Issue Date: <mm/dd/yyyy>
Revision Date: <mm/dd/yyyy>

Document Purpose

This Practices Guide is a brief document that provides an overview describing the best practices, activities, attributes, and related templates, tools, information, and key terminology of industry-leading project management practices and their accompanying project management templates. The purpose of this document is to provide guidance on the practice of Risk Management and to describe the practice overview, requirements, best practices, activities, and key terms related to these requirements.

Background

The Department of Health and Human Services (HHS) Enterprise Performance Life Cycle (EPLC) is a framework to enhance Information Technology (IT) governance through rigorous application of sound investment and project management principles and industry's best practices. The EPLC provides the context for the governance process and describes interdependencies between its project management, investment management, and capital planning components. The EPLC framework establishes an environment in which HHS IT investments and projects consistently achieve successful outcomes that align with Department and Operating Division goals and objectives.

The Enterprise Performance Life Cycle (EPLC) Planning Phase initiates risk management as part of the Project Management Plan (PMP), which includes identification, analysis, prioritization, and monitoring and control of risks. The activities during the Planning Phase are designed to help define preventative measures to reduce the probability of risks from occurring and identify countermeasures to successfully deal with any constraints if they develop.

Development of a Project Risk Management Plan is an activity that takes place early in the project life cycle with updates and refinements made throughout the project life cycle as necessary. Specific Critical Partners will assess completeness of Planning Phase activities concerning Risk Management. During the remaining phases of the EPLC the Risk Management components of the Project Management Plan are reviewed and appropriately updated.

Practice Overview

Project risk must be identified, managed, and addressed throughout the project in order for the project to be successful. Risk management plays an important role in maintaining project stability and efficiency throughout the project life cycle. It proactively addresses potential obstacles that may arise and hinder project success and/or block the project team from achieving its goals. Project risk can be anything that threatens or limits the goals, objectives, or deliverables of a project. Project risk is present in all projects and may have one or more causes and, if it occurs, one or more impacts.

Risks related to IT systems or applications must be identified and documented based on the methodology in NIST SP 800-30, Risk Management Guide for Information Technology Systems.

Risk vs. Issues

There is often confusion between Risk Management and Issue Management and how the activities of each interface and interact with each other. According to the Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK):

- **A risk** is an uncertain event or condition that, if it occurs, has a positive or negative impact on a project's objectives such as time, cost, scope, quality, etc.
- **An issue** is a point or matter in question or in dispute, or a point or matter that is not settled and is under discussion or over which there are opposing views or disagreements. Often project issues are first identified as a risk and through the risk management planning process may already have a planned approach to managing the issue.

The project manager is responsible for identifying and analyzing the risks. All stakeholders (e.g., users, designers, requirements, and sponsor) involved in the project are asked to provide input on what they deem to be the risks for the project. The project manager consolidates the information collected and creates the list of risks with accompanying attributes.

Process

Project risk management is an iterative process that begins in the early phases of a project and is conducted throughout the project life cycle. It is the practice of systematically thinking about all possible outcomes before they happen and defining procedures to accept, avoid, or minimize the impact of risk on the project.

Types of risk that are considered during this process are:
- Financial risk such as investments, funding, capital expenditure, etc.
- Legal risk such as lawsuits, change in law, etc.
- Government/Political risk such as regulatory change, legislative change, policy change, etc.
- Physical risk such as natural disasters, fire, accidents, death, etc.
- Intangible risk such as human resources, knowledge, skill sets, relationships, etc.
- Technical risk such as IT security, infrastructure, software, etc.
- Security risk such as facility, information, documentation, etc.

The Capital Planning and Investment Control (CPIC) process focuses specifically on the following types of risk areas:
- Schedule
- Initial Costs
- Life-cycle Costs
- Technical Obsolescence
- Feasibility
- Reliability of Systems
- Dependencies/Interoperability
- Surety Considerations
- Future Procurements
- Project Management
- Overall Project Failure
- Organizational/Change Management
- Business
- Data/Information
- Technology
- Strategic
- Security
- Privacy
- Project Resources

Effective risk management accomplishes:
- Identification of risk
- Evaluation and prioritization of identified risks
- Assignment of risk owners
- Development of risk response plans
- Monitoring and controlling risks
- Tracking and reacting accordingly

Project teams should hold meetings to identify risk and to define an appropriate strategy for dealing with those risks. These activities are documented and used in the development of a Risk Management Plan (RMP). The RMP describes the approach and processes for assessing and controlling risks in the project. PMI PMBOK defines a RMP as a document that describes how project risk management will be structured and performed on the project. It is contained in or is a subsidiary plan of the Project Management Plan (PMP). During the creation of the RMP a prioritization process follows the identification of risk whereby the risks with the greatest potential impact are prioritized first.

