CHAPTER 7:

RISK MANAGEMENT PLAN

7.1. INTRODUCTION

The scope of this document pertains to the Project and its internal and external risks. The risk management methodology identified in this document will be primarily used during the entire Project.

In software development, we tend to ignore risks. Potential risks of a project must be identified as early as possible. It is rather naive

to suppose that a software project will run smoothly from start to finish. It won't. We should identify the risks of a software project early on and provide measures to deal with them. Doing so is not a sign of unwarranted pessimism. Rather, it is a sign of wisdom.

7.2. RISKS

A risk is a possible future negative event that may affect the success of an effort. So, a risk is not a problem, yet. It may become one, though, and risk management is concerned with preventing risks from becoming problems. Some common examples of risks and ways to deal with them, are:

- Requirements may be unstable, immature, unrealistic, or excessive. If we merely list the requirements and start to realize the system in a linear development mode, it is likely that a lot of rework will be needed. This results in schedule and budget overruns, since this rework was not planned. If the requirements volatility is identified as a major risk, an evolutionary development strategy can be chosen. This situation fits the exploration-problem category as identified in the previous section.
- If there is little or no user involvement during the early development stages, a real danger is that the system will not meet user needs. If this is identified as a risk, it can be mitigated by having users participate in design reviews.
- If the project involves different or complex domains, the spread of application knowledge within the project team may be an issue. Recognizing this risk may result in timely attention and resources for a training program for team members.

- If the project involves more than one development site, communication problems may arise. A common way to deal with this is to pay attention to socialization issues, for instance by scheduling site visits.

7.2.1. Risk Factors

Table 7.1 Some Risk Factors

Risk	Description
Personnel shortfall	May manifest itself in a variety of ways, such as inexperience with the domain, tools or development techniques to be used, personnel turnover, loss of critical team members, or the mere size of a team.
Unrealistic schedule/ budget	Estimates may be unrealistic with respect to the requirements.
Wrong functionality	May have a variety of causes, such as an imperfect understanding of the customer needs, the complexity of communication with the client, insufficient domain knowledge of the developers and designers.
Wrong user interface	In certain situations, the user-friendliness of the interface is critical to its success.
Gold plating	Developers may wish to develop ‘nice’ features not asked for by the customer.
Requirements volatility	If many requirements change during development, the amount of rework increases.
Bad external components	The quality or functionality of externally supplied components may be below what is required for this project.
Bad external tasks	Subcontractors may deliver inadequate products, or the skills obtained from outside the team may be inadequate.
Real-time shortfalls	The real-time performance of (parts of) the system may be inadequate.

Risk	Description
Capability shortfalls	An unstable environment or new or untried technology pose a risk to the development schedule.

7.2.2. Risk Categories

Table 7.2 Risk Categories

	Level of control		
		Low	High
Relative importance	Low	Customers and users (C1)	Scope and requirements (C2)
	High	Environment (C4)	Execution (C3)

- C1: Risks related to customers and users. Examples include a lack of user participation, conflicts between users, or a user organization resisting change. Part of this can be mitigated through an agile approach. But equally often, such risks are beyond the project manager's control.
- C2: Risks that have to do with the scope of the project and its requirements. Various factors from figure 8.3 fall into this category: wrong functionality, gold plating, requirements volatility. Project managers should be able to control this type of risk.
- C3: Risks that concern the execution of the project: staffing, methodology, planning, control. Factors like personnel shortfall and an unrealistic schedule or budget belong to this category. Again, project managers should be able to control these risks.
- C4: Risks that result from changes in the environment, such as changes in the organization in which the system is to be embedded, or dependencies on outsourcing partners. Project managers often have few means to control these risks.

7.3. RISK MANAGEMENT PROCESS

The Project Management Plan will continue to be executed throughout the

The Project Risk Management Paradigm, depicted in Figure 1, summarizes the Risk Management process for the project. This paradigm portrays the high-level process steps of the Risk Management process, which are:

Step 1 – Identify
Step 2 – Analyze
Step 3 – Plan
Step 4 – Implement
Step 5 – Track and Control
Continuous Process – Communicate

