

# Risk Management

Resource and Patient Management  
System

Office of Information Technology  
Albuquerque, New Mexico



# Briefing Objectives

- Establish and document a project level Risk Management Process
  - Risk Management drivers – review OMB drivers and industry sources for risk management directives
  - Risk Management vocabulary – define common terms associated with risk management
  - Risk Management processes – describe the IHS processes for risk management
  - Risk Management references – provide some references for additional understanding

# Risk Management Drivers

- Office of Management and Budget
  - Circular A-11/Exhibit 300
  - Circular A-130
- Project Management Institute
  - Guide to the Project Management Body of Knowledge (PMBOK<sup>®</sup> Guide)
    - Project Risk Management knowledge area
- Software Engineering Institute<sup>™</sup>
  - Capability Maturity Model<sup>®</sup> Integrated
    - Risk Management Process Area

<sup>®</sup> “PMBOK” is registered in the U.S. Patent and Trademark Office by the Project Management Institute

<sup>™</sup> “Carnegie Mellon Software Engineering Institute” is a trademark of Carnegie Mellon University

<sup>®</sup> “Capability Maturity Model” is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

# Risk Management Drivers

- Risk management is the right thing to do.
  - Baggage system – Denver International Airport
    - The software will be delayed resulting in ...
    - \$500 million in extra financing



# IHS Risk Management Goals

- To ensure the lowest possible risk in managing software projects by establishment of a risk management process. The goals of the process are:
  - Identify and analyze risks early and determine their relative importance.
  - Make timely and appropriate decisions based on risk assessment and monitoring.
  - Provide a tracking system to document, monitor and update risks systematically.
  - Establish a common vocabulary for documenting risks.
  - Provide required input to Exhibit 300 reporting process.
  - Mitigate risks by addressing them appropriately.

# Key Definitions

- Risk. An uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives.
- Risk Management. A continuous, forward-looking process to systematically plan, anticipate and mitigate risks to proactively minimize their impact on the project.

# Key Definitions

- Risk Description/Risk Statement. An expression documenting a risk event and the consequence of the occurrence of the risk event.
- Risk Attributes/Parameters. Defined characteristics associated with a risk description e.g., impact, probability, risk area.

# Anatomy of a Risk Statement

## Event

Turnover in project development staff.

Integration of components provided by vendors/subcontractors requires more effort and cost than provided in the project plan.

Delays in receipt of Government furnished software/hardware will delay development activity.

Agency budgetary allocations do not provide for full funding for development which requires a re-allocation of functions to incremental releases.

User/system needs are not adequately captured.

## Consequence

Delay of deliverables.

Increased cost, delays in deliverables, and/or negative impacts on product quality.

Failure to make project deliverables on time.

Deferred user expectations.

Delivered system that does not meet all user expectations.

# Risk Parameters

- Area of Risk.
  - A classification scheme established in OMB circular A-11 (policy source for Exhibit 300) for identifying and reporting risks.
  - There are 11 areas applicable to all capital asset investments.
  - There are 8 additional areas applicable to IT investments.
  - Projects subject to Exhibit 300 reporting must identify at least one risk for each area of risk.

# OMB Risk Areas

- **Schedule**: Risk associated with the adequacy of the time estimated and allocated for the development, deployment, and operation of the system. Two risk areas bearing on schedule risk are:
  - The risk that the schedule estimates and objectives are not realistic and
  - The risk that program execution will fall short of the schedule objectives.
- **Initial Cost**: Risk associated with an incomplete or inaccurate cost estimate to start the project.
- **Life-Cycle Costs**: Risk associated with the ability of the system to achieve the program's life-cycle cost objectives. This includes the effects of errors in the cost estimating technique(s) used (given that the technical requirements were properly defined). Lifecycle costs include planning, development, operations, and retirement costs.

# OMB Risk Areas

- **Technical Obsolescence**: Risk that strategies for avoiding the use of outdated technical resources over the system life are not planned for and implemented.
- **Feasibility**: Risk of insufficient ability to successfully develop and implement the project within defined technical, scope, cost, and schedule parameters to successfully meet the performance goals.
- **Reliability of Systems**: Risk of inability of the system to provide planned and desired functionality as needed and expected.

