

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT



Chief Information Officer Human Resources Line of Business

Migration Planning Guidance Templates Risk Analysis Report

October 2011

a New Day for Federal Service

Table Of Contents

- 1. Introduction 1
- 2. Proposed Methodology 1
 - 2.1 Risk Analysis Steps..... 2
 - 2.1.1 Step 1: Identify the Relevant Risks..... 2
 - 2.1.2 Step 2: Evaluate the Risks 2
 - 2.1.3 Step 3: Identify Manner to Address the Risk 3
- 3. Risk Summary Template 5

1. Introduction

Risk management serves to identify potential risks and plan for their occurrence in order to improve the effectiveness of project management. Risk management examines the factors that can delay or prevent the planned activities from being carried out and milestones from being achieved. Using this approach will help to anticipate problems and reduce their probability of occurring and/or of mitigating their impact should they occur. This document contains a methodology and template that Customer Agencies and Shared Service Centers (SSCs) can use for risk analysis and reporting.

Customer Agencies and SSCs are encouraged to develop a risk analysis report after the preparation/analysis step of the migration phase. The report should include the following:

- A risk summary matrix identifies
 - Migration risks
 - A probability the identified risks will materialize (low to high scale)
 - The impact of the risks on migration efforts (low to high scale)
 - An overall severity score (low to high scale)
- A brief description of the risk management action the SSC will take to mitigate the risk

2. Proposed Methodology

Risk analysis is an iterative process and should be directly tied into the process for managing and tracking issues throughout the life of the customer migration to the SSC. The approach used for analyzing risks involves several steps:

1. Identify the risks that are relevant to the customer migration.
2. Evaluate the risks for probability (low; medium; high) and for impact (low impact; medium impact; high impact) to determine which risks deserve the most attention. The risks will be evaluated by their severity factor, which is the product of the probability and impact scores.
3. Describe how risks will be managed/addressed based on their severity factor. For example, a risk with a high severity factor might warrant a contingency plan, whereas a low risk would only warrant being placed on a tracking list.

2.1 Risk Analysis Steps

2.1.1 Step 1: Identify the Relevant Risks

The objective is to identify the maximum possible range of risks associated with a particular project. Risk identification requires a thorough and systematic search through all characteristics of the project, including but not limited to customer expectations, contracting terms, technical and functional requirements, initial project plans, and the project environment.

The SSC transition strategy/management team should meet with the customer agency's transition strategy/management team to identify risks and mitigating actions. This could be done in a facilitated work session environment focused on the following:

- Brainstorm for relevant potential risks and consider various potential negative impacts to the migration schedule
- In addition to identifying risks, develop risk statements which outline the potential impacts on the migration effort

2.1.2 Step 2: Evaluate the Risks

The second step involves evaluating the risks in preparation for taking appropriate actions. The objective is to analyze and prioritize the identified risks. An important concept for this analysis is the expression of a risk as a function of two components, the probability of its occurrence and the likely impact on migration should it occur. Shared Service Centers and Customer Agencies should consider evaluating the migration risks according to the following criteria:

- By the probability of occurrence
- By the potential for negative impact, in terms of:
 - Financial loss – impacts to project costs resulting from budget overruns or penalties
 - Time loss – impacts to the project schedule and established milestones
 - Functionality loss – impacts to one or more properties that the solution should possess
 - Resource loss – impacts to staff, skills, equipment, and other resources

Once risks are identified, rate each risk on two dimensions on a scale of low, medium, and high. The first dimension is the probability of that risk occurring. The second dimension is the potential for negative impact if the risk were to become an issue. Estimating the risk impact can be a subjective effort, and best estimates using expert judgment must be employed in these instances. These two dimensions can be plotted onto a matrix to show the overall severity of each risk, as shown in Figure 1: Severity Table.

