Chapter 1

Why do a risk analysis?

In business and government one faces having to make decisions all the time where the outcome is uncertain. Understanding the uncertainty can help us make a much better decision. Imagine that you are a national healthcare provider considering which of two vaccines to purchase. The two vaccines have the same reported level of efficacy (67%), but further study reveals that there is a difference in confidence attached to these two performance measures: one is twice as uncertain as the other (see Figure 1.1).

All else being equal, the healthcare provider would purchase the vaccine with the smallest uncertainty about its performance (vaccine A). Replace vaccine with investment and efficacy with profit and we have a problem in business, for which the answer is the same—pick the investment with the smallest uncertainty, all else being equal (investment A). The principal problem is determining that uncertainty, which is the central focus of this book.

We can think of two forms of uncertainty that we have to deal with in risk analysis. The first is a general sense that the quantity we are trying to estimate has some uncertainty attached to it. This is usually described by a distribution like the ones in Figure 1.1. Then we have risk events, which are random events that may or may not occur and for which there is some impact of interest to us. We can distinguish between two types of event:

- A risk is a random event that may possibly occur and, if it did occur, would have a negative impact on the goals of the organisation. Thus, a risk is composed of three elements: the scenario; its probability of occurrence; and the size of its impact if it did occur (either a fixed value or a distribution).
- An opportunity is also a random event that may possibly occur but, if it did occur, would have a positive impact on the goals of the organisation. Thus, an opportunity is composed of the same three elements as a risk.

A risk and an opportunity can be considered the opposite sides of the same coin. It is usually easiest to consider a potential event to be a risk if it would have a negative impact and its probability is less than 50%, and, if the risk has a probability in excess of 50%, to include it in a base plan and then consider the opportunity of it not occurring.

1.1 Moving on from “What If” Scenarios

Single-point or deterministic modelling involves using a single “best-guess” estimate of each variable within a model to determine the model’s outcome(s). Sensitivities are then performed on the model to determine how much that outcome might in reality vary from the model outcome. This is achieved by selecting various combinations for each input variable. These various combinations of possible values
around the “best guess” are commonly known as “what if” scenarios. The model is often also “stressed” by putting in values that represent worst-case scenarios.

Consider a simple problem that is just the sum of five cost items. We can use the three points, minimum, best guess and maximum, as values to use in a “what if” analysis. Since there are five cost items and three values per item, there are $3^5 = 243$ possible “what if” combinations we could produce. Clearly, this is too large a set of scenarios to have any practical use. This process suffers from two other important drawbacks: only three values are being used for each variable, where they could, in fact, take any number of values; and no recognition is being given to the fact that the best-guess value is much more likely to occur than the minimum and maximum values. We can stress the model by adding up the minimum costs to find the best-case scenario, and add up the maximum costs to get the worst-case scenario, but in doing so the range is usually unrealistically large and offers no real insight. The exception is when the worst-case scenario is still acceptable.

Quantitative risk analysis (QRA) using Monte Carlo simulation (the dominant modelling technique in this book) is similar to “what if” scenarios in that it generates a number of possible scenarios. However, it goes one step further by effectively accounting for every possible value that each variable could take and weighting each possible scenario by the probability of its occurrence. QRA achieves this by modelling each variable within a model by a probability distribution. The structure of a QRA model is usually (there are some important exceptions) very similar to a deterministic model, with all the multiplications, additions, etc., that link the variables together, except that each variable is represented by a probability distribution function instead of a single value. The objective of a QRA is to calculate the combined impact of the uncertainty in the model’s parameters in order to determine an uncertainty distribution of the possible model outcomes.

---

1 I discuss the exact meaning of “uncertainty”, randomness, etc., in Chapter 4.
Chapter 1 Why do a risk analysis?

1.2 The Risk Analysis Process

Figure 1.2 shows a typical flow of activities in a risk analysis, leading from problem formulation to decision. This section and those that follow provide more detail on each activity.

