

RISK MANAGEMENT

A Project Management Process Area at Maturity Level 3

Purpose

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

Introductory Notes

Risk management is a continuous, forward-looking process that is an important part of project management. Risk management should address issues that could endanger achievement of critical objectives. A continuous risk management approach effectively anticipates and mitigates risks that may have a critical impact on a project.

Deleted: is applied to

Deleted: anticipate

Deleted: mitigate the

Effective risk management includes early and aggressive risk identification through collaboration and the involvement of relevant stakeholders, as described in the stakeholder involvement plan addressed in the Project Planning process area. Strong leadership across all relevant stakeholders is needed to establish an environment for free and open disclosure and discussion of risk.

Deleted: the

Deleted: the

Deleted: ,

Deleted: the

Risk management must consider both internal and external sources of cost, schedule, performance, and other risks. 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 earlier, rather than the later, phases of the project.

Deleted: for

Deleted: and

Deleted: risk as well as

Deleted: the

When the project identifies and assesses project risks during project planning and manages risks throughout the life of the project, risk identification includes identifying risks associated with the acquisition process and the use of a supplier to perform project work. Initially, the acquisition strategy identifies risks associated with an acquisition. The approach to the acquisition is planned based on those risks. As the project progresses to the selection of a supplier, risks specific to the supplier's technical and management approach become important to the success of the acquisition.

These risks refer to the capability of the supplier to meet contractual requirements, including schedules and cost targets. When the project selects a supplier and awards the supplier agreement, the acquirer continues to manage project risks, including risks related to the supplier meeting its contractual requirements. Typically the acquirer does not manage risks being addressed or managed by the supplier.

Deleted: Development

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 as needed.

Deleted: when

Both the acquirer and supplier must understand project risks and how to modify the risk management strategy and plans as a project progresses through its lifecycle. Managing project risks requires a close partnership between the acquirer and supplier. Both must share appropriate risk management documentation, understand the risks, and develop and execute risk management activities.

The complexity of an acquirer-supplier relationship increases the need for early and aggressive risk identification. For example, acquirer capabilities, supplier experience working with the acquirer, financial stability of the supplier, and availability of well-defined dispute resolution processes all influence the risk of a project.

As represented in the Project Planning and Project Monitoring and Control process areas, organizations initially may focus on risk identification for awareness, and react to the realization of these risks as they occur. The Risk Management process area describes an evolution of these specific practices to systematically plan, anticipate, and mitigate risks to proactively minimize their impact on the project.

Deleted: may

Deleted: simply

Although the primary emphasis of the Risk Management process area is on the project, these concepts can also be applied to manage organizational risks.

Deleted: the

Related Process Areas

Refer to the Project Planning process area for more information about identifying project risks and planning the involvement of relevant stakeholders.

Deleted: identification of

Deleted: for

Refer to the Project Monitoring and Control process area for more information about monitoring project risks.

Refer to the Decision Analysis and Resolution process area for more information about using a formal evaluation process to evaluate alternatives for the selection and mitigation of identified risks.

Refer to the Solicitation and Supplier Agreement Development process area for more information about establishing supplier agreements.

Specific Goal and Practice Summary

SG 1 Prepare for Risk Management

- SP 1.1 Determine Risk Sources and Categories
- SP 1.2 Define Risk Parameters
- SP 1.3 Establish a Risk Management Strategy

SG 2 Identify and Analyze Risks

- SP 2.1 Identify Risks
- SP 2.2 Evaluate, Categorize, and Prioritize Risks

Risk Management (RSKM)

Deleted: Development

SG 3 Mitigate Risks

- SP 3.1 Develop Risk Mitigation Plans
- SP 3.2 Implement Risk Mitigation Plans

Deleted: ¶

Specific Practices by Goal

SG 1 Prepare for Risk Management

Preparation for risk management is conducted.

Prepare for risk management by establishing and maintaining a strategy for identifying, analyzing, and mitigating risks. Typically, this strategy is documented in a risk management plan. The risk management strategy addresses specific actions and the management approach used to apply and control the risk management program. The strategy typically includes identifying sources of risk, the scheme used to categorize risks, and parameters used to evaluate, bound, and control risks for effective handling.

