approved? | The decision box determines if the Risk Elimination Plan was approved. | * Was the Risk Elimination Plan approved? | Risk Tracking Tool, Word templates, etc. Document that the risk is “Planned (Contingency). |
| **13** | Implement Risk Elimination Plan | The Risk Owner is responsible for implementing the approved Risk Elimination Plan. | * Implement the approved Risk Elimination Plan | Risk Tracking Tool, Word templates, etc. Document implementation under “History” |
| **14** | Risk Mitigation Plan Approval Process | The Risk Owner is responsible for using the project management approval process or any other appropriate approval process to get the Risk Mitigation Plan approved. The Approval Process should be same process as that established when documenting the governance structure of the project or program. The risk needs to be approved at the escalation level. | * Seek approval of the Risk Mitigation Plan using the appropriate process | None required for the approval process. |
| **15** | Plan Approved? | The decision box determines if the Risk Mitigation Plan was approved. Plan needs to be approved at the escalation level. | * Was the Risk Mitigation Plan approved? | Risk Tracking Tool, Word templates, etc. Document that the risk is “Planned (Contingency)”. |
| **16** | Implement Risk Mitigation Plan | The Risk Owner is responsible for implementing the approved Risk Mitigation Plan. | * Implement the approved Risk Mitigation Plan | Risk Tracking Tool, Word templates, etc. Document implementation under “History” |
| **17** | Contingency Plan Approval Process | The Risk Owner is responsible for using the project management approval process or any other appropriate approval process to get the Contingency Plan approved. The Approval Process should be the same process as that established when documenting the governance structure of the project or program. Plan needs to be approved at the escalation level. | * Seek approval of the Contingency Plan using the appropriate process | None required for the approval process. |
| **18** | Plan Approved? | The decision box determines if the Contingency Plan was approved. | * Was the Contingency Plan approved? | Risk Tracking Tool, Word templates, etc. Document that the risk is “Planned (Contingency)”. |
| **19** | Monitor, escalate, and report on Risk and related Plan(s) | The Risk Coordinator is responsible for escalating the risks and reporting on the risks. The Risk Owners share the responsibility for escalating and reporting the risks for which they have responsibility. The risk Impact and/or Probability may change during the monitoring process and when this happens the Risk Coordinator and Risk Owner will work together to update the appropriate ratings and provide written justification for those changes. | * Review the status and progress on the individual risks on a periodic basis * Escalate risks as appropriate * Report on risks on a periodic basis * “Deliver bad news early” * Change risk Impact and/or Probability as appropriate * Document reasons for any changes to Risk Impact and/or Probability | Risk Tracking Tool, Word templates, etc. Document that the risk is “Planned (Contingency)”. |
| **20** | Risk Triggered? | The Risk Coordinator monitors the risk and determines if the risk has actually occurred. The Risk Coordinator will monitor the risk trigger(s) to see if the trigger happens causing the risk to become a reality. | * Monitor the risk trigger(s) to determine if the risk has occurred | None |
| **21a** | Document Risk Trigger Details | A risk trigger is an event that causes the risk to be realized. The Risk Coordinator documents what the risk trigger was, when the risk was triggered, and any additional details about the trigger in the “History” field. Escalate risk if needed. | * Document what the risk trigger was, when the risk was triggered, and any details about the trigger | Risk Tracking Tool, Word templates, etc. |
| **21b** | Close Risk? | The Risk Coordinator determines if the risk should be closed. | * Is the risk ready to be closed? | None |
| **22** | Handle as an issue? | The Risk Coordinator determines if the risk that has occurred has to be handled as an issue. | * Should the risk that has occurred be handled as an issue? | None |
| **23a** | Issue Management Process | The issue that is identified by the Risk Management Process is submitted to the Issue Management Process. | * Issue is submitted to the Issue Management Process | Risk Tracking Tool, Word templates, etc. Document that the risk is “Closed”. |
| **23b** | Implement Contingency Plan | The Risk Owner is responsible for implementing the approved Contingency Plan. | * Implement the approved Contingency Plan | Risk Tracking Tool, Word templates, etc. Document that the risk is “Planned (Contingency). |

# Recommended Risk Tracking

The following factors and definitions are recommended to track risks:

* Risk ID
  + *A unique number which identifies the risk*
* Risk Title
  + *A brief descriptive name or phrase for the risk*
* Risk Delegated To
  + *Enter the name or the group responsible for following up on behalf of the assignee*
* Risk Due/Closed Date
* Date by when the Risk is anticipated to manifest or to be closedRisk Description
  + *The likely causes and consequences of the risk*
* Likelihood of Occurrence Values – The likelihood scoring range is from 1 to 3.
  + *(1) Low- Minimal probability of taking place*
  + *(2) Moderate- Equal probability of occurring or not taking place*
  + *(3) High- Extreme probability of taking place*
* Occurrence Severity – the impact (level of severity 1 through 3, and 10) should the risk actually happen:
* ***1- Low****- Risk occurrence will have a minor affect on the SMA business outcomes and will require minimal or no effort to address. The SMA can use workarounds to continue business processes and systems without affecting outcomes.*

***2- Moderate****- Risk occurrence will have some affect on the SMA business outcomes. The SMA can use short term workarounds, but there would be the possibility of affecting the effectiveness or efficiency of the area (e.g., longer timeframes, greater cost). Avoiding or mitigating the risk will require some expenditure of resources.*

* + ***3- High****- Risk occurrence will have an extreme affect on the SMA business outcomes and require more expenditure of resources to address. Using short term workarounds could not prevent negative affects to outcomes (e.g., longer timeframes, greater cost).*
  + ***10- Catastrophic****- Risk occurrence will derail operations and the SMA will not be able to accomplish one or more primary objectives. The incident will tarnish the agency’s reputation and temporary fixes will not be feasible to mitigate the risks.*
* Risk Levels associated with the risk scores calculated by multiplying the severity and likelihood values
  + *1-3: Low*
  + *4-5 Moderate*
  + *6-9 High*
  + *10-30 Catastrophic (Impact on budget, schedule, and scope)*
* Risk Mitigation Plan
  + *The mitigation strategy execution plan*
* Risk Contingency Plan
  + *The fallback (acceptance) plan should the risk occur*
* Risk History
  + *Precede each entry with a Date*
* Risk Link Attachment
  + *Include any relevant risk history documents (e.g., emails, presentations, etc.)*

# Project Risk Management Checklist

The SMA ICD-10 Project Manager should reference the Project Risk Management checklist in Table 3 to manage the risk management process.

Table 3: Project Risk Management Checklist

| **Activity Number and Title** | **Task Checklist** |
| --- | --- |
| 1. Develop, Implement, and Manage Risk Management Plan | 🞎 Develop, Implement, and Manage a Risk Management Plan |
| 2. Identify Potential Risk | 🞎 Identify Potential Risks |
| 3. Submit Potential Risks | 🞎 Submit the Potential Risks electronically |
| 4. Research, Clarify, Consolidate, and Prioritize Risks | * Do you understand the risk? * Do you need to reword or consolidate the risk? * Any additional research required? * What is the initial Probability and Impact of the risk? * Update Risk Summary Template as appropriate |
| 5. Close Risk? | * Should the risk be closed? |
| 6a. Assign Risk Owner | * Assign a Risk Owner – Who is the best person to manage this risk? |
| 6b. Close Risk? | * Update the tool to reject or close a given risk |
| 7. Assess / Validate Risk Impact and Probability | * Is the risk clearly stated? * Is the risk valid? * What is the impact of the risk? Modify Impact, if applicable * What is the probability of occurrence? Modify Probability, if applicable * Update Risk Summary Template as appropriate |
| 8. Close Risk? | * Can this Risk be eliminated by taking some action(s)? |
| 9. Risk Magnitude yellow or red? | * Determine if the Risk Magnitude is yellow or red |
| 10a. Develop Risk Elimination Plan | * Develop Risk Elimination Plan, if possible |
| 10b. Develop Risk Mitigation Plan | * Develop Risk Mitigation Plan, if Risk Score is yellow or red |
| 10c. Develop Contingency Plan | * Develop Contingency Plan, if risk cannot be eliminated regardless of Risk Score |
| 11. Risk Elimination Plan Approval Process | * Seek approval of the Risk Elimination Plan using the appropriate process established by Project/Program Governance structure |
| 12. (Risk Elimination) Plan Approved? | * Was the Risk Elimination Plan approved? |
| 13. Implement Risk Elimination Plan | * Implement the approved Risk Elimination Plan |
| 14. Risk Mitigation Plan Approval Process | * Seek approval of the Risk Mitigation Plan using the appropriate process established by Project / Program Governance Structure |
| 15. (Risk Mitigation) Plan Approved? | * Was the Risk Mitigation Plan approved? |
| 16. Implement Risk Mitigation Plan | * Implement the approved Risk Mitigation Plan |
| 17. Contingency Plan Approval Process | * Seek approval of the Contingency Plan using the appropriate process established by Project / Program Governance Structure |
| 18. (Contingency) Plan Approved? | * Was the Contingency Plan approved? |
| 19. Monitor, escalate, and report on risk and related Plan(s) | * Review the status and progress on the individual Risks on a periodic basis * Escalate Risks as appropriate (Program level risks should be escalated to “1-Program Directors”) * Report on Risks on a periodic basis * “Deliver bad news early” * Change Risk Impact and/or Probability as appropriate * Document reasons for any changes to Risk Impact and/or Probability |
| 20. Risk Occurred? | * Monitor the Risk to determine if the Risk has occurred |
| 21a. Document Risk Trigger Details | * Document what the Risk trigger was, when the risk was triggered, and any details about the trigger |
| 21b. Close Risk? | * Is the risk ready to be closed? |
| 22. Handle as an issue? | * Should the risk that has occurred be handled as an issue? |
| 23a. Issue Management Process | * Issue is submitted to the Issue Management Process |
| 23b. Implement Contingency Plan | * Implement the approved Contingency Plan |