# OMB Risk Areas

- **Dependencies and Interoperability Between this System and Others:** Risk associated with the reliance on other systems (existing or in development) within the Agency and across the Federal Government (e.g. technical interfaces, schedule dependencies). Risk is increased if the success of a project is directly linked to the success/implementation or on-going maintenance of other systems.
- **Surety (Asset Protection) Considerations:** Risk associated with the impact of loss, damage, or theft and the adequacy of physical protection, continuity of operations, and disaster recovery plans, and operations for the system.
- **Future Procurements:** Risk associated with the use of closed or proprietary software/source code, as well the dependence on a single vendor or product.

# OMB Risk Areas

- **Project Management**: Risk associated with the existence of an experienced project management team, appropriate project management structures, executive management support, governance, clear and defined responsibilities, as well as demonstrated experience in managing projects of similar size and scope. Also relates to the degree to which program plans and strategies exist and are realistic and consistent.
- **Overall Project Failure**: Risk associated with the negative impact resulting from the occurrence of one or more identified or unidentified risks, leading to catastrophic results for the project.
  - It refers to the aggregation of identified risks associated with this initiative and the likelihood (probability and impact) that one or more occurrences of risk will cause this initiative to fail. It also includes the risk that unidentified risks occur leading to the project becoming obsolete.

# OMB Risk Areas

- **\* Organizational/Change Management:** Risk associated with organizational/agency/government-wide cultural resistance to change and standardization; risk associated with bypassing, lack of use, improper use, or adherence to new systems and processes due to organizational structure and culture; and inadequate training.
- **\* Business:** Risk that the business goals of the program or initiative will not be achieved; risk that the program effectiveness targeted by the project will not be achieved.
- **\* Data/Information:** Risk associated with the loss/misuse of data or information, risk of increased burden on citizens and businesses due to data collection requirements if the associated business processes or the project require access to data from other sources (federal, state and/or local agencies).

\* Required for IT investments

# OMB Risk Areas

- **\* Technology**: Risk associated with immaturity of commercially available technology; risk of technical problems/failures with applications and their ability to provide planned and desired technical functionality.
  - Technical risk addresses the possibility that the application of software engineering theories, principles, and techniques will fail to yield the appropriate software product.
  - Technical risk is comprised of the underlying technological factors that may cause the final product to be: overly expensive, delivered late, or otherwise unacceptable to the customer.

\* Required for IT investments

# OMB Risk Areas

- **\* 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.
  - Risk that strategic goals and objectives, including PMA goals, may change.
  - Risk that the objectives of the project are not clearly linked to program needs, to the agency's overall strategies, and to government-wide policies and standards.
  - Risk that the initiative is not based on clearly understood needs or opportunities and is inconsistent with the overall strategies and architectures used by the agency and the federal government (i.e., Federal Enterprise Architecture).

\* Required for IT investments

# OMB Risk Areas

- **\* Security:** Risk associated with the security/vulnerability of systems, websites, information and networks.
  - Risk of intrusions and connectivity to other (vulnerable) systems.
  - Risk associated with the misuse (criminal/fraudulent) of information.
  - *[Note: This risk category must include in the risk description the level of risk (high, medium, basic/low) 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.]*

\* Required for IT investments

# OMB Risk Areas

- **\* Privacy:** Risk associated with the vulnerability of the collection, use, storage, transmission, and disposal of personally identifiable or proprietary information.
- **\* Project Resources:** Risk that addresses the adequacy of people, funds, schedule, and tools that are the necessary ingredients for successfully implementing the project (if any are inadequate, to include the qualifications of the people, there is risk).

\* Required for IT investments

# Probability of Occurrence

- Probability of Occurrence/Likelihood. A risk attribute that expresses the chances that a risk event will occur

Likelihood	Attribute
75% or greater chance of occurring	High
25-75% chance of occurring	Medium
Less than 25% chance of occurring	Low (Basic for the security risk area for exhibit 300 reporting)

# Impact Area

- A risk attribute consisting of three categories to specify the aspect of a project that is most hazarded by a risk.
  - Cost: The ability of the project to meet cost targets is hazarded
  - Schedule: The ability of the project to meet schedule milestones is hazarded
  - Technical: The ability of the project to meet technical expectations, i.e., quality, performance, depth of documentation is hazarded

# Impact

- A risk attribute indicating the degree of severity the impact area is hazarded by the risk.
- The definitions of impact vary by impact area.

