Developing Effective Risk Responses

Dr. David Hillson, Manager of Consultancy, Project Management Professional Services Limited

Introduction

The importance of effective risk management for project success is not disputed. Considerable attention has been given to ensuring comprehensive identification and objective assessment of project risks, to provide a clear understanding of the extent of risk exposure faced by a project. Many techniques have been developed to support these stages in the risk process, which work well when used properly.

However identification and assessment will be worthless unless responses can be developed and implemented which really make a difference in addressing identified risks. Yet risk response development is perhaps the weakest part of the risk process, and it is here that many organisations fail to gain the full benefits of project risk management.

This paper presents a comprehensive approach to effective risk response development. Prerequisites are listed, together with seven key criteria for effective responses. The importance of first determining the appropriate response strategy is stressed, followed by guidelines on how to design actions to implement the chosen strategy.

The Weak Spot in the Risk Process

There is broad agreement on the required stages for an effective risk process, for example as outlined in the Project Management Institute's *"Guide to the Project Management Body of Knowledge"* (PMBOK) (PMI 1996), or the UK Association for Project Management's *"Project Risk Analysis & Management (PRAM) Guide"* (Simon et al 1997). These stages can be summarised under five headings, starting with *definition* of the objectives and scope of the risk process. This is followed by comprehensive *identification* of all risks, objective *assessment* of their significance, *planning* of appropriate responses, and *management* of those responses to achieve the required result. This process is not complex, and is simply a common-sense and structured approach to dealing with uncertainty, ensuring that proper account is taken of every foreseeable risk. The aim is to allow proactive management in advance, rather than waiting for risks to mature into problems which require a crisis response.

There are many techniques available for risk identification and assessment, and these steps are well understood. Most organisations attempting to manage their risks seem able to identify and assess them with reasonable success. The difficulty often comes when the next stage is reached **– planning** how to respond. This may however be the most important stage of the process, since the effectiveness of responses will directly determine whether risk exposure increases or decreases on the project. How can we ensure that we develop the best possible responses during the planning phase?

Prerequisites

The first consideration is whether the preceding stages of the risk process have been completed satisfactorily. This is necessary in order to provide the input required for development of risk responses. The following prerequisites should be in place before effort is spent on risk response development :

- List of identified and assessed risks, screened to ensure that only genuine risks remain, assessed for probability and impacts, and categorised by source of risk and area affected. Where time for response planning is limited, it will be helpful to prioritise the list of risks, so that available time can be spent on the most significant risks first.
- List of potential responses (if previously identified during the risk identification stage), to be reviewed and confirmed.
- List of project stakeholders, able to act as owners of risk responses.
- Agreed risk threshold for the project, to define the "acceptable" level of risk as a target for risk responses to meet.

If any of these prerequisites are missing, the effectiveness of response development is likely to be compromised. It is clearly essential to know which risks require responses. Equally important is agreement from project stakeholders that their responsibility towards the project includes a commitment to address risk within their area of influence, taking ownership of responses where necessary. Finally, the acceptability threshold is vital, to define a target against which the effectiveness of responses can be measured. Without such a target, too much effort might be spent on reducing risk below what would be acceptable, or responses might not go far enough in reducing exposure.

Proceedings of the 30th Annual Project Management Institute 1999 Seminars & Symposium
Philadelphia, Pennsylvania, USA: Papers Presented October 10 to 16, 1999

Criteria for Effective Responses

To be effective, risk responses must meet a number of important criteria. All responses must be :

1. Appropriate – the correct level of response must be determined, based on the "size" of the risk. This ranges from a crisis response where the project cannot proceed without the risk being addressed, through to a "do nothing" response for minor risks. It is important not too spend inordinate amounts of time or effort developing inappropriate responses for minor risks, but also not to spend too little time considering how to respond to key risks.

2. Affordable – the cost-effectiveness of responses must be determined, so that the amount of time, effort and money spent on addressing the risk does not exceed the available budget or the degree of risk exposure. Each risk response should have an agreed budget.

3. Actionable – an action window should be determined, defining the time within which responses need to be completed in order to address the risk. Some risks require immediate action, while others can safely be left until later.

4. Achievable – there is no point in describing responses which are not realistically achievable or feasible, either technically or within the scope of the respondent's capability and responsibility.

5. Assessed – all proposed responses must work! The effectiveness of a response is best determined by making a "post-response risk assessment" of the size of the risk assuming effective implementation of the response.

