Risk Management Toolkit

ansvar

Contents

Introduction 4

Purpose of the Toolkit 4

Benefits of risk management 5

Risk management process 6

- Step 1: Risk identification 7
- Step 2: Risk assessment 8
- Step 3: Risk prioritisation 8
- Step 4: Risk mitigation 9
- Step 5: Risk monitoring 10

Conclusion 11

Appendices 13

- Appendix A: Risk management policy statement 14
- Appendix B: Risk categories 15
- Appendix C: Risk assessment criteria 16
- Appendix D: Risk register format 18
- Appendix E: Glossary of terms 20

Introduction

The upside of risk management is that each threat has the potential to be turned into an opportunity.

Risk: A threat that an event or action will adversely affect an organisation's ability to achieve its objectives, perform its duties or meet expectations of its stakeholders.

Risk Management: The practice of identifying risks in advance, analysing them and taking precautionary steps to reduce/curb the risk.

Risk is part of everyday life

It is generally recognised that risk will always exist and can never be completely eliminated. Risk management is therefore a critical activity to ensure risks are understood and appropriately addressed. When fully implemented, risk management will support the achievement of your objectives, innovation and growth.

An effective risk management framework is a key element of good governance and it provides confidence that you are dealing with risks (and opportunities).

The Risk Management Toolkit

The Toolkit seeks to promote the identification, assessment and response to key risks that may adversely impact upon the achievement of your objectives. It also seeks to maximise the rewards that can be gained through effectively managing your risks.

The Toolkit aims to clarify your arrangements for managing risk and further embed risk management within the thinking of everyone concerned, from the Board and Senior Leadership Team to employees and volunteers.

Purpose of the toolkit

The purpose of this Risk Management Toolkit is to establish a framework for the effective and systematic management of risk, which will ensure that risk management is embedded throughout your organisation and makes a real contribution to your objectives.

In practice, risks exist at many different levels, e.g., high level strategic risks to lower level everyday operational risks.

The framework outlined in the Toolkit can be applied at any level, e.g., Board, Senior Leadership Team, down to Organisational Departments.

It is important however that a mechanism is in place to enable risks to be escalated up (bottom up) and strategic risks to be cascaded down (top down).

A Risk Management Policy Statement should also be compiled and communicated to everyone to further demonstrate your commitment to risk management.