Deleted: Preparation is conducted

Deleted: This is typically

Deleted: the

Deleted: This

Deleted: the

Deleted: ;

Deleted: ;

Deleted: the

SP 1.1 Determine Risk Sources and Categories

Determine risk sources and categories.

Identifying 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 to risks that can have serious consequences on meeting project objectives.

Deleted: Identification of

Deleted: for those

Deleted: more

Acquirers initially identify and categorize risk sources and categories for the project and refine those sources and categories over time (e.g., schedule, cost, sourcing, contract management, supplier execution, technology readiness, human safety, reliability related risks and other issues outside the control of the acquirer). The supplier is also a source of risk (e.g., financial stability of the supplier and the possibility of the supplier's acquisition by another organization).

Typical Work Products

1. Risk source lists (external and internal)
2. Risk categories list

Subpractices

1. Determine risk sources.

Risk sources are fundamental drivers that cause risks in a project or organization. There are many sources of risks, both internal and external to a project. Risk sources identify where risks may originate.

Deleted: the

Deleted: with

Deleted: ,

Deleted: common areas

Deleted:

Deleted: Development

Typical internal and external risk sources include the following:

- Uncertain requirements
- Unprecedented efforts (i.e., estimates unavailable)
- Infeasible design
- Unavailable technology
- Unrealistic schedule estimates or allocation
- Inadequate staffing and skills
- Cost or funding issues
- Uncertain or inadequate subcontractor capability
- Uncertain or inadequate supplier capability
- Inadequate communication with customers
- Disruptions to the continuity of operations

Deleted: —

Deleted: vendor

Deleted: actual or potential

Deleted: or with their representatives

Many of these sources of risk are often accepted without adequately planning for them. Early identification of both internal and external sources of risk can lead to early identification of risks. Risk mitigation plans can then be implemented early in the project to preclude occurrence of risks or reduce consequences of their occurrence.

Deleted: adequate

Deleted: the

Deleted: the

2. Determine risk categories.

Risk categories are the "bins" used for collecting and organizing risks. Identifying risk categories aids the future consolidation of activities in risk mitigation plans.

Deleted: reflect

Deleted: A reason for identifying

Deleted: is to help in

Deleted: the

Deleted: the

Deleted: The phases

Deleted: The types

Deleted: The types

Deleted: Program

Deleted: s

The following factors may be considered when determining risk categories:

- Phases of the project's lifecycle model (e.g., requirements, design, manufacturing, test and evaluation, delivery, and disposal)
- Types of processes used
- Types of products used
- Project management risks (e.g., contract risks, budget/cost risks, schedule risks, resource risks, performance risks, and supportability risks)
- Supplier risks (e.g., financial viability of the supplier and the geographic location of supplier resources)
- Product safety, security, and reliability

A risk taxonomy can be used to provide a framework for determining risk sources and categories.

SP 1.2 Define Risk Parameters

Define parameters used to analyze and categorize risks and to control the risk management effort.

Deleted: the

Deleted: ,

Deleted: the parameters used

Parameters for evaluating, categorizing, and prioritizing risks include the following:

- Risk likelihood (i.e., probability of risk occurrence)
- Risk consequence (i.e., impact and severity of risk occurrence)

Deleted: Development

- Thresholds to trigger management activities

Risk parameters are used to provide common and consistent criteria for comparing risks to be managed. Without these parameters, it is difficult to gauge the severity of an unwanted change caused by a risk and to prioritize the actions required for risk mitigation planning.

Deleted: the various

Deleted: would be very

Deleted: the

Deleted: the

Deleted: necessary

Acquirers should document the parameters used to analyze and categorize risks so they are available for reference throughout the life of the project since circumstances change over time. Using these parameters, risks can easily be re-categorized and analyzed when changes occur.

The acquirer may use tools such as failure mode and effects analysis to examine risks such as potential failures in products or processes. A tool may also be used to evaluate risk management priorities for mitigating known threat vulnerabilities.

