

## **RISK MANAGEMENT**

---

Maturity Level 3

### **Purpose**

---

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. [PA148]

### **Introductory Notes**

---

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. [PA148.N101]

Effective risk management includes early and aggressive risk identification through the collaboration and 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 the free and open disclosure and discussion of risk. [PA148.N102]

While 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. [PA148.N103]

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. [PA148.N104]

As represented in the Project Planning and Project Monitoring and Control process areas, organizations may initially focus simply 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.

[PA148.N105]

Although the primary emphasis of the Risk Management process area is on the project, the concepts may also be applied to manage organizational risks. [PA148.N106]

## Related Process Areas

---

*Refer to the Project Planning Process Area for more information about identification of project risks and planning for involvement of relevant stakeholders.* [PA148.R101]

*Refer to the Project Monitoring and Control process area for more information about monitoring project risks.* [PA148.R102]

*Refer to the Decision Analysis and Resolution process area for more information about using a formal evaluation process to evaluate alternatives for selection and mitigation of identified risks.* [PA148.R103]

## Specific and Generic Goals

---

### SG 1 Prepare for Risk Management [PA148.IG101]

***Preparation for risk management is conducted.***

### SG 2 Identify and Analyze Risks [PA148.IG102]

***Risks are identified and analyzed to determine their relative importance.***

### SG 3 Mitigate Risks [PA148.IG103]

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

### GG 3 Institutionalize a Defined Process [CL104.GL101]

***The process is institutionalized as a defined process.***

## Practice-to-Goal Relationship Table

SG 1 Prepare for Risk Management [PA148.IG101]		
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 [PA148.IG102]		
SP 2.1		Identify Risks
SP 2.2		Evaluate, Categorize, and Prioritize Risks
SG 3 Mitigate Risks [PA148.IG103]		
SP 3.1		Develop Risk Mitigation Plans
SP 3.2		Implement Risk Mitigation Plans
GG 3 Institutionalize a Defined Process [CL104.GL101]		
GP 2.1	(CO 1)	Establish an Organizational Policy
GP 3.1	(AB 1)	Establish a Defined Process
GP 2.2	(AB 2)	Plan the Process
GP 2.3	(AB 3)	Provide Resources
GP 2.4	(AB 4)	Assign Responsibility
GP 2.5	(AB 5)	Train People
GP 2.6	(DI 1)	Manage Configurations
GP 2.7	(DI 2)	Identify and Involve Relevant Stakeholders
GP 2.8	(DI 3)	Monitor and Control the Process
GP 3.2	(DI 4)	Collect Improvement Information
GP 2.9	(VE 1)	Objectively Evaluate Adherence
GP 2.10	(VE 2)	Review Status with Higher Level Management

## Specific Practices by Goal

### SG 1 Prepare for Risk Management

#### ***Preparation for risk management is conducted.*** [PA148.IG101]

Preparation is conducted by establishing and maintaining a strategy for identifying, analyzing, and mitigating risks. This is typically documented in a risk management plan. The risk management strategy addresses the specific actions and management approach used to apply and control the risk management program. This includes identifying the sources of risk, the scheme used to categorize risks, and the parameters used to evaluate, bound, and control risks for effective handling. [PA148.IG101.N101]

#### **SP 1.1 Determine Risk Sources and Categories**

##### ***Determine risk sources and categories.*** [PA148.IG101.SP101]

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. [PA148.IG101.SP101.N101]

#### Typical Work Products

1. Risk source lists (external and internal) [PA148.IG101.SP101.W101]
2. Risk categories list [PA148.IG101.SP101.W102]

#### Subpractices

1. Determine risk sources. [PA148.IG101.SP101.SubP101]

Risk sources are the fundamental drivers that cause risks within a project or organization. There are many sources of risks, both internal and external to a project. Risk sources identify common areas where risks may originate. Typical internal and external risk sources include the following: [PA148.IG101.SP101.SubP101.N101]

- Uncertain requirements
- Unprecedented efforts—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 vendor capability

Many of these sources of risk are often accepted without adequate planning. 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 the risks or reduce the consequences of their occurrence. [PA148.IG101.SP101.SubP101.N102]