An example Risk Management Policy Statement can be found in **Appendix A.**

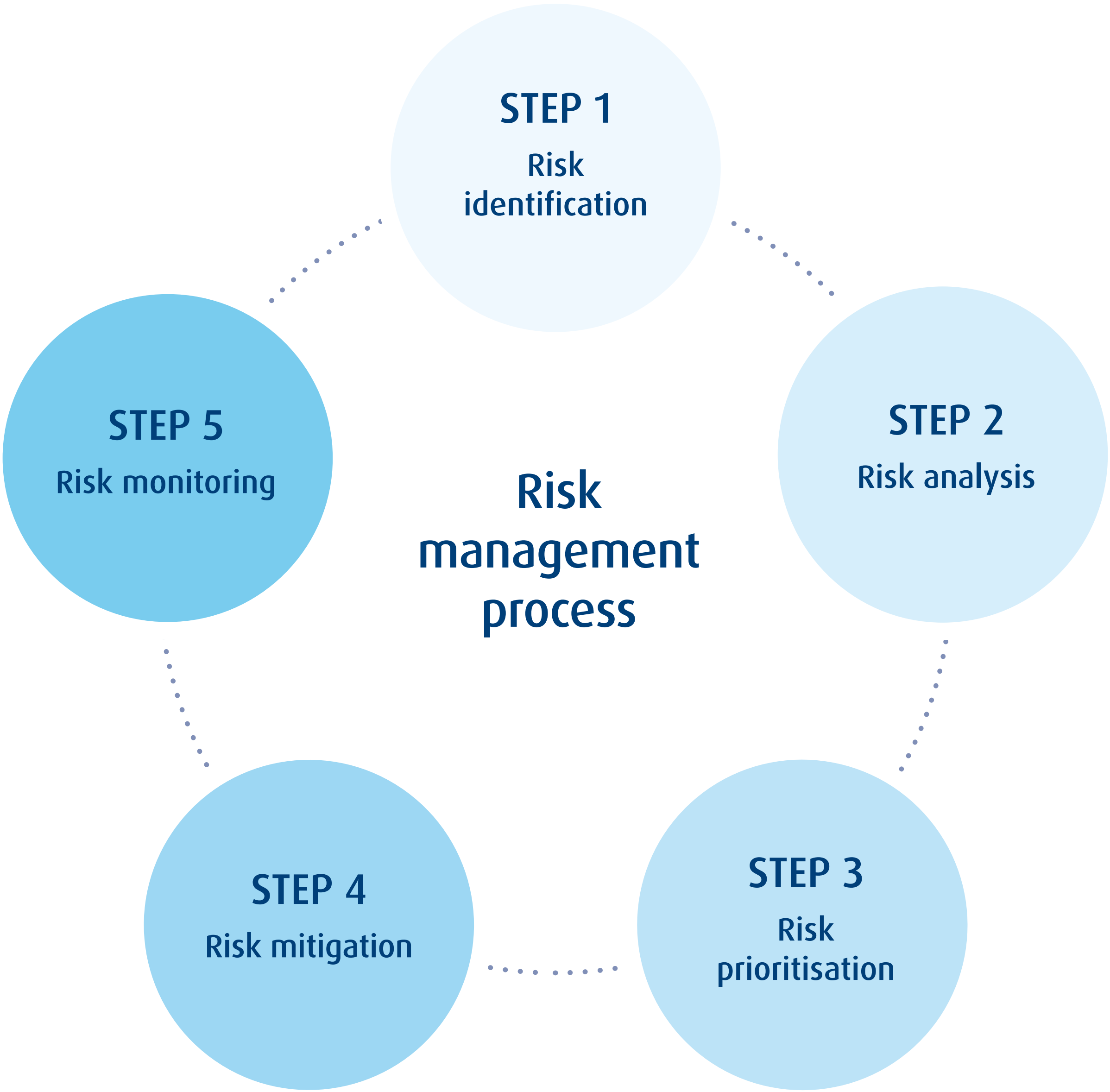
Benefits of risk management

Successful implementation of risk management will produce many benefits for you, including:

- Supports achievement of objectives
- Fewer shocks and unwelcome surprises
- Improved management information and decision making
- A consistent approach to the way risks are managed
- Provides a platform to maximise opportunities & be innovative
- Improved strategic planning
- Improved service delivery and performance
- Reduced losses
- Cost savings
- Greater assurance
- Good governance
- Protects your reputation

Risk management process

The risk management process consists of **5 basic steps** – these are indicated in the diagram below and should be driven by your objectives.


STEP 1
Risk identification
STEP 2
Risk analysis
STEP 3
Risk prioritisation
STEP 4
Risk mitigation
STEP 5
Risk monitoring
Risk management process

Step 1: Risk identification

Risk identification attempts to identify your exposure to uncertainty. To ensure that key risks are identified the process requires imagination, creativity & wide involvement, as well as a methodical framework.

This is probably one of the most important steps in the process, as you can only attempt to manage risks you have identified.

To try and achieve a robust risk assessment it is useful to consider the whole spectrum of risk.

A detailed list with examples can be found in **Appendix B.**

Strategic

Strategic risks are uncertain future events that could negatively impact on the achievement of your vision and strategic objectives

Operational

Operational risks are uncertain future events that could negatively impact the day to day operations of your establishment

People

People risks are uncertain future events that could negatively impact the staff/volunteers of your establishment or the people you interact with

Legal/Regulatory

Legal/regulatory risks are uncertain future events that could negatively impact on your ability to comply with the legal and regulatory landscape

Financial

Financial risks are uncertain future events that could negatively impact your finances

Hazard

Hazard risks are uncertain future events that negatively impact on you, caused by a hazard of some sort

Using the prompts above, various techniques can be used to begin to identify risks including:

- A ‘brainstorm’ session/workshop
- Interviews and questionnaires
- Own risk experience
- Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis
- Experience of others
- Exchange of information/best practice with other organisations/partners

In practice most organisations will conduct a brainstorming session/workshop utilising some of the above techniques as part of a specially extended regular meeting, such as a Senior Leadership Team meeting or Strategy Day.