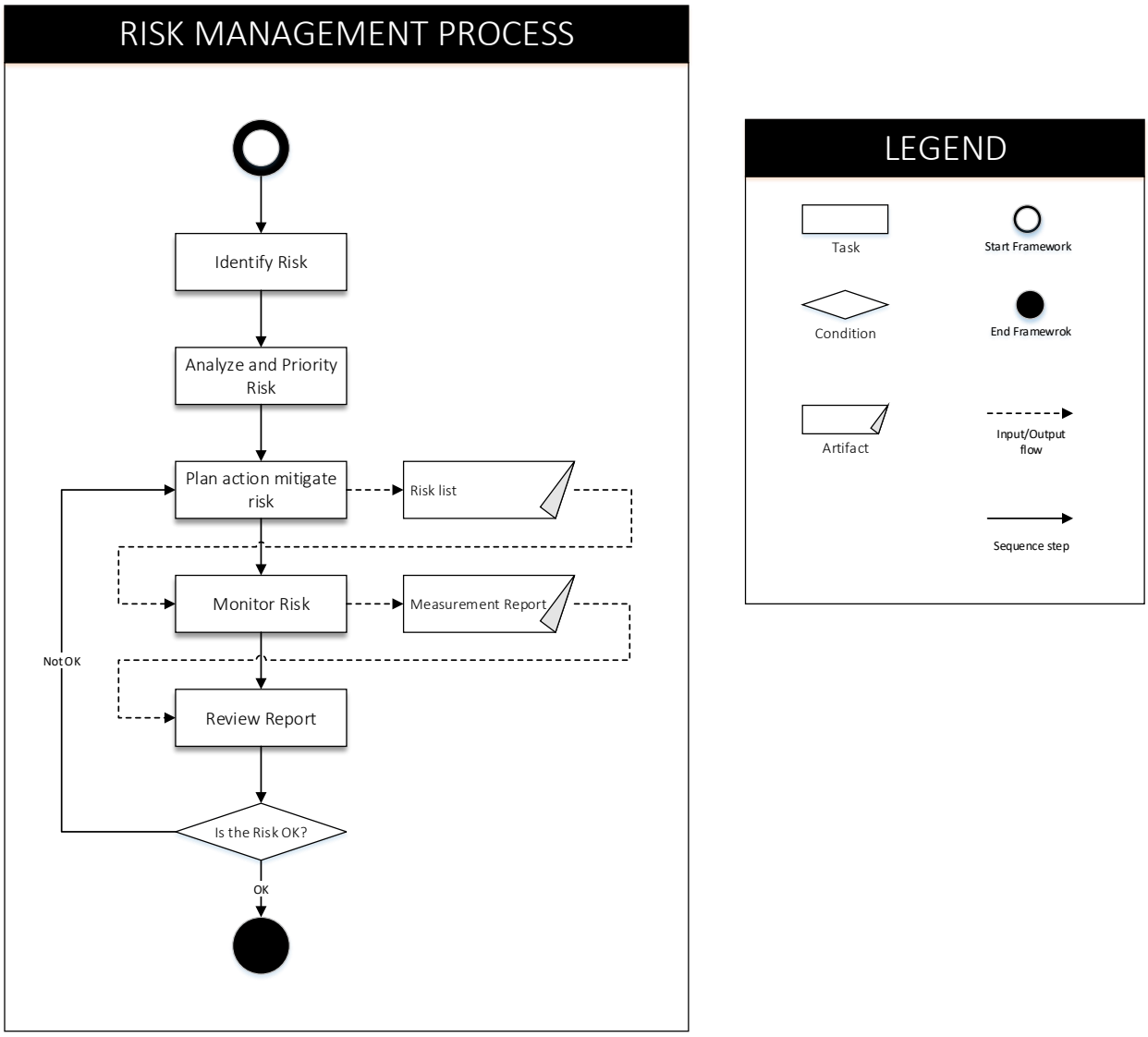

Figure 7.26 Risk Management Process

7.3.1. Step 1 – Identify Risk

The objective of Step 1 – Identify is to search and find risks before they become problems using risk identification. Risk identification involves a process where concerns about a project are transformed into identified risks. Identified risks can be described and measured. A detailed discussion of the identification process is provided in the sub-paragraphs below.

- Identify and Collect Candidate Risks

  Through the use of risk identification methods and the application of industry standards, all team members search for and identify potential issues and concerns which could impact the overall success of the project. Methods to identify risks may include: monitoring project activities, examining artifacts and documentation, observing, interviewing, polling, surveying, brainstorming, participating in discussions and meetings, conducting focus sessions. These potential issues and concerns result in candidate risks.

