

An excerpt from:

RISK ANALYSIS: A QUANTITATIVE GUIDE 3RD EDITION

BY DAVID VOSE

©David Vose. No reproduction of any part is permitted without written permission of the author.

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 measure: one is twice as uncertain as the other (see Figure 1.1).

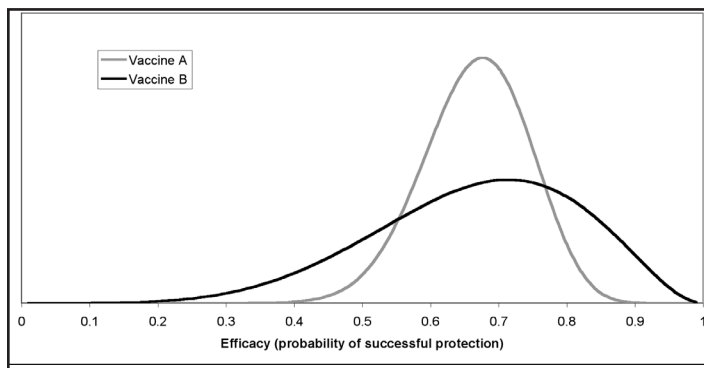


Figure 1.1 Efficacy comparison for two vaccines: the vertical axis represents how confident we are about the true level of efficacy. I've omitted the scale to avoid some confusion at this stage (see Section III.1.2)

All else being equal, the healthcare provider would purchase the vaccine with the smallest uncertainty about its performance (vaccine A). Replace vaccine by investment and efficacy by 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 events:

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 had 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.

1.2 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.

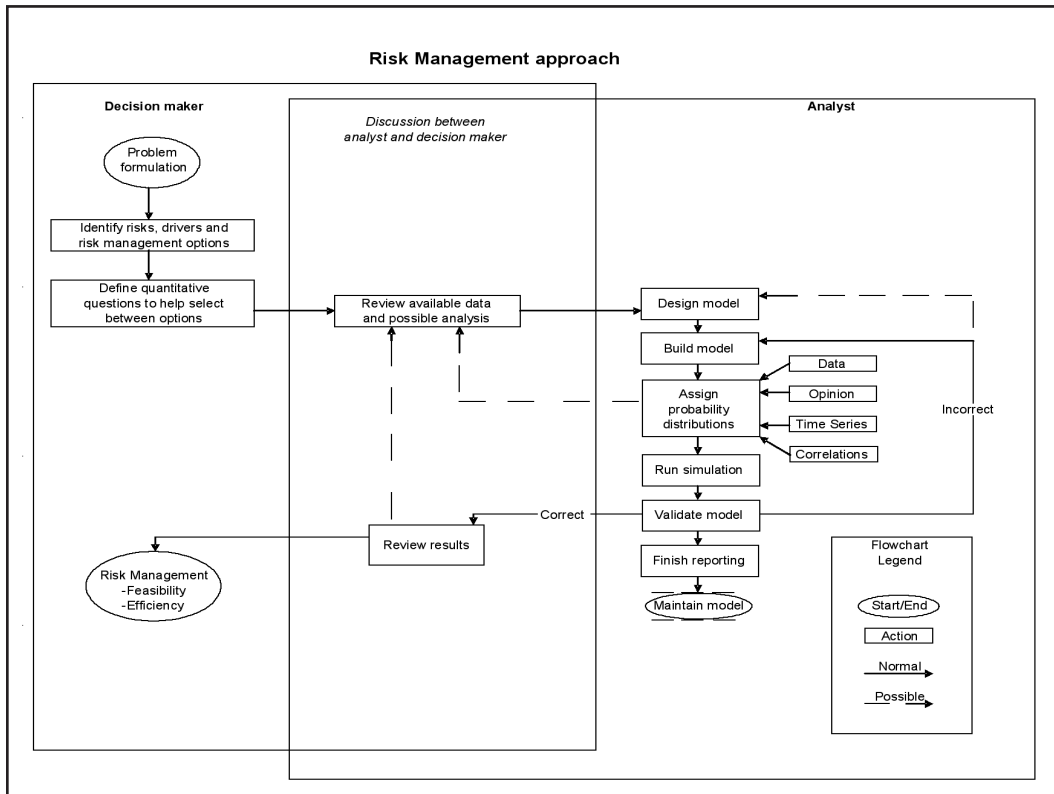


Figure 1.2 The risk analysis process

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 sub-sections 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.