What is vital is that this is a group exercise that considers the views of a range of relevant staff, or governing body members for the risk identification element.

No one person can identify all the risks, so involving others will ensure the process is as comprehensive as possible.

Step 2: Risk analysis

The information gathered needs to be analysed and put into risk scenarios to provide a clear and shared understanding. There are **3 parts to a risk scenario** detailed below.

Risk Scenario		
Background	**Cause**	**Consequence**
What? Why? Where?	How? Why? When?	How big? How bad? How much?

- Background - what is it, why is it a risk (some context).
- Cause is the risk 'event' – what could trigger the risk to occur.
- Consequence - what is the 'worst likely' chain of events if the risk was to happen.

Risk scenarios provide the background to the risk, its root cause and possible consequences so its full impact can be assessed.

Step 3: Risk prioritisation

It's **accepted** that you cannot manage all of your identified risks, due to limited time and resources, so following risk identification and risk analysis you will need to evaluate and prioritise the risks. This should occur in a facilitated workshop - again this should be a group exercise to get a range of views - ideally involving those who identified the risks initially.

The workshop participants should look at the risk scenarios and decide their ranking according to **risk impact and likelihood.**
Detailed Risk Assessment Criteria can be found in **Appendix C.**

A risk matrix can then be used to plot the risks (each risk should be given an identifying number which is then plotted into the appropriate section of the matrix) and once completed this risk profile will clearly illustrate the priority of each risk.

When assessing the potential impact of a risk and its consequences you should link this back to the appropriate strategic objectives.

Impact is assessed by asking what the impact would be.

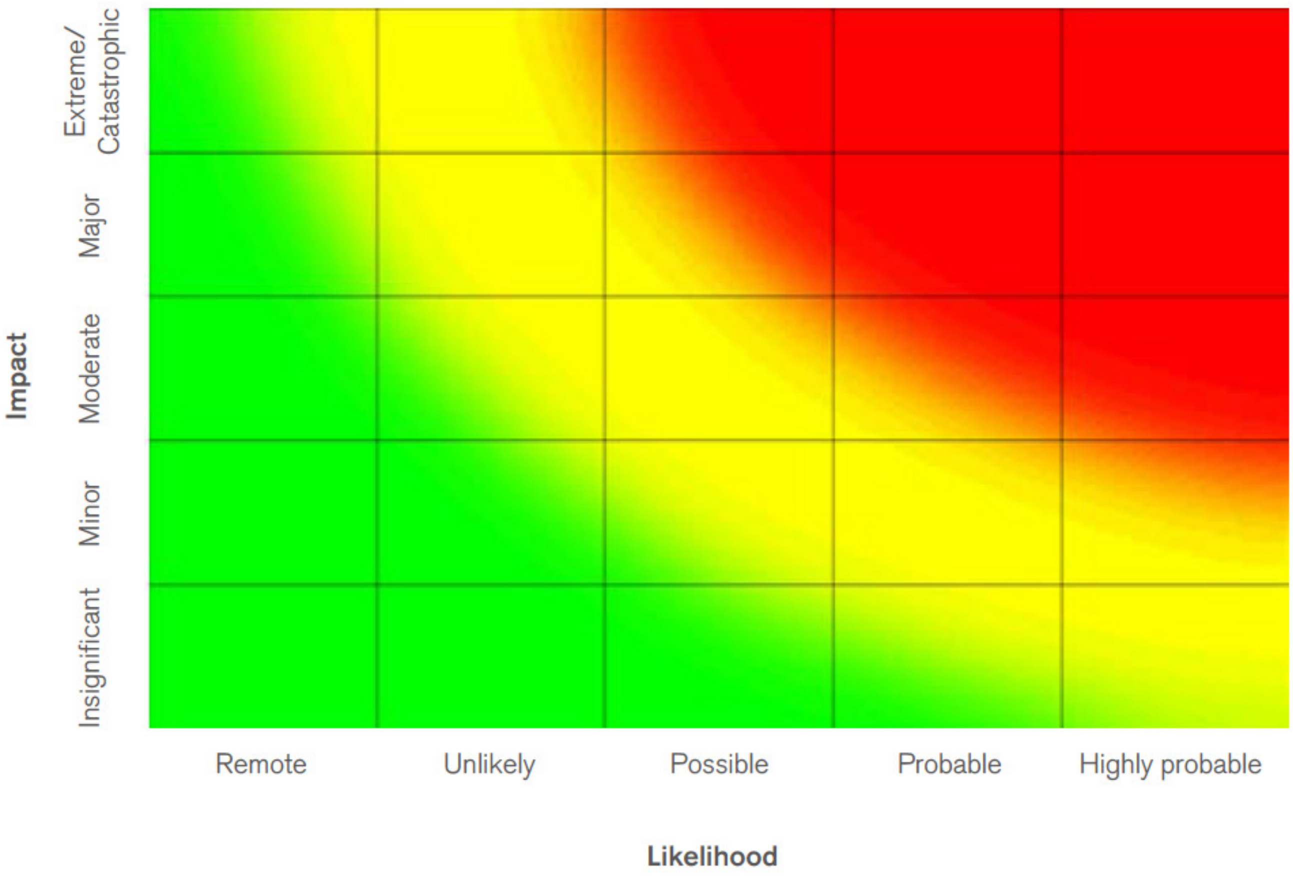
Likelihood is assessed by asking how likely it is that the risk event could occur.