Risk Analysis Report

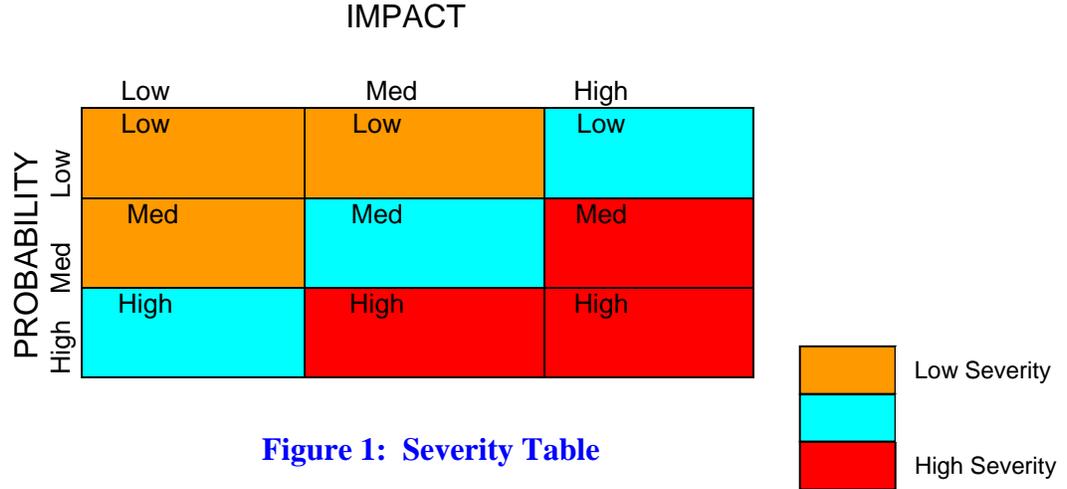


Figure 1: Severity Table

2.1.3 Step 3: Identify Manner to Address the Risk

The third step involves identifying the appropriate manner to address the risks. The severity of each risk is an important element in making this evaluation. The second element involves the degree to which action can be taken on that risk. Although the migration team may not have direct control over the risk, it can be possible for action to be taken that will reduce the probability of occurrence and/or decrease the negative impact if the risk becomes an issue (an actionable risk). For some risks, however, actions cannot be taken prior to the occurrence of the issue (non-actionable risk). Examples of non-actionable risks may be the risk of loss of funding or a policy change. In this case, the potential for a loss of funding may be out of the control of the migration team, and it is likely that no direct actions are appropriate unless the loss in funding occurs.

Risk Management Actions

		Actionable	Not Actionable
Degree of Risk Severity	High	Containment Plan	Contingency Plan
	Medium	Containment Plan	Contingency Plan
	Low	Track as needed	Track as needed

Figure 2: Risk Management Actions Matrix

The Risk Management Actions are defined as follows:

Containment Plans: These plans involve specific actions that will be taken to:

- Reduce the probability of the risk turning into an issue
- Reduce the negative impact to the project if the risk becomes an issue

Containment Plans might include the following types of actions:

- Negotiating firm commitments for individuals with critical knowledge or expertise
- Involving additional (or alternate) personnel in important roles, activities, or pivotal decisions
- Revisiting the project plan and lengthening schedules for certain activities
- Adding education and follow-up support mechanisms to existing plans for training (e.g., mentoring, “chalk talks,” single subject short courses)

Contingency Plans: These plans involve preparation for actions to be taken in the event a non-actionable risk becomes an issue. Contingency Plans might include the following types of action:

- Identifying and preparing backup resources for critical activities or areas
- Revisiting the project plan to make updates to timeline and milestones

3. Risk Summary Template

After the risk analysis is complete, each SSC will summarize the risks, probability of occurrence, impact on migration, severity, management actions, and status in a table. This template will be submitted to the HR LOB Program Management Office (PMO). Below is an example of the risk summary table that will be submitted by the SSC.

- **Number** – sequential numbering of risk
- **Risk Description** – identify and describe the risk
- **Risk Category**
 - Categorize the risk category by following project plan phases
 1. Project Management
 2. Preparation/Analysis
 3. Design/Development
 4. Implementation (testing)
 5. Post Implementation Evaluation
 - Risks must be grouped by the following categories as stated in OMB’s Exhibit 300, into one of eight IT risk categories.¹
 1. **Organizational and Change Management:** Business process reengineering acceptance by users and management, time and commitment managers will need to spend overseeing the change, lack of participation by business owners in the reengineering process, necessary change in manuals and handbooks, personnel management issues, labor unions, and ability of the organization to change.
 2. **Business:** Poorly written contracts, market or industry changes, new competitive products become available, and creating a monopoly for future procurements.
 3. **Data/Information:** Data standards are not defined; data acquisition and/or conversion costs are unknown.
 4. **Strategic:** Project does not tie to the Department’s mission or strategic goals; project is not part of the Department’s IT Capital Planning and Investment Control (CPIC) process.
 5. **Technology:** Lack of expertise, software and hardware maturity or immaturity, installation requirements, customization, O&M requirements, component delivery schedule/availability, uncertain and changing requirements, design errors and/or omissions, and technical obsolescence.

¹Risk categories and definitions taken from OMB Circular No. A-11 (2006), Capital Programming Guide

Risk Analysis Report

6. Security: Project does not conform to the requirements of OMB Circular A-130, *Management of Federal Information Resources* (November 28, 2000).
 7. Privacy: Project does not conform to the requirements of OMB Circular A-130.
 8. Project Schedule and Resources: Scope creep, requirement changes, insufficient or unavailable resources, overly optimistic task durations, unnecessary activities within schedule, and critical deliverables or reviews not planned into the schedule.
- **Probability** – identify the probability the risk will occur
 - **Impact** – identify the level of impact on the migration if the risk were to occur
 - **Severity** – enter product of the probability and impact ratings. Please use the Severity Table described earlier in this document to determine a severity rating.
 - **Risk Management Action** – describe how risks will be managed/addressed based on their severity factor. For example, a risk with a high severity factor might warrant a contingency plan, whereas a low risk would only warrant being placed on a tracking list.
 - **Status** – describe outcomes from risk management actions and any new risks.

Risk Summary Template Example

Note: *The customer agency and SSCs working together are strongly encouraged to develop a risk report.*

Number	Risk Description	Risk Category		Probability	Impact	Severity	Risk Management Action	Status
		Project Plan Phase	Risk					
	Identify and describe risk	Insert project plan phase (e.g., prep/analysis, design, development)	Security	Low	Low	Low	Identify action that will be taken and provide summary bullets describing the action	Report on risk status including outcomes from risk management actions and new risks



UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
CHIEF INFORMATION OFFICER
1900 E Street, NW
Washington, DC 20415