8 Risk

8.1 PURPOSE

The purpose of the Risk theme is to identify, assess and control uncertainty and, as a result, improve the ability of the project to succeed.

Risk taking in projects is inevitable since projects are enablers of change and change introduces uncertainty, hence risk.

Management of risk should be systematic and not based on chance. It is about the proactive identification, assessment and control of risks that might affect the delivery of the project's objectives.

The project should establish and maintain a cost-effective risk management procedure. The aim is to support better decision making through a good understanding of risks – their causes, likelihood, impact, timing, and the choice of responses to them.

Management of risk is a continual activity, performed throughout the life of the project. Without an ongoing and effective risk management procedure it is not possible to give confidence that the project is able to meet its objectives and therefore whether it is worthwhile for it to continue. Hence effective risk management is a prerequisite of the continued business justification principle.

8.2 RISK DEFINED

8.2.1 What is a risk?

A risk is an uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives. It consists of a combination of the probability of a perceived threat or opportunity occurring, and the magnitude of its impact on objectives, where:

- **Threat** is used to describe an uncertain event that could have a negative impact on objectives
- **Opportunity** is used to describe an uncertain event that could have a favourable impact on objectives.

8.2.2 What is at risk?

In the context of a project, it is the project's objectives that are at risk. These will include completing the project to a number of targets, typically covering time, cost, quality, scope, benefits and risk.

For more information on these targets, see section 2.5.

8.2.3 What is risk management?

The term risk management refers to the systematic application of procedures to the tasks of identifying and assessing risks, and then planning and implementing risk responses. This provides a disciplined environment for proactive decision making.

For risk management to be effective, risks need to be:

- **Identified** This includes risks being considered that could affect the achievement of the project's objectives, and then described to ensure that there is a common understanding of these risks
- **Assessed** This includes ensuring that each risk can be ranked in terms of estimated likelihood, impact and immediacy, and understanding the overall level of risk associated with the project
- **Controlled** This includes identifying appropriate responses to risks, assigning risk owners, and then executing, monitoring and controlling these responses.

Risk management applies from the strategic, operational, programme and project perspectives. The approach to the management of risk can be common across all of these perspectives but risk management procedures should be tailored to suit each one. See Figure 8.1 for organizational perspectives.