The combination of both allows you to plot the risks on the matrix and sets the risks in perspective against each other. Those risks towards the top right hand corner with higher impacts and likelihoods are the most pressing, with the priority falling as you move down to the bottom left hand corner.

It is important when scoring the impact and likelihood of risks that a balanced view is taken with contributions from, and hopefully consensus of, relevant staff and other stakeholders. However, if there is real doubt over where to score a risk or agreement cannot be reached then it is best to place the risk in the higher category of impact and likelihood.

At the beginning of this stage, a timeframe needs to be agreed and the impact and likelihood should be considered with the relevant timeframe. For example the likelihood of a risk occurring in the next 12 months could be very different to its likelihood of occurring in the next 3 years. It is suggested that strategic risks are assessed over the medium term, e.g., 3 years and more operational risks over the short term, e.g., 1 year.

Having assessed the impact and likelihood of each risk, the risk is plotted onto the risk matrix (heat map) below:



Step 4: Risk mitigation

Once the risks have been prioritised the next step is to mitigate (manage) them in some way. This is vitally important as it is during this stage that improvement actually occurs. There are a number of strategies available to manage a risk however the options are generally – **Tolerate, Treat, Transfer or Terminate** – commonly referred to as the 4 T's.

Response	Which means	Example
Tolerate	Do nothing 'extra' to manage the risk	- There will be some risks where your current control measures in place are sufficient to reduce the likelihood and impact of the risk to a tolerable level and there is no added value in doing more, e.g., it's not cost effective or realistic to try and manage it any further - Alternatively there are some risks that are outside of your control and the organisation has no influence over them, e.g., government introducing new legislation that has a negative impact - You have to accept that these risks exist, monitor them and take limited action if and when possible.

Response	Which means	Example
Treat	Mitigating the risk by managing either - The likelihood - The impact - Or both	- This is the most likely form of management for the majority of risks. Developing SMART actions to manage the likelihood of risks occurring, their impact if they were to occur, or both - Often preventative controls are used to mitigate likelihood, to ensure something does not happen, e.g. training so that staff do not do something in the wrong way or firewalls to prevent computer virus attacks. The impact is often mitigated with some kind of contingency, e.g. alternative service providers or alternative service arrangements.
Transfer	Insurance, outsourcing and partnerships	- Insurance, although essential for many types of risk, will not be applicable for all types of risks you may face - Outsourcing or entering into partnerships may allow you to transfer certain risks – however by entering into such arrangements you will inevitably be faced with new and different risks which will have to be managed.
Terminate	Stop doing an activity	- In some instances, a risk could be so serious that there is no other option but to terminate the activity that is generating the risk.

Consideration should also be given here to the 'cost-benefit' of each control weighed against the potential cost-impact of the risk occurring.

NB: The cost-impact here should include all aspects including financial, resourcing and reputational.

