

Form: generic Plan for Project Risk Management  
Table of Contents

<b>PLAN FOR PROJECT RISK MANAGEMENT .....</b>	<b>2</b>
DEFINITIONS OF PROJECT RISK MANAGEMENT .....	2
<i>PMI Reference</i> .....	3
<i>IEEE Reference</i> .....	4
<i>LBB Reference</i> .....	5
<i>DIR/SAO Quality Assurance Review Guide – Risk Management</i> .....	6
GOALS FOR RISK MANAGEMENT .....	7
<i>Risk Management Planned Milestones</i> .....	7
RISK MANAGEMENT PROCESS OVERVIEW .....	8
<i>Risk Management Process Steps – (An Iterative Process)</i> .....	9
<b>APPENDIX.....</b>	<b>10</b>
GLOSSARY .....	11
FORMS FOR RISK MANAGEMENT .....	13
<i>FORM: Risk Identification Factors (Risk Cue Table) Example</i> .....	14
<i>Form: Risk Statement Exposure Ranking Example</i> .....	16
<i>Form: Risk Detail Example</i> .....	17
CHECKLIST: RISK PROCESS.....	18

## Plan for Project Risk Management

The *Plan for Project Risk Management* uses the Project Management Institute's PMBOK™ terminology and two of the five project processes,<sup>1</sup> *planning* and *controlling*, which contain the risk project management knowledge areas (core competence).

Project management is an integrative endeavor – an action, or failure to take action, in one area will usually affect other areas. The interactions may be straightforward and well understood, or they may be subtle and uncertain.<sup>2</sup>

**This *Plan for Project Risk Management* is only one sub-plan for the entire project's planning documentation.** Strictly speaking, risk involves only the possibility of suffering harm or loss. In the project context, however, risk identification is also concerned with opportunities (positive outcomes) as well as threats (negative outcomes).<sup>3</sup>

## Definitions of Project Risk Management

The Texas Department of Human Services (TDHS) **PROJECT Risk Management** is *a subset of project management that includes the processes concerned with identifying, analyzing, and responding to project risk. It consists of risk identification, risk quantification, risk response development, and risk response control.*<sup>4</sup>

IEEE describes risk management:<sup>5</sup>

*Risk management is part of the overall management process related to potential technical, cost and schedule risks. Risk management is a tool for problem prevention: identifying the things that could go wrong, assessing their impact, and determining which potential problems need to be avoided. Risk management is an activity that should be performed by all levels of the project to ensure adequate coverage of all potential problem areas. Open communication is required to provide all project personnel with the freedom to identify issues without negative consequences to themselves. Joint management of risks between acquirer and supplier, with support from developer/maintainer/operator, is necessary to enable identification of the most important risks to the program and to support efficient allocation of mitigation resources. Risk management may make use of*

---

<sup>1</sup> Project Management Institute. 1996. *A Guide to the Project Management Body of Knowledge (PMBOK™)*. Upper Darby, PA: PMI. P. 27.

<sup>2</sup> PMBOK™. P. 28.

<sup>3</sup> PMBOK™. P. 111.

<sup>4</sup> PMBOK™. P. 168.

<sup>5</sup> IEEE. *IEEE Standards Software Engineering, Volume One: Customer and Terminology Standards (Std IEEE/EIA 12207.2-1997, Annex L: Risk management)*. New York, NY: IEEE. P. 97.

*other supporting processes, such as problem resolution, quality assurance, and joint reviews.*

### **PMI Reference**

**Risk Event:** *A discrete occurrence that may affect the project for better or worse.*<sup>6</sup>

**Risk Identification:** *Determining which risk events are likely to affect the project.*<sup>7</sup>

**Risk Quantification:** *Evaluating the probability of risk event occurrence and effect.*<sup>8</sup>

**Risk Response Control:** *Responding to changes in risk over the course of the project.*<sup>9</sup>

**Risk Response Development:** *Defining enhancement steps for opportunities and mitigation steps for threats.*<sup>10</sup>

The core activities included in the project's Planning Process are: *risk identification, risk quantification, and risk response development*, while *the risk response control* is a portion of the project's Controlling Process.

Different application areas often use different names for the processes described here. For example:<sup>11</sup>

- *Risk identification and risk quantification* are sometimes treated as a single process, and the combined process may be called risk analysis or risk assessment.
- *Risk response development* is sometime called response planning or risk mitigation
- *Risk response development and risk response control* are sometimes treated as a single process, and the combined process may be called risk management

---

<sup>6</sup> PMBOK™. P. 169.

<sup>7</sup> PMBOK™. P. 169.