# Impact (Cost Impact Area)

Impact	Definition
Low	The consequence of the risk event may result in a cost impact of 3% or less of the project budget and there is sufficient management reserve to address the issue.
Medium	The consequence of the risk event may result in a cost impact between 3% and 10% of the project budget or less than or equal to 3% of the project budget without sufficient management reserve to address the issue. The issue is capable of being addressed by reallocation of resources or other means.
High	The consequence of the risk event may result in a cost over run exceeding 10% of the budget.

# Impact (Schedule Impact Area)

Impact	Definition
Low	The consequence of the risk event may result in a schedule delay of up to 5% but management reserve is sufficient or resources are available to prevent any schedule disruption.
Medium	The consequence of the risk event may result in a schedule delay of between 5% and 10% and/or schedule deviations are identified.
High	The consequence of the risk event may result in a schedule delay of more than 10%. Major schedule milestones will be missed.

# Impact (Technical Impact Area)

Impact	Definition
Low	The consequence of the risk event may result in minor technical issues capable of being addressed through routine project management actions.
Medium	The consequence of the risk event may result in technical issues that would require special actions beyond routine management but do not result in an inability to meet specifications or deliver on time and within budget.
High	The consequence of the risk event may result in major technical issues that would prevent meeting specifications or delivery of an acceptable product.

# Risk Score/Criticality Level

- A risk attribute that provides a measure of relative risk priority.

Likelihood \ Impact	High	Medium	Low
High	9	6	3
Medium	6	4	2
Low	3	2	1

# Risk Type

- A risk attribute that describes the source of mitigation action.
  - **Internal**: the mitigation action can be performed internal to the immediate executing project organization. Risk mitigation must be realized by action of upper management.
  - **External**: the mitigation action must be accomplished outside the immediate executing project organization. Risk mitigation must be realized through the actions of upper management or elements outside the immediate project staff.

# Risk Status

- A risk attribute that addresses the currency of the risk hazard.
  - Active: the consequence resultant from the occurrence of the risk event is possible.
  - Inactive: the consequence resultant from the occurrence of the risk event is no longer possible.
  - Narrative text may also be included in field such as “Mitigation in place, monitoring for change”
  - OMB requires identification of remaining milestones to mitigate risks and other status information be listed as current status on Exhibit 300.

# Summary

## ■ Risk Attributes Summary

- Area of Risk (OMB categories)
- Probability of Occurrence/Likelihood (Low, Medium, High)
- Impact Area (Cost, Schedule, Technical)
- Impact/Risk Consequence (Low, Medium, High)
- Risk Score/Criticality Level (Low 1-2, Medium 3-5, High 6-9)
- Risk Type (Internal, External)
- Risk Status (Active, Inactive, Narrative Text)

# Mitigation Trigger Threshold

- Predefined indicators that increased levels of mitigation are required to address a risk.
- Mitigation trigger thresholds must be documented in risk mitigation plans.