Step 5: Risk monitoring

Your approach should be one where monitoring:

- Is a part of existing performance monitoring
- Focuses on those risks above the tolerance line (score) that, because of their likelihood and impact, make them priorities and,
- Be delegated to one responsible body, e.g., The Senior Leadership Team.

The Senior Leadership Team should:

- Take overall responsibility for risk
- Take overall responsibility for ensuring that processes are in place to effectively manage risks within the organisation
- Identify new/emerging risks for inclusion in the Risk Register
- Assess and scrutinise key strategic risks on a minimum of a quarterly basis as part of their work programme. High level risks should be reported more frequently
- Address risk issues that cannot be tackled at a more operational level
- Identify good practice and share learning
- Review the risk management approach and make suggested changes.

The organisation Risk Register will be the prime record which contains risk information.

The Risk Register format can be found in **Appendix D.**

The Risk Register template can be found in a separate Excel spreadsheet document.

Conclusion

This Toolkit will set the foundation for integrating risk management into your culture. It will also formalise a process to be applied across the organisation to ensure consistency and clarity in understanding the role and benefits of strategic risk management.

The reporting and escalation of risks should interlock with existing arrangements for performance reporting to ensure it is part of 'business as usual' rather than be seen as an additional process.

The adoption of the Toolkit will formalise the risk management work to date based on recognised good practice risk management principles.

A glossary of risk management terms can be found in **Appendix E.**

Appendices

Appendix A: Risk management policy statement (example) 14

Appendix B: Risk categories (including examples) 15

Appendix C: Risk assessment criteria 16

Appendix D: Risk register format 18

Appendix E: Glossary of terms 20

Appendix A: Risk management policy statement (example)

It is policy to proactively identify, understand and manage the risks inherent in our products, services and future plans to encourage responsible and informed risk taking.

Risk management is all about understanding, assessing and managing the risks and opportunities.

accept the need to take proportionate risks to achieve its strategic objectives, but expects these to be appropriately identified, assessed and managed. Through managing risks and opportunities in a structured manner, the organisation will be in a stronger position to ensure it meets its objectives.

risk management approach aims to:

- Be proportionate and reflect the size, shape and nature of the organisation
- Provide a consistent and structured framework to manage risks and maximise opportunities
- Ensure that risk management becomes an integral part of organisational planning and decision making
- Enable the organisation to deliver its priorities and services economically, efficiently and effectively
- Align risk management and performance management to drive improvement and better outcomes
- Guard against impropriety, malpractice, waste and poor value for money
- Ensure compliance with legislation, such as that covering the environment, health and safety, employment practice and equalities
- Minimise the prospects of any damage to the organisation's reputation/and or undermining of public confidence in the organisation.

Once complete the risk management policy statement should be signed off by the most senior member of staff in the organisation to acknowledge their approval/authorisation.

Signed by

Date

Appendix B: Risk categories (including examples)

Risk categories	Examples
Strategic risks	• Mergers • Diversification • Competition • Change in strategic direction • Government policy change • Loss of a key supplier • Conflict of interest • Reputation issue • Inadequate financial forecasting/reporting linked to strategic planning.
Operational risks	• Loss of a critical system • Loss of confidential data • Loss of insurance for key operations • Reduced productivity levels and standards of service • Failure to react appropriately in the event of a business interruption • Health and safety.
People risks	• Key person dependency/succession planning • Inadequate training • Recruitment and retention • Capacity and capability.
Legal/Regulatory risks	• Breach of data protection • A lack of awareness leading to non-compliance with key pieces of legislation (HMRC, GDPR, HSE, Charity Commission) • Failure to recognise and respond to a change in legislation • Employee initiates legal action, e.g., tribunal case.
Financial risks	• Increase in pension fund liabilities • Inability to meet monthly pension payments • Negative movements in the interest rate, significant decreasing return on investment • A member of staff commits a fraudulent act • A significant increase in the cost base of the organisation, e.g., increase in supplier costs.
Hazards	• Fire in a key building • Flood denies access to a key building/site • A major health and safety incident occurs • A member of staff is injured while performing their duties • Theft of cash or key piece of equipment.
Others (please add)	• The above list are just examples – additional category areas can be added relevant to your particular situation.

