Guidelines for Risk Management Process Review

The purpose of risk management is to identify potential problems before they occur so that risk-handling activities may be planned and invoked as needed across the life of the product or project to mitigate adverse impacts on achieving objectives.

Risk management is a continuous, forward-looking process that is an important part of business and technical management processes. Risk management should address issues that could endanger achievement of critical objectives. A continuous risk management approach is applied to effectively anticipate and mitigate the risks that have critical impact on the project.

Effective risk management includes early and aggressive risk identification through the collaboration and involvement of relevant stakeholders. Strong leadership across all relevant stakeholders is needed to establish an environment for the free and open disclosure and discussion of risk.

Although technical issues are a primary concern both early on and throughout all project phases, risk management must consider both internal and external sources for cost, schedule, and technical risk. Early and aggressive detection of risk is important because it is typically easier, less costly, and less disruptive to make changes and correct work efforts during the earlier, rather than the later, phases of the project.

Risk management can be divided into three parts: defining a risk management strategy; identifying and analyzing risks; and handling identified risks, including the implementation of risk mitigation plans when needed.

For the purpose of this review, please address the following points:

1. **Demonstrate that you have a process to determine risk sources and categories.**
   Identification of risk sources provides a basis for systematically examining changing situations over time to uncover circumstances that impact the ability of the project to meet its objectives. Risk sources are both internal and external to the project. As the project progresses, additional sources of risk may be identified. Establishing categories for risks provides a mechanism for collecting and organizing risks as well as ensuring appropriate scrutiny and management attention for those risks that can have more serious consequences on meeting project objectives.

   *Typical work products* would include: (1) risk source lists (external and internal) and (2) risk categories lists.

2. **Demonstrate that you have a process to define the parameters used to analyze and categorize risks, and the parameters used to control the risk management effort.**
   Parameters for evaluating, categorizing, and prioritizing risks typically include risk likelihood (i.e., the probability of risk occurrence), risk consequence (i.e., the impact and severity of risk occurrence), and thresholds to trigger management activities.
Risk parameters are used to provide common and consistent criteria for comparing the various risks to be managed. Without these parameters, it would be very difficult to gauge the severity of the unwanted change caused by the risk and to prioritize the necessary actions required for risk mitigation planning.

*Typical work products* would include: (1) risk evaluation, categorization, and prioritization criteria and (2) risk management requirements (control and approval levels, reassessment intervals, etc.).

3. **Demonstrate that you have a process to establish and maintain the strategy to be used for risk management.** A comprehensive risk management strategy addresses items such as: (1) The scope of the risk management effort, (2) Methods and tools to be used for risk identification, risk analysis, risk mitigation, risk monitoring, and communication, (3) Project-specific sources of risks, (4) How these risks are to be organized, categorized, compared, and consolidated, (5) Parameters, including likelihood, consequence, and thresholds, for taking action on identified risks, (6) Risk mitigation techniques to be used, such as prototyping, simulation, alternative designs, or evolutionary development, (7) Definition of risk measures to monitor the status of the risks, and (8) Time intervals for risk monitoring or reassessment.

The risk management strategy should be guided by a common vision of success that describes the desired future project outcomes in terms of the product that is delivered, its cost, and its fitness for the task. The risk management strategy is often documented in an organizational or a project risk management plan. The risk management strategy is reviewed with relevant stakeholders to promote commitment and understanding.

*A typical work product* would be the project risk management strategy.

4. **Demonstrate that you have a process to identify and document the risks.** The identification of potential issues, hazards, threats, and vulnerabilities that could negatively affect work efforts or plans is the basis for sound and successful risk management. Risks must be identified and described in an understandable way before they can be analyzed and managed properly. Risks are documented in a concise statement that includes the context, conditions, and consequences of risk occurrence.

Risk identification should be an organized, thorough approach to seek out probable or realistic risks in achieving objectives. To be effective, risk identification should not be an attempt to address every possible event regardless of how highly improbable it may be. Use of the categories and parameters developed in the risk management strategy, along with the identified sources of risk, can provide the discipline and streamlining appropriate to risk identification. The identified risks form a baseline to initiate risk management activities. The list of risks should be reviewed periodically to reexamine possible sources of risk and changing conditions to uncover sources and risks previously overlooked or nonexistent when the risk management strategy was last updated.
Risk identification activities focus on the identification of risks, not placement of blame. The results of risk identification activities are not used by management to evaluate the performance of individuals.

There are many methods for identifying risks. Typical identification methods include (1) Examine each element of the project work breakdown structure to uncover risks; (2) Conduct a risk assessment using a risk taxonomy. Interview subject matter experts; (3) Review risk management efforts from similar products. Examine lessons-learned documents or databases; (4) Examine design specifications and agreement requirements.

*A typical work product* would be a list of identified risks, including the context, conditions, and consequences of risk occurrence.