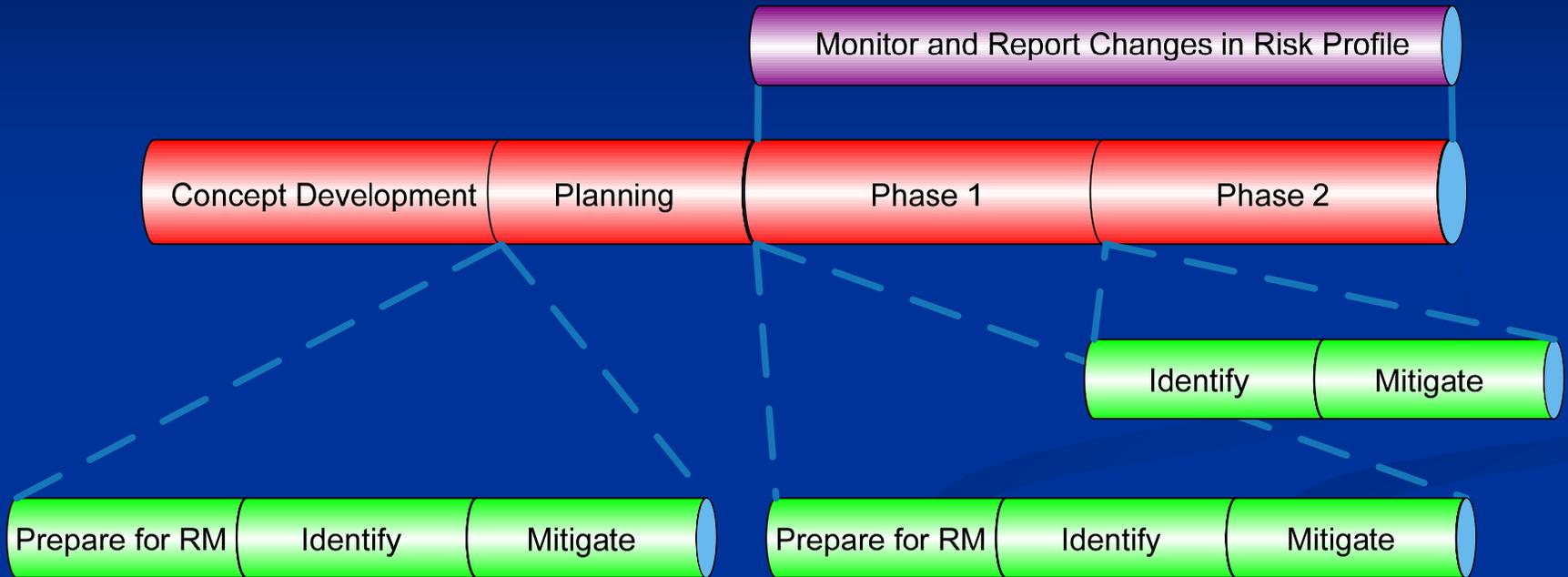
# Transition Indicator

- The observable event that indicates a risk has become a problem. The risk has materialized.

# Overall Risk Management Process

- Prepare for Risk Management
- Identify and Analyze Risks
- Mitigate Risks

# Process Timeline



# Process

## Prepare for Risk Management

- Inputs
- 
- RPMS Risk Management Plan
- Risk taxonomy
- Suggested risk sources
- Contracting documents
- Project scope statement
- Applicable policy
  - IHS
  - HHS
  - OMB
- Risk strategies from other projects
- Risk profiles from other projects

### Tools, Techniques, & References

- Determine risk sources
- Establish risk attributes and parameters
- Establish risk management strategy

### Outputs

- Project risk taxonomy
- Potential risk sources applicable to the project
- Project risk attributes and parameters
- Project risk management strategy

# Risk Taxonomy

- Use a taxonomy to guide brainstorming sessions to discover risks.

Product Engineering	Development Environment	Program Constraints
Requirements	Development Process	Resources
Stability	Formality	Schedule
Completeness	Suitability	Staff
Clarity	Process Control	Budget
Validity	Familiarity	Facilities
Feasibility	Product Control	
Precedent		
Scale		

# SEI Risk Questionnaire

## ■ Resources

### ■ Schedule

- Is the schedule inadequate or unstable
  - Has the schedule been stable?
  - Is the schedule realistic?
    - Is the estimation method based on historical data?
    - Has the method worked well in the past?
  - Is there anything for which adequate schedule was not planned?
    - Analysis and studies
    - QA
    - Training
    - Maintenance courses and training
    - Capital equipment
    - Deliverable development system
  - Are there external dependencies which are likely to impact the schedule?

# Establish a Management Strategy

- Methods and tools for risk identification, analysis, mitigation, monitoring and communication
- Time intervals for monitoring and reassessment
- Criteria for risk reporting and establishment of escalation thresholds

# Process

## Identify and Analyze Risks

### Inputs

- RPMS Risk Management Plan
- Project risk taxonomy
- Project risk attributes and parameters
- Risk risk management strategy
- Risk profiles from other projects

### Tools, Techniques, & References

- Identify risks
- Analyze risks
- Assign attributes to risks
- Document risks

### Outputs

- Project risk profile

# Process

- Do not avoid the “unthinkable” or absolutely fatal risk.
  - “It is unthinkable that the software will be late!”
  - Fatal risks often require the most management
- Do not avoid risks where there is no readily apparent mitigation path.
  - Document the risk and continue effort to find the mitigation path.
  - Awareness of the risk is the first step to mitigation.

