

**“Best Management Practice”
for
Identifying and Managing Risk**

Bureau of Land Management
System Coordination Office

Identifying and Managing Risk
Version Control Number 2.3
April 28, 2003

INDEX

- 1.0 Purpose
- 2.0 Applicability
- 3.0 Management Objective
- 4.0 Standardized Guidelines for Project Managers
 - 4.1 Background Information
 - 4.2 The Process
 - 4.3 Risk Identification and Management Guidelines
 - 4.4 Including Risk Management Activities within the Project Schedule
- 5.0 Roles and Responsibilities
- 6.0 Risk Identification and Management Procedures
 - 6.1 Risk Identification
 - 6.2 Risk Management
 - 6.3 Risk Status Review

Appendices

- Appendix 1 - Risk Identification Form
- Appendix 2 - Risk Management Plan

Referenced Documentation

1.0 Purpose

This guide is part of the overall project management “Best Management Practices” that have been developed by the System Coordination Office (SCO) WO-570D. It provides project managers with uniform requirements and specific instructions for identifying and mitigating the risks associated with their projects. These guidelines may change as experience is gained and the project management framework undergoes continuous improvement.

The purpose of this guide is to provide project managers with specific objectives, requirements, suggestions, and procedures for managing risk within BLM projects. It does not provide an exhaustive treatment of the subject matter. It is strongly suggested that the project manager has or receives formal training in risk management.

2.0 Applicability

These standardized guidelines apply to *all* projects, or efforts being managed as projects, that were approved by the ITIB. *All* Project Managers working on such projects will be evaluated based on their conformance to these guidelines. Projects that are required to submit a Capital Asset Plan/Business Case (aka Exhibit 300) must use this BMP in the development of their Risk Management Plan (See Appendix 2). The Risk Management Plan should become an appendix to the overall Project Management Plan.

3.0 Management Objective

The objective of these guidelines is to describe and establish a standardized process for identifying, mitigating and/or managing the wide range of inherent risks associated with IT Projects.

Project Managers that incorporate these guidelines into their overall project plan and schedule will have in place all of the components of a formal risk management plan.

4.0 Standardized Guidelines for Project Managers

4.1 Background Information

Project Managers must have a basic understanding of the definition of a “project” risk. Project Managers must also understand that they *cannot* afford to *not* understand risk and its impact on project success.

A project risk can be defined as a discrete possible future occurrence that may affect the project for better (positive outcomes, opportunities) or worse (negative outcomes, threats). Risk has three components – the risk “event”, the probability

of occurrence, and the impact of the occurrence.

Project Managers must understand that risk management:

- is an integral part of project management that includes the processes required to identify, quantify, respond to, and control project risks;
- is an attempt to predict future outcomes based on present knowledge;
- maximizes positive events while minimizing adverse events;
- is an ongoing function throughout the life of the project, requiring continuous risk identification, assessment, planning, and monitoring
- is highly situational and subjective - there is no simple textbook formula or guide for managing risks;
- includes four major processes – identification, quantification, response development, and control;
- requires the participation of everyone involved in the project, including software engineers, data specialists, managers, customers, and contractors; and,
- *is not free* – it must be planned for within the project schedule and budget.

The need to manage risk increases with the complexity of the system, as the complexity of the system increases, both the technical and non-technical risks increase. Risk management activities and their corresponding costs must be included in the project schedule and budget estimates.

4.2 The Process

The Risk Management process includes two phases;

- **Risk assessment** involves identifying, analyzing and prioritizing risks, and
- **Risk response** involves developing/planning risk response strategies, executing those plans, evaluating the results of the responses and documenting the results.

There are several ways that a Project Manager may choose to manage or respond to a specific risk. These options can be categorized into three broad areas. As a Project Manager you may choose to:

- **Avoid** the specific threat, usually by eliminating the cause. (i.e., conduct a study/develop a prototype)
- **Mitigate** the specific threat by reducing the expected monetary or schedule impact of the risk, or by reducing the probability of it's occurrence.
- **Accept** the consequences of the risk.

Risk management activities need to be “balanced”; the magnitude of the effort required to identify, assess, manage, and monitor must be commensurate with the magnitude of the potential risk’s impact to the project. Making informed decisions by consciously assessing what could go wrong, as well as the likelihood and the severity of the impact, is at the heart of risk management.

4.3 Risk Identification and Management Guidelines

Project Managers must ensure that all identified risks are specific and fully defined.

Project Managers should follow these guidelines when identifying and managing risks.