1.2.1 Identifying the risks

Risk identification is the first step in a complete risk analysis, given that the objectives of the decision-maker have been well defined. There are a number of techniques used to help formalise the identification of risks. This part of a formal risk analysis will often prove to be the most informative and constructive element of the whole process, improving company culture by encouraging greater team effort and reducing blame, and should be executed with care. The organisations participating in a formal risk analysis should take pains to create an open and blameless environment in which expressions of concern and doubt can be openly given.

![Risk Management approach diagram]

Figure 1.2 The risk analysis process.
Prompt lists

Prompt lists provide a set of categories of risk that are pertinent to the type of project under consideration or the type of risk being considered by an organisation. The lists are used to help people think about and identify risks. Sometimes different types of list are used together to improve further the chance of identifying all of the important risks that may occur. For example, in analysing the risks to some project, one prompt list might look at various aspects of the project (e.g. legal, commercial, technical, etc.) or types of task involved in the project (design, construction, testing). A project plan and a work breakdown structure, with all of the major tasks defined, are natural prompt lists. In analysing the reliability of some manufacturing plant, a list of different types of failure (mechanical, electrical, electronic, human, etc.) or a list of the machines or processes involved could be used. One could also cross-check with a plan of the site or a flow diagram of the manufacturing process. Check lists can be used at the same time: these are a series of questions one asks as a result of experience of previous problems or opportune events.

A prompt list will never be exhaustive but acts as a focus of attention in the identification of risks. Whether a risk falls into one category or another is not important, only that the risk is identified. The following list provides an example of a fairly general project prompt list. There will often be a number of subsections for each category:

- administration;
- project acceptance;
- commercial;
- communication;
- environmental;
- financial;
- knowledge and information;
- legal;
- management;
- partner;
- political;
- quality;
- resources;
- strategic;
- subcontractor;
- technical.

The identified risks can then be stored in a risk register described in Section 1.6.

1.2.2 Modelling the risk problem and making appropriate decisions

This book is concerned with the modelling of identified risks and how to make decisions from those models. In this book I try not to offer too many modelling rules. Instead, I have focused on techniques that I hope readers will be able to put together as necessary to produce a good model of their problem. However, there are a few basic principles that are worth adhering to. Morgan and Henrion (1990) offer the following excellent “ten commandments” in relation to quantitative risk and policy analysis:
1. Do your homework with literature, experts and users.
2. Let the problem drive the analysis.
3. Make the analysis as simple as possible, but no simpler.
4. Identify all significant assumptions.
5. Be explicit about decision criteria and policy strategies.
6. Be explicit about uncertainties.
7. Perform systematic sensitivity and uncertainty analysis.
8. Iteratively refine the problem statement and the analysis.
10. Expose to peer review.

The responses to correctly identified and evaluated risks are many, but generally fall into the following categories:

- Increase (the project plan may be overly cautious).
- Do nothing (because it would cost too much or there is nothing that can be done).
- Collect more data (to better understand the risk).
- Add a contingency (extra amount to budget, deadline, etc., to allow for possibility of risk).
- Reduce (e.g. build in redundancy, take a less risky approach).
- Share (e.g. with partner, contractor, providing they can reasonably handle the impact).
- Transfer (e.g. insure, back-to-back contract).
- Eliminate (e.g. do it another way).
- Cancel project.

This list can be helpful in thinking of possible responses to identified risks. It should be borne in mind that these risk responses might in turn carry secondary risks. Fall-back plans should be developed to deal with risks that are identified and not eliminated. If done well in advance, they can help the organisation react efficiently, calmly and in unison in a situation where blame and havoc might normally reign.

### 1.3 Risk Management Options

The purpose of risk analysis is to help managers better understand the risks (and opportunities) they face and to evaluate the options available for their control. In general, risk management options can be divided into several groups.

**Acceptance (Do nothing)**

Nothing is done to control the risk or one’s exposure to that risk. Appropriate for risks where the cost of control is out of proportion with the risk. It is usually appropriate for low-probability, low-impact risks and opportunities, of which one normally has a vast list, but you may be missing some high-value risk mitigation or avoidance options, especially where they control several risks at once. If the chosen response is acceptance, some considerable thought should be given to risk contingency planning.
Increase

You may find that you are already spending considerable resources to manage a risk that is excessive compared with the level of protection that it affords you. In such cases, it is logical to reduce the level of protection and allocate the resources to manage other risks, thereby achieving a superior overall risk efficiency. Examples are:

- remove a costly safety regulation for nuclear power plants that affects a risk that would otherwise still be miniscule;
- cease the requirement to test all slaughtered cows for BSE and use saved money for hospital upgrades.