- Identify and Provide Candidate Risk Input to the Project Manager

  The project participants, including the project team, stakeholders, are key sources for identifying issues and concerns and submitting these as candidate risks to input to the Risk Management process. The Project participants voluntarily submit candidate risks to the Project Manager as input to Step 2.3.

  The methods used by the Project participants to submit candidate risks to the Project Manager include, but are not limited to, the following: verbal, email, or written communication.

  Project participants may submit candidate risks to the Project Manager using the Risk Candidate Identification Form, ensuring the key risk identification components identified are captured.

  While this form will be the primary tool used for this process, any communication method is acceptable. If this form is not used for submission, the Project Manager will enter the risk data directly into Risk Radar and provide a copy of the data entered to the originator for verification.

- Review Candidate Risks

  This step involves collecting candidate risk input from Project participants and reviewing these candidate risks. Candidate risks that can be described and measured become “identified risks”. The Project Manager will work with risk originators and the Mentor to achieve consensus on deciding whether or not candidate risks become identified risks.

Reviewing candidate risks includes defining the risk and capturing appropriate information about the candidate risk to support risk analysis in Step 2 – Analyze. "Defining the risk" involves understanding the definition of a risk, and applying the Criteria for Risk Identification provided as a guide.

Table 7.3 Criteria for Risk Identification

1. **Is it a risk?** Is the concern a risk? A risk is a **potential event** that would have an **impact** on the success of the project if the event were to occur. The following considerations support the question "*Is it a risk?"*
2. **Impact:** This step identifies consequences of the risk materializing. Is the impact of the potential risk event on the project significant enough to warrant inclusion in the Risk Management process? This is an initial, informal determination of the risk impact. A formal assessment of the risk impact is done in *Step 2 – Analyze*.
3. **Potential Event**. What is the minimum likelihood of the potential risk event occurring? This question considers the degree of uncertainty of the potential risk event. Risk events which have already occurred represent issues, not risks. However, if there is little or no likelihood of the risk event occurring, the risk may not warrant inclusion in the Risk Management process. Potential risk events that have an extremely low likelihood of occurring do not necessarily require the risk to be formally recognized by the Risk Management process. This is an initial, informal determination of the risk probability. A formal assessment of the risk probability is done in *Step 2 – Analyze*.

Table 7.4 Risk Identification Components

COMPONENT	DESCRIPTION
Originator	Name and organization of the person who identified and submitted the candidate risk to the Project Manager. This information will not be required for risk identification methods, which allow anonymous candidate risk input.

Origination Date	Date the candidate risk was either identified or submitted to the Project Manager (will vary due to the risk identification method used).
Risk Title	A brief (phrase or one sentence) description of the candidate risk that captures the key subject of the candidate risk or summarizes the risk description.
Risk Description	Concise description of the candidate risk. Capturing a statement of risk includes considering and recording the conditions that are causing concern of a possible loss to the project. A description of the perceived consequences resulting from the conditions is also included.
Risk Context	Detailed description of the candidate risk, including circumstances and supporting detail. Capturing the context of a risk involves recording information regarding the circumstances, events, and interrelationships within the project that supplements the risk statement. Context provides more detail than is presented by the risk description.

- Record Identified Risks

  "Candidate risks" will be recorded while they are being analyzed. If after analysis, it is determined not a risk to the project, it will be retired. Candidate risks that become identified risks will be actively mitigated and tracked in the Risk List.

  The Project Manager records the identified risk from step 1-3 in the Risk List as a discrete risk item.

7.3.2. Step 2 – Analyze

The objective of Step 2 – Analyze is to transform risk items into information that can be used to aid decision-making and to validate the risk information, using risk analysis. Risk analysis involves classification and prioritization of risk items, providing recommendations for mitigating and measuring risk items, and reviewing risk item information. The tools and methodologies used for analysis may include: Risk List, expert knowledge, and root cause analysis. The Project Manager, Mentor will review resulting

risk analyses with the Stakeholders as required. The outputs of this step are retired identified risks or identified risks that have been classified and prioritized with recommended mitigations and measurements. A detailed discussion of the analysis process is provided in the sub-paragraphs below.=

- Verify/Determine Risk Classification

  The Risk Owner with the assistance of the Project Manager perform "root cause" analysis to determine risk class. Risk classes are categories for risk items. Risk classes are usually a higher level of abstraction derived from individual risk items. Individual risk items can belong to one or more classes. The level of abstraction should be tailored to meet the specific needs of the project.