6. Agreed – the consensus and commitment of stakeholders should be obtained before agreeing responses.

7. Allocated & Accepted – each response should be owned and accepted to ensure a single point of responsibility and accountability for implementing the response.

Each proposed response should be tested against these seven criteria before it is accepted.

Having defined the characteristics of a good risk response, consideration can be given to the specifics of developing such responses. It is proposed that a two-stage approach should be followed, first defining the appropriate *strategy* for dealing with a particular risk, then designing *tactics* to implement the chosen strategy.

Strategic Response Planning

A number of alternative strategies are available when planning risk responses, which can be described under four headings:

- *Avoid* – seeking to eliminate uncertainty
- *Transfer* – seeking to transfer ownership and/or liability to a third party
- *Mitigate* – seeking to reduce the size of the risk exposure to below an acceptable threshold
- *Accept* – recognising residual risks and devising responses to control and monitor them

It is considered important to determine the appropriate strategy first, then to design responses to implement the chosen strategy. This avoids the "scatter-gun" approach, where a number of alternative responses may be proposed, some of which may negate the effect of others. Determining strategy first will ensure that responses are aiming for the same goal, and avoid nugatory effort. There is no single "best" response strategy, and each risk must be considered on its own merits. Some risks may require a combination of strategies and multiple responses, whereas others may need only one strategy with a single response.

Strategy selection should be driven by consideration of the type and nature of the risk, manageability and amenability to reduction or control, the degree of severity of impact, available resources and cost-effectiveness. It is recommended that *avoidance* strategies should be considered as the first option, since it is clearly best to remove risk completely if possible. *Transfer* should be investigated second, although the scope for this is often limited (see below). The third choice is risk *mitigation*, seeking to reduce risk exposure, leaving *acceptance* as the last resort for residual risks which cannot be addressed by any other strategy.

Having selected the appropriate strategy, attention can then be given to development of tactical responses which target individual risks and aim to realise the strategy. Specific responses for each of the four strategic options are discussed in the following sections.

Specific Risk Responses

Risk avoidance responses

The risk avoidance strategy seeks to eliminate uncertainty. This can be achieved by two types of response : direct and indirect.

Where risk arises from lack of knowledge (epistemic uncertainty), it can be tackled directly. The following actions can lead directly to elimination of uncertainty :

- clarifying requirements
- defining objectives
- obtaining information
- improving communication
- undertaking research, prototyping or development

- acquiring expertise (via training or recruitment)

An alternative avoidance response might be devised to target the cause of the risk, where this is identified. Removing the source (or breaking the causal chain) can make it impossible for the risk to occur, thus eliminating the uncertainty.

Indirect avoidance responses involve doing the project in a different way, which can also eliminate much of the uncertainty by making any impact irrelevant to the project. Examples include:

- changing the scope of the project to exclude risky elements
- adopting a familiar approach instead of an innovative one
- using proven technology and/or methodology instead of leading edge
- building redundancy into the project design

It may also be possible to "design out" certain types of risk in the early stages of a project, by making strategic project decisions, which preclude certain risky possibilities.

Risk transfer responses

The risk transfer strategy aims to pass ownership and/or liability for a particular risk to a third party. The ability to transfer liability for risk exposure seems attractive to many organisations, and many seek to use this strategy whenever possible. Its main use however is limited to financial risk exposure, since while it is possible to arrange for some other party to pay money in the event of a risk occurring, it is often difficult to enhance performance shortfalls, and it is never possible to recover lost time. It is also important to remember that risk transfer nearly always involves payment of a risk premium, and the cost must be balanced against the benefit of transferring the risk to another party.

Risk transfer can include use of insurance, where payment of a premium allows any financial penalty to be borne by the insurer, including third-party liability and professional indemnity. Performance bonds, warranties and guarantees are also financial instruments for risk transfer, as are more exotic arrangements including derivatives and hedge funds. Some organisations may consider self-insurance or use of captives (owned or rented).

An alternative group of risk transfer responses use the contract as a means to pass liability for risk. Use of a fixed price effectively transfers financial risk to the contractor, whereas a cost-plus or reimbursable contract leaves the risk with the client. Other forms of contract apportion risk in different ways, including risk-reward or risk-sharing contracts, or target-cost incentivisation arrangements.

Specific risks can be explicitly excluded from the project, and remain to be borne by the client or customer. Alternatively, liquidated damages or penalty/incentive payments pass risk to the contractor. Joint ventures, teaming or partnership arrangements can also involve explicit risk transfer among the various parties, and this is usually captured in the contractual relationship between them.