Components of Risk Management

The RMP describes how risk management activities will be performed. It documents how risks were identified, analyzed, and prioritized; how the project team will react to risk symptoms and triggers; who is responsible for managing which risks; how risks will be tracked throughout the project lifecycle, and how risks will be mitigated and/or what contingency plans may be executed. The process of obtaining the necessary information to properly complete and execute the RMP is a four part process that includes:

- Risk identification
- Risk analysis
- Risk response planning
- Risk monitoring, controlling, and reporting

Risks are tracked in the Risk Management Log.

Risk Identification

Risk identification is an iterative process that is conducted throughout the entire project life cycle. Any person associated with the project should be encouraged to continually identify potential project risks. PMI PMBOK defines risk identification as the process of determining which risks might affect the project and then documenting characteristics of those risks. Formal risk identification is performed in the early part of the project life cycle and may be done as a risk identification meeting that might include the following types of participants:

- Project managers
- Project team members
- Stakeholders
- Subject matter experts

    - **Format for Risk Statements** – Risk identification statements should follow one of the two OMB Exhibit 300 prescribed formats:

        - If (risk event) occurs, then (consequence) will happen.
        - (Risk event) may occur, during (activity, event, etc.), thereby causing an impact to (consequence).

A Risk Management Log will be generated and updated as needed and will be stored electronically in the project library.

A risk's severity is perceived as it relates to threats to project success, opportunities, and impact on schedule, cost, scope, quality, productivity, etc. There are two types of risk: known risk and unknown risk.

Known risk is risk that has been identified and can be analyzed. Examples of know risk may include aspects of the project environment such as poor project management practices, lack of resources, multiple projects, external dependencies, etc. Identified risks need to be proactively managed throughout the project life cycle by identifying who owns the management of that risk and by outlining risk symptoms, triggers, and contingency plans that would prevent the risk from occurring or that would lessen the project impact should it occur. At times risks may simply be accepted by the project if the reward for taking that risk is in balance with the potential consequences.

Unknown risk is risk that has not yet been identified. Examples of unknown risk may include unexpected legal changes, natural disasters, resource losses, etc. Unknown risk cannot be managed proactively and thus most often is addressed by allocating an acceptable level of general contingency against the project as a whole that is adequate enough to manage a reasonable level of unknown risk.

The following methods can be used to assist in the identification of risks.

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

Additional advanced risk identification techniques exist outside the scope of this document. These techniques can be further researched by the reader, if needed, and include techniques such as:

- Delphi Technique
- Root Cause Analysis
- Cause-and-Effect Diagramming
- Influence Diagramming
- Flow Charting

Risk Analysis

Risk analysis is primarily concerned with prioritizing and classifying risks and then determining which risks require the development of mitigation strategies and/or contingency plans. Risk analysis reflects the project's tolerance for risk and defines thresholds and tolerance levels in areas such as cost, schedule, staffing, resources, quality, etc. that, if triggered, may require implementation of defined contingency and/or mitigation plans. Risk analysis is not a one-time event, it is an iterative process that is performed continuously throughout the life of the project as new risks are identified and existing risks change. The PMI PMBOK identifies a number of approaches to risk analysis. However, two high-level types of risk analysis apply best to most every project type, they include:

- **Qualitative Risk Analysis** includes methods for prioritizing the identified risks for further action, such as Quantitative Risk Analysis or Risk Response Planning. It assesses the priority of identified risks using their probability of occurring, the corresponding impact on project objectives if the risks do occur, as well as other factors such as the time frame and risk tolerance of the project constraints of cost, schedule, scope, and quality.
- **Quantitative Risk Analysis** is performed on risks that have been prioritized by the Qualitative Risk Analysis process as potentially and substantially impacting the project's competing demands. It analyzes the effect of those risk events and assigns a numerical rating to those risks. When complete, it also presents a quantitative approach to decision making when uncertainty arises.