  The SEI Risk Taxonomy from Taxonomy-Based Risk Identification, 1993, and the PMI A Guide to the Project Management Body of Knowledge, 2004, will be used as guidelines for identifying risk classes. Identified Risk Classes are:

Table 7.5 Risk Classification

A. Product Engineering	**B. Development Environment**	**C. Program Constraints**
1. Requirements	1. Development Process	1. Resources
a. Stability	a. Formality	a. Schedule
b. Completeness	b. Suitability	b. Staff
c. Clarity	c. Process Control	c. Budget
d. Validity	d. Familiarity	d. Facilities
e. Feasibility	e. Product Control	2. Contract
f. Precedent	2. Development System	a. Type of Contract
g. Scale	a. Capacity	b. Restrictions
2. Design	b. Suitability	c. Dependencies
a. Functionality	c. Usability	3. Program Interfaces
b. Difficulty	d. Familiarity	a. Customer
c. Interfaces	e. Reliability	b. Associate Contractors
d. Performance	f. System Support	c. Subcontractors
e. Testability	g. Deliverability	d. Prime Contractor
f. Hardware Constraints	3. Management Process	e. Corporate Management
g. Non-Developmental Software	a. Planning	f. Vendors
3. Code and Unit Test	b. Project Organization	g. Politics

A. Product Engineering	B. Development Environment	C. Program Constraints
a. Feasibility	c. Management Experience	
b. Testing	d. Program Interfaces	
c. Coding/Implementation	4. Management Methods	
4. Integration and Test	a. Monitoring	
a. Environment	b. Personnel Management	
b. Product	c. Quality Assurance	
c. System	d. Configuration Management	
5. Engineering Specialties	5. Work Environment	
a. Maintainability	a. Quality Attitude	
b. Reliability	b. Cooperation	
c. Safety	c. Communication	
d. Security	d. Morale	
e. Human Factors		
f. Specifications		

- Verify/Determine Risk Impact

  Determining the risk impact considers the consequences the risk would have on the project if the risk event occurs. Risk impact is a description of the anticipated consequences of a risk event occurring. The Criteria for Risk Impact in Table 3 is a guide for evaluating the risk consequences and determining the risk impact, expressed as “low”, “medium” or “high”, impact is recorded as a number from 1 to 3. Impact values 1 correspond to a Low value, 2 is Medium, and 3 is High.

  The determination of risk impact is a subjective, qualitative process which considers the criticality of internal and external project factors within the specific context of the Project.

Table 7.6 Criteria for Risk Impact

IMPACT	CRITERIA
High	Risk consequences include one or more of the following: Significant schedule delay. For example, delay in a critical path activity by more than 2 months. Significant cost increase. For example, project budget or cost increase by more than 20%.

IMPACT	CRITERIA
	Significant technical change. For example, system performance decreases by more than 50%. Significant resource change. For example, loss of more than 20% of personnel, or loss of more than 10% of key management personnel. Significant political repercussions. For example, non-compliance with current legislation that involves significant penalties. Significant user dissatisfaction. For example, more than 20% of users are extremely dissatisfied with more than 20% of system functions or performance characteristics.
Medium	Risk consequences include one or more of the following, but do not include any consequences identified as "High" above: Moderate schedule delay. For example, delay in a critical path activity by 2-8 weeks, or delay in a non-critical path activity by more than 1 month. Moderate cost increase. For example, project budget increase by 10-20%. Moderate technical change. For example, system performance decreases by 20-50%. Moderate resource change. For example, loss of 10-20% of personnel, or loss of 5-10% of key management personnel. Moderate political repercussions. For example, moderate dissatisfaction of political parties or special interest groups. Moderate user dissatisfaction. For example, 10-20% of users are extremely dissatisfied with 10-20% of system functions or performance characteristics, or more than 20% of users are moderately dissatisfied with more than 20% of system functions or performance characteristics. Moderate client dissatisfaction. For example, payments to custodial parents are inaccurate.
Low	Risk consequences include one or more of the following, but do not include any consequences identified as "High" or "Medium" above: Minor schedule delay. For example, delay in a critical path activity by less than 2 weeks, or delay in a non-critical path activity by less than 1 month. Minor cost increase. For example, project budget increase by less than 10%. Minor technical change. For example, system performance decreases by less than 20%. Minor resource change. For example, loss of less than 10% of personnel, or loss of less than 5% of key management personnel.