# Best Practices for Risk Management Process Items

## Identify and Classify Risk

Focusing attention on the value in determining risks facing each area of concern, and ensuring that risk planning is not perceived solely as an administrative exercise, is a process driven by the Risk Coordinator.

Initially, focusing management attention on risks is assisted by reviewing the following information sources for direction:

* Risks and constraints
* Project descriptions and deliverable definitions
* Existing project documentation, or documentation employed from other projects
* Knowledge transfer from functional/technical experts with experience in similar projects, application software, or technology platforms
* Previously identified risks from similar development projects.

The risks identified by the Program Directors and Risk Coordinators are documented into specifically defined, tangible risk items, for which a response/action should be well-defined and measurable. This ensures that all analysis and reporting of risks maintain a deliverable-focus, for which progress towards high-level objectives can be compared. It is important to distinguish between risks and issues. Risks are items that could occur in the future. They are intended to proactively consider events that could impact the project. Issues are events that have already occurred and require resolution.

Identification of vague or non-specific risks results in responses or actions that are ambiguous, intangible, unclearly defined, and difficult to mitigate adequately.

Additionally, it is important not to attempt to document all possible risks and outcomes, as this can often introduce improbable scenarios, that:

* Create unnecessary concern and confusion
* Shift the focus away from the real or probable risks
* Dilute the pool of risks, leading to diminishing returns on effort
* Reduce credibility for the risk mitigation process

Risk documentation is more concerned with identifying the areas where the consequences of the risk are most severe, and where corrective responses or actions will produce the largest benefits in risk reduction. Furthermore, risk documentation takes the areas where risks are most likely to occur and develops detailed assessment criteria from which specific risks are documented. Typical sources of assessment criteria are shown below:

* Unrealistic budget or schedule estimates
* Delivery on critical path, or unrealistic deliverable and milestone deadlines
* New technologies and platforms, complex/leading edge technologies, and complex environments
* Functionally complex data models, including processing functionality
* Staffing considerations for experts, numbers, and experience required
* External dependencies, including legislative changes

## Risk Classification

Risk categorization is achieved by defining five characteristic sources of risks. Select Risk Classification from the Risk Classification drop-down field. These describe the generic areas where specific risks are likely to occur, and formalize the categorization initially performed during Risk Planning:

### Cost

Cost-based risks outline the non-achievement of the financial benefits of ICD-10 Implementation. These cost risks include additional costs in changing/solving design, application program, or operational problems.

### Time

Schedule-based risks focus on the non-achievement of the program benefits within the specified time frame. These schedule-based risks arise from extensions from scope changes, resource unavailability, and additional schedule extensions from solving those risks outlined in Cost above.

### Quality

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

Operational-based risks focus on the peripheral organizational and business operational re-engineering changes, arising from ICD-10 Implementation. These risks consider both the transitional and the long-term effects of the program’s introduction, including the organizational and behavioral change required, the human and physical resource planning, and communication required to facilitate a smooth transition to the new structure.

### Scope

External-based risks consider the environmental factors largely outside of the control of the ICD-10 Leadership, which can directly/indirectly affect the successful delivery of ICD-10. Implementation Risks arising from legislative regulations, legal requirements, and the strategic direction and priority conflicts of a controlling body, are profiled under this category.

