Risk Management Plan

PPM Version 2.0

<Project or Solution Name>

U.S. Department of Housing and Urban Development

<Month, Year>

Solution Information

	Information
Solution Name	*<Solution Name>*
Solution Acronym	*<Solution Acronym>*
Project Cost Accounting System (PCAS) Identifier	*<PCAS Identifier>*
Document Owner	*<Owner Name>*
Primary Segment Sponsor	*<Segment Sponsor Name>*
Version/Release Number	*<Version/Release Number>*

Document History

<Provide information on how the development and distribution of the Risk Management Plan is controlled and tracked. Use the table below to provide the release number, date, author, and a brief description of the reason for creating the revised version.>

Release No.	Date	Author	Revision Description

Contents

1. Risk Management Procedure

1.1 Process

<Summarize the steps necessary for responding to project risk.>

The IT Project Manager (IT PM) working with the project team and project sponsors will ensure that risks are actively identified, analyzed, and managed throughout the life of the project. Risks will be identified as early as possible in the project so as to minimize their impact. The steps for accomplishing this are outlined in the following sections. The <IT project manager or other designee> will serve as the risk manager for this project.

<A distinction may need to be made between overall project risk management and IT system or application risk management. Risks related to IT systems or applications must be identified and documented based on the methodology in NIST SP 800-30, Rev. 1 Risk Management Guide for Information Technology Systems and applicable updates. >

1.2 Roles and Responsibilities

Role	Responsibilities
Business Lead	The Business Lead assists in identifying and determining the context, consequence, impact, timing, and priority of the risk.
Risk Manager or IT Project Manager	The risk manager or IT PM is a member of the Integrated Project Team (IPT). The risk manager or IT PM determines if the risk is unique, identifies risk interdependencies across projects, verifies if risk is internal or external to project, and assigns risk classification and tracking number. During the life of the project, they continually monitor the projects for potential risks.
EA Lead	The EA Lead owns the EA related activities in the Architecture Phase of the IT Management Framework and work closely with other stakeholders throughout other ITM phases.
Integrated Project Team (IPT)	The IPT is responsible for identifying the risks, the dependencies of the risk within the project, the context and consequence of the risk. They are also responsible for determining the impact, timing, and priority of the risk as well as formulating the risk statements.
Risk Owner(s)	The risk owner determines which risks require mitigation and contingency plans; he/she generates the risk mitigation and contingency strategies and performs a cost benefit analysis of the proposed strategies. The risk owner is responsible for monitoring and controlling and updating the status of the risk throughout the project life cycle. The risk owner can be a member of the project team.
Other Key Stakeholders	The other stakeholders assist in identifying and determining the context, consequence, impact, timing, and priority of the risk.

Table 1 - Risk Management Roles and Responsibilities

1.3 Risk Identification

Risk identification will involve the IPT, appropriate stakeholders, and will include an evaluation of environmental factors, organizational culture and the *Project Management Plan* (PMP) including the project scope, schedule, cost, or quality. Careful attention will be given to the project deliverables, assumptions, constraints, and the *Project Schedule* (WBS), business case, life cycle cost information*,* and other key project documents. Reference the 19 Risk categories as defined by OMB in Appendix C.

Methods for Risk Identification

The following methods will be used to assist in the identification of risks associated with *<Project Name>:*

- *Brainstorming*
- *Interviewing*
- *SWOT (Strengths, Weaknesses, Opportunities and Threats)*
- *Diagramming*

Risks should be documented in the *Risk Management Log*, which is generated and updated as needed, and will be embedded at the end of this document and/or stored electronically in the project library located at *<file location>.*

1.4 Risk Analysis

All risks identified will be assessed to identify the range of possible project outcomes. Risks will be prioritized by their level of importance and recorded within the *Risk Management Log*.

1.4.1 Qualitative Risk Analysis

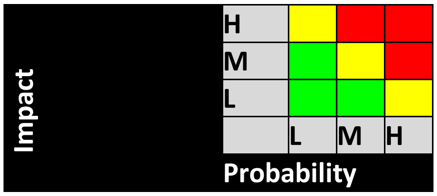
The probability and impact of occurrence for each identified risk will be assessed by the IT Project Manager, with input from the project team using the following approach:

Probability

- High – Greater than *<70%>* probability of occurrence
- Medium – Between *<30%>* and *<70%>* probability of occurrence
- Low – Below *<30%>* probability of occurrence

Impact

- High – Risk that has the potential to greatly impact project cost, project schedule or performance
- Medium – Risk that has the potential to slightly impact project cost, project schedule or performance
- Low – Risk that has relatively little impact on cost, schedule or performance



Impact

H	🟨	🟥	🟥
M	🟩	🟨	🟥
L	🟩	🟩	🟨
	L	M	H

Probability

Risks that fall within the RED and YELLOW zones will have risk response plan which may include both a risk response strategy and a risk contingency plan.

