How to complete a risk assessment

by Bernie Eccles and Professor Ian Bruce
Cass Business School Centre for Charity Effectiveness, 2010
How to complete a risk assessment

Bernie Eccles and Professor Ian Bruce OBE

A note about the design of this publication

KnowHow NonProfit has designed this publication to be accessible for people using screen readers. The source file for this PDF has been edited in the Royal National Institute for the Blind (RNIB) Word template. As such, we have deliberately chosen to prioritise an accessible structure over eye-catching design. We believe this makes our PDFs easier to read for everyone.
Introduction

There are four stages involved in preparing a risk assessment for a project, organisation or set of operating processes. These are:

- risk identification: identifying the main risks
- risk assessment: assessing the likelihood of each risk occurring and the consequences for the organisation
- risk mitigation: identifying the most appropriate actions to reduce or eliminate the risk
- contingency assessment: identifying the contingencies that need to be put in place following the risk assessment.

Risk management is an ongoing process and should be fully integrated into project management and review processes.

Risk identification

The first step in completing a risk assessment is to identify the risks associated with the management and operational processes for the organisation or project. A good way to do this is to hold a brainstorming session. The aim should be to identify risks, without going on to debate or assess them at this stage.

A typical local voluntary organisation should think about potential risks within each of the following areas:

- trustees
- organisation
- funding
- paid staff
- volunteer staff
- health and safety
- client service levels
- IT
- premises
- finance.

Each area may have several risks associated with it. The funding area, for example, may contain risks involving loss of core funding, loss of a significant grant or contract, or late payments.
Once you have identified all of the risks for your organisation or project, you can review the list to remove any overlaps and to make sure it covers all of the important risk areas.

**Risk assessment**

Risk assessment involves rating each risk against two dimensions: probability and impact.

**Probability**

The ‘probability’ aspect of risk assessment involves deciding how likely it is that the risk will occur. Each risk should fall into one of three categories:

- high probability: the risk might occur once every one to two years
- medium probability: the risk might occur once every three to five years
- low probability: the risk might occur less frequently than once in five years.

**Impact**

The ‘impact’ aspect of risk assessment involves considering what the potential impact of the risk would be on the organisation, client or project. Each risk should fall into one of three categories:

- high impact: the organisation might be forced to terminate activities as a result of a catastrophic failure or occurrence defined by the risk
- medium impact: the organisation would continue but the risk will have significantly affected its performance, timescales or costs
- low impact: the impact would be small and easily managed at a relatively routine level within the organisation.
Risk classifications

Once you have decided the probability and impact of each risk, you can plot them on a risk classification chart like the one below.

The four quadrants on the chart define different categories of risk which require different management approaches. These are described below.

**Critical risks**
- major risks with high probability and high impact
- require explicit management to keep them under control
- example: late payment of a grant that causes the charity to become insolvent.

**Difficult/insurance risks**
- risks which are unlikely to occur but which would have severe consequences if they did occur
- difficult to manage
- example: a catastrophic power failure in the organisation’s operational headquarters, causing all computers and systems to fail.
Routine risks

- commonly occurring risks which have only a minor impact on the organisation
- as they occur frequently, action to mitigate the risk should be built into a routine process
- example: minor human errors in delivery processes or procedures.

Low importance risks

- risks which have both low likelihood and low impact
- responsibility for these risks might be delegated to lower levels in the organisation
- these risks may be monitored to see if they develop into more important risks.

Risk mitigation

The next step is to decide how to manage the higher importance risks. In some cases the only action might be to monitor the risk and see if it becomes more significant.

Risk mitigation actions might include:

- define actions which would eliminate the risk or reduce it to an acceptable level. For example, in the event of a late grant or contract payment, the organisation could seek to generate or borrow a contingency fund of one to three months’ revenue.
- insure against unlikely but high impact risks. For example, to mitigate against a power failure, the organisation could pay for a back-up computer server housed offsite, with systems and processes automatically transferred to the back-up server.
- redefine or redesign the activity generating the risk to be lower risk. For example, to reduce routine human errors, manual activities could be transferred to computer-based processes with operator prompts and support.
- monitor the risk to see if it develops into a higher category risk. For example, monitoring the reliability of key office equipment to ensure that items can be replaced cost-effectively and in good time.
Once you have defined the actions for each risk, you will need to estimate the resources, workload and costs for each action. You can then assess the resources and costs against the risks to decide whether they are sensible and in proportion. It is very easy to generate a large list of actions which require a significant amount of budget and resources. It is often necessary to review and revise the list to achieve an appropriate set of risk mitigation actions.