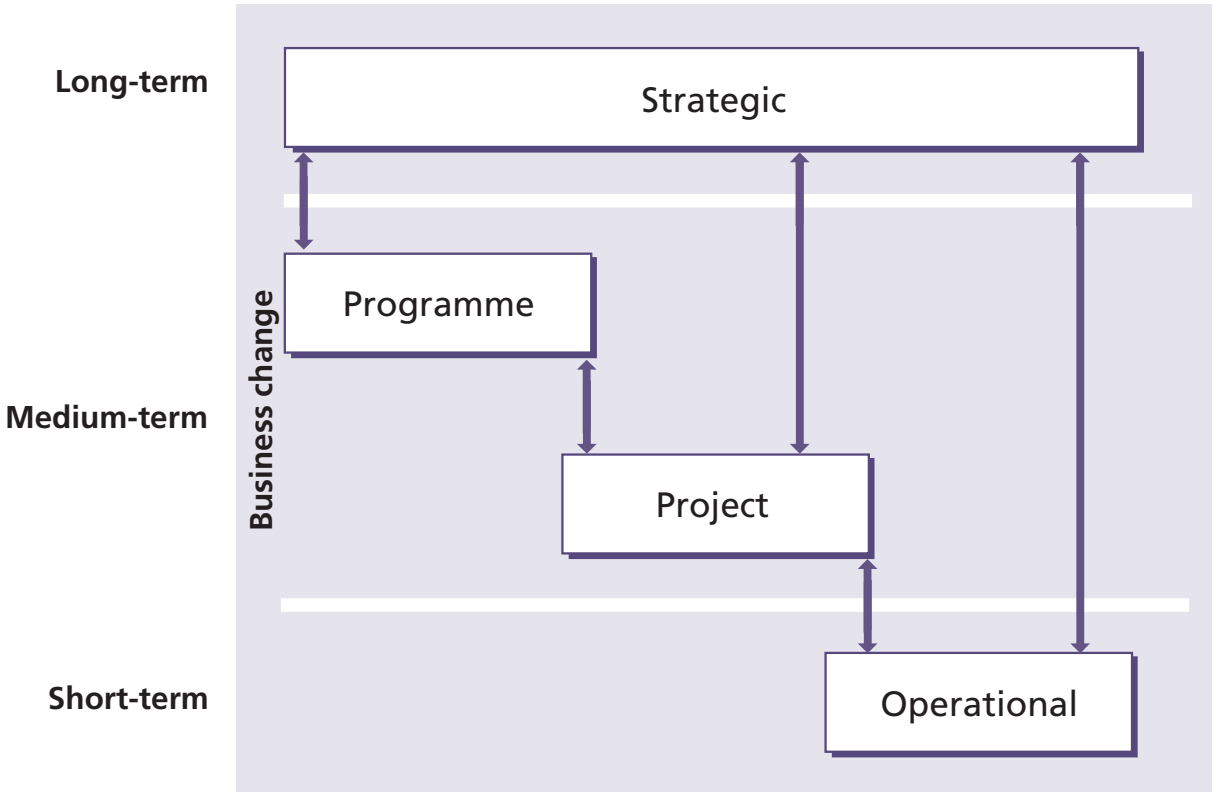

Figure 8.1 Organizational perspectives

8.3 THE PRINCE2 APPROACH TO RISK

8.3.1 Management of Risk (M_o_R®) principles

PRINCE2's approach to the management of risk is based on OGC's publication *Management of Risk: Guidance for Practitioners* (TSO, 2007). Management of risk is based on a number of risk management principles, of which the following are appropriate within a project context:

- Understand the project's context
- Involve stakeholders
- Establish clear project objectives
- Develop the project risk management approach
- Report on risks regularly
- Define clear roles and responsibilities
- Establish a support structure and a supportive culture for risk management
- Monitor for early warning indicators
- Establish a review cycle and look for continual improvement.

8.3.2 Risk management in projects

A starting point for all projects will be to identify whether there are any corporate or programme policies and processes that need to be applied. This information may be in the form of a risk management policy and/or a risk management process guide (or similar documents).

- An organization's risk management policy should communicate how risk management will be implemented throughout the organization to support the realization of its strategic objectives. This will include information such as the organization's risk appetite (an organization's unique attitude towards risk taking that in turn dictates the amount of risk that it considers acceptable), risk tolerances, procedures for escalation and defined roles and responsibilities
- An organization's risk management process guide should describe the series of steps and their respective associated activities necessary to implement risk management. This guide

should provide a best-practice approach that will support a consistent method of risk management across the organization.

Where the project forms part of the programme, the project's approach to risk management will be determined by the programme's Risk Management Strategy.

PRINCE2 recommends that every project should have its own Risk Management Strategy (defining the project procedures for risk management from identification through to implementation) and a means of control, i.e. the Risk Register.

For more information on the risk management policy and process guide documents, see OGC's *Management of Risk: Guidance for Practitioners* (TSO, 2007).

8.3.3 Risk Management Strategy

Having reviewed the organizational- and programme-level documents, and before embarking on any risk management activities, a Risk Management Strategy should be developed for the project. The purpose of this strategy is to describe how risk management will be embedded in the project management activities.

A key decision that needs to be recorded within the Risk Management Strategy is the Project Board's attitude towards risk taking, which in turn dictates the amount of risk that it considers acceptable. This information is captured in the form of risk tolerances, which represent the levels of exposure that, when exceeded, will trigger an Exception Report to bring the situation to the attention of the Project Board.

Example of risk tolerance

A large electrical retailer would not tolerate any unnecessary disruption to its support systems during the peak trading period, which extends from the middle of November through to the end of January. Projects are not permitted to introduce any changes to the support systems during this period. Therefore any risks in the Risk Register that mean the support systems would change in this peak trading window would need to be escalated to the Project Board.

See Appendix A for the Product Description of a Risk Management Strategy.

8.3.4 Risk Register

The purpose of the Risk Register is to capture and maintain information on all of the identified threats and opportunities relating to the project. Each risk on the Risk Register is allocated a unique identifier as well as details such as:

- Who raised the risk
- When it was raised
- The category of risk
- The description of the risk (cause, risk event, effect)
- Probability, impact and expected value
- Proximity
- Risk response category
- Risk response actions
- Risk status
- Risk owner
- Risk actionee.

Project Support will typically maintain the Risk Register on behalf of the Project Manager. The Risk Management Strategy will describe the procedure for registering risks and maintaining the risk register.