Typical Work Products

1. Risk evaluation, categorization, and prioritization criteria
2. Risk management requirements (e.g., control and approval levels, and reassessment intervals)

Deleted: ,

Subpractices

1. Define consistent criteria for evaluating and quantifying risk likelihood and severity levels.

Consistently used criteria (e.g., bounds on likelihood and severity levels) allow impacts of different risks to be commonly understood, to receive the appropriate level of scrutiny, and to obtain the management attention warranted. In managing dissimilar risks (e.g., personnel safety versus environmental pollution), it is important to ensure consistency in the end result (e.g., a high risk of environmental pollution is as important as a high risk to personnel safety).

Deleted: the

Deleted: the

Deleted: the

2. Define thresholds for each risk category.

For each risk category, thresholds can be established to determine acceptability or unacceptability of risks, prioritization of risks, or triggers for management action.

Examples of thresholds include the following:

- Project-wide thresholds could be established to involve senior management when product costs exceed 10 percent of the target cost or when cost performance indices (CPIs) fall below 0.95.
- Schedule thresholds could be established to involve senior management when schedule performance indices (SPIs) fall below 0.95.
- Performance thresholds could be established to involve senior management when specified key items (e.g., processor utilization or average response times) exceed 125 percent of the intended design.

Deleted: Cost Performance Indexes

Deleted: Schedule Performance Indexes

Deleted: set

For each identified risk, establish points at which more aggressive risk monitoring is employed or to signal the implementation of risk mitigation plans. These points can be redefined later in the project as necessary.

Deleted: Development

Deleted: These may be refined later, for

Deleted: to

3. Define bounds on the extent to which thresholds are applied against or within a category.

There are few limits to which risks can be assessed in either a quantitative or qualitative fashion. Definition of bounds (or boundary conditions) can be used to help define the extent of the risk management effort and avoid excessive resource expenditures. Bounds may include the exclusion of a risk source from a category. These bounds can also exclude any condition that occurs less than a given frequency.

Deleted: scope

SP 1.3 Establish a Risk Management Strategy

Establish and maintain the strategy to be used for risk management.

A comprehensive risk management strategy addresses items such as the following:

- The scope of the risk management effort
- Methods and tools to be used for risk identification, risk analysis, risk mitigation, risk monitoring, and communication
- Project-specific sources of risks
- How risks are to be organized, categorized, compared, and consolidated
- Parameters used for taking action on identified risks, including likelihood, consequence, and thresholds
- Risk mitigation techniques to be used, such as prototyping, piloting, simulation, alternative designs, or evolutionary development
- The definition of risk measures used to monitor the status of risks
- Time intervals for risk monitoring or reassessment

Deleted: these

Deleted: , for taking action on identified risks

Deleted: Definition

Deleted: the

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

Deleted: the

Deleted: that is

Deleted: a

Deleted: The risk management

A risk management strategy must be developed early in the project, so that relevant risks are identified and managed aggressively. The acquisition strategy evolves based on risk identification and analysis. Early identification and assessment of critical risks allows the acquirer to formulate risk handling approaches and streamline the project definition and solicitation around critical product and process risks.

Typical Work Products

1. Project risk management strategy

SG 2 Identify and Analyze Risks

Risks are identified and analyzed to determine their relative importance.

The degree of risk affects the resources assigned to handle the risk and the timing of when appropriate management attention is required.

Risk analysis entails identifying risks from identified internal and external sources and evaluating each identified risk to determine its likelihood and consequences. Risk categorization, based on an evaluation against established risk categories and criteria developed for the risk management strategy, provides information needed for risk handling. Related risks may be grouped to enable efficient handling and effective use of risk management resources.

- Deleted: impacts
- Deleted: an identified
- Deleted: determination
- Deleted: Analyzing risks
- Deleted: the
- Deleted: identified
- Deleted: then
- Deleted: Categorization of the risk
- Deleted: the
- Deleted: the
- Deleted: for
- Deleted: *the*

SP 2.1 Identify Risks

Identify and document risks.

Identifying 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 understandably 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 that may affect achieving objectives. To be effective, risk identification should not attempt to address every possible event regardless of how improbable it may be. Using categories and parameters developed in the risk management strategy, and identified sources of risk can provide the discipline and streamlining appropriate for risk identification. Identified risks form a baseline for initiating risk management activities. 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 focuses on identifying risks, not placement of blame. The results of risk identification activities should never be used by management to evaluate the performance of individuals.