1.4.2 Quantitative Risk Analysis

Analysis of risk events that have been prioritized using the qualitative risk analysis process and their effect on project activities will be estimated, a numerical rating is applied to each risk based on quantitative analysis, and then documented in this section of the *Risk Management Plan* and *Risk Management Log*.

1.5 Risk Response

Each major risk (those falling in the Red & Yellow zones) will be assigned to a risk owner for monitoring and controlling purposes to ensure that the risk will not "fall through the cracks."

For each major risk, one of the following approaches will be selected to address it:

- **Avoid** – Eliminate the threat or condition or to protect the project objectives from its impact by eliminating the cause
- **Mitigate** – Identify ways to reduce the probability or the impact of the risk
- **Accept** – Nothing will be done
- **Contingency** –Define actions to be taken in response to risks
- **Transfer** – Shift the consequence of a risk to a third party together with ownership of the response by making another party responsible for the risk (buy insurance, outsourcing, etc.)

For each risk that will be mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include prototyping, adding tasks to the project schedule, adding resources, etc. Any secondary risks that result from risk mitigation response will be documented and follow the risk management protocol as the primary risks.

For each major risk that is to be mitigated or that is accepted, a course of action will be outlined in the event that the risk does materialize in order to minimize its impact.

1.6 Risk Monitoring, Control, and Reporting

The level of risk on a project will be tracked, monitored and controlled and reported throughout the project life cycle.

<Describe the methods and metrics that will be used to track the project's risk status throughout the life cycle as well as how this status will be reported to the stakeholders/ management.>

Risks are assigned a risk owner(s) who will track, monitor and control and report on the status and effectiveness of each risk response action to the IT Project Manager and risk management team on a *<insert timeframe>.*

All project change requests will be analyzed for their possible impact to the project risks.

As risk events occur, the list will be re-prioritized during weekly reviews and risk management plan will reflect any and all changes to the risk lists including secondary and residual risks.

The risk manager (IT PM) shall:

- Review, reevaluate, and modify the probability and impact for each risk item
- Analyze any new risks that are identified and add these items to the risk list (or risk database).
- Monitor and control risks that have been identified
- Review and update the top ten risk list *[timeframe, as needed, every two weeks, etc.]*
- Escalate issues/ problems to management <List factors that would need to be escalated to management. Examples: documented mitigation actions are not effective or producing the desired results; the overall level of risk is rising.>

The risk owner shall:

- Help develop the risk response and risk trigger and carry out the execution of the risk response, if a risk event occurs.
- Participate in the review, re-evaluation, and modification of the probability and impact for each risk item on a weekly basis.
- Identify and participate in the analysis of any new risks that occur.
- Escalate issues/problems to PM that,
  - Significantly impact the projects triple constraint or trigger another risk event to occur.
  - Require action prior to the next weekly review
  - Risk strategy is not effective or productive causing the need to execute the contingency plan.

Risk activities will be recorded in the <Document Name/ Risk Database Name> located on *<full network path location>*.

1.7 Risk Contingency Budgeting

A risk contingency budget can be established to prepare in advance for the possibility that some risks will not be managed successfully. The risk contingency budget will contain funds that can be tapped so that your project doesn't go over budget.

There is a total of *<$X>* in the *<Project Name>* project budget allocated for Risk Management activities. These activities may include, but are not limited to, identifying, analyzing, tracking, controlling, managing, and planning for risks. This also includes creating and updating the risk response strategies and contingency plans.

<Above is only an example of text that could be used. Enter whatever information is appropriate to outline/ define the budget associated with the Risk Management activities on the project.>

2. Tools and Practice

A *Risk Management Log* will be maintained by the IT PM and will be reviewed as a standing agenda item for project team meetings.