2. Determine risk categories. [PA148.IG101.SP101.SubP102]

Risk categories reflect the “bins” for collecting and organizing risks. A reason for identifying risk categories is to help in the future consolidation of the activities in the risk mitigation plans. [PA148.IG101.SP101.SubP102.N101]

The following factors may be considered when determining risk categories:

[PA148.IG101.SP101.SubP102.N102]

- The phases of the project's life-cycle model (e.g., requirements, design, manufacturing, test and evaluation, delivery, disposal)
- The types of processes used
- The types of products used
- Program management risks (e.g., contract risks, budget/cost risks, schedule risks, resources risks, performance risks, supportability risks)

A risk taxonomy can be used to provide a framework for determining risk sources and categories. [PA148.IG101.SP101.SubP102.N103]

## SP 1.2 Define Risk Parameters

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

[PA148.IG101.SP102]

Parameters for evaluating, categorizing, and prioritizing risks include the following: [PA148.IG101.SP102.N101]

- Risk likelihood (i.e., probability of risk occurrence)
- Risk consequence (i.e., impact and severity of risk occurrence)
- 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. [PA148.IG101.SP102.N102]

### Typical Work Products

1. Risk evaluation, categorization, and prioritization criteria  
[PA148.IG101.SP102.W101]
2. Risk management requirements (control and approval levels, reassessment intervals, etc.) [PA148.IG101.SP102.W102]

### Subpractices

1. Define consistent criteria for evaluating and quantifying risk likelihood and severity levels. [PA148.IG101.SP102.SubP101]

Consistently used criteria (e.g., the bounds on the likelihood and severity levels) allow the 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 (for example, personnel safety versus environmental pollution), it is important to ensure consistency in end result (e.g., a high risk of environmental pollution is as important as a high risk to personnel safety).

[PA148.IG101.SP102.SubP101.N101]

2. Define thresholds for each risk category. [PA148.IG101.SP102.SubP102]

For each risk category, thresholds can be established to determine acceptability or unacceptability of risks, prioritization of risks, or triggers for management action. [PA148.IG101.SP102.SubP102.N101]

Examples of thresholds include the following: [PA148.IG101.SP102.SubP102.N102]

- Project-wide thresholds could be established to involve senior management when product costs exceed 10% of the target cost or when Cost Performance Indexes (CPIs) fall below 0.95.
- Schedule thresholds could be established to involve senior management when Schedule Performance Indexes (SPIs) fall below 0.95.
- Performance thresholds could be set to involve senior management when specified key design items (e.g., processor utilization) exceed 125% of the intended design.

These may be refined later, for each identified risk, to establish points at which more aggressive risk monitoring is employed or to signal the implementation of risk mitigation plans. [PA148.IG101.SP102.SubP102.N105]

3. Define bounds on the extent to which thresholds are applied against or within a category. [PA148.IG101.SP102.SubP103]

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 scope the extent of the risk management effort and avoid excessive resource expenditures. Bounds may include exclusion of a risk source from a category. These bounds may also exclude any condition that occurs less than a given frequency. [PA148.IG101.SP102.SubP103.N101]

### SP 1.3 Establish a Risk Management Strategy

***Establish and maintain the strategy to be used for risk management.*** [PA148.IG101.SP103]

A comprehensive risk management strategy addresses items such as the following: [PA148.IG101.SP103.N101]

- 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 these risks are to be organized, categorized, compared, and consolidated
- Parameters, including likelihood, consequence, and thresholds, for taking action on identified risks
- Risk mitigation techniques to be used, such as prototyping, simulation, alternative designs, or evolutionary development
- Definition of risk measures to monitor the status of the risks
- 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. [PA148.IG101.SP103.N102]

#### Typical Work Products

1. Project risk management strategy [PA148.IG101.SP103.W101]

## SG 2 Identify and Analyze Risks

### ***Risks are identified and analyzed to determine their relative importance.***

[PA148.IG102]

The degree of risk impacts the resources assigned to handle an identified risk and the determination of when appropriate management attention is required. [PA148.IG102.N101]

Analyzing risks entails identifying risks from the internal and external sources identified and then evaluating each identified risk to determine its likelihood and consequences. Categorization of the risk, based on an evaluation against the established risk categories and criteria developed for the risk management strategy, provides the information needed for risk handling. Related risks may be grouped for efficient handling and effective use of risk management resources. [PA148.IG102.N102]

#### SP 2.1 Identify Risks

### ***Identify and document the risks.*** [PA148.IG102.SP101]

***For Integrated Product and Process Development***

*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.* [PA148.IG102.SP101.AMP101]

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. [PA148.IG102.SP101.N101]

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.