The cost and time risk sources are known as the risk indicators, as they are often the most tangible measure of overall progress towards project objectives or goals. The technological, operational, and external risk sources are referred to as risk drivers, as these are the sources of all project risks, which additionally drive the cost and schedule risks.

The recognition that the management of the sources of technological, operational, and external risks is inter-related to the management of cost and schedule risks, an important link in effectively responding and reporting risk-reducing activities.

## Analyze Risk

Following specific definitions of the risks above, the most likely overall response to the risk should be decided. This may be an obvious set of actions that annul or limit the risk occurring, or alternatively may be an intuitive best guess of the available actions that are likely to be effective.

Risk quantification extends the value of the understanding, documenting, and reporting on ICD-10 Implementation risks, by attempting to assign each risk to a numerical scale.

This introduces a common format to risk quantification, based on easily understood numerical scales. These assist in realizing and focusing on the true impact of each risk, and in the prioritization of the risk-reducing activities and responses identified. The following three parameters for each risk are quantified:

The SMA should score each risk associated with the ICD-10 transition. Below is a possible way to apply a risk score.

The SMA could score each risk by the likelihood (L) and severity (S) of occurrence.

The risk score (R) is equal to the value of the likelihood (L) multiplied by the severity (S).

**Risk (R) = Likelihood (L) x Severity (S)**

The likelihood scoring range is from 1 to 3.

Table 4 describes the likelihood of occurrence values.

Table 4: Likelihood of Occurrence Values

| Value | Level | Description |
| --- | --- | --- |
| 1 | Low | Minimal probability of taking place |
| 2 | Moderate | Equal probability of occurring or not taking place |
| 3 | High | Extreme probability of taking place |

The occurrence severity values range could be scored from 1 to 3, and 10. Catastrophic risks have a value of 10 because the risk impedes the SMA from achieving fundamental functions (e.g., payment). A risk of this nature has a significantly higher value to ensure catastrophic risks receive sufficient weight and attention. Table 5 describes the occurrence severity values.

Table 5: Occurrence Severity

| **Value** | **Level** | **Description** |
| --- | --- | --- |
| 1 | Low | Risk occurrence will have a minor affect on the SMA business outcomes and will require minimal or no effort to address. The SMA can use workarounds to continue business processes and systems without affecting outcomes. |
| 2 | Moderate | Risk occurrence will have some affect on the SMA business outcomes. The SMA can use short term workarounds, but there would be the possibility of affecting the effectiveness or efficiency of the area (e.g., longer timeframes, greater cost). Avoiding or mitigating the risk will require some expenditure of resources. |
| 3 | High | Risk occurrence will have an extreme affect on the SMA business outcomes and require more expenditure of resources to address. Using short term workarounds could not prevent negative affects to outcomes (e.g., longer timeframes, greater cost). |
| 10 | Catastrophic | Risk occurrence will derail operations and the SMA will not be able to accomplish one or more primary objectives. The incident will tarnish the agency’s reputation and temporary fixes will not be feasible to mitigate the risks. |

Table 6 describes the risk levels associated with the risk scores calculated by multiplying the severity and likelihood values.

Table 6: Risk Levels

|  |  |
| --- | --- |
| **Risk Score** | **Risk Level** |
| 1-3 | Low |
| 4-5 | Moderate |
| 6-9 | High |
| 10-30 | Catastrophic |

## Determine Approach to Identified Risk

Following submission, risks will be monitored and reported on a weekly basis by ICD-10 Program Leadership. The Risk Coordinator will work with projects or ICD-10 PMO Manager to update the risk artifacts/record as necessary.

The Program and Project Leadership will address risks on a prioritized basis. Risks will be prioritized according to their impact and the ability to influence the risk. A risk response will be developed for every risk.

## Track Risk

The ICD-10 PMO Manager is responsible for monitoring the status of risks and the actions taken to mitigate them. Risks are monitored and tracked via various reports and managed during routine communication points.

## Mitigate Risk

Overall, ICD-10 Implementation risk response analysis covers five characteristic responses, discussed below:

### Avoidance

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

### Control

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

### Acceptance

These describe the factors that may directly affect the success of ICD-10 Implementation, but are outside of the sphere of influence of ICD-10 Implementation Leadership, and can therefore only be accepted. In addition, acceptance of risks as a response may be based on the cost-ineffectiveness of any available response or solution. An example: acceptance response could be created from a legislative or legal risk, over which no control could be leveraged.