IMPACT	CRITERIA
	Minor political repercussions. For example, minor dissatisfaction of political parties or special interest groups. Minor user dissatisfaction. For example, less than 20% of users are extremely dissatisfied with less than 20% of system functions or performance characteristics. Minor client dissatisfaction. For example, overpayments to custodial parents.

- Verify/Determine Risk Probability

  Determining risk probability involves considering the likelihood of the risk occurrence. The Criteria for Risk Probability is a guide for the risk probability as either high, medium, or low.

Table 7.7 Criteria for Risk Probability

PROBABILITY	CRITERIA
High	It is almost certain or very likely that the risk will occur. There is approximately a 65% or higher confidence level that the risk will occur.
Medium	It is somewhat probable that the risk will occur. There is approximately a 35-65% confidence level that the risk will occur.
Low	It is unlikely or improbable that the risk will occur. There is approximately a less than 35% confidence level that the risk will occur.

- Verify/Determine Risk Timeframe

  The risk timeframe is the period of time within which the risk is expected to occur. The Criteria for Risk Timeframe is a guide for evaluating the period of time a risk is expected to occur and determining the risk timeframe, expressed in terms of short-term, medium-term, or long-term.

Table 7.8 Criteria for Risk Timeframe

TIMEFRAME	CRITERIA
Short-Term	The risk is expected to occur within a very short period of time, e.g., ≤ 180 days.

Medium-Term	The risk is expected to occur within the near future, e.g., > 180 and ≤ 360 days.
Long-Term	The risk is expected to occur in the far future, e.g., > 360 days in the future.

- Verify/Determine Risk Exposure

  The risk exposure is derived from the risk attributes of impact and probability, and is used in conjunction with timeframe to prioritize risks for mitigation and escalation. Determine risk exposure for each risk from the intersection of that risk's impact and probability.

Table 3.9 Determination of Risk Exposure

	Probability			
Impact		**High**	**Medium**	**Low**
	High			Medium
	Medium		Medium	Low
	Low	Medium	Low	Low

- Verify/Determine Risk Severity

  The severity of the risk is a determination of the importance of the risk based upon 1) potential impact of the risk on the project, 2) the probability of occurrence, and 3) the risk timeframe.

Table 3.10. Determination of Risk Severity

	Exposure			
Time Frame		**High**	**Medium**	**Low**
	Short-Term			Medium
	Med-Term		Medium	Low
	Long-Term	Medium	Low	Low

- Develop Recommended Mitigations and/or Contingencies

  Develop recommended actions to mitigate the risk. Mitigation is a response to a risk, designed to reduce or eliminate the probability and/or impact of the risk:

Elimination – removing the threat of the risk event occurring by eliminating the cause.

Reduction – reducing the severity of the risk by either reducing the impact on the project, the probability of occurrence, or both.

If no mitigation actions are available, the risk impact is accepted:

Acceptance – accepting the consequences of the risk event. Acceptance can be active (e.g., developing a contingency plan to be executed if the risk event occurs), or acceptance can be passive (e.g., taking no action, allowing the risk event to occur, and accepting the resulting consequences).

- Review Risks

The Project Manager, Product Owner, Mentor review the risk to validate all of the risk information identified at this time, including the Risk Class, Risk Impact, Risk Probability, Risk Timeframe, Risk Severity, and Recommended Mitigations. The Risk Review will include Stakeholders as needed. Risk information is revised based on input from the reviewers. The result of this step is to validate the risk as a "confirmed risk".

7.3.3. Step 3 – Plan

The objective of *Step 3 – Plan* is to take ownership of risk mitigation. Risk planning involves assigning risk ownership, developing risk mitigations, contingencies, developing measurements, reviewing and approving risk mitigations and measurements, translating mitigations into action plans, and updating risk measures in the Risk List. A detailed discussion of the planning process is provided in the sub-paragraphs below.

- Assign Risk Owner

Identify the person to be assigned responsibility for developing risk mitigations, contingencies, measurements, mitigation action plans, and implementing and tracking mitigation action plan progress.

When someone external to the Project Team can control risk events or mitigation, a Risk Owner will be identified on the Project team and will be responsible for coordination and reporting on risk planning with the external contact.

- Develop Mitigations and Contingencies

Develop the plan to eliminate, reduce, or accept the risk.

The Risk Owner is responsible for developing mitigations for the risk. Mitigations developed by the Risk Owner may be based on previously identified mitigations as identified or may be developed independently.