# Process

Mitigate Risks		
<p>Inputs</p> <ul style="list-style-type: none"><li>• RPMS Risk Management Plan</li><li>• Project risk profile</li></ul>	<p>Tools, Techniques, &amp; References</p> <ul style="list-style-type: none"><li>• Identify mitigation approach</li><li>• Document risk mitigation plan</li><li>• Establish risk monitoring and reporting procedures</li></ul>	<p>Outputs</p> <ul style="list-style-type: none"><li>• Risk mitigation plans</li><li>• Risk status update reports</li></ul>

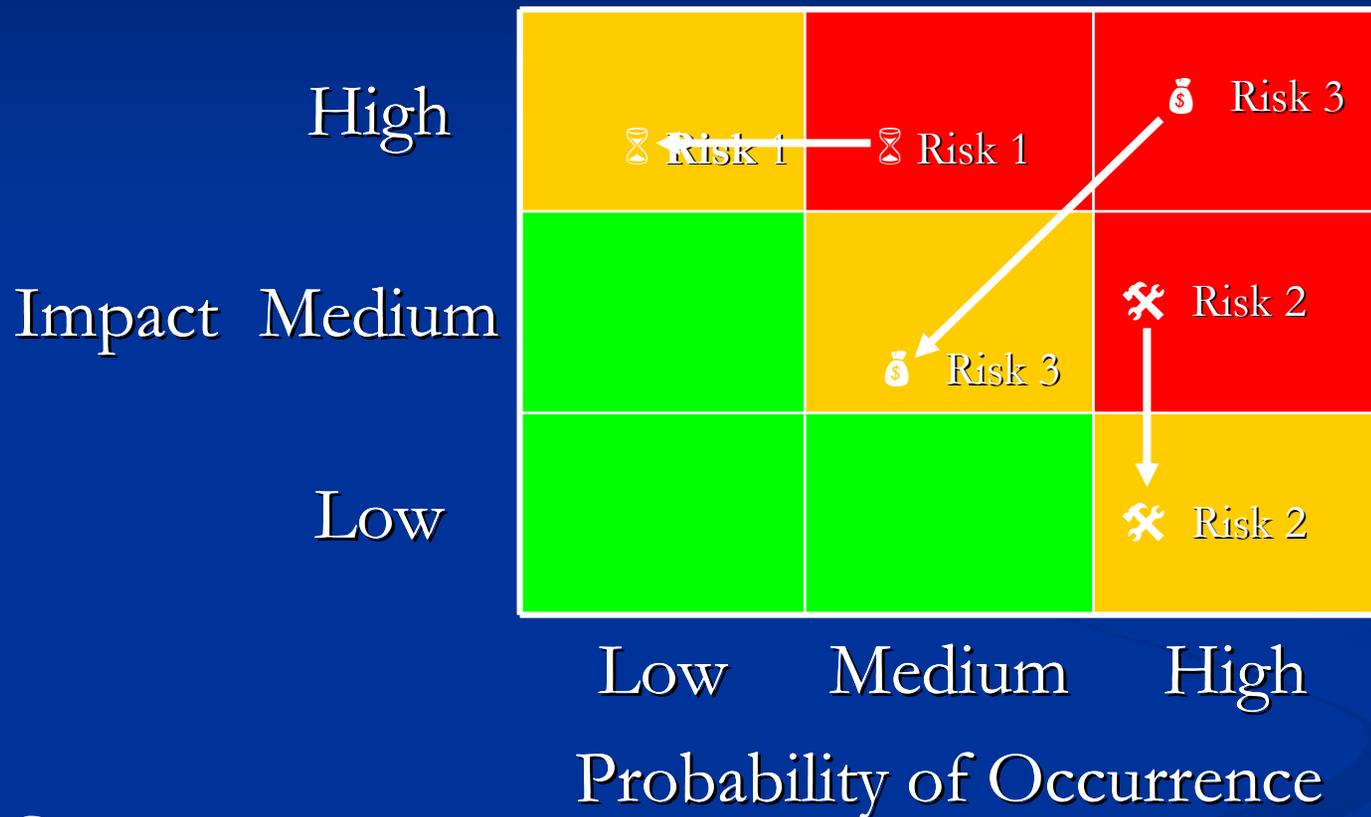
# Strategies to deal with risk

- **Avoid**: remove the possibility for the occurrence of the causal event. Modify the program element while continuing to meet agency needs.
- **Control**: agree to assume the risk and perform mitigation
  - Mitigation – reduce the probability or impact associated with a risk to an acceptable level
- **Transfer**: reassign the consequence to another entity (insurance)
- **Monitor**: agree to assume the risk and monitor the risk parameters for change without active mitigation until the need for mitigation is identified.
- **Accept**: agree to assume the risk and potential consequence.

# Mitigation

- Mitigation plans and strategies for addressing risks must:
  - Be documented – formality should be commensurate with the risk addressed.
  - Include mitigation trigger thresholds and mitigation escalation approaches where appropriate.
  - Be maintained and reviewed on a regular basis.

# Consider the Results of Mitigation



💰 Cost

⌚ Schedule

⚡ Technical Performance

# Consider Risk Mitigation Costs

- There are often costs associated with risk mitigation
  - Mitigation costs should be factored into project budget
  - OMB requires an indication that risk mitigation costs were or were not considered in the summary of spending stages on Exhibit 300. Negative responses require an explanation.
- Risk mitigation cost and schedule impacts must be considered during project planning activities.

# Reporting and Documenting Risks

- **Investment Level Risks**: Documented and maintained in the ProSight Investment Portfolio Management (IPM) tool
- **Component Project Risks**: Documented and maintained in an Excel spreadsheet containing the same data as the ProSight tool

# Reporting Risks

- **Primary/Secondary Risk**. Due to OMB Exhibit 300 reporting requirements, one risk for each risk area must be reported. Tool and reporting requirements limit the number of primary risks reported to 19. Therefore 19 risks corresponding to a single risk for each area are primary risks. The tool supports recording up to 20 additional risks as secondary risks which may represent any combination of risk areas.