### Transfer

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

### Investigation

Investigation-based responses do not define any mitigation for reducing an individual risk. They are responses to risks where no clear solution is identified, and further research is required. However, investigative responses should not be ignored, as they immediately and directly lead to a greater aggregated ICD-10 Implementation risk. This is because the probability quantifier for each risk includes the effect of the applied response, for which there is none, and the level of control quantifier indicates the level of influence to apply that response, which is low.

Individuals will list the identified risks and identify and record potential actions that could be taken to avoid or mitigate the risks. Actions will be identified which should be immediately incorporated into the project plan to partially reduce the risk, as well as actions that should be treated as contingent risk responses. Additionally, risk mitigation owners will be assigned to each risk.

## Escalation Process

In addition to the Approval Process established by the ICD-10 PMO, the Risk Management Process requires an escalation process to address potential conflicts and disagreements. The ICD-10 PMO has the authority to close the risk. When the Risk Owner disagrees with the PMO Manager, he or she can appeal to the ICD-10 Executive Sponsor for further clarification and possible intervention.

# Suggested Risk Reporting

The following Core Set of Risk reports should be generated by the Risk Reporting System by the SMA, as recommended by the SMA. However the SMA may identify other reports deemed of appropriate value. The SMA should determine what additional reporting is required to effectively enable the risk management process. Table 7 outlines recommended risk reports.

**Generated:** Indicates the risk report owner

**Report Name:** Indicates the name of the report

**Contents:** Indicates the report content and layout

**Sort Criteria:** Indicates the report sorting functionality that the report should account for.

Table 7: Recommended Risk Reports

| **Generated** | **Report Name** | **Contents** | **Sort Criteria** |
| --- | --- | --- | --- |
| **As needed by PMO team** | **Executive Risk Summary** | Used for reporting on risks at the executive level. Composed of three separate reports: Risk Overview, Risk Stats, and Top Risks. | 1. State (Open) 2. Impact 3. Escalation (1-Program Directors) |
| **As needed by PMO team** | **All Risks Detailed Report** | Ability to filter by project, severity or elevate to sponsor field. Sorts all Risks by severity. | 1. State (Open) 2. Impact 3. Escalation (1-Program Directors) |
| **As needed by Teams** | **Risk by Owner** | Ability to filter by Project, System Risk Exposure/Score, Owner, and Next Review date. Sorts all Risks by Risk Exposure/Score. | 1. State (Open) 2. Impact 3. Escalation (1-Program Directors) |
| **Weekly by PMO Team** | **Risk Detail** | Ability to filter by Project, System Risk Exposure/Score, Owner, and Next Review date. Sorts all Risks by Risk Exposure/Score. Will be used primarily within ICD-10 Implementation for the weekly management of Risks. | 1. State (Open) 2. Impact 3. Escalation (1-Program Directors) |
| **As needed by Teams** | **Risk Summary** | Ability to filter by Project, System Risk Exposure/Score, Owner, and Next Review date. Sorts all Risks by Risk Exposure/Score. | 1. State (Open) 2. Impact 3. Escalation (1-Program Directors) |

# The items provided in this Risk Management Plan are intended to be an aide/guide to the SMAs in their efforts to manage the program risks.

# Appendix: SMA Medicaid Information Technology Architecture (MITA) Risks

Note: For this appendix, please refer to the MITA Impact Analysis.

## ****1.1 Purpose****

This document identifies risks SMAs may face during ICD-10 Implementation. The document categorizes risks using the MITA Business Framework (Version 2). SMAs should evaluate all business processes to identify if there are additional risks based on the SMAs unique business processes, policies, and systems.

*Note: The MITA Business Process risks identified below are not a comprehensive list of all risks the SMAs may face.*