[PA148.IG102.SP101.N102]

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.

[PA148.IG102.SP101.N104]

There are many methods for identifying risks. Typical identification methods include the following: [PA148.IG102.SP101.N103]

- Examine each element of the project work breakdown structure to uncover risks.
- 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.

**Typical Work Products**

1. List of identified risks, including the context, conditions, and consequences of risk occurrence [PA148.IG102.SP101.W101]

### Subpractices

1. Identify the risks associated with cost, schedule, and performance in all appropriate product life-cycle phases. [PA148.IG102.SP101.SubP101]

Cost, schedule, and performance risks should be examined during all phases of the product life cycle to the extent they impact project objectives. There may be potential risks discovered that are outside the scope of the project's objectives but vital to customer interests. For example, the 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 provided requirements for the cost of supporting the fielded product. The customer should be informed of such risks, but actively managing those risks may not be necessary. The 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 ability to verify and validate the product.

[PA148.IG102.SP101.SubP101.N101]

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

[PA148.IG102.SP101.SubP101.N102]

Schedule risks may include risks associated with planned activities, key events, and milestones. [PA148.IG102.SP101.SubP101.N103]

Performance risks may include risks associated with the following:

[PA148.IG102.SP101.SubP101.N104]

- 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 to provide originally required performance, such as maintaining safety and security performance. [PA148.IG102.SP101.SubP101.N105]

There are other risks that do not fall into cost, schedule, or performance categories. [PA148.IG102.SP101.SubP101.N106]

Examples of these other risks include the following: [PA148.IG102.SP101.SubP101.N107]

- Risks associated with strikes
- Diminishing sources of supply
- Technology cycle time
- Competition

2. Review environmental elements that may impact the project.

[PA148.IG102.SP101.SubP102]

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 disasters, political changes, and telecommunications failures. [PA148.IG102.SP101.SubP102.N101]

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. [PA148.IG102.SP101.SubP103]

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.

[PA148.IG102.SP101.SubP104]

*Refer to the Project Planning process area for more information about identifying project risks.* [PA148.IG102.SP101.SubP104.R101]

5. Document the context, conditions, and potential consequences of the risk. [PA148.IG102.SP101.SubP105]

Risks statements are typically documented in a standard format that contains the risk context, conditions, and consequences of occurrence. The risk context provides additional information such that the intent of the risk can be easily understood. In documenting the context of the risk, consider the relative time frame of the risk, the circumstances or conditions surrounding the risk that has brought about the concern, and any doubt or uncertainty. [PA148.IG102.SP101.SubP105.N101]

6. Identify the relevant stakeholders associated with each risk.

[PA148.IG102.SP101.SubP106]

## SP 2.2 Evaluate, Categorize, and Prioritize Risks

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

[PA148.IG102.SP102]

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. [PA148.IG102.SP102.N101]

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

[PA148.IG102.SP102.N103]

### Typical Work Products

1. List of risks, with a priority assigned to each risk [PA148.IG102.SP102.W101]

### Subpractices

1. Evaluate the identified risks using the defined risk parameters.

[PA148.IG102.SP102.SubP101]

Each risk is evaluated and assigned values in accordance with the defined risk parameters, which may include likelihood, consequence (severity, or impact), and thresholds. 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. [PA148.IG102.SP102.SubP101.N101]

Often, a scale with three to five values is used to evaluate both likelihood and consequence. Likelihood, for example, can be categorized as remote, unlikely, likely, highly likely, or a near certainty. [PA148.IG102.SP102.SubP101.N102]

Examples for consequences include the following: [PA148.IG102.SP102.SubP101.N104]

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

Probability values are frequently used to quantify likelihood. Consequences are generally related to cost, schedule, environmental impact, or human measures (such as labor hours lost and severity of injury). [PA148.IG102.SP102.SubP101.N105]