Project components may identify and track as many risks as are identified and appropriate using local resources (Excel risk templates). The risks should be documented, reviewed and reported in accordance with direction on the following slides and the RPMS Risk Management Plan.

# Reporting Schedule - Investment Level

Risk Score	Reporting Schedule
Green 1-2	Risks are reported to OIT leadership semi-annually with status updates for any probability and severity changes. This report is performed by electronically distributing an exported report from the IPM tool following the annual Exhibit 300 submission process and again mid-year of that time. Any mitigation activity that has been implemented as a result of a mitigation trigger threshold being exceeded is also reported at this time.
Yellow 3-5	Risks are reported to OIT leadership quarterly with status updates for any probability and severity changes. This report is performed by electronically distributing an exported report from the IPM tool at the end of each fiscal year quarter. Any mitigation activity that has been implemented as a result of a mitigation trigger threshold being exceeded is also reported at this time.
Red 6-9	Risks are reported to OIT leadership monthly with status updates for any probability and severity changes. This report is performed by electronically distributing an exported report from the IPM tool at the end of every reporting month. Any mitigation activity that has been implemented as a result of a mitigation trigger threshold being exceeded is also reported at this time.

# Reporting Schedule - Project Level

Risk Score	Reporting Schedule
Green 1-2	Risks are reported/updated in the Serena tool weekly. Newly identified risks and any mitigation activity that has been implemented as a result of a mitigation trigger threshold being exceeded is also reported at this time. Program managers receive information pertaining to new risks in a monthly risk report.
Yellow 3-5	Risks are reported/updated in the Serena tool as they are identified. Newly identified risks and any mitigation activity that has been implemented as a result of a mitigation trigger threshold being exceeded are reported to program managers during bi-weekly status meetings with program managers.
Red 6-9	Risks are reported/updated in the Serena tool as they are identified. Newly identified risks and any mitigation activity that has been implemented as a result of a mitigation trigger threshold being exceeded are reported to program managers when they are identified and during bi-weekly status meetings with program managers.