There are many methods used for identifying risks. Typical identification methods include the following:

- Examine each element of the project work breakdown structure.
- Conduct a risk assessment using a risk taxonomy.
- Interview subject matter experts.
- Review risk management efforts from similar products.
- Examine lessons-learned documents or databases.
- Examine design specifications and agreement requirements.

- Deleted: IPPD Addition¶
- The particular risks associated with conducting the project using integrated teams should be considered, such as risks associated with loss of inter-team or intra-team coordination.¶
- ¶
- ¶
- The identification of
- Deleted: in an understandable way
- Deleted: in
- Deleted: be an
- Deleted: highly
- Deleted: Use of the
- Deleted: , along with the
- Deleted: ,
- Deleted: to
- Deleted: The identified
- Deleted: to initiate
- Deleted: The list of risks
- Deleted: activities focus
- Deleted: the identification of
- Deleted: are not
- Deleted: to uncover risks

Some risks are identified by examining the supplier's WBS, product, and processes using the categories and parameters developed in the risk management strategy. Risks can be identified in many areas (e.g., requirements, technology, design, testing, vulnerability to threats, and lifecycle costs). An examination of the project in these areas can help to develop or refine the acquisition strategy and the risk-sharing structure between the acquirer and supplier.

The acquirer considers risks associated with a supplier's capability (e.g., meeting schedule and cost requirements for the project), including potential risks to the acquirer's intellectual capital or security vulnerabilities introduced by using a supplier.

Typical Work Products

1. List of identified risks, including the context, conditions, and consequences of risk occurrence

Typical Supplier Deliverables

1. List of identified risks, including the context, conditions, and consequences of risk occurrence

Subpractices

1. Identify the risks associated with cost, schedule, and performance.

Cost, schedule, and performance risks should be examined in the acquirer's intended environment to the extent that they impact project objectives. Potential risks may be discovered that are outside the scope of project objectives but vital to customer interests. For example, risks in development costs, product acquisition costs, cost of spare (or replacement) products, and product disposition (or disposal) costs have design implications. The customer may not have considered the full cost of supporting a fielded product or using a delivered service. The customer should be informed of such risks, but actively managing those risks may not be necessary. Mechanisms for making such decisions should be examined at project and organization levels and put in place if deemed appropriate, especially for risks that impact the project's ability to verify and validate the product.

Deleted: There

Deleted: potential risks

Deleted: the project's

Deleted: the

Deleted: The mechanisms

In addition to the cost risks identified above, other cost risks may include those associated with funding levels, funding estimates, and distributed budgets.

Schedule risks may include risks associated with planned activities, key events, and milestones.

Deleted: Development

Performance risks may include risks associated with the following:

Deleted: -----Page Break-----

- Requirements
- Analysis and design
- Application of new technology
- Physical size
- Shape
- Weight
- Manufacturing and fabrication
- Functional performance and operation
- Verification
- Validation
- Performance maintenance attributes

Performance maintenance attributes are those characteristics that enable an in-use product or service to provide required performance, such as maintaining safety and security performance.

Deleted: originally

There are other risks that do not fall into cost, schedule, or performance categories.

Examples of these other risks include those related to the following:

Deleted: <#>Risks associated with strikes[]

- Strikes
- Diminishing sources of supply
- Technology cycle time
- Competition

2. Review environmental elements that may impact the project.

Risks to a project that frequently are missed include those supposedly outside the scope of the project (i.e., the project does not control whether they occur but can mitigate their impact), such as weather, natural or manmade disasters that affect the continuity of operations, political changes, and telecommunications failures.

3. Review all elements of the work breakdown structure as part of identifying risks to help ensure that all aspects of the work effort have been considered.

4. Review all elements of the project plan as part of identifying risks to help ensure that all aspects of the project have been considered.

Refer to the Project Planning process area for more information about identifying project risks.