It may be logical but nonetheless politically unacceptable. There are not too many politicians or CEOs who want to explain to the public that they’ve just authorised less caution in handling a risk.

Get more information

A risk analysis can describe the level of uncertainty there is about the decision problem (here we use uncertainty as distinct from inherent randomness). Uncertainty can often be reduced by acquiring more information (whereas randomness cannot). Thus, a decision-maker can determine that there is too much uncertainty to make a robust decision and request that more information be collected. Using a risk analysis model, the risk analyst can advise the least-cost method of collecting extra data that would be needed to achieve the required level of precision. Value-of-information arguments (see Section 5.4.5) can be used to assess how much, if any, extra information should be collected.

Avoidance (Elimination)

This involves changing a method of operation, a project plan, an investment strategy, etc., so that the identified risk is no longer relevant. Avoidance is usually employed for high-probability, high-impact type risks. Examples are:

- use a tried and tested technology instead of the new one that was originally envisaged;
- change the country location of a factory to avoid political instability;
- scrap the project altogether.

Note that there may be a very real chance of introducing new (and perhaps much more important) risks by changing your plans.

Reduction (Mitigation)

Reduction involves a range of techniques, which may be used together, to reduce the probability of the risk, its impact or both. Examples are:

- build in redundancy (standby equipment, back-up computer at different location);
- perform more quality tests or inspections;
- provide better training to personnel;
- spread risk over several areas (portfolio effect).

Reduction strategies are used for any level of risk where the remaining risk is not of very high severity (very high probability and impact) and where the benefits (amount by which risk is reduced) outweigh the reduction costs.
Contingency planning

These are plans devised to optimise the response to risks should they occur. They can be used in conjunction with acceptance and reduction strategies. A contingency plan should identify individuals who take responsibility for monitoring the occurrence of the risk, and/or identified risk drivers for changes in the risk’s probability or possible impact. The plan should identify what to do, who should do it and in which order, the window of opportunity, etc. Examples are:

- have a trained firefighting team on site;
- have a preprepared press release;
- have a visible phone list (or email distribution list) of whom to contact if the risk occurs;
- reduce police and emergency service leave during a strike;
- fit lifeboats on ships.

Risk reserve

Management’s response to an identified risk is to add some reserve (buffer) to cover the risk should it occur. Appropriate for small to medium impact risks. Examples are:

- allocate extra funds to a project;
- allocate extra time to complete a project;
- have cash reserves;
- have extra stock in shops for a holiday weekend;
- stockpile medical and food supplies.

Insurance

Essentially, this is a risk reduction strategy, but it is so common that it is worth mentioning separately. If an insurance company has done its numbers correctly, in a competitive market you will pay a little above the expected cost of the risk (i.e. probability $\times$ expected impact should the risk occur). In general, we therefore insure for risks that have an impact outside our comfort zone (i.e. where we value the risk higher than its expected value). Alternatively, you may feel that your exposure is higher than the average policy purchaser, in which case insurance may be under your expected cost and therefore extremely attractive.

Risk transfer

This involves manipulating the problem so that the risk is transferred from one party to another. A common method of transferring risk is through contracts, where some form of penalty is included into a contractor’s performance. The idea is appealing and used often but can be very inefficient. Examples are:

- penalty clause for running over agreed schedule;
- performance guarantee of product;
- lease a maintained building from the builder instead of purchasing;
- purchase an advertising campaign from some media body or advertising agency with payment contingent on some agreed measure of success.
You can also consider transferring risks to you, where there is some advantage to relieving another
party of a risk. For example, if you can guarantee a second party against some small risk resultant from
an activity you wish to take that provides you with much greater benefit than the other party’s risk, the
second party may remove its objection to your proposed activity.