See Appendix A for the Product Description of a Risk Register.

8.3.5 Risk management procedure

PRINCE2 recommends a risk management procedure comprising the following five steps:

- Identify (context and risks)
- Assess (i.e. Estimate and Evaluate)
- Plan
- Implement
- Communicate.

The first four steps are sequential, with the 'Communicate' step running in parallel because the findings of any of the other steps may need to be communicated prior to the completion of the overall process. All of the steps are iterative in nature in that when additional information becomes available, it is often necessary to revisit earlier steps and carry them out again to achieve the most effective result.

Figure 8.2 shows the elements of the risk management procedure, which are described in sections 8.3.5.1–8.3.5.5.

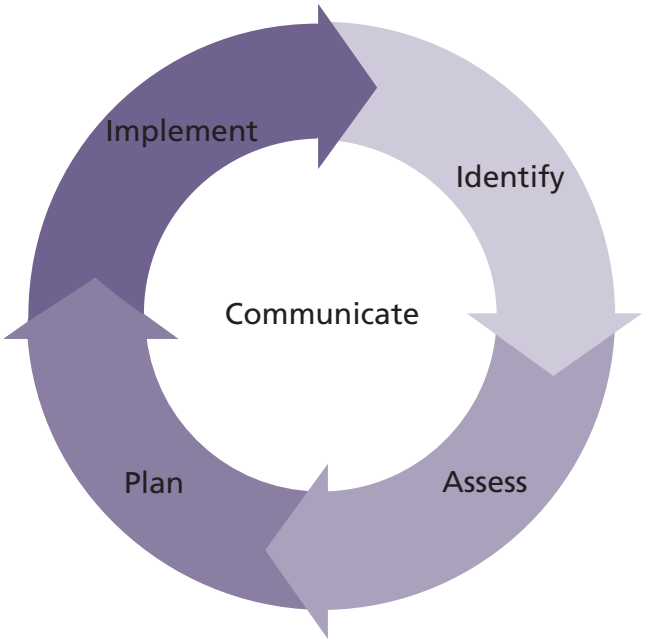

Figure 8.2 The risk management procedure

8.3.5.1 Identify

Identify context

The primary goal of the 'Identify context' step is to obtain information about the project in order to understand the specific objectives that are at risk and to formulate the Risk Management Strategy for the project. The Risk Management Strategy describes how risks will be managed during the project. It is created during the initiation stage and then reviewed and possibly updated at the end of each stage. The project's Risk Management Strategy should be based on the corporate risk management policy or on the programme's Risk Management Strategy.

The following will have an influence on the project's Risk Management Strategy:

- Customer's quality expectations
- Number of organizations involved and the relationship between them
- The needs of the stakeholders involved with the project
- The importance, complexity and scale of the project
- What assumptions have been made
- The organization's own environment (e.g. legislative or governance requirements)
- The organization's approach to risk management as described by its risk management policy.

This information will be derived from the project mandate, the Project Brief and the Project Product Description. The Risk Management Strategy will include decisions on the:

- Risk management procedure
- Tools and techniques to be used
- Records to be kept
- Risk reporting
- Timing of risk management activities
- Roles and responsibilities for the risk management procedure
- Risk scales to be used (for likelihood, impact, proximity)
- Any categorization of risks (and possibly the risk breakdown structure to use)
- Risk response categories to be used
- Early warning indicators
- Any risk tolerances
- Whether a risk budget will be established and, if so, how it will be controlled.

The early warning indicators (relevant to the project) will provide advanced warning that one or more of the project's objectives could be at risk. Early warning indicators could include progress performance data (see Chapter 10) such as:

- Percentage of Work Packages accomplished/not accomplished to schedule
- Percentage of approvals accomplished/not accomplished to schedule
- Number of issues being raised (per week/month)
- Percentage of issues that remain unresolved
- Average number of days that issues remain unresolved
- Average number of defects captured in quality inspections
- Adherence to budget (e.g. rate of spend behind or ahead of planned spend)
- Adherence to schedule (e.g. days behind or ahead of schedule).

Other early warning indicators could include non-project data such as customer satisfaction, absenteeism levels, staff attrition rates etc., if they are relevant to the project. It is also useful to analyse and report on the direction of travel of these early warning indicators (i.e. are they improving/deteriorating) as that can be of more significance than their snapshot value.