<sup>8</sup> PMBOK™. P. 169.

<sup>9</sup> PMBOK™. P. 169.

<sup>10</sup> PMBOK™. P. 169.

<sup>11</sup> PMBOK™. P. 111.

## IEEE Reference

DHS Projects with a significant information technology component(s) are likely to have software “sub-projects/components” and those associated risks, which will also use the IEEE Standard for Application and Management of the Systems Engineering Process, which states:

The enterprise should conduct risk management to systematically control the uncertainty in the project’s ability to meet cost, schedule, and performance objectives. The enterprise conducts that part of risk management that directly impacts the technical effort and involves risk-management preparation, risk assessment, risk-handling option assessment, and risk control. These activities are described in the Glossary (see page 11).<sup>12</sup>

IEEE Standard 1220-1998 (Section 3.8.3, Risk Management) describes *the technical risk program, including the approach, methods, procedures, and criteria for risk assessment (identification and quantification), selection of the risk-handling options, and integration into the decision process. Also describes the risks associated with the development and verification requirements. Identifies critical risk areas. Describes plans to minimize technical risks (additional prototyping, technology and integration verification, and evolutionary system development). Identifies risk control and monitoring measures including special verifications, technical performance measure parameters, and critical milestones/events. Describes the method of relating technical performance measurements (TPM), the master schedule, and the detail schedule to cost and schedule performance measurement, and the relationship to the SBS (System Breakdown Structure).*<sup>13</sup>

IEEE recommends:

*For precedented system developments, with incrementally improved or evolutionary growth products, the enterprise should refine established system definitions and product-line strategies to satisfy the market opportunity or customer order. For unprecedented systems where the concept is not already defined, the enterprise should create and evaluate candidate alternative concepts that would satisfy a market opportunity or customer order. One or more of the alternative concepts should be selected for further system definition during this stage of development. The risks associated with each alternative system should be assessed to include risk identification and quantification. Additionally, the enterprise should complete preliminary*

<sup>12</sup> IEEE. 1999. *IEEE Standard for Application and Management of the Systems Engineering Process* (Std. 1220-1998). Piscataway, NJ: IEEE. P. 60.

<sup>13</sup> IEEE Std. 1220-1998. P. 72.

*system and product specifications for each viable alternative, along with system- and product-interface specifications and a system baseline.<sup>14</sup>*

IEEE standards require the identification of human/system interface issues and system and subsystem risks:

*The enterprise shall identify the interface requirements between humans and products or subsystems. These interface requirements include performance, workloads, design constraints, and usability.<sup>15</sup>*

*The enterprise shall mitigate system-level risks to include products risks that were assessed to be critical to system development during concept selection. For critical risks associated with products, the enterprise utilizes simulation, scale-model tests, or prototype tests to demonstrate mitigation of risks to an acceptable level. The enterprise should assess subsystem risks and prioritize critical risks based upon probability of occurrence and related consequences to cost, schedule, and/or performance.<sup>16</sup>*

### **LBB Reference**

The LBB's Project Development Plan template<sup>17</sup>, which is based on the IEEE and ISO standards, suggests the following information be included (LBB PDP Section 5.4) to describe the project's risk management plan:

*Describe the process that will be used to identify, analyze, build mitigation and contingency plans, and manage the risks associated with the project. Describe mechanisms for tracking the specific risks, the mitigation plans, and any contingency plans. Risk factors that should be considered when identifying the specific project risks include contractual risks, organization-related risks, technological risks, risks due to size and complexity of the product, risks in personnel acquisition and retention, risks in achieving customer acceptance of the product, and others specific to the context of the project.*

---

<sup>14</sup> IEEE. 1999. *IEEE Standard for Application and Management of the Systems Engineering Process (Std. 1220-1998)*. Piscataway, NJ: IEEE. P. 18-19.

<sup>15</sup> IEEE. Std. 1220-1993. P. 20.

<sup>16</sup> IEEE. Std. 1220-1993. P. 20.

<sup>17</sup> Note: LBB Project Development Plan is adapted from the IEEE standards for Software Project Management Plans, 1058-1998, and from the data requirements of ISO standard 12207 Software Life Cycle Processes.