1.4 Evaluating Risk Management Options

The manager evaluating the possible options for dealing with a defined risk issue needs to consider
many things:

- Is the risk assessment of sufficient quality to be relied upon?
- How sensitive is the ranking of each option to model uncertainties?
- What are the benefits relative to the costs associated with each risk management option?
- Are there any secondary risks associated with a chosen risk management option?
- How practical will it be to execute the risk management option?
- Is the risk assessment of sufficient quality to be relied upon? (See Chapter 3.)
- How sensitive is the ranking of each option to model uncertainties?

On this last point, we almost always would like to have better data, or greater certainty about the
form of the problem: we would like the distribution of what will happen in the future to be as narrow
as possible. However, a decision-maker cannot wait indefinitely for better data and, from a decision-
analytic point of view, may quickly reach the point where the best option has been determined and no

![Figure 1.3](image)

**Figure 1.3** Different possible outputs compared with a threshold T.
further data (or perhaps only a very dramatic change in knowledge of the problem) will make another option preferable. This concept is known as decision sensitivity. For example, in Figure 1.3 the decision-maker considers any output below a threshold T (shown with a dashed line) to be perfectly acceptable (perhaps this is a regulatory threshold or a budget). The decision-maker would consider option A to be completely unacceptable and option C to be perfectly fine, and would only need more information about option B to be sure whether it was acceptable or not, in spite of all three having considerable uncertainty.

1.5 Inefficiencies in Transferring Risks to Others

A common method of managing risks is to force or persuade another party to accept the risk on your behalf. For example, an oil company could require that a subcontractor welding a pipeline accept the costs to the oil company resulting from any delays they incur or any poor workmanship. The welding company will, in all likelihood, be far smaller than the oil company, so possible penalty payments would be catastrophic. The welding company will therefore value the risk as very high and will require a premium greatly in excess of the expected value of the risk. On the other hand, the oil company may be able to absorb the risk impact relatively easily, so would not value the risk as highly. The difference in the utility of these two companies is shown in Figures 1.4 to 1.7, which demonstrate that the oil company will pay an excessive amount to eliminate the risk.

A far more realistic approach to sharing risks is through a partnership arrangement. A list of risks that may impact on various parties involved in the project is drawn up, and for each risk one then asks:

- How big is the risk?
- What are the risk drivers?
- Who is in control of the risk drivers? Who has the experience to control them?
- Who could absorb the risk impacts?
- How can we work together to manage the risks?

![Utility gain](image)

Figure 1.4 The contractor’s utility function is highly concave over the money gain/loss range in question. That means, for example, that the contractor would value a loss of 100 units of money (e.g. $100 000) as a vastly larger loss in absolute utility terms than a gain of $100 000 might be.
Figure 1.5 Over that same money gain/loss range, the oil company has an almost exactly linear utility function. The contractor, required to take on a risk with an expected value of $-60,000, would value this as $-X$ utiles. To compensate, the contractor would have to charge an additional amount well in excess of $100,000. The oil company, on the other hand, would value $-60,000 in rough balance with $+60,000, so will be paying considerably in excess of its valuation of the risk to transfer it to the contractor.

Figure 1.6 Imagine the risk has a 10% probability of occurring, and its impact would be $-300,000, to give an expected value of $-30,000. If $300,000 is the total capital value of the contractor, it won’t much matter to the contractor whether the risk impact is $300,000 or $3,000,000 – they still go bust. This is shown by the shortened utility curve and the horizontal dashed line for the contractor.

- What arrangement would efficiently allocate the risk impacts and rewards for good risk management?
- Can we insure, etc., to share risks with outsiders?

The more one can allocate ownership of risks, and opportunities, to those who control them the better – up to the point where the owner could not reasonably bear the risk impact where others can. Answering the questions above will help you construct a contractual arrangement that is risk efficient, workable and tolerable to all parties.
Chapter 1 Why do a risk analysis?

Figure 1.7 In this situation, the contractor now values any risk with an impact that exceeds its capital value at a level that is less than the oil company (shown as “Discrepancy”). It may mean that the contractor can offer a more competitive bid than another, larger contractor who would feel the full risk impact, but the oil company will not have covered the risk it had hoped to transfer, and so again will be paying more than it should to offload the risk. Of course, one way to avoid this problem is to require evidence from the contractor that they have the necessary insurance or capital base to cover the risk they are being asked to absorb.