Risk identification techniques

Risks can be identified using a number of techniques, such as:

- **Review lessons** Risks are driven by uncertainty, so one of the most effective ways to reduce uncertainty is to review similar previous projects to see what threats and opportunities affected them
- **Risk checklists** These are in-house lists of risks that have either been identified or have occurred on previous similar projects. Risk checklists are useful aids to ensure that risks identified on previous projects are not overlooked
- **Risk prompt lists** These are publicly available lists that categorize risks into types or areas and are normally relevant to a wide range of projects. Risk prompt lists are useful aids to help stimulate thinking about sources of risk in the widest context
- **Brainstorming** This enables group thinking, which can be more productive than individual thinking. However, it is important to avoid criticism during the brainstorm as this can stop people contributing. In addition to identifying risks, brainstorming can also be used to understand the stakeholders' views of the risks identified
- **Risk breakdown structure** This is a hierarchical decomposition of the project environment assembled to illustrate potential sources of risk. Each descending level represents an increasingly detailed definition of sources of risk to the project. The structure acts as a prompt and an aid to support the project management team in thinking through the potential sources of risk to the objectives. There are numerous ways to break down risk and it may be useful to do more than one list. For example, a risk breakdown structure could be broken down by PESTLE (political, economical, sociological, technological, legal/legislative, environmental), product breakdown structure, stage, benefits/objectives etc. Figure 8.3 shows a risk breakdown structure relating to financial risk. These structures will help to identify appropriate risk owners to develop responses.

Identify risks

The primary goal of the 'Identify risks' step is to recognize the threats and opportunities that may affect the project's objectives.

PRINCE2 recommends the following actions:

- Capture identified threats and opportunities in the Risk Register
- Prepare early warning indicators to monitor critical aspects of the project and provide information on the potential sources of risk
- Understand the stakeholders' view of the specific risks captured.

An effective way of identifying risks is to use a risk workshop. This is a group session designed to identify threats and opportunities. The session should be facilitated by someone who is able to use a range of identification techniques, such as those listed in the boxed example. Workshops should lead to the identification of a broad range of risks and possible risk owners.

An important aspect of identifying risks is being able to provide a clear and unambiguous expression of each one. A useful way of expressing risk is to consider the following aspects of each risk:

- **Risk cause** This should describe the source of the risk, i.e. the event or situation that gives rise to the risk. These are often referred to as risk drivers. They are not risks in themselves, but the potential trigger points for risk. These may be either internal or external to the project
- **Risk event** This should describe the area of uncertainty in terms of the threat or the opportunity
- **Risk effect** This should describe the impact(s) that the risk would have on the project objectives should the risk materialize.

The cause, event and effect relationship is shown in Figure 8.4.

The cause, event and effect relationship could also be expressed in a sentence, for example:

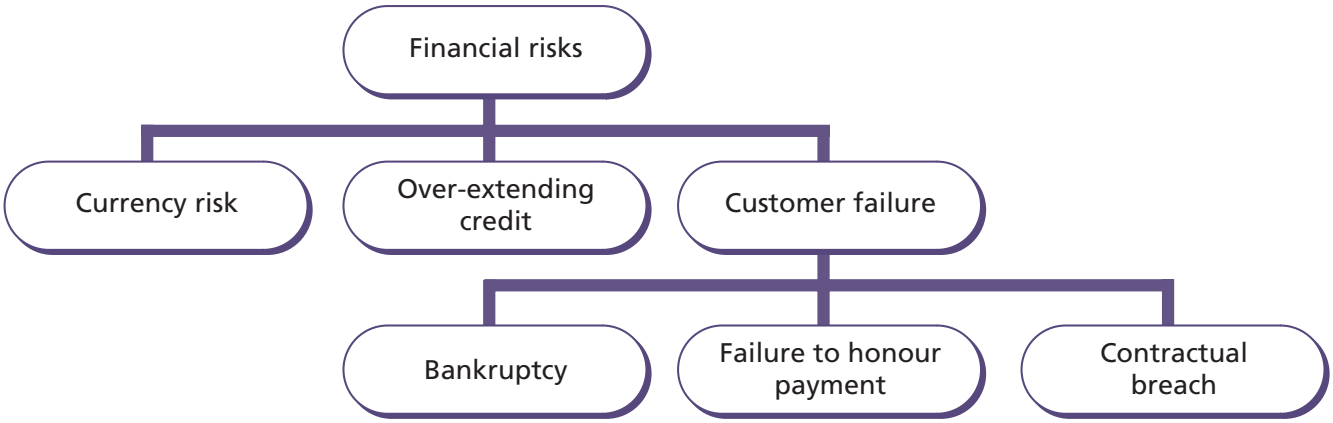

Figure 8.3 Example of a risk breakdown structure

- **Threat** Because it has been raining heavily (risk cause), there is a threat that the river flowing through the farmer's field might overflow (risk event), which would severely damage the farmer's crop (risk effect)
- **Opportunity** Because the weather has been particularly mild this winter (risk cause), there is an opportunity that fewer people will be hospitalized with influenza (risk event), which will mean that there will be less disruption to planned routine operations (risk effect).

8.3.5.2 Assess

Estimate

The primary goal of the 'Estimate' step is to assess the threats and the opportunities to the project in terms of their probability and impact. The risk proximity will also be of interest to gauge how quickly the risk is likely to materialize if no action were taken.

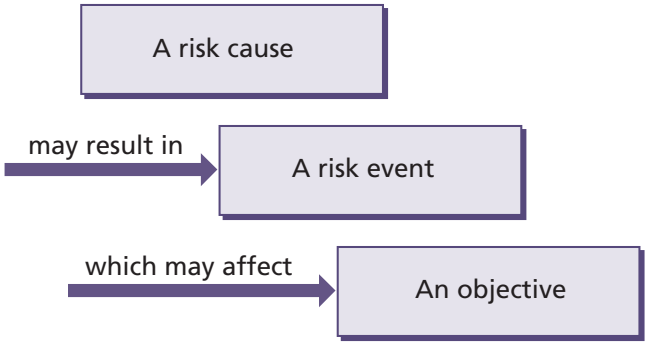

Figure 8.4 Risk cause, event and effect

Risk estimation techniques

Risks can be estimated using a number of techniques, such as:

- **Probability trees** These are graphical representations of possible events resulting from given circumstances. A probability tree can be used to predict an outcome in a qualitative way when historical data is used to populate the likelihood of each circumstance happening. Probability trees assist in communicating to project participants or decision makers the likelihood of the different possible outcomes to a set of circumstances
- **Expected value** This technique quantifies risk by combining the cost of the risk impact with the probability of the risk occurring. Expected value is useful when a tangible measure of risk is required to enable risks to be prioritized. For example, if the cost of a risk was £160,000 and its likelihood of occurrence was estimated at 25%, then the expected value would be £40,000
- **Pareto analysis** This technique ranks or orders risks once they have been assessed to determine the order in which they should be addressed. Pareto analysis can be used to focus management effort on those risks that have the potential to have the greatest impact on the project objectives
- **Probability impact grid** This grid contains ranking values that may be used to rank threats and opportunities qualitatively. The probability scales are measures of probability derived from percentages, and the impact scales are selected to reflect the level of

impact on project objectives. The values within the grid cells are the combination of a particular probability and impact, and are determined by multiplying the probability by the impact. A probability impact grid can be used to provide an assessment of the severity of a risk and enable risks to be ranked so that management time and effort can be prioritized. For example, the Project Board may set their risk tolerance at any risk with a value of greater than 0.18, and they may require a proactive response for any risk with a value of greater than 0.045, as depicted by the dark shading shown in Figure 8.5.

PRINCE2 recommends that the following is understood:

- The probability of the threats and opportunities in terms of how likely they are to occur
- The impact of each threat and opportunity in terms of the project objectives. For example, if the objectives are measured in time and cost, the impact should also be measured in units of time and cost
- The proximity of these threats and opportunities with regard to when they might materialize
- How the impact of the threats and opportunities may change over the life of the project.

A useful way of summarizing the set of risks and their estimations is to plot them onto a summary risk profile, an example of which is shown in Figure 8.6. This profile represents a situation at a specific point in time, i.e. a snapshot of the risk environment. The numbered markers in the matrix represent unique risk identifiers used in the Risk Register on which this is based. The risks above and to the right of the dotted risk tolerance line represent those that the organization will not tolerate except under special circumstances. In the depicted case, the Project Manager would refer risks 1, 3 and 4 to the Project Board.

The summary risk profile can also be used to show trends. For example, risk 6 may have previously been recorded as 'low probability, high impact', indicating that its likelihood of occurring is increasing.