### **DIR/SAO Quality Assurance Review Guide – Risk Management**

Risk management involves monitoring already known risk factors and actively seeking the emergence of new elements of risk, so that action can be taken before problems occur. Based upon the output that identifies, analyzes, and prioritizes risk factors according to both the probability and the consequence of failure, the agency develops an action plan, or risk management plan, to increase the probability of producing a desired outcome while minimizing the risk of failure.<sup>18</sup>

The purpose of the risk management plan is to communicate both preventive action, or risk avoidance, and corrective action, or risk mitigation, to each of the identified risk factors, particularly those with a medium to high rating level.<sup>19</sup>

The agency project manager is responsible for developing, maintaining, and updating the risk management plan. The following steps represent the process:<sup>20</sup>

1. Upon completion of the internal or independent risk analysis, the agency prepares a risk management plan.
2. The completed risk management plan is submitted to the QAT (DIR/SAO Quality Assurance Team) for review, if required.
3. Based on the information provided in the risk analysis and the risk management plan, the QAT retains or modifies its initial assignments of risk and project monitoring levels. The QAT notifies the agency of its decision.

High risk factors are assigned high priority and should be incorporated in the risk management plan. Lesser risks should be addressed as resources are available. The risk management plan is separate from the Project Development Plan (PDP), but it should reference specific milestones or processes in the PDP that could be affected by the risk factors.<sup>21</sup>

The following elements should be included in a risk management plan:<sup>22</sup>

1. Overview of the risk items – A discussion of the overall set of risk items and their relationship to the project plan.
2. Risk matrix – The risk factor matrix or list that classifies each risk element by a unique identifier.
3. Risk description – A description of each risk element, showing its relationship to specific project events or activities. The description should reference which project milestone or process would be impacted by the risk element.

---

<sup>18</sup> DIR/SAO Quality Assurance Review Guide – Risk Management. March 7, 2000 web site. P. 1. <http://lanter.dir.state.tx.us/ooops/qat/section6.htm>

<sup>19</sup> DIR/SAO Quality Assurance Review Guide – Risk Management. March 7, 2000 web site. P. 1. <http://lanter.dir.state.tx.us/ooops/qat/section6.htm>

<sup>20</sup> DIR/SAO Quality Assurance Review Guide – Risk Management. March 7, 2000 web site. P. 1. <http://lanter.dir.state.tx.us/ooops/qat/section6.htm>

<sup>21</sup> DIR/SAO Quality Assurance Review Guide – Risk Management. March 7, 2000 web site. P. 1. <http://lanter.dir.state.tx.us/ooops/qat/section6.htm>

<sup>22</sup> DIR/SAO Quality Assurance Review Guide – Risk Management. March 7, 2000 web site. P. 2 - 3. <http://lanter.dir.state.tx.us/ooops/qat/section6.htm>

4. Objective and alternatives to averting the risk – Describe the goals or objective in averting the risk. Describe alternative approaches to averting the risk, showing impact to project cost, schedule, and quality.
5. Deliverables of the risk management plan – Identify the tasks, milestones and personnel assigned to the risk reduction effort.
6. Resource requirements of selected approach – Identify the tasks and resource requirements of the selected approach.
7. Risk integration and relation to the Project Development Plan – Provide a narrative that addresses the interrelationship of risk factors, and that references each individual or compound risk factor back to the overall Project Development Plan.

## **Goals for Risk Management**

The PROJECT's risk management goals:

- Will follow the Agency, regulatory, and partnership (state and federal) policies
- Will maximize the opportunities available for the project's stakeholders, schedule, and products with documented enhancement plans and responsibilities for the likely and high impact opportunities for the project
- Will minimize the threats for the project's stakeholders, schedule, and outputs with documented mitigation plans and responsibilities for the likely and high-impact threats
- Will routinely assess need for further risk identification/quantification and subsequent mitigation plans

### **Risk Management Planned Milestones**

The following risk management milestones are designated for the project:

1. Identify a comprehensive list of all possible risks (internal and external) for the project prior to the project's schedule (WBS) baseline creation
2. Complete initial enhancement/mitigation plan(s) to address appropriate opportunities/threats by (date)
3. Routine reviews for risk triggers
4. Weekly status reports for implemented contingency plans

## Risk Management Process Overview

The planning process for the management of risks for this project include risk *identification, quantification, and response development*. It is important to understand that even the most thorough and comprehensive analysis cannot identify all risks and probabilities correctly; control and iteration are required.<sup>23</sup>

Annex L of IEEE 1227.2-1997 provides the following description for *risk planning*:<sup>24</sup>  
*A risk management plan should be developed. This plan should describe risk management activities, procedures and schedules for performing these activities, documentation and reporting requirements, organizations and personnel responsible for performing specific activities, and requirements for communicating risks and risk status with other organizations (e.g., acquirer, supplier, subcontractor).*

The controlling process for the management of risks for this project include *risk response control*. Risk response control involves executing the risk management plan in order to respond to risk events over the course of the project. When changes occur, the basic cycle of identify, quantify, and respond is repeated.<sup>25</sup>

Annex L of IEEE 1227.2-1997 provides the following description for risk tracking and control:<sup>26</sup>

*Risks and mitigation plans should be tracked for significant changes in attributes, predefined triggers, thresholds, events, or mitigation plan progress or failure. Status reports required for the project should include risk management information. Upon review, risks should be closed when their probability of impact has reached a sufficiently low level or their mitigation plans have succeeded. Failing or unsuccessful mitigation plans should be revised. Contingency actions specified in mitigation plans should be implemented if contingency triggers occur. Joint resolution agreements should be required for controlling actions where the risks are jointly visible or jointly controlled.*

---

<sup>23</sup> PMBOK™. P. 121.