Risk mitigation actions should be reviewed regularly, as risks and the appropriate responses can change over time. The risks for projects and mature operational processes should reduce substantially over time as understanding and experience grow. For projects close to completion, the total risk should fall to almost zero.

**Contingency assessment**

The last stage in the risk assessment process is to decide what contingencies should be put in place to assure management that projects and operational performance are secure.

There are four aspects to consider when assessing contingency:

- performance
- funding
- timescale
- cost.

**Performance**

This is the standard of client performance or service that has been promised to a grant provider or advertised externally. In general, an organisation will promise around five to ten per cent less than the standard they believe they can achieve on a routine basis.

**Funding**

This area of contingency covers the amount and timing of the funds or income that needs to be raised. Most organisations would not want to assume that the funding they have been promised will come into the organisation in full and on time, so will try to commit
resources only when the funding is assured. Some organisations align core funding areas with more certain sources of income and other services or resources with smaller, less certain funding sources. It can also be sensible to hold an appropriate level of funding in reserve.

**Timescale**

This contingency relates to the completion date of a project or the date at which a certain level of performance is achieved. The typical contingency is to quote a later completion date than is necessary, to allow for things that might go wrong.

**Cost**

Project costs or ongoing operational costs, including inflation, should be a major area of contingency. The management team might decide to forecast a somewhat higher cost than they believe they can achieve, to allow for additional costs and resources that would be required if things go wrong or the project runs for longer than planned.
Risk assessment matrix

A risk assessment matrix collates information on risks, probabilities, impacts and mitigating actions. The example below shows some of the risks that might apply to a medium to large-sized local voluntary organisation delivering funded services.

<table>
<thead>
<tr>
<th>Risk area</th>
<th>Risk description</th>
<th>Probability</th>
<th>Impact</th>
<th>Mitigating actions</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| Funding             | Loss / reduction of core funding         | Low         | High   | • document in detail how the organisation helps core funders to meet their key objectives  
                    |                                          |             |        | • quantify in numerical terms the volume and quality of outcomes achieved by the organisation  
<pre><code>                |                                          |             |        | • communicate regularly with core funders.                                              | Chair and chief executive     |
</code></pre>
<table>
<thead>
<tr>
<th>Risk area</th>
<th>Risk description</th>
<th>Probability</th>
<th>Impact</th>
<th>Mitigating actions</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| Trustees  | Inadequate trustee coverage resulting in failure to address key areas of governance | Low         | Medium  | • target recruitment of suitable volunteers through networks, volunteering websites and local publications  
• identify back-up trustees to share/overlap responsibilities  
• identify professional experts to provide support/advice  
• organise subcommittees in appropriate areas to ensure trustees are kept informed effectively  
• trustees to attend staff meetings where appropriate. | Chief executive |
| Paid staff | Loss of key permanent staff | Medium      | High    | • identify 'shadows' or deputies for all key staff and provide training  
• identify recruitment agencies and interim managers in advance of losses. | Chief executive and key staff |
<table>
<thead>
<tr>
<th>Risk area</th>
<th>Risk description</th>
<th>Probability</th>
<th>Impact</th>
<th>Mitigating actions</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| Health and safety | Significant accident or incident                     | Low         | Medium     | • define appropriate health and safety policies and audit them regularly  
  • undertake a separate health and safety risk assessment  
  • record and report all accidents/incidents and ensure lessons are learnt.                                                                                                                                       | Chief executive / safety officer      |
| IT                | Complete loss of IT services due to computer or power failure | Low         | High       | • ensure all equipment has automatic local back-up  
  • ensure all data is regularly backed-up and filed by each operator  
  • explore the cost-effectiveness of computer back-up at a separate site.                                                                                                                                 | IT manager                            |
| Client service levels | Target service levels not met by a significant margin | Low – medium | High       | • monitor service levels on a monthly basis  
  • define and monitor targets for staff numbers and productivity levels  
  • identify specific actions needed to address reduced service levels and report on actions monthly.                                                                                                               | Chief executive and key staff         |
<table>
<thead>
<tr>
<th>Risk area</th>
<th>Risk description</th>
<th>Probability</th>
<th>Impact</th>
<th>Mitigating actions</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>Major fraud or error</td>
<td>Low</td>
<td>High</td>
<td>• define and audit all financial processes&lt;br&gt;• second review of all significant payments, with two signatures on cheques&lt;br&gt;• two-person review of all financial transactions.</td>
<td>Finance director and chief executive</td>
</tr>
</tbody>
</table>
KnowHow NonProfit is part of the Cass Business School Centre for Charity Effectiveness and is currently funded by a Big Lottery Fund grant to the City Centre for Charity Effectiveness Trust Ltd (registered charity no. 1101084).