The Risk Owner will also be required to develop contingency plans for each risk. These contingency plans will be executed as actions if the risk event occurs.

- Develop Measurements

  Develop the methods to track the risk mitigation actions and to measure the effectiveness of the actions. The Risk Owner is responsible for developing measurements of risk mitigation.
  Contingency plan measurements will be focused on the effectiveness of the contingency plan in addressing the actual impacts of the event.

- Review Mitigations, Contingencies and Measurements

  The Project Manager reviews the risk mitigations, contingencies, and measurements developed by the Risk Owner. Review by the Product Owner if the risk has been assigned the appropriate probability, impact, and timeframe, and provides direction regarding whether the mitigation and contingency plans are appropriate for the severity of the risk. If needed, risk mitigations, contingencies and measurements are revised based on the review.

- Approve Mitigations, Contingencies and Measurements

  Project Manager approves the risk mitigations, contingencies and measurements.

- Develop Mitigation and Contingency Action Plans

  The Risk Owner will develop detailed action plans to implement risk mitigations and contingencies. While the Risk Owner may delegate the action plan development, the responsibility for the mitigation/contingency plan remains with the assigned Risk Owner. As a result, the Risk Owner will remain the primary point of contact with Project Manager for tracking mitigation/ contingency action plans for the risk.

- Update Project Risk List

  The Risk Analyst updates the Project Risk List risk information based on risk planning, including Risk Owner, Risk Mitigations, Risk Measurements, and Mitigation.

7.3.4. Step 4 – Implement

The objective of *Step 4 – Implement* is to actively mitigate risks. Risk implementation involves the execution of risk mitigation action plans and recording risk information changes in the Risk List. A detailed discussion of the implementation process is provided in the sub-paragraphs below.

- Execute Mitigation and Contingency Action Plans

  The Risk Owner is responsible for the execution of the risk mitigation and contingency action plans.

- Update Project Risk Database

  Project Manager updates the Risk List risk status information based on the implementation status of the action plans, as provided by the Risk Owner.

7.3.5. Step 5 – Track and Control

The objective of *Step 5 – Track and Control* is to insure that all steps of the Risk Management process are being followed and, as a result, risks are being mitigated and contingency plans are followed as necessary. Risk tracking and control involves the oversight and tracking of risk mitigation and contingency action plan execution, re-assessment of risks, reporting risk status, and recording risk information changes in the Risk List. Detailed discussions of the track and control processes are provided in the sub-paragraphs below.

- Oversee Mitigation and Contingency Action Plan Execution

  The Project Manager is responsible for oversight of the execution of mitigation and contingency action plans for all risks identified in the Risk List.

- Track Action Plan Execution and Provide Feedback

  The Risk Owner is responsible for tracking the execution of mitigation and contingency action plans and providing feedback to the Project Manager on risk status. If mitigation or contingency plans require approval from the Project Manager in order for the associated project activities to proceed, a Management Tracking System (MTSII) issue will be created. The issue shall reference the Risk ID number in the MTSII Description field so that reviews can reference the associated risk. The associated MTSII Issue number shall be documented in the Historical Events section of the risk record in the Project Risk Database. The risk status will continue to be monitored and updated while the issue is being addressed and resolved. Risk mitigation or contingency activities will continue until the risk has been retired.

7.3.6. Communicate – Continuous Process:

Effective risk management requires ongoing communication throughout the project life cycle. Team will include communication of project risks as an ongoing activity throughout

each of the above 5 steps (Identify, Analyze, Plan, Implement, Track and Control). As the primary contact between the Risk Management process and the Risk Owners, Project Manager bear the responsibility of ensuring that members of the project team understand the value of their input in the process and feel free to submit risks in a forum and format with which they are most comfortable.

7.3.7. Risk Candidate Identification Form

Originator			**Date**		
Risk Title					
Risk Description					
Concern **Consequences**					
Risk Context					
Date Identified			**Impact to Critical Path:**	☐ Yes ☐ No	
Probability of Risk		(1=low, 3=high)	**Impact to Project:**		(1=low, 3=high)
Impact Start Date			**Impact End Date:**		
Responsible Person					
Program Area					
Affected Project Phase					
Risk Areas	☐ Schedule				
	☐ Performance				

	☐ Other	
Risk Control	☐ Internal, ☐ External ☐ Both	
Current Status	☒ Candidate Risk	
Recommended Mitigations		
Recommended Contingencies		
Other Noted Historical Events		