5. Document the context, conditions, and potential consequences of each risk.

Deleted: the

Risk statements are typically documented in a standard format that contains the risk context, conditions, and consequences of occurrence. The risk context provides additional information about the risk such as the relative time frame of

Deleted: s

Deleted: that the intent of the risk can be easily understood. In documenting the context of the risk, consider

Deleted: Development

the risk, the circumstances or conditions surrounding the risk that has brought about the concern, and any doubt or uncertainty.

- 6. Identify the relevant stakeholders associated with each risk.

SP 2.2 Evaluate, Categorize, and Prioritize Risks

Evaluate and categorize each identified risk using defined risk categories and parameters, and determine its relative priority.

Deleted: the

The evaluation of risks is needed to assign a 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.

Deleted: ,

Deleted: ,

Collectively, the activities of risk evaluation, categorization, and prioritization are sometimes called a risk assessment or risk analysis.

Deleted: "

Deleted: "

Deleted: "

Deleted: "

The acquirer should conduct a risk assessment before solicitation to evaluate if the project can achieve its technical, schedule, and budget constraints. Technical, schedule, and cost risks should be discussed with potential suppliers before the solicitation is released. Using this approach, critical risks inherent in the project can be identified and addressed in the solicitation.

Typical Work Products

- 1. List of risks and their assigned priority

Deleted: , with a priority

Deleted: to each risk

Typical Supplier Deliverables

- 1. List of risks and their assigned priority

Subpractices

- 1. Evaluate identified risks using defined risk parameters.

Deleted: the

Deleted: the

Each risk is evaluated and assigned values according to defined risk parameters, which may include likelihood, consequence (severity or impact), and thresholds.

Deleted: in accordance with the

The assigned risk parameter values can be integrated to produce additional measures, such as risk exposure, which can be used to prioritize risks for handling.

Deleted: ,

Often, a scale with three to five values is used to evaluate both likelihood and consequence.

Deleted:

Likelihood, for example, can be categorized as remote, unlikely, likely, highly likely, or a near certainty.

Deleted: Examples

Deleted: Development

Example categories for consequence include the following:

- Low
- Medium
- High
- Negligible
- Marginal
- Significant
- Critical
- Catastrophic

Deleted: s

Probability values are frequently used to quantify likelihood. Consequences are generally related to cost, schedule, environmental impact, or human measures (e.g., labor hours lost and severity of injury).

Risk evaluation is often a difficult and time-consuming task. Specific expertise or group techniques may be needed to assess risks and gain confidence in the prioritization. In addition, priorities may require reevaluation as time progresses.

Deleted: This

Deleted: the

2. Categorize and group risks according to defined risk categories.

Deleted: the

Risks are categorized into defined risk categories, providing a means to review them according to their source, taxonomy, or project component. Related or equivalent risks may be grouped for efficient handling. The cause-and-effect relationships between related risks are documented.

Deleted: the

Deleted: look at risks

An acquirer's risk categories may include sourcing, contract management, and supplier execution, in addition to project management, technology, and requirements.

3. Prioritize risks for mitigation.

A relative priority is determined for each risk based on assigned risk parameters. Clear criteria should be used to determine risk priority. Risk prioritization helps to determine the most effective areas to which resources for risks mitigation can be applied with the greatest positive impact to the project.

Deleted: the

Deleted: the

Deleted: The intent of

Deleted: is

Deleted: of risks

SG 3 Mitigate Risks

Risks are handled and mitigated, as appropriate, to reduce adverse impacts on achieving objectives.

Deleted: where

The steps in handling risks include developing risk-handling options, monitoring risks, and performing risk-handling activities when defined thresholds are exceeded. Risk mitigation plans are developed and implemented for selected risks to proactively reduce the potential impact of risk occurrence. Risk mitigation planning can also include contingency plans to deal with the impact of selected risks that may occur despite attempts to mitigate them. Risk parameters used to trigger risk-handling activities are defined by the risk management strategy.

Deleted: This

Deleted: The risk

SP 3.1 Develop Risk Mitigation Plans

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 planning is developing alternative courses of action, workarounds, and fallback positions, and 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 risk occurrence, the extent of damage incurred should the risk occur (sometimes called a contingency plan), or both. Risks are monitored and when they exceed established thresholds, risk mitigation plans are deployed to return the impacted effort to an acceptable risk level. If the risk cannot be mitigated, a contingency plan can be invoked. Both risk mitigation and contingency plans often are generated only for selected risks for which consequences of the risks are high or unacceptable; other risks may be accepted and simply monitored.