The probability of occurrence for each identified risk can be assessed as one of the following three categories and should be based on an assessment by the project manager, with input from the project team.

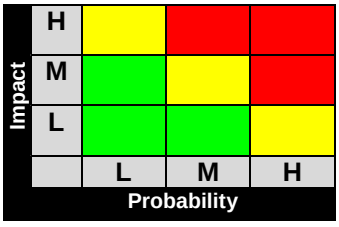
- High – Greater than 70% probability of occurrence
- Medium – Between 30% and 70% probability of occurrence
- Low – Below 30% probability of occurrence

The impact of each identified risk can be assessed as one of the following three categories and should be based on an assessment by the project manager, with input from the project team.

- 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

Based on the probability and impact assessments of each risk, the project manager may map the risks using red/green/yellow color-coding.

- Green: LL (Low Probability, Low Impact), LM (Low Probability, Medium Impact), ML (Medium Probability, Low Impact)
- Yellow: LH (Low Probability, High Impact), MM (Medium Probability, Medium Impact), HL (High Probability, Low Impact)
- Red: MH (Medium Probability, High Impact), HM (High Probability Medium Impact), HH (High Probability, High Impact)



Additional advanced risk analysis techniques exist outside the scope of this document. These techniques can be further researched by the reader, if needed, and include techniques such as:

- Process Assessment
- Probability and Impact Analysis
- Probability Distributions
- Sensitivity Analysis
- Decision Tree Analysis
- Modeling and Simulation

Risk Response Planning

Risk response planning includes the identification and assignment of one or more persons to take responsibility for each identified risk and defines the actions to be taken against that risk through the development of measures and action plans to respond to risk should it occur. PMI PMBOK defines Risk Response Planning as the process of developing options and actions to enhance opportunities and to reduce threats to project objectives. Risk response actions may include:

- **Mitigation** – Risk mitigation involves taking early action to prevent or reduce the likelihood of risk.
- **Contingency** – Contingency plans define actions to be taken in response to identified risk triggers in hopes of reducing potential project impact from identified risk.
- **Transference** – Risk transference involves shifting the responsibility and ownership of the risk to another party. This is typically done by purchasing insurance against the type of risk.
- **Avoidance** – Risk avoidance involves changing the project to eliminate the threat from identified risk.
- **Acceptance** – Risk acceptance simply involves acknowledging the risk as part of the project and accepting the consequences of its occurrence. An example of this is political or legislative risk that is out of the control of the project team.

For the most part, project risk response planning will consist of defining risk thresholds, identifying risk triggers, and then planning a mitigation strategy and/or developing contingency plans. A risk trigger is an event or events that activate the execution of a particular action, usually associated with mitigation strategy or execution of contingency plans. Risk thresholds define the boundaries of fluctuation allowed from expected levels to those defined as triggers. Mitigation strategies identify actions that may minimize or eliminate project risks before it occurs. A risk may have several mitigation activities that attempt to balance the probability and severity of the risk occurrence with the cost-effectiveness of the mitigation strategy. Risk triggers should be identified that indicate when the mitigation strategy is no longer effective and contingency plans should be executed.

Risk tracking and monitoring and control follow the progress of the probability of risk occurrence and, if necessary, identifies when risk symptoms escalate to a point requiring implementation of contingency plans. By monitoring risk, plans can be adjusted to deal with project change that may alter risk levels. If a risk probability/impact drops and/or the risk actually occurs, the risk may be a candidate for retirement or closure. If the risk does occur, defined contingency plans minimize the risk's effect on project deliverables.

Risk Monitoring and Controlling, and Reporting

The Project Manager is ultimately responsible for managing risks and should regularly review and update the status of each identified risk and ensure that risks are under control. Risk monitoring and control is the process of identifying, analyzing, and planning for risk, keeping track of identified risks, and reanalyzing existing risks, monitoring risk symptoms and triggers, and reviewing the execution of risk responses strategies while evaluating their effectiveness.

Risk reporting is the process of regularly reviewing and providing status about identified risk. Project work should be continuously monitored for updates and changes, this practice should also include the review and update of risk. When reporting or reviewing project progress, risk management status should be included.