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

[PA148.IG102.SP102.SubP101.N103]

2. **Categorize and group risks according to the defined risk categories.** [PA148.IG102.SP102.SubP102]

Risks are categorized into the defined risk categories, providing a means to look at risks 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. [PA148.IG102.SP102.SubP102.N101]

3. **Prioritize risks for mitigation.** [PA148.IG102.SP102.SubP103]

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

[PA148.IG102.SP102.SubP103.N101]

### SG 3 Mitigate Risks

***Risks are handled and mitigated, where appropriate, to reduce adverse impacts on achieving objectives.*** [PA148.IG103]

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. This may also include contingency plans to deal with the impact of selected risks that may occur despite attempts to mitigate them. The risk parameters used to trigger risk-handling activities are defined by the risk management strategy. [PA148.IG103.N101]

#### 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.*** [PA148.IG103.SP101]

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.

[PA148.IG103.SP101.N102]

Options for handling risks typically include alternatives such as the following: [PA148.IG103.SP101.N103]

- Risk avoidance: Changing or lowering requirements while still meeting the user’s needs
- Risk control: Taking active steps to minimize risks
- Risk transfer: Reallocating design requirements to lower the risks
- Risk monitoring: Watching and periodically reevaluating the risk for changes to the assigned risk parameters
- 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. [PA148.IG103.SP101.N104]

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.

[PA148.IG103.SP101.N105]

Adequate consideration should be given early to technology demonstrations, models, simulations, and prototypes as part of risk mitigation planning. [PA148.IG103.SP101.N106]

#### Typical Work Products

1. Documented handling options for each identified risk

[PA148.IG103.SP101.W101]

2. Risk mitigation plans [PA148.IG103.SP101.W102]

3. Contingency plans [PA148.IG103.SP101.W104]
4. List of those responsible for tracking and addressing each risk [PA148.IG103.SP101.W103]

#### Subpractices

1. Determine the levels and thresholds that define when a risk becomes unacceptable and triggers the execution of a risk mitigation plan or a contingency plan. [PA148.IG103.SP101.SubP101]

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.

[PA148.IG103.SP101.SubP101.N101]

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 both 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. [PA148.IG103.SP101.SubP101.N102]

2. Identify the person or group responsible for addressing each risk. [PA148.IG103.SP101.SubP102]
3. Determine the cost-to-benefit ratio of implementing the risk mitigation plan for each risk. [PA148.IG103.SP101.SubP103]

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

[PA148.IG103.SP101.SubP103.N101]

4. Develop an overall risk mitigation plan for the project to orchestrate the implementation of the individual risk mitigation and contingency plans. [PA148.IG103.SP101.SubP104]

The complete set of risk mitigation plans may not be affordable. A tradeoff analysis should be performed to prioritize the risk mitigation plans for implementation. [PA148.IG103.SP101.SubP104.N101]

5. Develop contingency plans for selected critical risks in the event their impacts are realized. [PA148.IG103.SP101.SubP105]

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 the 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. [PA148.IG103.SP101.SubP105.N101]

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. [PA148.IG103.SP101.SubP105.N102]

### SP 3.2 Implement Risk Mitigation Plans

***Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate.*** [PA148.IG103.SP102]

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 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. [PA148.IG103.SP102.N101]

#### Typical Work Products

1. Updated lists of risk status [PA148.IG103.SP102.W101]
2. Updated assessments of risk likelihood, consequence, and thresholds [PA148.IG103.SP102.W102]
3. Updated lists of risk-handling options [PA148.IG103.SP102.W103]
4. Updated list of actions taken to handle risks [PA148.IG103.SP102.W104]
5. Risk mitigation plans [PA148.IG103.SP102.W105]

#### Subpractices

1. Monitor risk status. [PA148.IG103.SP102.SubP101]

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.