## ****1.2 Operations Management Risks****

* **Authorize Treatment Plan Impact Risks**
  + SMAs could inadvertently deny prior-authorization on Treatment Plans that actually deserve prior authorization due to confusion in mapping ICD-9 codes to ICD-10 codes.
  + SMAs could overpay and authorize too many treatment plans from improper ICD-9 to ICD-10 manual code mapping.
* **Authorize Referral Impact Risks**
  + SMAs could inadvertently deny referrals for medically necessary procedures if they map an ICD-10 code received from a provider incorrectly to an ICD-9 code.
  + SMAs could add unnecessary delays to the referrals process as they attempt to map received ICD-9 codes to ICD-10 codes manually.
  + SMAs could overpay and accept too many referrals from improper ICD-9 to ICD-10 manual code mapping.
* **Authorize Service Impact Risks**
  + SMAs could inadvertently deny services for medically necessary procedures if they map an ICD-10 code received from a provider incorrectly to an ICD-9 code.
  + SMAs could add unnecessary delays to the authorize service process as they attempt to map received ICD-9 codes to ICD-10 codes manually.
  + SMAs could overpay and authorize too many services from improper ICD-9 to ICD-10 manual code mapping.
* **Edit Claim/Encounter Impact Risks**
  + SMAs could end up mapping incorrectly and denying claims/encounters inappropriately.
  + SMAs could end up overpaying or underpaying on current claims/encounters without this process working correctly with the new ICD-10 codes.
  + Incorrect ICD-10 data passed to Audit Claim/Encounter could lead to future overpayments or underpayments for services.
  + Managed care entities would have issues sending their ICD-10 encounter data if SMAs are not using ICD-10 codes as well.
* **Price Claim/Value Encounter Impact Risks**
  + SMAs could end up overpricing/valuing claims/encounters, which would require the providers to pay more than they perhaps can/should.
  + SMAs could end up under-pricing/undervaluing claims/encounters, which would require the SMA to pay more than they perhaps can/should.
* **Audit Claim/Encounter Impact Risks**
  + SMAs could end up mapping incorrectly and auditing/denying claims/encounters inappropriately.
  + SMAs could end up overpaying or underpaying on current claims/encounters without this process working correctly with the new ICD-10 codes.
  + Incorrect ICD-10 data archived in this process could lead to future overpayments or underpayments for services.
* **Prepare Remittance Advice/Encounter Report Impact Risks**
  + SMAs could confuse providers with reports that lose information due to manual ICD-10 to ICD-9 to back to ICD-10 code mapping. The confusion would lead to more provider inquiries, burdening the SMA as they receive and respond to those inquiries.
  + SMAs could prepare incorrect reports, also leading to provider confusion and more provider inquiries.
* **Prepare Home and Community Based Services (HCBS) Payment Impact Risks**
  + SMAs could confuse HCBS providers with reports that lose information due to manual ICD-10 to ICD-9 to back to ICD-10 code mapping. The confusion would lead to more HCBS provider inquiries, burdening the SMA as they address those inquiries.
  + SMAs could prepare incorrect reports, also leading to HCBS provider confusion and more provider inquiries.
* **Prepare Explanation of Benefits (EOB) Impact Risks**
  + SMAs could explain benefits incorrectly leading to confusion in claims processing if ICD-9 to ICD-10 manual mapping is incorrect.
  + SMAs could determine incorrect services received by the Recipient and described, via ICD-10 codes, by a provider in the ICD-9 to ICD-10 manual mapping effort. This could lead to incorrect payments on claims that would either incorrectly reduce payments to providers or result in overpayments by the SMA.
* **Prepare Health Insurance Premium Payment Impact Risks**
  + SMAs could end up overpaying or underpaying on current premiums without this process working correctly with the new ICD-10 codes.
* **Prepare Medicare Premium Payment Impact Risks**
  + SMAs could end up overpaying or underpaying on current premiums without this process working correctly with the new ICD-10 codes.
  + SMAs could end up overpaying or underpaying on future premiums without this process working correctly with the new ICD-10 codes.
* **Prepare Capitation Premium Payment Impact Risks**
  + SMAs could end up overpaying or underpaying on current premiums without this process working correctly with the new ICD-10 codes.
  + SMAs could end up overpaying or underpaying on future premiums without this process working correctly with the new ICD-10 codes.
* **Manage Payment Information Impact Risks**
  + SMAs could inadvertently deny services if this central process maps ICD-9 to ICD-10 codes incorrectly.
  + SMAs could add unnecessary delays to the processing claims/encounters if this central process maps ICD-9 to ICD-10 codes incorrectly.
  + SMAs could overpay and authorize too many services if this central process maps ICD-9 to ICD-10 codes incorrectly, which would heavily burden the SMA.
  + SMAs could underpay and authorize too few services if this central process maps ICD-9 to ICD-10 codes incorrectly, which would heavily burden the providers.

**Impact Level**

The risks identified in the previous section have associated work efforts that are involved to ensure that Operations Management is prepared to transition to ICD-10. Table 8 identifies the Impact Level for these processes in Operations Management.