Evaluate

The primary goal of the 'Evaluate' step is to assess the net effect of all the identified threats and opportunities on a project when aggregated together. This will enable an assessment to be made of the overall severity of the risks facing the project, to determine whether this level of risk is within the risk tolerance set by the Project Board and whether the project has continued business justification.

Risk evaluation techniques

Risks can be evaluated by using techniques such as:

- **Risk models** Take, for example, the Monte Carlo analysis. This model enables simulation of 'what if' scenarios using random numbers to determine whether each risk within a given range occurs or not. The simulations are repeatedly run to predict the 'average' level of risk to the project's time or cost. The scenarios can also be used to model extreme cases (e.g. if nearly all the risks occur)
- **Expected monetary value** This technique takes the expected values of a number of risks and sums them to arrive at an overall value. It provides a quick and easy assessment of a group of risks to understand their combined effect. An example is shown in Table 8.1.

Table 8.1 Example of the expected monetary value technique

Risk ID	Likelihood (%)	Impact (£)	Expected value (£)
1	60	20,000	12,000
2	30	13,000	3,900
3	10	4,000	400
4	5	10,000	500
		Expected monetary value	16,800

8.3.5.3 Plan

The primary goal of the 'Plan' step is to prepare specific management responses to the threats and opportunities identified, ideally to remove or reduce the threats and to maximize the opportunities. Attention to the Plan step ensures as far as possible that the project is not taken by surprise if a risk materializes.

Probability							
	0.9	Very high 71–90%	0.045	0.09	0.18	0.36	0.72
	0.7	High 51–70%	0.035	0.07	0.14	0.28	0.56
	0.5	Medium 31–50%	0.025	0.05	0.10	0.20	0.40
	0.3	Low 11–30%	0.015	0.03	0.06	0.12	0.24
	0.1	Very low up to 10%	0.005	0.01	0.02	0.04	0.08
			Very low	Low	Medium	High	Very high
			0.05	0.1	0.2	0.4	0.8
			Impact				

Figure 8.5 Probability impact grid

The Plan step involves identifying and evaluating a range of options for responding to threats and opportunities. It is important that the risk response is proportional to the risk and that it offers value for money. A key factor in the selection of responses will be balancing the cost of implementing the responses against the probability and impact of allowing the risk to occur. Any chosen responses should be built into the appropriate level of plan, with a provision made for any fallback plans.

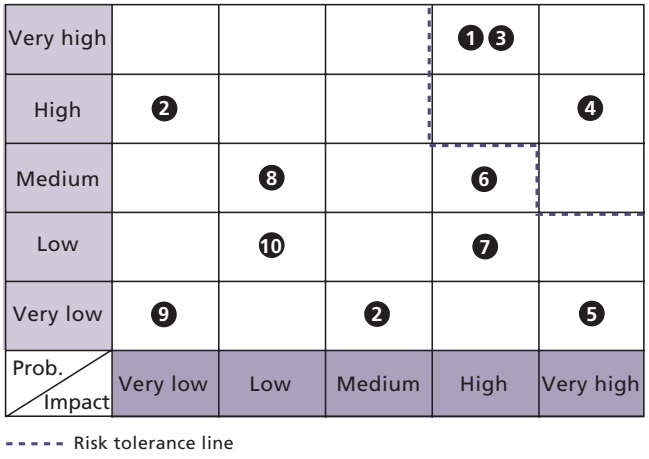

Figure 8.6 Summary risk profile

The various types of response for threats and opportunities are summarized in Figure 8.7.

The types of response are explained further in Table 8.2.

Risk responses do not necessarily remove the inherent risk in its entirety, leaving residual risk. If the inherent risk was significant and the risk response was only partially successful, the residual risk can be considerable. It may be appropriate to select more than one risk response.

In some cases, implementing a risk response will reduce or remove other related risks. It is also possible that the responses to risks, once implemented, will change some aspect of the project. This in turn may lead to secondary risks, i.e. risks that may occur as a result of invoking a risk response. It is essential that these are identified, assessed and controlled in the same way as the inherent risk.

It is advisable to review lessons from previous similar projects when planning risk responses. This will help in identifying the range of responses available and in evaluating how effective they are likely to be.