[PA148.IG103.SP102.SubP101.N101]

A periodic mechanism for monitoring should be employed. [PA148.IG103.SP102.SubP101.N102]

2. Provide a method for tracking open risk-handling action items to closure. [PA148.IG103.SP102.SubP102]

*Refer to the Project Monitoring and Control process area for more information about tracking action items.* [PA148.IG103.SP102.SubP102.R101]

3. Invoke selected risk-handling options when monitored risks exceed the defined thresholds. [PA148.IG103.SP102.SubP103]

Quite often, risk handling is only performed for those 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. [PA148.IG103.SP102.SubP103.N101]

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 within plans and baseline schedules. This re-planning effort needs to closely consider the effects on adjacent or dependent work initiatives or activities. [PA148.IG103.SP102.SubP103.N102]

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

[PA148.IG103.SP102.SubP103.N102.R101]

4. Establish a schedule or period of performance for each risk-handling activity that includes the start date and anticipated completion date. [PA148.IG103.SP102.SubP104]
5. Provide continued commitment of resources for each plan to allow successful execution of the risk-handling activities.

[PA148.IG103.SP102.SubP105]

6. Collect performance measures on the risk-handling activities.

[PA148.IG103.SP102.SubP106]

### **GG 3 Institutionalize a Defined Process** [CL104.GL101]

***The process is institutionalized as a defined process.***

#### **Commitment to Perform**

##### **GP 2.1 (CO 1) Establish an Organizational Policy**

***Establish and maintain an organizational policy for planning and performing the risk management process.*** [GP103]

Elaboration:

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

[PA148.EL101]

## Ability to Perform

---

### GP 3.1 (AB 1) Establish a Defined Process

***Establish and maintain the description of a defined risk management process.*** [GP114]

### GP 2.2 (AB 2) Plan the Process

***Establish and maintain the plan for performing the risk management process.*** [GP104]

Elaboration:

Typically, this plan for performing the risk management process is included in (or referenced by) the project plan, which is described in the Project Planning process area. The plan for performing the risk management process differs from both the risk management strategy and the risk mitigation plans described in the specific practices in this 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, from determining risk sources and categories all the way through to the implementation of risk mitigation plans. In contrast, the risk management strategy called for in one specific practice would address the project-specific risk strategy for things such as risk sources, thresholds, tools, and techniques, and would monitor time intervals. The risk mitigation plans called for in another specific practice would address more focused items such as the levels that trigger risk-handling activities. [PA148.EL103]

### GP 2.3 (AB 3) Provide Resources

***Provide adequate resources for performing the risk management process, developing the work products, and providing the services of the process.*** [GP105]

Elaboration:

Examples of resources provided include the following tools: [PA148.EL106]

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

**GP 2.4 (AB 4) Assign Responsibility**

***Assign responsibility and authority for performing the process, developing the work products, and providing the services of the risk management process.*** [GP106]

**GP 2.5 (AB 5) Train People**

***Train the people performing or supporting the risk management process as needed.*** [GP107]

Elaboration:

Examples of training topics include the following: [PA148.EL108]

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

## **Directing Implementation**

---

**GP 2.6 (DI 1) Manage Configurations**

***Place designated work products of the risk management process under appropriate levels of configuration management.*** [GP109]

Elaboration:

Examples of work products placed under configuration management include the following: [PA148.EL110]

- Risk management strategy
- Identified risk items
- Risk mitigation plans

**GP 2.7 (DI 2) Identify and Involve Relevant Stakeholders**

***Identify and involve the relevant stakeholders of the risk management process as planned.*** [GP124]

Elaboration:

Examples of activities for stakeholder involvement include the following: [PA148.EL120]

- 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 (DI 3) Monitor and Control the Process**

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

[GP110]

Elaboration:

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

[PA148.EL113]

- 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, funding)
- Occurrence of unanticipated risks
- Risk categorization volatility
- Comparison of estimated vs. actual risk mitigation effort and impact

**GP 3.2 (DI 4) 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.***

[GP117]

---

**Verifying Implementation**

**GP 2.9 (VE 1) Objectively Evaluate Adherence**

***Objectively evaluate adherence of the risk management process against its process description, standards, and procedures, and address noncompliance.*** [GP113]

Elaboration:

Examples of activities reviewed include the following: [PA148.EL116]

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

Examples of work products reviewed include the following: [PA148.EL117]

- Risk management strategy
- Risk mitigation plans

**GP 2.10 (VE 2) Review Status with Higher Level Management**

***Review the activities, status, and results of the risk management process with higher level management and resolve issues.*** [GP112]

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. [PA148.EL118]

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. [PA148.EL119]