3. Closing a Risk

A risk will be considered closed when it meets the following criteria:

- *<List the criteria when a risk can be closed>*
- *<Who has the authority to close a risk? >*

<Examples:

- *Risk is no longer valid*
- *Risk event has occurred*
- *Risk is no longer considered a risk*
- *Risk closure at the direction of the IT Project Manager>*

Appendix A: References

<Insert the name, version number, description, and physical location of any documents referenced in this document. Add rows to the table as necessary.>

Table 2 below summarizes the documents referenced in this document.

Document Name	Description	Location
<Document Name and Version Number>	*<Document description>*	*<URL to where document is located>*

Table 2 - Appendix A: References

Appendix B: Key Terms

Terms Table below provides definitions and explanations for terms and acronyms relevant to the content presented within this document.

Term	Definition
[Insert Term]	*<Provide definition of term and acronyms used in this document>*

Table 3 - Appendix B: Key Terms

Appendix C: 19 OMB Risk Category Definitions

1. Table 3 - Appendix B: Key Terms
2. **Schedule**: Risk associated with schedule slippages, either from lack of internal controls or those associated with late delivery by vendors, resulting in missed milestones.
3. **Initial costs**: Risk associated with “cost creep” or miscalculation of initial costs that result in an inaccurate baseline against which to estimate and compare future costs.
4. **Life-cycle costs**: Risk associated with misestimating life-cycle costs and exceeding forecasts, reliance on a small number of vendors without sufficient cost controls.
5. **Technical obsolescence**: Risk associated with technology that becomes obsolete before the completion of the life cycle and cannot provide the planned and desired functionality.
6. **Feasibility**: Risk that the proposed alternative fails to result in the desired technological outcomes; risk that business goals of the program or initiative will not be achieved; risk that the program effectiveness targeted by the project will not be achieved.
7. **Reliability of systems**: Risk associated with vulnerability/integrity of systems.
8. **Dependencies and interoperability between this investment and others**: Risk associated with interoperability between other investments; risk that interoperable systems will not achieve desired outcomes; risk of increased vulnerabilities between systems.
9. **Surety (asset protection) considerations**: Risk associated with the loss/misuse of data or information; risk of technical problems/failures with applications; risk associated with the security/vulnerability of systems.
10. **Risk of creating a monopoly for future procurements**: Risk associated with choosing an investment that depends on other technologies or applications that require future procurements to be from a particular vendor or supplier.
11. **Capability of agency to manage the investment**: Risk of financial management of investment, poor operational and technical controls, or reliance on vendors without appropriate cost, technical and operational controls; risk that business goals of the program or initiative will not be achieved; risk that the program effectiveness targeted by the project will not be achieved.
12. **Overall risk of project failure**: Risk that the project/investment will not result in the desired outcomes.
13. **Project resources/financial**: Risk associated with "cost creep," miscalculation of life-cycle costs, reliance on a small number of vendors without cost controls, or (poor) acquisition planning.

14. **Technical/technology**: Risk associated with immaturity of commercially available technology and reliance on a small number of vendors; risk of technical problems/failures with applications and their ability to provide planned and desired technical functionality.
15. **Business/operational**: Risk associated with business goals; risk that the proposed alternative fails to result in process efficiencies and streamlining; risk that business goals of the program or initiative will not be achieved; risk that the investment will not achieve operational goals; risk that the program effectiveness targeted by the project will not be achieved.
16. **Organizational and change management**: Risk associated with organizational-, agency-, or government-wide cultural resistance to change and standardization; risk associated with bypassing or lack of use or improper use or adherence to new systems and processes because of organizational structure and culture; inadequate training planning.
17. **Data/information**: Risk associated with the loss or misuse of data or information, risk of compromise of citizen or corporate privacy information; risk of increased burdens on citizens and businesses because of data collection requirements if the associated business processes or the project (being described in the Exhibit 300) requires access to data from other sources (federal, state, and/or local agencies).
18. **Security**: Risk associated with the security/vulnerability of systems, web sites, information and networks; risk of intrusions and connectivity to other (vulnerable) systems; risk associated with the evolution of credible threats; risk associated with the misuse (criminal/fraudulent) of information; must include level of risk (high, medium, basic) and what aspect of security determines the level of risk (e.g., need for confidentiality of information associated with the project/system, availability of the information or system, or reliability of the information or system).
19. **Strategic**: Risk associated with strategic/government-wide goals (i.e., President's Management Agenda and e-Gov initiative goals); risk that the proposed alternative fails to result in the achievement of those goals or in making contributions to them.
20. **Privacy**: Risk associated with the vulnerability of information collected on individuals or risk of vulnerability of proprietary information on businesses.