<table>
<tr><th>Threat responses</th><th>Opportunity responses</th></tr>
<tr><td>Avoid</td><td>Exploit</td></tr>
<tr><td>Reduce
(probability and/or impact)

Fallback
(reduces impact only)

Transfer
(reduces impact only, and often only the financial impact)</td><td>Enhance</td></tr>
<tr><td colspan="2">Share</td></tr>
<tr><td>Accept</td><td>Reject</td></tr>
</table>

Figure 8.7 Threat and opportunity responses

Consideration should also be given to the effect the possible responses could have on:

- The Project Plan, Stage Plan and Work Packages
- The Business Case
- Corporate and/or programme management.

8.3.5.4 Implement

The primary goal of the 'Implement' step is to ensure that the planned risk responses are actioned, their effectiveness monitored, and corrective action taken where responses do not match expectations.

An important part of the Implement step is to ensure that there are clear roles and responsibilities allocated to support the Project Manager in the management of project risks. The main roles in this respect are:

- **Risk owner** A named individual who is responsible for the management, monitoring and control of all aspects of a particular risk assigned to them, including the implementation of the selected responses to address the threats or to maximize the opportunities
- **Risk actionee** An individual assigned to carry out a risk response action or actions to respond to a particular risk or set of risks. They support and take direction from the risk owner.

Example of a risk owner and risk actionee

There is a risk that a key supplier may go bankrupt. The commercial director has been appointed as the risk owner. A number of risk responses have been identified and selected. One of the risk responses (fallback) is to identify possible alternative suppliers who have the capacity to undertake the affected Work Packages at short notice, and to obtain some quotes from them. The Procurement Manager is the risk actionee for this particular risk response.

In many cases, the risk owner and risk actionee are likely to be the same person. The risk owner should be the person most capable of managing the risk. Allocating too many risks to any one individual should be avoided.

Table 8.2 Risk responses

Response	Definition	Example
Avoid (threat)	Typically involves changing some aspect of the project, i.e. the scope, procurement route, supplier or sequence of activities, so that the threat either can no longer have an impact or can no longer happen.	A critical meeting could be threatened by air travel disruption so the project chooses to hold the meeting by conference call instead.
Reduce (threat)	Proactive actions taken to: ■ Reduce the probability of the event occurring, by performing some form of control ■ Reduce the impact of the event should it occur.	To reduce the likelihood of users not using a product, the number of training events is increased. To reduce the timescale impact should a prototype be damaged in transit, two prototypes are built.
Fallback (threat)	Putting in place a fallback plan for the actions that will be taken to reduce the impact of the threat should the risk occur. This is a reactive form of the 'reduce' response which has no impact on likelihood.	The company's test facility is only available for two weeks in August. To reduce the impact should the product not be available in time, there is a fallback plan to hire an alternate test facility (at a greater expense).
Transfer (threat)	A third party takes on responsibility for some of the financial impact of the threat. (For example, through insurance or by means of appropriate clauses in a contract.) This is a form of the 'reduce' response which only reduces the financial impact of the threat.	To reduce the financial impact should a prototype be damaged in transit, it is insured. To reduce the financial impact if a product is not available to launch in time for a trade show, the contract with the supplier includes liquidated damage clauses for any delays.
Accept (threat)	A conscious and deliberate decision is taken to retain the threat, having discerned that it is more economical to do so than to attempt a threat response action. The threat should continue to be monitored to ensure that it remains tolerable.	There is a threat that a competitor may launch a rival product first, thus affecting the expected market share for the product. The choice is to accelerate the project by increasing the resources, to reduce the product's scope so that it can be finished earlier, or to do nothing. Accelerating the project may lead to product quality issues; reducing the scope may make the product less appealing; so the risk is accepted and the 'do nothing' option is chosen.
Share (threat or opportunity)	Modern procurement methods commonly entail a form of risk sharing through the application of a pain/gain formula: both parties share the gain (within pre-agreed limits) if the cost is less than the cost plan; and share the pain (again within pre-agreed limits) if the cost plan is exceeded. Several industries include risk-sharing principles within their contracts with third parties.	The cost of the project could be adversely affected due to fluctuations in the cost of oil. The customer and supplier agree to share the cost of price increases or the savings from price reductions equally from a midpoint fixed at the time of agreeing the contract.
Exploit (opportunity)	Seizing an opportunity to ensure that the opportunity **will** happen and that the impact **will** be realized.	There is a risk that the project will be delayed. If it is delayed, a later version of software could be implemented instead which would reduce ongoing maintenance. The Project Board agree to change the project timescale and scope, enabling the later version of the software to be bought and implemented.