1.6 Risk Registers

A risk register is a document or database that lists each risk pertaining to a project or organisation, along with a variety of information that is useful for the management of those risks. The risks listed in a risk register will have come from some collective exercise to identify risks. The following items are essential in any risk register entry:

- date the register was last modified;
- name of risk;
- description of what the risk is;
- description of why it would occur;
- description of factors that would increase or decrease its probability of occurrence or size of impact (risk drivers);
- semi-quantitative estimates of its probability and potential impact;
- \( P-I \) scores;
- name of owner of the risk (the person who will assume responsibility for monitoring the risk and effecting any risk reduction strategies that have been agreed);
- details of risk reduction strategies that it is agreed will be taken (i.e. strategy that will reduce the impact on the project should the risk event occur and/or the probability of its occurrence);
- reduced impact and/or probability of the risk, given the above agreed risk reduction strategies have been taken;
- ranking of risk by scores of the reduced $P - I$;
- cross-referencing the risk event to identification numbers of tasks in a project plan or areas of operation or regulation where the risk may impact;
- description of secondary risks that may arise as a result of adopting the risk reduction strategies;
- action window – the period during which risk reduction strategies must be put in place.

The following items may also be useful to include:

- description of other optional risk reduction strategies;
- ranking of risks by the possible effectiveness of further risk mitigation \[\text{effectiveness} = \frac{\text{total decrease in risk}}{\text{cost of risk mitigation action}}\];
- fall-back plan in the event the risk event still occurs;
- name of the person who first identified the risk;
- date the risk was first identified;
- date the risk was removed from the list of active risks (if appropriate).

A risk register should include a description of the scale used in the semi-quantitative analysis, as explained in the section on $P - I$ scores. A risk register should also have a summary that lists the top risks (ten is a fairly usual number but will vary according to the project or overview level). The “top” risks are those that have the highest combination of probability and impact (i.e. severity), after the reducing effects of any agreed risk reduction strategies have been included. Risk registers lend themselves perfectly to being stored in a networked database. In this way, risks from each project or regulatory body’s concerns, for example, can be added to a common database. Then, a project manager can access that database to look at all risks to his or her project. The finance director, lawyer, etc., can look at all the risks from any project being managed by their departments and the chief executive can look at the major risks to the organisation as a whole. What is more, head office has an easy means for assessing the threat posed by a risk that may impact on several projects or areas at the same time. “Dashboard” software can bring the outputs of a risk register into appropriate focus for the decision-makers.

1.6.1 $P - I$ tables

The risk identification stage attempts to identify all risks threatening the achievement of the project’s or organisation’s goals. It is clearly important, however, that attention is focused on those risks that pose the greatest threat.

Defining qualitative risk descriptions

A qualitative assessment of the probability $P$ of a risk event (a possible event that would produce a negative impact on the project or organisation) and the impact(s) it would produce, $I$, can be made by assigning descriptions to the magnitudes of these probabilities and impacts. The assessor is asked to describe the probability and impact of each risk, selecting from a predetermined set of phrases such as: nil, very low, low, medium, high and very high. A range of values is assigned to each phrase in order to maintain consistency between the estimates of each risk. An example of the value range that might be given to each phrase in a risk register for a particular project is shown in Table 1.1.

Note that in Table 1.1 the value ranges are not evenly spaced. Ideally there is a multiple difference between each range (in this case roughly 3). If the same multiple is applied for probability and impact
Table 1.1  An example of the value ranges that could be associated with qualitative descriptions of the probabilities and impacts of a risk on a project.