<sup>24</sup> IEEE. *IEEE Standard 12207.2-1997*. P. 97.

<sup>25</sup> PMBOK™. P. 121.

<sup>26</sup> IEEE. *IEEE Standard 12207.2-1997*. P. 98.



**Risk Management Process Steps – (An Iterative Process)**

1. PROJECT will initially identify and document the potential risks using the *DHS Risk Identification Factors List* to clarify project specific risks from a generic listing of potential risk.
2. PROJECT will document project specific statements from the potential risk listing using the *DHS Risk Exposure Rating form*.
3. PROJECT will document the risk exposure for each specific risk statement using the *DHS Risk Exposure Rating form*
4. PROJECT will document mitigation plans as needed for those risks with greatest threat/opportunity
5. PROJECT will document actions taken to identify, quantify, plan and control risks for a historical comparison on at least a quarterly basis.

## **APPENDIX**

**Items listed in the Appendix (Glossary, Forms, and Checklist) of the PROJECT'S Plan for Risk Management will only be listed in the initial risk plan or if any changes occur to these items during the life cycle of the project.**

## Glossary

**Criticality.** *The degree of impact that a requirement, module, error, fault, failure, or other item has on the development or operation of a system.*<sup>27</sup>

**Risk Assessment:** *includes identifying and describing those circumstances which might result in adverse effects; quantifying these circumstances to determine their likelihood and potential cost, schedule, and performance effects; and ranking and integrating these risks to produce a risk assessment for each element of the SBS (System Breakdown Structure) appropriate to the stage of development.*<sup>28</sup>

**Risk Control:** *involves continuously assessing risk in order to provide current risk information, and to ensure that risk stays within acceptable levels.*<sup>29</sup>

**Risk Event:** *A discrete occurrence that may affect the project for better or worse.*<sup>30</sup>

**Risk-handling Option Assessment:** *involves evaluating risk-handling options to determine those that are feasible and that reduce risks to acceptable levels. Lower-level risk-handling options should be integrated with higher-level options that are feasible and that provide the best balance between cost, schedule, performance, and risk for the technical effort and the project.*<sup>31</sup>

**Risk Identification:** *Determining which risk events are likely to affect the project.*<sup>32</sup>

**Risk Quantification:** *Evaluating the probability of risk event occurrence and effect.*<sup>33</sup>

**Risk Management Preparation:** *includes identifying acceptable levels of risk for each stage of development; identifying potential sources of risk; identifying and evaluating risk-management tools and techniques; training team members to accomplish risk-management activities; deciding on the means by which the analysis and decisions that occur should be documented; and deciding on how risk-management information should be captured, processed, and disseminated.*<sup>34</sup>

---

<sup>27</sup> IEEE. 1999. *IEEE Standard Glossary of Software Engineering Terminology (Std. 610.12-1990)*. Piscataway, NJ: IEEE. P. 23

<sup>28</sup> IEEE. 1999. *IEEE Standard for Application and Management of the Systems Engineering Process (Std. 1220-1998)*. Piscataway, NJ: IEEE. P. 60.

<sup>29</sup> IEEE, Std 1220-1998. P. 61.

<sup>30</sup> *PMBOK*<sup>TM</sup>. P. 169.

<sup>31</sup> IEEE, Std 1220-1998. P. 60.

<sup>32</sup> *PMBOK*<sup>TM</sup>. P. 169.

<sup>33</sup> *PMBOK*<sup>TM</sup>. P. 169.

<sup>34</sup> IEEE, Std 1220-1998. P. 60.

**Risk Response Control:** *Responding to changes in risk over the course of the project.*<sup>35</sup>

**Risk Response Development:** *Defining enhancement steps for opportunities and mitigation steps for threats.*<sup>36</sup>

---

<sup>35</sup> PMBOK™. P. 169.

<sup>36</sup> PMBOK™. P. 169.

## **FORMS for Risk Management**

**FORM: Risk Identification Factors (Risk Cue Table) Example**