- *All* risks identified will be documented using the Risk Identification Form (Appendix 1);
- *All* risks will be quantified and/or qualified for probability and impact;
- *All* risks will be prioritized to determine which risks will be addressed, understanding there will never be enough time or resources to respond to all risks;
- Risks response strategies will be developed for each significant risk and recorded in the risk management plan (Appendix 2).
- The status of all risk response strategies will be discussed during the project status reviews with the Project Proponent, the Portfolio Manager/AD’s IRM Advisor and/or the Project Sponsor;
- Risk management activities will be included within the project schedule and their status updated; and,
- Risk management activities will be assigned to a specific manager or project team member.

4.4 Including Risk Management Activities within the Project Schedule

The risk assessment and risk response activities are incorporated into each project schedule. Formalizing risk management efforts by including risk evaluations (reviews and risk management plan reviews) into the schedule will ensure that risk assessments are conducted continuously throughout the project’s life cycle. Doing so will also ensure that clear lines of responsibility are assigned to each risk management activity and that their costs are calculated and tracked.

5.0 Roles and Responsibilities

Project Manager - Responsible overall for identifying and managing risks, developing metrics, and integrating the risk plan with the project management plan. The Project Manager must submit an updated Risk Management Plan (Appendix 2) on a quarterly basis as part of the quarterly reporting to the SCO.

System Coordination Office Staff - Provides Project Managers with risk management support.

Risk Identifier - Everyone associated with the project is responsible for providing proactive risk identification and analysis. There must be an open and retaliation-free environment where project team members feel comfortable in identifying risk.

Risk Management Specialist - Works with each Project Manager to ensure that the established project planning documentation included the identification of risks, risk mitigation and risk monitoring. He/she would also ensure that the Project Manager has a common view of the project unique and shared identified risks and that a risk management plan be specifically tailored for each project. This person could have multiple project assignments but should be specifically identified as the Risk Management Specialist on the Integrated Project Team, as documented in the Capital Asset Plan and Business Case (Exhibit 300).

6.0 Risk Identification and Management Procedures

6.1 Risk Assessment

Since it is the responsibility of everyone associated with a project to identify and document risks, each Project Manager should foster an atmosphere that is conducive and open for anyone to identify a risk. A risk identification process that is communicated to all project staff needs to be established and supported.

Appendix 1 provides a means by which risk identification can be easily captured, documented, and analyzed.

Each risk must be:

- identified by project and by phase/stage, along with who identified the risk, the date it was identified, and who was assigned as the primary point of contact;
- analyzed for its probability of occurrence (high, medium, low);
- analyzed in terms of impact to the project schedule and budget;

- given an overall risk (severity) rating (high, medium, low) by the Project Manager;
- described as completely as possible;
- categorized within the mandatory and optional areas of risk as identified by OMB (Circular A-11, Part 300); and
- prioritized among all identified risks.

6.2 Risk Response Development and Control

After all risks have been identified, rated and categorized, each risk is then prioritized. Not all risks identified in the previous stage will be carried into the risk plan for mitigation and management. Project managers should establish a pragmatic cut-off that is consistent with the scope of the project. Each significant risk must then include a description of the risk response strategy and activities. The risks must then be categorized by strategy – eliminate, mitigate, or accept.

Appendix 2, the Risk Management Plan, provides a means by which risks can be easily tracked and managed. It identifies the priority, area of risk, description, overall rating, risk response strategy category, and status (new, increasing, static, decreasing, eliminated). The Risk Management Plan will be used to track and communicate risk response activities, their status and their potential impact on the schedule/budget.

6.4 Areas of Risk

The following areas of risk are consistent with OMB Circular A-11 risk requirements. There are both mandatory and optional categories or areas of risk that should be addressed in the risk management plan.

MANDATORY RISK AREAS – at least one risk must be identified, rated and prioritized, and include a risk response strategy in each of the following risk areas.

Technology Risks Lack of expertise, software/hardware/telecommunications maturity/immaturity, cost, installation requirements (single/multi-sites), customization, O&M requirements, component (hardware/software) delivery schedules, component unavailability, uncertain and/or changing requirements, design errors and/or omissions, technical obsolescence.

Response strategies: avoiding or isolating custom designed components, use of prototyping, training.

***Project Schedule
and Resource
Risks***

Scope creep, requirements changes, insufficient or unavailable resources, overly optimistic task durations, schedule delays, unnecessary activities within the schedule, critical deliverables/reviews not planned into the schedule.

Response strategies: planning the appropriate amount of slack/float into the project schedule, obtaining supervisory commitment for resources.

Business Risks

Incomplete contracts, market/industry changes, new competitive products become available, creating a monopoly for future procurements.

Response strategies: Well developed Market Analysis with future considerations.

Cost Risk

Incremental funding, poor estimations, procurement timing.

Response strategies: Up to date estimations, CY+2 budget planning.