Deleted: plan

Deleted: to develop

Deleted: with

Deleted: of the risk

Deleted: "

Deleted: "

Deleted: the

Deleted: the

Deleted: are

Deleted: where the

Deleted: determined to be

Options for handling risks typically include alternatives such as the following:

- Risk avoidance: changing or lowering requirements while still meeting user needs
- Risk control: taking active steps to minimize risks
- Risk transfer: reallocating requirements to lower risks
- Risk monitoring: watching and periodically reevaluating the risk for changes in assigned risk parameters
- Risk acceptance: acknowledging risk but not taking action

Deleted: Changing

Deleted: the user's

Deleted: Taking

Deleted: Reallocating

Deleted: the

Deleted: Watching

Deleted: to the

Deleted: Acknowledgment of

Deleted: any

Often, especially for high risks, more than one approach to handling a risk should be generated.

For example, in the case of an event that disrupts the continuity of operations, approaches to risk management can include establishing the following:

- Resource reserves to respond to disruptive events
- Lists of available back-up equipment
- Back-up personnel for key personnel
- Plans for and results of testing emergency response systems
- Posted procedures for emergencies
- Disseminated lists of key contacts and information resources for emergencies

Deleted: appropriate

Deleted: to be available

Deleted: /for

In many cases, risks are 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 (i.e., the combination of likelihood and consequence) that will trigger risk mitigation planning or invoke a contingency plan.

Deleted: will be

Deleted: ,

Deleted: if it is needed

Thresholds for supplier risks that affect the project (e.g., schedule, quality, or risk exposure due to supplier risks) are specified in the supplier agreement along with escalation procedures if thresholds are exceeded.

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

Typical Work Products

1. Documented handling options for each identified risk
2. Risk mitigation plans
3. Contingency plans
4. Disaster recovery or continuity plans
5. List of those responsible for tracking and addressing each risk

Typical Supplier Deliverables

1. Documented handling options for each identified risk
2. Risk mitigation plans
3. Contingency plans
4. Disaster recovery or continuity plans
5. List of those responsible for tracking and addressing each risk

Subpractices

1. Determine the levels and thresholds that define when a risk becomes unacceptable and triggers the execution of a risk mitigation plan or contingency plan.

Deleted: a

Risk level (derived using a risk model) is a measure combining the uncertainty of reaching an objective with the consequences of failing to reach the objective.

Risk levels and thresholds that bound planned or acceptable performance must be clearly understood and defined to provide a means with which risk can be understood. Proper categorization of risk is essential for ensuring an appropriate priority based on severity and the associated management response. There may be multiple thresholds employed to initiate varying levels of management response. Typically, thresholds for the execution of risk mitigation plans are set to engage before the execution of contingency plans.

2. Identify the person or group responsible for addressing each risk.
3. Determine the cost-to-benefit ratio of implementing the risk mitigation plan for each risk.

Deleted: the

Deleted: the

Deleted: the

Deleted: then

Risk mitigation activities should be examined for benefits they provide versus resources they will expend. Just like any other design activity, alternative plans may need to be developed and costs and benefits of each alternative assessed. The most appropriate plan is selected for implementation.

Deleted: At times the risk may be significant and the benefits small, but the risk must be mitigated to reduce the probability of incurring unacceptable consequences.

Deleted: Development

- 4. Develop an overall risk mitigation plan for the project to orchestrate the implementation of individual risk mitigation and contingency plans.

Deleted: the

The complete set of risk mitigation plans may not be affordable. A tradeoff analysis should be performed to prioritize risk mitigation plans for implementation.

Deleted: the

- 5. Develop contingency plans for selected critical risks in the event their impacts are realized.

Risk mitigation plans are developed and implemented as needed to proactively reduce risks before they become problems. Despite best efforts, some risks may be unavoidable and will become problems that impact the project. Contingency plans can be developed for critical risks to describe actions a project may take to deal with the occurrence of this impact. The intent is to define a proactive plan for handling the risk, either to reduce the risk (mitigation) or respond to the risk (contingency), but in either event to manage the risk.