<table>
<thead>
<tr>
<th>Category</th>
<th>Probability (%)</th>
<th>Delay (days)</th>
<th>Cost ($k)</th>
<th>Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>10–50</td>
<td>&gt;100</td>
<td>&gt;1000</td>
<td>Failure to meet acceptance criteria</td>
</tr>
<tr>
<td>High</td>
<td>5–10</td>
<td>30–100</td>
<td>30–100</td>
<td>Failure to meet &gt; 1 important specification</td>
</tr>
<tr>
<td>Medium</td>
<td>2–5</td>
<td>10–30</td>
<td>100–300</td>
<td>Failure to meet an important specification</td>
</tr>
<tr>
<td>Low</td>
<td>1–2</td>
<td>2–10</td>
<td>20–100</td>
<td>Failure to meet &gt; 1 minor specification</td>
</tr>
<tr>
<td>Very low</td>
<td>&lt;1</td>
<td>&lt;2</td>
<td>&lt;20</td>
<td>Failure to meet a minor specification</td>
</tr>
</tbody>
</table>

Table 1.2  An example of the descriptions that could be associated with impacts of a risk on a corporation.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Jeopardises the existence of the company</td>
</tr>
<tr>
<td>Major</td>
<td>No longer possible to achieve business objectives</td>
</tr>
<tr>
<td>Moderate</td>
<td>Reduced ability to achieve business objectives</td>
</tr>
<tr>
<td>Minor</td>
<td>Some business disruptions but little effect on business objectives</td>
</tr>
<tr>
<td>Insignificant</td>
<td>No impact on business strategy objectives</td>
</tr>
</tbody>
</table>

scales, we can more easily determine severity scores as described below. The value ranges can be selected to match the size of the project. Alternatively, they can be matched to the effect the risks would have on the organisation as a whole. The drawback in making the definition of each phrase specific to a project is that it becomes very difficult to perform a combined analysis of the risks from all projects in which the organisation is involved. From a corporate perspective one can describe how a risk affects the health of a company, as shown in Table 1.2.

Visualising a portfolio of risks

A $P-I$ table offers a quick way to visualise the relative importance of all identified risks that pertain to a project (or organisation). Table 1.3 illustrates an example. All risks are plotted on the one table, allowing easy identification of the most threatening risks as well as providing a general picture of the overall riskiness of the project. Risk numbers 13, 2, 12 and 15 are the most threatening in this example.

The impact of a project risk that is most commonly considered is a delay in the scheduled completion of the project. However, an analysis may also consider the increased cost of the project resulting from

Table 1.3  Example of a $P-I$ table for schedule delay.

<table>
<thead>
<tr>
<th>Impact</th>
<th>Profit impact for identified risks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V High</td>
</tr>
<tr>
<td></td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Med</td>
</tr>
<tr>
<td></td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>V Low</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>V Low</th>
<th>Low</th>
<th>Med</th>
<th>High</th>
<th>V High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
each risk. It might further consider other, less numerically definable impacts on the project, for example: the quality of the final product; the goodwill that could be lost; sociological impacts; political damage; or strategic importance of the project to the organisation. A $P−I$ table can be constructed for each type of impact, enabling the decision-maker to gain a more rounded understanding of a project’s riskiness.

$P−I$ tables can be constructed for the various types of impact of each single risk. Table 1.4 illustrates an example where the impacts of schedule delay, $T$, cost, $\$, and product quality, $Q$, are shown for a specific risk. The probability of each impact may not be the same. In this example, the probability of the risk event occurring is high, and hence the probability of schedule delay and cost impacts are high, but it is considered that, even if this risk event does occur, the probability of a quality impact is still low. In other words, there is a fairly small probability of a quality impact even when the risk event does occur.

### Ranking risks

$P−I$ scores can be used to rank the identified risks. A scaling factor, or weighting, is assigned to each phrase used to describe each type of impact. Table 1.5 provides an example of the type of scaling factors that could be associated with each phrase/impact type combination.

In this type of scoring system, the higher the score, the greater is the risk. A base measure of risk is probability * impact. The categorising system in Table 1.1 is on a log scale, so, to make Table 1.5 consistent, we can define the severity of a risk with a single type of impact as

$$S = P + I$$

which leaves the severity on a log scale too. If a risk has $k$ possible types of impact (quality, delay, cost, reputation, environmental, etc.), perhaps with different probabilities for each impact type, we can

### Table 1.4

$P−I$ table for a specific risk.

<table>
<thead>
<tr>
<th>Impact for Risk # 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
</tr>
<tr>
<td>V High</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Med</td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>V Low</td>
</tr>
<tr>
<td>V Low</td>
</tr>
</tbody>
</table>

| Probability |

### Table 1.5

An example of the scores that could be associated with descriptive risk categories to produce a severity score.