Table 8: Operations Management Business Processes Impact Levels

| **MITA Business Function** | **MITA Business Process** | **Impact Level (1-3)** | **Impact Classification** |
| --- | --- | --- | --- |
|  | Authorize Treatment Plan | 2 | Moderate |
| Service Authorization | Authorize Referral | 2 | Moderate |
|  | Authorize Service | 2 | Moderate |
|  | Edit/Claim Encounter | 3 | High |
| Payment Management 🡪 Claims/Encounter Adjudication | Price Claim/Value Encounter | 3 | High |
|  | Audit Claim/Encounter | 3 | High |
|  | Prepare Remittance Advice/Encounter Report | 1 | Low |
| Payment Management 🡪 Payment Reporting | Prepare HCBS Payment | 1 | Low |
|  | Prepare EOB | 1 | Low |
|  | Prepare Health Insurance Premium Payment | 1 | Low |
| Payment Management 🡪Capitation and Premium Preparation | Prepare Medicare Premium Payment | 1 | Low |
|  | Prepare Capitation Premium Payment Impact | 1 | Low |
| Payment Information Management | Manage Payment Information | 3 | High |

## ****1.3 Program Management Risks****

* **Designate Approved Service/Drug Formulary** 
  + SMAs may incorrectly determine fiscal impacts and medical appropriateness for various benefit plans.
  + The SMAs may incorrectly define coverage criteria or incorrectly establish limitations or authorization requirements for approved codes.
  + Resulting information passes to Manage Rates Setting, which establishes rates for services and drugs. These processes need to synchronize with ICD-10 codes to correctly pay and process claims.
  + The SMA independently update their existing code set and evaluate their unique policies based on Drug formularies.
* **Manage Rate Setting** 
  + SMAs may incorrectly define rates for products and services.
  + SMAs may inadvertently change rates for non-requested products or services based on incorrect mapping between ICD-9 and ICD-10 codes.
  + SMAs may not be able to update medical products and services pricing, thus inhibiting ability to correctly add additional products and services for the formulary or reimburse for them.
* **Develop and Maintain Benefit Package**
  + SMAs may not be able to appropriately synchronize with federal and state laws and policies.
  + Budgetary impact and implementation feasibility analyses may be flawed due to an inability to assess ICD-10 codes accurately.
  + SMAs design benefits packages around specific diagnoses and conditions tied to ICD-10 codes. Without updating to ICD-10 codes, SMAs may not be able to design accurate benefit packages.
* **Perform Accounting Functions**
  + SMAs must manage the risk of providing recipients with incorrect refund amounts. (Note: Manage Recoupment is a successor process).
  + SMAs may not generate accurate financial reports and program analysis without correct ICD-10 implementation.
  + Federal and state reporting requirements may require ICD-10 use in reporting data.
* **Maintain Benefit/Reference Information** 
  + SMAs will need to manage benefit and reference information received from the Edit Claim/Encounter, Audit Claim/Encounter or Price Claim/Encounter processes accurately, assuming these processes use ICD-10 codes.

**Impact Level**

The risks identified in the previous section have associated work efforts that are involved to ensure that Program Management is prepared to transition to ICD-10. Table 9 identifies the Impact Level for these processes in Program Management.

Table 9: Program Management Business Processes Impact Levels

| **MITA Business Function** | **MITA Business Process** | **Impact Level (1-3)** | **Impact Classification** |
| --- | --- | --- | --- |
|  | Designate Approved Service/Drug Formulary | 3 | High |
| Benefit Administration | Manage Rate Setting | 2 | Moderate |
|  | Develop and Maintain Benefit Package | 3 | High |
| Accounting | Perform Accounting Functions | 2 | Moderate |
| Program Information | Maintain Benefit/Reference Information | 2 | Moderate |

## ****1.4 Provider Management Risks****

* **Enroll Provider**
  + SMAs need to determine rates and contracting parameters, based on updated ICD-10 codes. [Currently, it is unclear if provider enrollment forms contain ICD-10 data.]
* **Disenroll Provider**
  + SMAs will need to manage the impact of ICD-10 on disenrolling providers and re-assigning members to providers with similar allowed services.
* **Manage Provider Grievance and Appeal**
  + For some states, generating a new grievance or appeal can be the same as generating a new claim, which requires ICD-10 codes. Without the codes, the SMA may be unable to process the claim.

**Impact Level**

The risks identified in the previous section have associated work efforts that are involved to ensure that Provider Management is prepared to transition to ICD-10. Table 10 identifies the Impact Level for these processes in Provider Management.