Developing the Risk Management Plan

A RMP is the foundation document for early identification of potential project problems. A good RMP is not necessarily lengthy. A RMP can be very short and still have great value or can simply be incorporated into the Project Management Plan. The content of the RMP will vary depending upon the complexity of the project. The size of and time invested to develop a RMP should be balanced with the size and complexity of the project. Large, more complex projects justify a significant effort in developing a comprehensive RMP.

The information documented within the RMP identifies risk reduction techniques, developed contingency plans, and describes the process that will be used to identify, analyze, and manage risks throughout the project life cycle.

Either directly or by reference to other documents, the RMP should address the following:

- **Risk Management Procedures** – Summarize how risk management activities will be performed during the project.
  - **Process** – Summarize the steps necessary for responding to project risk.
  - **Risk Identification** – Summarize the approach that will be used to identify risk and the risks identified during that process. Among other things, risks identified should include technical, political, and managerial aspects of the project that may impact areas such as schedule, cost, functionality, performance, reliability, availability, resources, etc.
  - **Risk Analysis** – Summarize the probability of risk occurrence and assess the likelihood of the risk occurring. Summarize the potential impact of the risk on the project's objectives. Based on the probability and impact assessments for each risk, map the risks using red/green/yellow color-coding.
  - **Qualitative Risk Analysis** – Summarize the probability of occurrence for each identified risk based on an assessment by the project manager, with input from the project team.
  - **Quantitative Risk Analysis** – Summarize the probability and impact assessments of each risk, the project manager may map the risks using red/green/yellow color-coding.
  - **Response** – Summarize the techniques and actions that will be taken to respond to identified risks. Prioritize risk based on identified qualitative and quantitative characteristics. Define risk thresholds and assign oversight responsibility of the risk to team members. Identify the risk symptoms and triggers and then document mitigation and contingency plans, risk transfer, avoidance, and/or acceptance strategies. The RMP should include milestones and completion dates for actions which will be taken for mitigating risks.
  - **Risk Monitoring, Controlling, and Reporting** – Summarize how risk will be monitored, controlled, and reported throughout the project's life.
- **Tools and Practices** – Summarize any tools that will be used to log and track risk and risk status updates, where the tools are located, where information will be stored, etc. Summarize processes defined specifically for the purpose of risk management such as how risk will be evaluated, measured, reported on, etc.

Best Practices

The following best practices are recommended for **Project Risk Management**:

- **Identify Early** – Identify potential project risks as early in the project life cycle as possible. Document these initially identified risks in the project charter and clearly communicate their potential consequences to project sponsors and stakeholders.
- **Identify Continuously** – Continually identify and reevaluate project risk. When new risk is identified communicate updates as needed.
- **Analyze** – Analyze the potential impact of identified project risk. Repeat this analysis process throughout the project life cycle, make updates, and communicate changes as needed.
- **Reprioritize** – As risks are continually analyzed throughout the project life cycle, reprioritize risks as potential project impact adjusts to changing project events.
- **Define and Plan** - Define risk thresholds and triggers, risk response strategies, and contingency plans. The greater probability of occurrence and/or impact on project goals, the more detailed this information should be. Build risk management activities into project plans and budgets. Project costs should be adjusted to address costs associated with mitigating project risk.
- **Communicate** – Communicate regularly regarding risk status and changes in the level or overall project risk. Solicit feedback from project team members and stakeholders regarding known risk and the prospects of unknown risk. Store the risk management log in a location accessible to the project team so that, if necessary, anyone can obtain updates at any time.
- **Update** – Update the risk management log on a regular basis, both informally and formally.
- **Educate** – Educate the entire project team and stakeholders on risk management and encourage them to actively identify, communicate, and mitigate risk.

Practice Activities

For software development projects the following practice activities are appropriate:

- **Identify** –Identify project risk.
- **Evaluate/Analyze** – Analyze identified risks and evaluate potential impact on project goals.
- **Prioritize** – Prioritize risks based on probability of occurrence and potential impact on project goals.
- **Plan** – Develop risk response strategies and contingency plans. Document risk symptoms and triggers used to identify when implementation of planned risk action should be executed.

- **Track/Monitor and Control** – Track risk using some form of Risk Management Log. Continuously monitor risk status as the project progresses and report status of change.
- **React** – When appropriate react to escalating risk by executing risk response strategies or executing contingency plans.
- **Close** – When risk is no longer a reasonable threat, or the risk has occurred and is now an issue, that particular risk may be closed in the risk management log.