Deleted: the

Some risk management literature may consider contingency plans a synonym or subset of risk mitigation plans. These plans also may be addressed together as risk-handling or risk action plans.

SP 3.2 Implement Risk Mitigation Plans

Monitor the status of each risk periodically and implement the risk mitigation plan, as appropriate.

To effectively control and manage risks during the work effort, follow a proactive program to regularly monitor risks and the status and results of risk-handling actions. The risk management strategy defines the intervals at which risk status should be revisited. This activity may result in the discovery of new risks or new risk-handling options that can require replanning and reassessment. In either event, acceptability thresholds associated with the risk should be compared to the risk status to determine the need for implementing a risk mitigation plan.

Deleted: the

Deleted: the

Deleted: against

The acquirer shares selected risks with the supplier. Risks associated with the acquisition process are tracked and resolved or controlled until mitigated. This monitoring includes risks that may be escalated by the supplier.

Typical Work Products

- 1. Updated lists of risk status
- 2. Updated assessments of risk likelihood, consequence, and thresholds

- 3. Updated list of risk-handling options

Deleted: lists

- 4. Updated list of actions taken to handle risks

- 5. Risk mitigation plans

Typical Supplier Deliverables

- 1. Updated list of risk status

2. Updated assessments of risk likelihood, consequence, and thresholds

3. Updated list of risk-handling options

4. Updated list of actions taken to handle risks

5. Risk mitigation plans

Subpractices

1. Monitor risk status.

After a risk mitigation plan is initiated, the risk is still monitored. Thresholds are assessed to check for the potential execution of a contingency plan.

A mechanism for monitoring should be employed.

Deleted: periodic

2. Provide a method for tracking open risk-handling action items to closure.

Refer to the Project Monitoring and Control process area for more information about tracking action items.

3. Invoke selected risk-handling options when monitored risks exceed defined thresholds.

Often, risk handling is only performed for risks judged to be "high" and "medium." The risk-handling strategy for a given risk may include techniques and methods to avoid, reduce, and control the likelihood of the risk or the extent of damage incurred should the risk (anticipated event or situation) occur or both. In this context, risk handling includes both risk mitigation plans and contingency plans.

Deleted: the

Deleted: Quite often

Deleted: those

Risk-handling techniques are developed to avoid, reduce, and control adverse impact to project objectives and to bring about acceptable outcomes in light of probable impacts. Actions generated to handle a risk require proper resource loading and scheduling in plans and baseline schedules. This replanning must closely consider the effects on adjacent or dependent work initiatives or activities.

Deleted: with

Deleted: effort needs to

Refer to the Project Monitoring and Control process area for more information about revising the project plan.

4. Establish a schedule or period of performance for each risk-handling activity that includes a start date and anticipated completion date.

Deleted: the

5. Provide a continued commitment of resources for each plan to allow the successful execution of risk-handling activities.

Deleted: the

6. Collect performance measures on risk-handling activities.

Deleted: the

Deleted: Generic Practices by Goal

Continuous Only

[1]

Risk Management (RSKM)

Generic Practices by Goal

Continuous Only**GG 1 Achieve Specific Goals**

The process supports and enables achievement of the specific goals of the process area by transforming identifiable input work products to produce identifiable output work products.

GP 1.1 Perform Specific Practices

Perform the specific practices of the risk management process to develop work products and provide services to achieve the specific goals of the process area.

GG 2 Institutionalize a Managed Process

The process is institutionalized as a managed process.

Staged Only**GG 3 Institutionalize a Defined Process**

The process is institutionalized as a defined process.

This generic goal's appearance here reflects its location in the staged representation.

GP 2.1 Establish an Organizational Policy

Establish and maintain an organizational policy for planning and performing the risk management process.

Elaboration:

This policy establishes organizational expectations for defining a risk management strategy and identifying, analyzing, and mitigating risks.

GP 2.2 Plan the Process

Establish and maintain the plan for performing the risk management process.