Table 10: Provider Management Business Processes Impact Levels

| **MITA Business Function** | **MITA Business Process** | **Impact Level (1-3)** | **Impact Classification** |
| --- | --- | --- | --- |
| Provider | Enroll Provider | 1 | Low |
| Enrollment | Disenroll Provider | 1 | Low |
| Provider Support | Manage Provider Grievance and Appeal | 2 | Moderate |

## ****1.5 Contractor Management Risks****

* **Award Health Services Contract** 
  + There is a risk of inaccurate contract negotiations since the US system will update to ICD-10 codes, this process needs to accommodate this change.
  + There is a risk of incorrect mapping from ICD-9 codes to ICD-10 codes during RFP evaluation or contract negotiations, resulting in protest or overpayment for services after contract award.
  + There is a risk of creating incorrect service requests in RFPs.

**Impact Level**

The risk identified in the previous section has associated work efforts that are involved to ensure that Contractor Management is prepared to transition to ICD-10. Table 11 identifies the Impact Level for these processes in Contractor Management.

Table 11: Contractor Management Business Processes Impact Levels

| **MITA Business Function** | **MITA Business Process** | **Impact Level (1-3)** | **Impact Classification** |
| --- | --- | --- | --- |
| Health Services | Manage Health Services Contract | 2 | Moderate |
| Contracting | Award Health Services Contract | 2 | Moderate |

## ****1.6 Member Management Risks****

* **Enroll Member**
  + Members may not receive additional benefits for which they qualify.
  + Incorrect health eligibility data may be placed into the Member data store, which is a central information repository for several processes. Inaccuracy of initial information may cause complications for the SMA and the member in various processes retrieving data from the data store.
* **Disenroll Member**
  + There is a risk of inaccurately processing a member’s failure to meet enrollment criteria as a result of a change in health status.
  + There is a risk of incorrect preparation of member premium payment if health status information upon disenrollment is inaccurate.
* **Determine Eligibility**
  + SMAs may incorrectly assign benefit packages.
  + SMAs may establish incorrect eligibility categories.
  + SMAs may deny applicants who are eligible to receive certain services.
* **Manage Member Information**
  + SMAs access the member information for eligibility verification. The lack of ICD-10 use here may interfere with appropriate eligibility determinations.
  + Member information management directly affects essential Member Management and Operations Management business processes, including encounter, claims, and payment processes. Incorrect ICD-10 updating and synchronization could disrupt daily operations.
* **Inquire Member Eligibility**
  + SMAs may authorize services and benefits incorrectly resulting in overpayment.
  + SMAs may be unable to authorize services and benefits thus impeding recipients from receiving basic and necessary services.
* **Manage Member Grievance and Appeal**
  + If this process has not properly updated ICD-10 codes, the SMA risks approving or denying an appeal in a manner not in accordance with federal or state law.
  + Appeal processes result in policy changes. Inaccurate ICD-10 code usage could result in an undesirable policy change.

**Impact Level**

The risks identified in the previous section have associated work efforts that are involved to ensure that Member Management is prepared to transition to ICD-10. Table 12 identifies the Impact Level for these processes in Member Management.

Table 12: Member Management Business Processes Impact Levels

| **MITA Business Function** | **MITA Business Process** | **Impact Level (1-3)** | **Impact Classification** |
| --- | --- | --- | --- |
| Enrollment | Enroll Member | 1 | Low |
| Enrollment | Disenroll Member | 1 | Low |
| Eligibility Determination | Determine Eligibility | 2 | Moderate |
| Member Information | Manage Member Information | 2 | Moderate |
| Management | Inquire Member Eligibility | 1 | Low |
| Prospect and Current Member Support | Manage Member Grievance and Appeal | 2 | Moderate |

1. The term “project” refers to any ICD-10 relevant project team. Project teams can be aligned to business processes, policy groups or systems. [↑](#footnote-ref-1)
2. The term “program” refers to the ICD-10 Implementation program overall. [↑](#footnote-ref-2)
3. Workgroups can be comprised of internal SMA resources and external contractor or vendor SMEs (as needed). Workgroups can be especially useful in:

   * Addressing recommended actions and raising issues and risks to leadership;
   * Facilitating communications across MITA business areas to limit duplication of work effort spanning multiple MITA business areas; and
   * Reaching beyond the SMA fostering communication with other SMAs or focus groups implementing ICD-10.

   [↑](#footnote-ref-3)