Whichever type of risk transfer mechanism is selected, it is important to pass responsibility for the risk as part of the arrangement. Risk transfer does not only shift the liability, but also involves a change in ownership of the risk. It must however be accepted that transferring the risk does not remove it, but simply gives another party responsibility for its management. It is therefore essential that recipients of transferred risks must be able to actually manage the risks allocated to them, otherwise the project will remain exposed to an uncontrolled risk.

Risk mitigation responses

The number of risks which can be addressed by avoidance or transfer responses is usually limited. This leaves mitigation or acceptance as the strategies to be used most often. The purpose of risk mitigation is to reduce the "size" of the risk exposure to below a threshold of "risk acceptability". It is clearly important to define this threshold before embarking on any mitigation, since it forms the target against which response effectiveness can be measured. Acceptable risk can be determined in terms of risk severity (High/Medium/Low), or using a probability-impact ranking system (P-I scores), or plotting regions on an iso-risk diagram or P-I Grid.

The "size" of a risk can be reduced by tackling either its probability to make it less likely, or its impact to make it less severe, or both. Preventative responses are better than curative ones, since they are more proactive, and if fully successful can lead to risk avoidance.

- Preventative responses tackle the causes of the risk, seeking to reduce the chance of the risk occurring (i.e. lower probability). If trigger conditions for a risk can be identified, these can be targeted in order to make the risk less likely. (Of course if probability is reduced to zero, then this is effectively an avoidance response.)
- Where it is not possible to reduce probability, a mitigation response might address the risk impact, targeting those impact drivers which determine the extent of the severity. Early action to protect against the worst effects of a risk can make it more acceptable.

The majority of identified risks will probably be the target of risk mitigation responses. This type of response however is very specific to the individual risk, since it addresses the particular causes of the risk and its unique effects on the project objectives. It is therefore not possible to provide a comprehensive list of mitigation response types.

Risk acceptance responses

Residual risks are those which remain after avoidance, transfer or mitigation responses have been taken. They also include those minor risks where any response is not likely to be cost-effective compared to the possible cost of bearing the risk impact. These must also be proactively managed, even if they cannot be influenced in the same way as other risks. The project must recognise and accept these risks, and adopt responses to protect against their occurrence.

The most usual risk acceptance response is contingency planning, including amounts of time, money or resource to account both for known risks and for those which are currently unknown. It is useful however to distinguish between these two types of contingency, since one relates to defined risks (known unknowns), whereas the other deals with unforeseen risks (unknown unknowns) :

- For *defined* risks, contingency should take the form of a *risk budget*, with the size determined by the impact of the risk. Risk budgets should be allocated against specific risks, with agreed release conditions defining when the contingency amount should become available for use.
- Risks which are currently *unforeseen* must be covered by "*true contingency*", which reflects the amount of residual uncertainty in the project (although this may be difficult to estimate accurately).

Other more general responses can form part of the risk acceptance strategy to protect the project or the organisation against the effects of accepted risks, including :

- development of a risk-aware culture in the project and the organisation
- incorporating risk management into routine project processes, with regular risk reviews, reports and updates
- taking account of identified risk and agreed responses in project strategy, including appropriate activities in the project plan and budget

These softer responses serve to develop a robust project culture, which can cope with the need to operate under conditions of uncertainty, and will allow residual risks to be accepted without disrupting the execution of the project.

Where risks with high potential impacts must be accepted, fallback plans should be developed, to be implemented in the case of the risk occurring (see below).

Fallback planning

For risks with potentially major impacts, it may be advisable to develop fallback plans, ready for implementation if the planned responses fail and the risk occurs. This is analogous to preparing disaster recovery plans or business continuity plans. A fallback plan should be fully defined, planned, costed and resourced. It should also have defined unambiguous trigger conditions, which determine when the risk has occurred and therefore when the fallback plan is to be implemented. The aim of a fallback plan is to minimise the impact of the risk, to prevent knock-on effects into other areas of the project, and to restore control.

Secondary Risks

Whenever a risk response is implemented it will inevitably change the risk profile of the project. Clearly the response is designed to improve the situation, but this cannot be assumed. Sometimes implementation of a response may introduce more risk into the project than it removes.

Risks that arise as a direct result of implementing a response are termed *secondary risks*. These should be identified for responses to key risks, and secondary risks should be assessed in the same way as primary risks. The project team should determine whether the risk position after implementation of a response is better or worse than it was beforehand. For example, suppose that Response R is proposed in order to address a primary risk (Risk A), with the result that the original Risk A is reduced to Risk a. However if Response R introduces a new Secondary Risk S, the project team needs to test whether $a+S<A$.