5. Demonstrate that you have a process to evaluate and categorize each identified risk using the defined risk categories and parameters, and determine its relative priority. The evaluation of risks is needed to assign relative importance to each identified risk, and is used in determining when appropriate management attention is required. Often it is useful to aggregate risks based on their interrelationships, and develop options at an aggregate level. When an aggregate risk is formed by a roll up of lower level risks, care must be taken to ensure that important lower level risks are not ignored.

*A typical work product* would be a list of risks, with a priority assigned to each risk.

6. Demonstrate that you have a process to develop a risk mitigation plan for the most important risks to the project, as defined by the risk management strategy. A critical component of a risk mitigation plan is to develop alternative courses of action, workarounds, and fallback positions, with a recommended course of action for each critical risk. The risk mitigation plan for a given risk includes techniques and methods used to avoid, reduce, and control the probability of occurrence of the risk, the extent of damage incurred should the risk occur (sometimes called a “contingency plan”), or both. Risks are monitored and when they exceed the established thresholds, the risk mitigation plans are deployed to return the impacted effort to an acceptable risk level. If the risk cannot be mitigated, a contingency plan may be invoked. Both risk mitigation and contingency plans are often generated only for selected risks where the consequences of the risks are determined to be high or unacceptable; other risks may be accepted and simply monitored.

Options for handling risks typically include alternatives such as: (1) Risk avoidance: Changing or lowering requirements while still meeting the user’s needs; (2) Risk control: Taking active steps to minimize risks; (3) Risk transfer: Reallocating design requirements to lower the risks; (4) Risk monitoring: Watching and periodically reevaluating the risk for changes to the assigned risk parameters; (5) Risk acceptance: Acknowledgment of risk but not taking any action. Often, especially for high risks, more than one approach to handling a risk should be generated.

In many cases, risks will be accepted or watched. Risk acceptance is usually done when the risk is judged too low for formal mitigation, or when there appears to be no viable way to
reduce the risk. If a risk is accepted, the rationale for this decision should be documented. Risks are watched when there is an objectively defined, verifiable, and documented threshold of performance, time, or risk exposure (the combination of likelihood and consequence) that will trigger risk mitigation planning or invoke a contingency plan if it is needed.

Adequate consideration should be given early to technology demonstrations, models, simulations, and prototypes as part of risk mitigation planning.

*Typical work products* would include: (1) Documented handling options for each identified risk; (2) Risk mitigation plans; (3) Contingency plans; and (4) a list of those responsible for tracking and addressing each risk

7. **Demonstrate that you have a process to monitor the status of each risk periodically and implement the risk mitigation plan as appropriate.** To control and manage risks effectively during the work effort, follow a program to monitor risks and their status and the results of risk-handling actions regularly. The risk management strategy defines the intervals at which the risk status should be revisited. This activity may result in the discovery of new risks or new risk-handling options that may require re-planning and reassessment. In either event, the acceptability thresholds associated with the risk should be compared against the status to determine the need for implementing a risk mitigation plan.

*Typical work products* would include: (1) Updated lists of risk status; (2) Updated assessments of risk likelihood, consequence, and thresholds; (3) Updated lists of risk-handling options; (4) Updated list of actions taken to handle risks; and (5) Risk mitigation plans.
8. **(Optional) If you complete 8-17, you will earn 2 additional contact hours!**
Demonstrate that you have established and maintain an organizational policy for planning and performing the risk management processes.

9. **Demonstrate that you establish and maintain a plan for performing the risk management process.** Typically, this plan for performing the risk management process is included in (or referenced by) the project plan. This would address the comprehensive planning for all of the specific practices in the project plan, from determining risk sources and categories all the way through to the implementation of risk mitigation plans.

10. **Demonstrate that you provide adequate resources for performing the risk management process, developing the work products, and providing the services of the process.** Examples of resources provided are: risk management databases, risk mitigation tools, prototyping tools, and modeling and simulation.

11. **Demonstrate that you assign responsibility and authority for performing the process, developing the work products, and providing the services of the risk management process.**

12. **Demonstrate that you train the people performing or supporting the risk management process as needed.**

13. **Demonstrate that you place designated work products of the risk management process under appropriate levels of configuration management.**

14. **Demonstrate that you identify and involve the relevant stakeholders of the risk management process as planned.**

15. **Demonstrate that you monitor and control the risk management process against the plan for performing the process and take appropriate corrective action.**

16. **Demonstrate that you objectively evaluate adherence of the risk management process against its process description, standards, and procedures, and address noncompliance.**

17. **Demonstrate that you review the activities, status, and results of the risk management process with higher level management and resolve issues.** Reviews of the project risk status are held on a periodic and event-driven basis with appropriate levels of management, to provide visibility into the potential for project risk exposure and appropriate corrective action. Typically, these reviews will include a summary of the most critical risks, key risk parameters (such as likelihood and consequence of these risks), and the status of risk mitigation efforts.

**YOU MAY USE YOUR OWN WORD DOC IN ORDER TO DO THIS. BE SURE TO INCLUDE YOUR NAME AND DATE TO YOUR DOCUMENT.**