

11.1 Risk Management Planning		11.2 Risk Identification		11.3 Qualitative Risk Analysis		11.4 Quantitative Risk Analysis		11.5 Risk Response Planning		11.6 Risk Monitoring and Control	
Integration	Scope	Time	Cost	Quality	Resource	Communications		Risk	Procurement		

[return to model](#)

11.5 Risk Response Planning

Risk response planning is the process of developing options and determining actions to enhance opportunities and reduce threats to the project’s objectives. It includes the identification and assignment of individuals or parties to take responsibility for each agreed risk response. This process ensures that identified risks are properly addressed. The effectiveness of response planning will directly determine whether risk increases or decreases for the project.

Risk response planning must be appropriate to the severity of the risk, cost effective in meeting the challenge, timely to be successful, realistic within the project context, agreed upon by all parties involved, and owned by a responsible person. Selecting the best risk response from several options is often required.



11.5.1 Inputs to Risk Response Planning

- .1 Risk management plan..** This plan is described in [Section 11.1.3](#).
- .2 List of prioritized risks.** This list from qualaitative risk analysis is described in [Section 11.3.3.2](#).
- .3 Risk ranking of the project.** This is described in [Section 11.3.3.1](#).
- .4 Prioritized list of quantified risks.** This list from quantitative risk analysis is described in [Section 11.4.3.1](#).
- .5 Probabilistic analysis of the project.** This is described in [Section 11.4.3.2](#).
- .6 Probability of achieving the cost and time objectives.** This is described in [Section 11.4.3.3](#).
- .7 List of potential responses.** In the risk identification process, actions may be identified that respond to individual risks or categories of risks.
- .8 Risk thresholds.** The level of risk that is acceptable to the organization will influence risk response planning (see [Section 11.1.3](#)).
- .9 Risk owners.** A list of project stakeholders able to act as owners of risk responses. Risk owners should be involved in developing the risk responses.
- .10 Common risk causes.** Several risks may be driven by a common cause. This situation may reveal opportunities to mitigate two or more project risks with one generic response.
- .11 Trends in qualitative and quantitative risk analysis results.** These are described in [Sections 11.3.3.4](#) and [11.4.3.4](#). Trends in results can make risk response or further analysis more or less urgent and important.

11.5.2 Tools and Techniques for Risk Response Planning

Several risk response strategies are available. The strategy that is most likely to be effective should be selected for each risk. Then, specific actions should be developed to implement that strategy. Primary and backup strategies may be selected.

.1 Avoidance. Risk avoidance is changing the project plan to eliminate the risk or condition or to protect the project objectives from its impact. Although the project team can never eliminate all risk events, some specific risks may be avoided.

Some risk events that arise early in the project can be dealt with by clarifying requirements, obtaining information, improving communication, or acquiring expertise. Reducing scope to avoid high-risk activities, adding resources or time, adopting a familiar approach instead of an innovative one, or avoiding an unfamiliar subcontractor may be examples of avoidance.

.2 Transference. Risk transfer is seeking to shift the consequence of a risk to a third party together with ownership of the response. Transferring the risk simply gives another party responsibility for its management; it does not eliminate it.

Transferring liability for risk is most effective in dealing with financial risk exposure. Risk transfer nearly always involves payment of a risk premium to the party taking on the risk. It includes the use of insurance, performance bonds, warranties, and guarantees. Contracts may be used to transfer liability for specified risks to another party. Use of a fixed-price contract may transfer risk to the seller if the project's design is stable. Although a cost-reimbursable contract leaves more of the risk with the customer or sponsor, it may help reduce cost if there are mid-project changes.

.3 Mitigation. Mitigation seeks to reduce the probability and/or consequences of an adverse risk event to an acceptable threshold. Taking early action to reduce the probability of a risk's occurring or its impact on the project is more effective than trying to repair the consequences after it has occurred. Mitigation costs should be appropriate, given the likely probability of the risk and its consequences.

Risk mitigation may take the form of implementing a new course of action that will reduce the problem—e.g., adopting less complex processes, conducting more seismic or engineering tests, or choosing a more stable seller. It may involve changing conditions so that the probability of the risk occurring is reduced—e.g., adding resources or time to the schedule. It may require prototype development to reduce the risk of scaling up from a bench-scale model.

Where it is not possible to reduce probability, a mitigation response might address the risk impact by targeting linkages that determine the severity. For example, designing redundancy into a subsystem may reduce the impact that results from a failure of the original component.

.4 Acceptance. This technique indicates that the project team has decided not to change the project plan to deal with a risk or is unable to identify any other suitable response strategy. Active acceptance may include developing a contingency plan to execute, should a risk occur. Passive acceptance requires no action, leaving the project team to deal with the risks as they occur.

A *contingency plan* is applied to identified risks that arise during the project. Developing a contingency plan in advance can greatly reduce the cost of an action should the risk occur. Risk triggers, such as missing intermediate milestones, should be defined and tracked. A *fallback plan* is developed if the risk has a high impact, or if the selected strategy may not be fully effective. This might include allocation of a contingency amount, development of alternative options, or changing project scope.

The most usual risk acceptance response is to establish a *contingency allowance*, or reserve, including amounts of time, money, or resources to account for known risks. The allowance should be determined by the impacts, computed at an acceptable level of risk exposure, for the risks that have been accepted.

11.5.3 Outputs from Risk Response Development

.1 Risk response plan. The risk response plan (sometimes called the *risk register*) should be written to the level of detail at which the actions will be taken. It should include some or all of the following:

- Identified risks, their descriptions, the area(s) of the project (e.g., WBS element) affected, their cause, and how they may affect project objectives.
- Risk owners and assigned responsibilities.
- Results from the qualitative and quantitative risk analysis processes.
- Agreed responses including avoidance, transference, mitigation, or acceptance for each risk in the risk response plan.
- The level of residual risk expected to be remaining after the strategy is implemented.
- Specific actions to implement the chosen response strategy.
- Budget and times for responses.
- Contingency plans and fallback plans.

.2 Residual risks. Residual risks are those that remain after avoidance, transfer, or mitigation responses have been taken. They also include minor risks that have been accepted and addressed, e.g., by adding contingency amounts to the cost or time allowable.

.3 Secondary risks. Risks that arise as a direct result of implementing a risk response are termed *secondary risks*. These should be identified and responses planned.

.4 Contractual agreements. Contractual agreements may be entered into to specify each party's responsibility for specific risks, should they occur, and for insurance, services, and other items as appropriate to avoid or mitigate threats.

.5 Contingency reserve amounts needed. The probabilistic analysis of the project (11.4.3.2) and the risk thresholds (11.1.3.1) help the project manager determine the amount of buffer or contingency needed to reduce the risk of overruns of project objectives to a level acceptable to the organization.

.6 Inputs to other processes. Most responses to risk involve expenditure of additional time, cost, or resources and require changes to the project plan. Organizations require assurance that spending is justified for the level of risk reduction. Alternative strategies must be fed back into the appropriate processes in other knowledge areas.

.7 Inputs to a revised project plan. The results of the response planning process must be incorporated into the project plan, to ensure that agreed actions are implemented and monitored as part of the ongoing project.

[return to model](#)

← [previous page](#) ◆ [next page](#) →