Appendix C: Risk assessment criteria

Risk likelihood measurement criteria

Scale	Description	Likelihood of occurrence	Probability of occurrence
1	Remote	1 – 5% (1 in 20yrs)	May only occur exceptional circumstances.
2	Unlikely	6 – 15% (1 in 6/7yrs)	Expected to occur in a few circumstances.
3	Possible	16 – 40% (1 in 2/3yrs)	Expected to occur in some circumstances.
4	Probable	41 – 75% (1 in 2yrs)	Expected to occur in many circumstances.
5	Highly probable	76 – 100% (1 in <2yrs)	Expected to occur frequently and in most circumstances.

Appendix C: Risk assessment criteria (Continued)

Risk impact measurement criteria

Scale	Description	Service/Operations	Safety/People	Financial
1	Insignificant	• No impact on service • No impact on reputation • Complaint unlikely • Litigation risk remote.	• No fatalities • Minor impact on people's health.	1 - 2% of turnover
2	Minor	• Slight impact on service • Slight impact on reputation • Complaint possible • Litigation possible.	• No fatalities • A small number of minor injuries (3/4) requiring first aid treatment.	3 -5% of turnover
3	Moderate	• Some service disruption • Potential for adverse publicity (avoidable with careful handling) • Complaint probable • Litigation probable.	• No fatalities • Significant number of people affected requiring first aid treatment.	6 -8% of turnover
4	Major	• Service disrupted • Adverse publicity not avoidable (local media) • Complaint probable • Litigation probable.	• Significant number of people affected • Hospitalisation required as well as medical treatment.	9 - 15% of turnover
5	Extreme/ Catastrophic	• Service interrupted for a significant time • Major adverse publicity not avoidable (national media) • Major litigation expected • Resignation of senior leadership and board members • Loss of beneficiary confidence.	• Fatality / fatalities • Large number of people affected • Multiple serious or extensive injuries.	>15% of turnover

Overall risk score = Risk Impact x Likelihood

Appendix D: Risk register format

(refer to separate Excel Spreadsheet for risk register template)

Risk register	
Heading	**Detail**
Risk number and Risk map ID	• Unique risk number/letter attached to the risk to enable monitoring and reporting.
Risk description	• A high level overview of the risk, e.g., risk headline.
Risk causes	• A list of the main drivers that could cause the risk to materialise.
Risk consequences	• A list of the key consequences that may arise should the risk occur.
Current risk mitigation	• A list of current controls that are in place to mitigate the risk. These should be specific and auditable, for example: fire safety assessment completed annually. A mitigation measure should either reduce the likelihood of the risk materialising and/or reduce the impact should the risk materialise – if it does not then its not a control.
Risk owner	• The person accountable for owning the risk and its management.
Connected strategic objectives	• The link between the risk and strategic organisational objective.
Impact	• A scored ranking of the impact to the organisation should the risk materialise.
Likelihood	• A scored ranking of the likelihood of that risk actually materialising.
Risk score	• A product of the impact score and likelihood score.
Ongoing or planned mitigation measures	• A list of ongoing or planned mitigation measures to further control the risk.
Risk review date	• A date when the risk will be reviewed to assess the effectiveness of controls and whether further action is required.

Appendix D: Risk register format (Continued)

Please note once the risk scores have been calculated for all the risks you have identified, you will then be able to sort the risk register in terms of a risk score so that you can clearly see the top risks facing the organisation.

This risk register can be sorted in this way:

☐ Select the whole risk register – from the title row down to the final risk

☐ Go to the toolbar and click on 'Data' and then 'Sort'

☐ Ensure 'my data has headers' is selected – this will mean all the headers in the risk register are now included in the dropdown menu of the first 'sort by' box

☐ Select the column for 'Risk Score' in the dropdown menu

☐ Select 'values'

☐ Select 'largest to smallest'

☐ Select OK.

Your register will now reorder the risks so that those presenting the biggest risks to the organisation are at the top of the risk register.

This sort can be reversed by following the same process but selecting 'Risk ID' in the dropdown menu rather than the 'Risk Score'.

NB: You need to be careful that all the columns and rows that are in use are selected prior to the sort, otherwise the information aligned to each risk will become mixed up.