<table>
<thead>
<tr>
<th>Category</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
</tr>
<tr>
<td>Low</td>
<td>2</td>
</tr>
<tr>
<td>Very low</td>
<td>1</td>
</tr>
</tbody>
</table>
Table 1.6 Segregation of risks into levels of severity.

<table>
<thead>
<tr>
<th>Impact</th>
<th>V High</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>V Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability</td>
<td>6 7 8 9 10</td>
<td>5 6 7 8 9</td>
<td>4 5 6 7 8</td>
<td>3 4 5 6 7</td>
<td>2 3 4 5 6</td>
</tr>
<tr>
<td>V Low</td>
<td>Low</td>
<td>Med</td>
<td>High</td>
<td>V High</td>
<td></td>
</tr>
</tbody>
</table>

still combine them into one score as follows:

$$S = \log_{10} \left[ \sum_{i=1}^{k} 10^{P_i + I_i} \right]$$

The severity scores are then used to determine the most important risks, enabling the management to focus resources on reducing or eliminating risks from the project in a rational and efficient manner. A drawback to this approach of ranking risks is that the process is quite dependent on the granularity of the scaling factors that are assigned to each phrase describing the risk impacts. If we have better information on probability or impact than the scoring system would allow, we can assign a more accurate (non-integer) score.

In the scoring regime of Table 1.5, for example, a high severe risk could be defined as having a score higher than 7, and a low risk as having a score lower than 5. Given the crude scaling used, risks with a severity of 7 may require further investigation to determine whether they should be categorised as high severity. Table 1.6 shows how this segregates the risks shown in a $P-I$ table into the three regions.

$P-I$ scores for a project provide a consistent measure of risk that can be used to define metrics and perform trend analyses. For example, the distribution of severity scores for a project gives an indication of the overall “amount” of risk exposure. More complex metrics can be derived using severity scores, allowing risk exposure to be normalised and compared with a baseline status. These permit trends in risk exposure to be identified and monitored, giving valuable information to those responsible for controlling the project.

Efficient risk management with severity scores

Efficient risk management seeks to achieve the maximum reduction in risk for a given amount of investment (of people, time, money, restriction of liberty, etc.). Thus, we need to evaluate in some sense the ratio (reduction in risk)/(investment to achieve reduction). If you use the log scale for severity described here, this would equate to calculating

$$\text{Efficiency} = \left( \sum_i 10^{S_{\text{new}}(i)} - \sum_i 10^{S_{\text{old}}(i)} \right) / \text{investment}$$
The risk management options that provide the greatest efficiency should logically be preferred, all else being equal.

**Inherent risks** are the risk estimates before accounting for any mitigation efforts. They can be plotted against a guiding risk response framework where the $P–I$ table is split, covered by overlapping areas of avoid, control, transfer and accept, as shown in Figure 1.8:

- “Avoid” applies where an organisation would be accepting a high-probability, high-impact risk without any compensating benefits.
- “Control” applies usually to high-probability, low-impact risks, normally associated with repetitive actions, and therefore usually managed through better internal processes.
- “Transfer” applies to low-probability, high-impact risks usually managed through insurance or other means of transferring the risk to parties better capable of absorbing the impact.
- “Accept” applies to the remaining low-probability, low-impact risks for which it may not be effective to focus on too much.

Figure 1.9 plots residual risks after any implemented risk mitigation strategies and tracks the progress in managing the residual risks compared with the previous year using arrows. Grey letters represent the status of the risk last year if it is different. A dashed arrow pointing out of the graph means that the risk

![Figure 1.8](image-url) **Figure 1.8** $P–I$ graph for inherent risks.
has been avoided. An enhancement to the residual risk graph that you might like to add is to plot each risk as a circle whose radius reflects how comfortable you are in dealing with the residual risk – for example, perhaps you have handled the occurrence of similar risks before and minimised their impact through good management, or perhaps they got out of hand. A small circle represents risks that one is comfortable managing, and a large circle represents the opposite, so the less manageable risks stand out in the plot.

Figure 1.9  $P-I$ graph for residual risks.