Enhance (opportunity)	Proactive actions taken to: ■ Enhance the probability of the event occurring ■ Enhance the impact of the event should it occur.	It is possible that the product completes user acceptance testing in a single test cycle, rather than the scheduled two, enabling it to be delivered early and prior to a competitor's rival product. The Project Board decide to hold a test rehearsal to increase the likelihood that the product will pass its first user acceptance tests, and prepare for the option of an earlier launch date.
Reject (opportunity)	A conscious and deliberate decision is taken not to exploit or enhance the opportunity, having discerned that it is more economical not to attempt an opportunity response action. The opportunity should continue to be monitored.	It is possible that the product completes user acceptance testing in a single test cycle, rather than the scheduled two, enabling it to be delivered early and prior to a competitor's rival product. The Project Board decide not to take advantage of an early release and to stick with the planned launch date.

8.3.5.5 Communicate

Communication is a step that is carried out continually. The 'Communicate' step should ensure that information related to the threats and opportunities faced by the project is communicated both within the project and externally to stakeholders. Risks are communicated as part of the following management products:

- Checkpoint Reports
- Highlight Reports
- End Stage Reports
- End Project Reports
- Lessons Reports.

Care should be taken in using these reports to communicate risks with external stakeholders and reference should be made to the Communication Management Strategy for the most appropriate method.

There are numerous other communication methods, such as bulletins, notice boards, dashboards, discussion threads, briefings etc., that could be considered alongside the PRINCE2 management products.

A number of aspects of communication should be recognized and addressed if risk management is to be effective:

- A project's exposure to risk is never static: effective communication is key to the identification of new risks or changes in existing risks. This depends on the maintenance of a good communications network, including relevant contacts and sources of information, to facilitate the identification of changes that may affect the project's overall risk exposure
- Effective risk management is dependent on participation and, in turn, participation is dependent on effective communication.

8.3.6 Risk budget

A risk budget, if used, is a sum of money included within the project budget and set aside to fund specific management responses to the project's threats and opportunities (for example, to cover the costs of any fallback plans should they need to be implemented).

In order to arrive at a risk budget for the project, a financial approach to risk management is needed. Each risk must be fully analysed for the impact costs, response costs and likelihood. The aggregation of the costs (for responses and impact) weighted by each risk's probability generates the expected monetary value for the set of risks. The expected monetary value can be used to determine a risk budget. The assumption is that the risk budget is expected to be used over the course of the project. Care needs to be taken that the aggregation of the factored costs is not skewed by a small number of large risks. This is where analytical techniques, such as Monte Carlo analysis and associated software tools, can help.

As the risk budget is part of the project budget, there may be a tendency to treat it as just another sum of money that the Project Manager can spend. This culture should be discouraged in favour of the Risk Management Strategy defining the mechanisms for control of, and access to, this budget. As the project progresses, some of the risks previously identified will occur and others will not. New risks may be identified during the life of the project whose response costs will not have been included within the risk budget. It is always prudent to set the risk budget to cover the known risks (as identified) and to make a provision for unknown risks (yet to be identified).

8.4 RESPONSIBILITIES

Table 8.3 outlines the responsibilities relevant to the Risk theme. Refer to Appendix C for further details of project management team roles and their associated responsibilities.

Table 8.3 Responsibilities relevant to the Risk theme

Role	Responsibilities
Corporate or programme management	Provide the corporate risk management policy and risk management process guide (or similar documents).
Executive	Be accountable for all aspects of risk management and, in particular, ensure a project Risk Management Strategy exists.
	Ensure that risks associated with the Business Case are identified, assessed and controlled.
	Escalate risks to corporate or programme management as necessary.
Senior User	Ensure that risks to the users are identified, assessed and controlled (such as the impact on benefits, operational use and maintenance).
Senior Supplier	Ensure that risks relating to the supplier aspects are identified, assessed and controlled (such as the creation of the project's products).
Project Manager	Create the Risk Management Strategy.
	Create and maintain the Risk Register.
	Ensure that project risks are being identified, assessed and controlled throughout the project lifecycle.
Team Manager	Participate in the identification, assessment and control of risks.
Project Assurance	Review risk management practices to ensure that they are performed in line with the project's Risk Management Strategy.
Project Support	Assist the Project Manager in maintaining the project's Risk Register.