Appendix E: Glossary of Terms

(The glossary below is not exhaustive, but contains common practice risk management terminology)

Term	Definition
Control	The control of risk involves taking steps to reduce the risk from occurring, such as application of policies or procedures.
Corporate Governance	Set of internal controls, processes, policies, affecting the way the organisation is directed, administered or controlled.
Hazard	A threat (natural or human) that has the potential to cause harm.
Loss	Any negative consequence, financial or otherwise.
Mitigation (Plan)	A strategy that reduces risk by lowering the likelihood of a risk event occurring or reducing the impact of the risk should it occur.
Objective	Something to work towards – goal.
Overall risk score	The score used to prioritise risks – impact multiplied by likelihood.
Residual Risk	The remaining level of risk after risk mitigation and control measures have been taken into consideration.
Risk	A threat that an event or action will adversely affect the organisation’s ability to achieve its objectives, perform its duties or meet the expectations of its stakeholders.
Risk Assessment	The overall process of risk analysis and evaluation.
Risk Category	Represents a collection or group of risk types with a common denominator, e.g., strategic, operational, people, legal/regulatory, financial, hazard.
Risk Cause	The main drivers that cause the risk to materialise.

Appendix E: Glossary of Terms (Continued)

Term	Definition
Risk Consequences	The main consequences to your organisation should the risk materialise.
Risk Impact	A qualitative description or score ranking of the impact to the organisation should the risk materialise.
Risk Likelihood	A qualitative description or score ranking of the probability or frequency of that risk actually materialising.
Risk Management	The practice of identifying risks in advance, analysing them and taking precautionary steps to reduce/curb the risk.
Risk Register	A risk register is a log of risks of all kinds that threaten an organisation's success in achieving its objectives. It is a dynamic living document which is populated through the organisation's risk assessment and evaluation process. The risk register enables risks to be quantified and ranked. It provides a structure for collating information about risks.
Risk Treatment	The action(s) taken to remove or reduce the risks.

Risk advice line

(provided by Ecclesiastical professionals or external specialists)

Phone: **0345 600 7531**

Email: **risk.advice@ecclesiastical.com**

Risk specialists are on hand to advise you on a range of topics, including:

- property protection, security, business continuity planning
- health and safety, food safety, environmental management
- construction safety, fire safety, occupational health, water safety or asbestos.

Available Monday to Friday 9am – 5pm (excluding public and bank holidays).

A free to download software package called ROBUST is also available from RISCAuthority, a funded research facility supported by a significant group of UK insurers, including Ecclesiastical. This is a comprehensive toolkit with all the details on how to complete a BC plan. For further details and to download visit:

https://robust.riscauthority.co.uk/

For further information speak to your insurance advisor or call us on **0345 60 20 999**

www.ansvar.co.uk

This guidance is provided for information purposes and is general and educational in nature and does not constitute legal advice. You are free to choose whether or not to use it and it should not be considered a substitute for seeking professional help in specific circumstances. Accordingly, Ecclesiastical Insurance Office plc and its subsidiaries shall not be liable for any losses, damages, charges or expenses, whether direct, indirect, or consequential and howsoever arising, that you suffer or incur as a result of or in connection with your use or reliance on the information provided in this guidance except for those which cannot be excluded by law. Where this guidance contains links to other sites and resources provided by third parties, these links are provided for your information only.

Ecclesiastical is not responsible for the contents of those sites or resources. You acknowledge that over time the information provided in this guidance may become out of date and may not constitute best market practice.

Ansvar Insurance
4th Floor, The Office, 1 Market Square,
Circus Street, Brighton, BN2 9AS

Phone: **0345 60 20 999**

Email: **ansvar.insurance@ansvar.co.uk**
www.ansvar.co.uk

Ansvar Insurance, is a business division of Ecclesiastical Insurance Office plc (EIO) Reg No 24869. EIO is registered in England at Benefact House, 2000, Pioneer Avenue, Gloucester Business Park, Brockworth, Gloucester, GL3 4AW, United Kingdom.

Ansvar is a trading name of Ecclesiastical Insurance Office who are authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Firm Reference Number 113848
Tel: **0800 111 6768**

All content © Ecclesiastical Insurance Office plc 2021
UW174(RM) 06/21 (RMT)