# Tracking and Reviewing

- Project and project component organizations must periodically review the risk profile (listing of identified risks) for:
  - Identification of new risks
  - Re-assignment of risk probability or impact attributes
  - Risks that are no longer active
  - Mitigation threshold trigger attainment.
  - Adequacy of ongoing mitigation efforts
  - Attainment of mitigation status milestones

# Review Schedule - Investment Level

Risk Score	Reviewing Schedule
Green 1-2	Risks are monitored semi-annually and, if necessary, re-scored for probability and severity based on current information. This semi-annual review should occur once during the annual Exhibit 300 submission process and again mid-year of that time. Mitigation trigger thresholds are examined to determine the need for mitigation implementation.
Yellow 3-5	Risks are monitored quarterly and, if necessary, re-scored for probability and severity based on current information. Mitigation trigger thresholds are examined to determine the need for mitigation implementation.
Red 6-9	Risks are monitored monthly and, if necessary, re-scored for probability and severity based on current information. Mitigation trigger thresholds are examined to determine the need for mitigation implementation.

# Review Schedule - Project Level

Risk Score	Reviewing Schedule
<b>Green</b> 1-2	Risks are reviewed monthly by the project manager and re-scored for probability and severity. During the review, the project is evaluated for new risks that may be encountered and risks that are no longer active. The possible attainment of mitigation trigger thresholds is reviewed monthly as well. The project risk profile (including all risk levels) is reviewed during milestone reviews.
<b>Yellow</b> 3-5	Risks are reviewed weekly and re-scored for probability and severity. The possible attainment of mitigation trigger thresholds is reviewed weekly as well. The project risk profile (including all risk levels) is reviewed during milestone reviews.
<b>Red</b> 6-9	Risks are reviewed daily and re-scored for probability and severity. The possible attainment of mitigation trigger thresholds is reviewed daily as well. The project risk profile (including all risk levels) is reviewed during milestone reviews.

# IHS Risk Matrix

Date Identified	Area of Risk	Description	Impact	Probability of Occurrence	Risk Score	Strategy for Mitigation	Mitigation Costs in Life Cycle Costing?	Current Status as of the date of this exhibit
Aug 1, 2005	1) Schedule	Budgeted resources are not routinely available to perform planned investment activities, resulting in schedule delays.	High	Medium	6	1) Implement proactive process for identifying and managing investment activity baselines, including modifying schedules (baselines) and identifying new resources to meet original baselines.	N	On-going
Feb 15, 2002	2) Initial Costs	Historical cost information for initial investment planning is incomplete and/or inaccessible resulting in underestimated budgets and discontinued and/or delayed investment activity.	Low	Medium	2	1) Establish and implement guidelines to ensure consistent initial investment development planning. 2) Track project cost and schedule data to develop a repository of historical information on which to base future work.	N/A	On-going
Feb 15, 2002	3) Life-cycle Costs	Historical life-cycle cost information for ongoing investment planning is incomplete and/or inaccessible resulting in underestimated budgets and discontinued and/or delayed investment activity.	Low	Medium	2	1) Establish and implement guidelines to ensure consistent ongoing investment development planning. 2) Track project cost and schedule data to develop a repository of historical information on which to base future work.	N/A	On-going

# References

- RPMS Risk Management Plan, October 2005
- Mary Beth Chrissis, Mike Konrad, Sandy Shrum. “CMMI Guidelines for Process Integration and Product Improvement.” Boston, Massachusetts: Addison Wesley, 2003.
- Marvin J. Carr, Suresh L. Konda, Ira Monarch, F. Carol Ulrich, Clay F. Walker. “Taxonomy-Based Risk Identification.” Technical Report CMU/SEI-93-TR-6, ESC-TR-93-183, June 1993.
- Office of Management and Budget. Circular No. A-11, Part 7, “Planning, Budgeting, Acquisition, and Management of Capital Assets.” July 2004.
- Program Management Institute, “A Guide to the Project Management Body of Knowledge (PMBOK® Guide), Third Edition
- Tom DeMarco, Timothy Lister “Waltzing with Bears Managing Risk on Software Projects”, Dorset House Publishing Co, 2003
- Williams, R.C.; Pandelios, G.P.; and Behrens, S.G., “Software Risk Evaluation Method Description - Version 2.0”, Technical Report CMU/SEI-99-TR-029