***Project Management
Risk***

Lack of training and/or experience of Project Manager, maturity of development methodology, agency's past abilities to manage the project (size and complexity), lack of performance measures, lack of process to monitor and compare actual performance to planned results.

Response strategies: Selection and assignment of a Project Manager from the Bureau's cadre of trained or experienced project managers. Proper application of project management, risk management, and EVMS.

***Organizational
and Change
Management***

Business process re-engineering acceptance by users/management, time and commitment managers will need to spend overseeing the change, lack of participation of business owners in the re-engineering process, necessary change in manuals and handbooks, personnel management issues, labor unions.

Response strategies: Project Charter with defined roles and responsibilities and personnel change management, Service Level Agreements.

Strategic Risks

Project does not tie to agency's mission or strategic goals, project is not part of the agency's IT Capital Planning and Investment Control (CPIC) process,

Response strategies: Tie mission or strategic goals to project, and IT CPIC process.

Security Risks

Project may not provide appropriate confidentiality, integrity, and availability of data and resources.

Response strategies: Assign responsibility for security, develop System Security Plan that ties to current Bureau Security Plans, ensure conformity to the requirements of OMB Circular A-130 through the use of cost-effective management, personnel, operational, and technical controls.

Privacy Risks

Privacy Impact Assessment not complete, system/data requirements unclear.

Response strategies: Ensure project conforms to the requirements of OMB Circular A-130 by meeting Agency requirements contained in the Privacy Act of 1974 and reporting and publication requirements detailed in OMB Circular A-130, assign privacy responsibilities within project team, work closely with the Privacy Officer.

Data Risks

Project conforms to the requirements of OMB Circular A-130, data standards not defined, data acquisition and/or conversion cost are unknown.

Response strategies: close coordination with Data Group, determination of data standards.

OPTIONAL RISK AREAS – the following are areas of risk that should be considered, but are not mandatory to address.

Integration Risks

Inconsistent technical and business requirements, unidentified requirements, conflicting testing schedules, incompatibility, excessive complexity.

Project Team Risks Conflicts between the development team and the testing team, resistance to project controls (schedule and cost controls, Configuration Management, and metrics), poorly defined or understood roles and responsibilities, insufficiently skilled staff, critical vacancies.

Requirements Risk Misunderstanding of requirements by stakeholders, unclear terminology, non-participation of key stakeholders in requirements identification, one-time requirement identification and validation.

Risk Identification Form

RISK IDENTIFICATION FORM		
Project Name:	Project Phase/Stage:	Area of Risk Category:
Probability of Occurrence: <i>(high, medium, low)</i>	Schedule Impact: <i>(schedule loss by x weeks)</i>	Overall Risk Rating: <i>(high, medium, low)</i>
Risk Description: <i>(describe the range of possible outcomes, expected timing, frequency)</i>		
Risk Response Strategy: <i>(describe how you plan to eliminate, mitigate, or accept the risk)</i>		
Risk Status: <i>(new, increasing, static, decreasing, eliminated)</i>		
Identified by:	Date Identified:	Assigned to:

[Project Name]

Risk Management Plan
as of [xx/xx/xx]

Priority	Area of Risk Category	Date Identified [xx/xx/xx]	Risk Description	Overall Risk Rating [high, medium, low]	Risk Mitigation Strategy [eliminate, mitigate, accept]	Risk Mitigation Status [new, increasing, static, decreasing, eliminated]
						New Date: xx/xx/xx Increasing Date: xx/xx/xx Static Date: xx/xx/xx Decreasing Date: xx/xx/xx Eliminated Date: xx/xx/xx
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Referenced Documentation

The following publications contain related information:

- Risk Management in Practice - Audrey J. Dorofee, Julie A. Walker and Ray C. Williams. April 1997. Crosstalk - The Journal of Defense Software Engineering
- Dealing with Dates - Solutions for the Year 2000, Robert A. Martin, MITRE Corporation, Crosstalk, the Journal of Defense Software Engineering, October 1997, pages 18-24.
- Software Risk Management - Higuera, Ron. And Haimes, Yacov, Technical Report CMU/SEI-96-TR-012, 1996. Software Engineering Institute, Carnegie Mellon University.
- Software Development Risk: Opportunity, Not Problem, Van Scoy, Roger L. Technical Report CMU/SEI-92-TR-30, 1992. Software Engineering Institute, Carnegie Mellon University.
- A Guide to the Project Management Body of Knowledge, William R Duncan, PMI, 1996 Chapter 11
Duncan, William, R., *A Guide to the Project Management Book of Knowledge [PMBOK]*, 1996, Project Management Institute
- Risk Management – Concepts and Guidance, Editor, Carl L. Pritchard. 1977. 218 pages.
- DOD Risk Management – www.acq.osd.mil/10/se/risk_management/index.htm