Cost-effectiveness of Risk Responses

Implementing risk responses is usually not free. Each response could involve expenditure of additional time, cost or resource. Clearly it is important that the organisation should be prepared to spend the required time, money or effort in responding to identified risks, otherwise the process will be ineffective. An important part of a risk-aware culture is the acceptance that it is better to incur definite known cost now in order to avoid the possibility of variable or unknown cost in the future. However, the organisation will require assurance that spend now is justified in order to remove exposure later. It is also important to be sure that the amount of expenditure is appropriate to the size of risk faced. For example, it would not be wise to spend $100,000 on a response to a risk whose maximum impact might be $10,000 (unless there were other impacts such as company reputation, safety or environmental implications, or "time is of the essence" considerations).

One way of measuring the cost-effectiveness of proposed responses is to convert the impact of the risk into money (including for example the cost of delay, or the cost of rectifying performance shortfalls), and then to calculate the Risk Reduction Leverage factor, as follows :

$$RRL = (\text{Cost Impact})_{\text{before response}} - (\text{Cost Impact})_{\text{after response}} \div (\text{Cost of response})$$

This gives the ratio of the improvement in risk exposure to the cost of obtaining that improvement. The larger the RRL, the more cost-effective the response. Values of RRL less than one cost more now than they might save later. As a guideline, effective responses should have values of RRL above 20. RRL can also be used to compare alternative proposed responses, allowing the most cost-effective response to be selected. Calculation of RRL is only possible however if all impacts of a risk can be converted into money, and if the "before and after" cost impacts can be estimated accurately.

Allocating Owners

Once responses have been developed, each should be assigned to an owner. This is a vital step, as the response owner will be responsible for ensuring the effective implementation of the agreed response. They will also be accountable for performing the response (or ensuring that it is performed by others). It is advisable to involve response owners in developing or refining responses which they own.

It is important to select the right owner for each risk response. This is defined as "the party best placed to manage the risk effectively". While the majority of risks may be owned by a member of the project team, any project stakeholder may be eligible to own a response. This includes other departments within the organisation (for example supplier risks may be owned by the procurement department, or resource risks by the personnel department). Some risks could be allocated to the customer or client, especially performance risks or those relating to requirement uncertainty. Others may be best placed with contractors or subcontractors who possess specialist expertise or have responsibility for particular elements of the project. The key consideration is to determine who can make a difference to the risk.

When allocating owners, it is important to build and retain co-operation and consensus, seeking to avoid contractual wrangling or the placing of blame. The necessary resources should be provided to enable the response to be implemented, and the project manager should monitor the status of risk responses regularly, not abdicating responsibility to the response owner.

Conclusion

Effective risk responses are vital if we are to make risk management work in reducing risk exposure for our projects. Following the steps outlined above will result in development of agreed responses for each risk, including an appropriate strategy (avoid, transfer, mitigate or accept) and specific responses to implement the chosen strategy. Each response will have an agreed owner, and will have been allocated sufficient resource, budget and timescale. Those responsible for the project will have identified clear actions to address their risks, with specified targets for risk reduction, and visible definition of residual risks which are being accepted. This information is vital not only for the project manager, but also for customers/clients and those responsible for the business case, creating confidence that risks are being managed effectively and that project objectives have the best chance of being achieved.

The risk management process will never deliver the promised benefits if response development is ineffective, since risks which have been identified and assessed will continue to pose a threat to the project until effective responses have been both planned and implemented. Risk management can only work if we actually do something different, putting our plans into action and building risk responses into the project. The guidelines outlined in this paper offer a framework for developing effective risk responses and maximising the benefits to be achieved through proactive risk management.

Acknowledgements

The content of this paper formed the basis for the author's contribution to the recent revision of the PMBOK chapter on Project Risk Management. Some of the concepts have been published in summary form elsewhere (Hillson 1999).

References

Simon, Peter W., Hillson, David A., Newland, Ken E. (eds.) 1997. *Project Risk Analysis & Management (PRAM) Guide*. High Wycombe, Bucks HP11 2DX, UK : Association for Project Management. ISBN 0.9531590.0.0

PMI 1996. *A Guide to the Project Management Body of Knowledge*. Upper Darby, PA 19082, USA : Project Management Institute. ISBN 1.880410.12.5

Hillson, David A. 1999. Take no risks with risk. *Project* magazine (Association for Project Management), Volume 12 Issue 1 (May) : 14-16. ISSN 0957-7033.