Elaboration:

This plan for performing the risk management process can be included in (or referenced by) the project plan, which is described in the Project Planning process area. The plan called for in this generic practice would address the comprehensive planning for all of the specific practices in this process area. In particular, this plan provides the overall approach for risk mitigation, but is distinct from mitigation plans (including contingency plans) for specific risks. In contrast, the risk mitigation plans called for in the specific practices would address more focused items such as the levels that trigger risk-handling activities.

GP 2.3 Provide Resources

Provide adequate resources for performing the risk management process, developing the work products, and providing the services of the process.

Elaboration:

Examples of resources provided include the following tools:

- Risk management databases
- Risk mitigation tools
- Prototyping tools
- Modeling and simulation

GP 2.4 Assign Responsibility

Assign responsibility and authority for performing the process, developing the work products, and providing the services of the risk management process.

GP 2.5 Train People

Train the people performing or supporting the risk management process as needed.

Elaboration:

Examples of training topics include the following:

Risk management concepts and activities (e.g., risk identification, evaluation, monitoring, and mitigation)

Measure selection for risk mitigation

GP 2.6 Manage Configurations

Place designated work products of the risk management process under appropriate levels of control.

Elaboration:

Examples of work products placed under control include the following:

Risk management strategy

Identified risk items

Risk mitigation plans

GP 2.7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the risk management process as planned.

Elaboration:

Examples of activities for stakeholder involvement include the following:

Establishing a collaborative environment for free and open discussion of risk

Reviewing the risk management strategy and risk mitigation plans

Participating in risk identification, analysis, and mitigation activities

Communicating and reporting risk management status

GP 2.8 Monitor and Control the Process

Monitor and control the risk management process against the plan for performing the process and take appropriate corrective action.

Elaboration:

Examples of measures and work products used in monitoring and controlling include the following:

- Number of risks identified, managed, tracked, and controlled
- Risk exposure and changes to the risk exposure for each assessed risk, and as a summary percentage of management reserve
- Change activity for the risk mitigation plans (e.g., processes, schedule, and funding)
- Occurrence of unanticipated risks
- Risk categorization volatility
- Comparison of estimated versus actual risk mitigation effort and impact
- Schedule for risk analysis activities
- Schedule of actions for a specific mitigation

GP 2.9 Objectively Evaluate Adherence

Objectively evaluate adherence of the risk management process against its process description, standards, and procedures, and address noncompliance.

Elaboration:

Examples of activities reviewed include the following:

- Establishing and maintaining a risk management strategy
- Identifying and analyzing risks
- Mitigating risks

Examples of work products reviewed include the following:

- Risk management strategy
- Risk mitigation plans

GP 2.10 Review Status with Higher Level Management

Review the activities, status, and results of the risk management process with higher level management and resolve issues.

Elaboration:

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 include a summary of the most critical risks, key risk parameters (such as likelihood and consequence of the risks), and the status of risk mitigation efforts.

Continuous Only

GG 3 Institutionalize a Defined Process

The process is institutionalized as a defined process.

This generic goal's appearance here reflects its location in the continuous representation.

GP 3.1 Establish a Defined Process

Establish and maintain the description of a defined risk management process.

GP 3.2 Collect Improvement Information

Collect work products, measures, measurement results, and improvement information derived from planning and performing the risk management process to support the future use and improvement of the organization's processes and process assets.

Elaboration:

Examples of work products, measures, measurement results, and improvement information include the following:

- Risk parameters
- Risk categories
- Risk status reports

Continuous Only

GG 4 Institutionalize a Quantitatively Managed Process

The process is institutionalized as a quantitatively managed process.

GP 4.1 Establish Quantitative Objectives for the Process

Establish and maintain quantitative objectives for the risk management process, which address quality and process performance, based on customer needs and business objectives.

GP 4.2 Stabilize Subprocess Performance

Stabilize the performance of one or more subprocesses to determine the ability of the risk management process to achieve the established quantitative quality and process-performance objectives.

GG 5 Institutionalize an Optimizing Process

The process is institutionalized as an optimizing process.

GP 5.1 Ensure Continuous Process Improvement

Ensure continuous improvement of the risk management process in fulfilling the relevant business objectives of the organization.

GP 5.2 Correct Root Causes of Problems

Identify and correct the root causes of defects and other problems in the risk management process.