1.2.1 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.

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 lists are used together to further improve 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 tasks 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

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.
9. Document clearly and completely.
10. Expose to peer review.

The response to correctly identified and evaluated risks are many, but generally fall into these 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 risks responses might in their turn carry secondary risks. Fallback 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 to 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 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 CEO's 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 5.4.6) 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. Example are:

- Use a tried and tested technology instead of the new one that was originally envisaged;
- Change 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 risk is reduced by) 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 pre-prepared press release;
- Have a phone list visible (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 shop 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 * 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 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; and
- 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?; and
- How practical will it be to execute the risk management option?

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 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, option C to be perfectly fine, and would only need more information about option B to be sure whether it was acceptable or not, despite all three having considerable uncertainty.

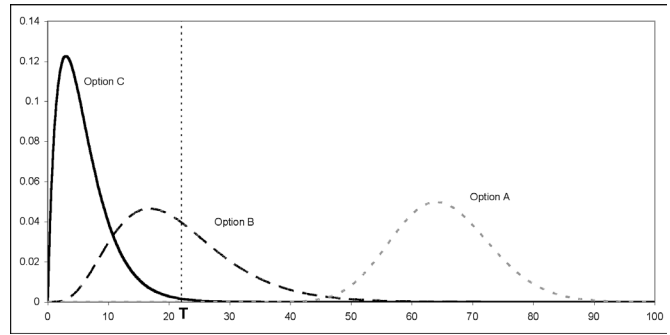


Figure 1.3 Different possible outputs compared to a threshold T

On sale from March 2008

Risk Analysis: A Quantitative Guide 3rd Edition – by David Vose

Contents

PART 1

Introduction
Chapter 1 – Why Do a Risk Analysis?
Chapter 2 – Planning a Risk Analysis
Chapter 3 – The Quality of a Risk Analysis
Chapter 4 – Choice of Model Structure
Chapter 5 – Understanding and Using the Results of a Risk Analysis

PART 2

Introduction
Chapter 6 – Probability Mathematics and Simulation
Chapter 7 – Building and Running a Model
Chapter 8 – Some Basic Random Processes
Chapter 9 – Data and Statistics
Chapter 10 – Fitting Distributions to Data
Chapter 11 – Sums of Random Variables
Chapter 12 – Forecasting with Uncertainty
Chapter 13 – Modelling Correlation and Dependencies
Chapter 14 – Eliciting from Expert Opinion
Chapter 15 – Testing and Modelling Causal Relationships
Chapter 16 – Optimisation in Risk Analysis
Chapter 17 – Checking and Validating a Model
Chapter 18 – Discounted Cashflow Modelling
Chapter 19 – Project Risk Analysis
Chapter 20 – Insurance and Finance Risk Analysis Modelling
Chapter 21 – Microbial Food Safety Risk Assessment
Chapter 22 – Animal Import Risk Assessment

APPENDICES

Appendix I – Guide for Lecturers
Appendix II – About ModelRisk
Appendix III – A Compendium of Distributions
Appendix IV – Further Reading
Appendix V – About Vose Consulting

- Published by John Wiley & Sons, Ltd
- Paper ISBN 10 digit: 0470512849
- Paper ISBN 13 digit: 9780470512845

 **VOSE**
CONSULTING
CONSULTING • SOFTWARE • TRAINING
WWW.VOSECONSULTING.COM

Founded in 1989, Vose Consulting is a leading international firm specializing in quantitative risk analysis. Our primary goal is to help clients make better, more informed decisions in the face of uncertainty and risk. We accomplish this goal through a combination of risk analysis consulting, training, and software. A core focus of our organization is the provision of cutting-edge risk-based consulting services to customers from industries in the private and public sectors.