ProtectUK

Risk Management Basics

ProtectUK publication date
19/03/2024

It is essential that you have a good understanding of risk management before undertaking a risk assessment. This knowledge will enable you to make informed decisions around risk and increase your confidence with adapting your risk assessment approach in the future.

Risk Management Basics unpacks some of the key risk management concepts and approaches to risk assessments. This is presented across three core activities in the risk assessment process:

If you are new to risk management, the concepts and techniques presented here may seem daunting at first. Do not worry. Section 3 of this guidance will walk you through applying this knowledge in practice step-by-step. You can return to this section at any point to refresh your knowledge.

Risk Identification

What is a risk?

Risk is the effect of uncertainty on objectives.

It is made up of three main elements: threat, vulnerability and impact:

Threat	The potential cause of a security incident that can result in damage or harm to an organisation
Vulnerability	Weakness of an asset or control that can be exploited so that an event with a negative consequence occurs
Impact	Outcome of a security incident affecting objectives

Vulnerabilities may exist across your organisation. However, a risk will only occur when there is a threat source present to exploit these weaknesses to cause harm.

Without a threat source, a vulnerability cannot be exploited. Without exploitation, there is no impact.

Each of these elements must therefore be present to give rise to risk.

The risk identification process looks at each of these elements in greater detail.

How do I identify risks?

Risk identification is the process of finding and describing risks that might prevent your organisation from achieving its objectives. This includes risks that may cause harm to your staff, customers, volunteers and other visitors to your site.

To identify risks, each individual element of risk is assessed in the context of your organisation. These assessments enable you to answer the following key questions:

Threat Assessment	Who might attack your organisation and how?
Vulnerability Assessment	What gaps and weaknesses currently exist in your security approach?
Impact Assessment	What harm or loss could be caused by a threat exploiting a vulnerability?

You will find step-by-step guidance, examples and further resources on how these assessments can

be performed in Section 3 - Risk Assessment Process.

For now, it is important to make note of the key questions you need to consider in order to identify risk.

What approaches can I use?

Identifying risks can be approached in different ways and can involve different levels of detail. The approach you select determines how you will explore threats, vulnerabilities and impact as part of your assessment.

It is important to consider how you wish to approach risk identification before commencing any risk assessment activities. This is because different options may involve greater time and resource commitments from your organisation.

In risk management, there are two main approaches to identifying risk: an **asset-based approach** and an **events-based approach**.

Each of these approaches seeks to address the key questions around risk noted above. However, this is carried out in different ways.

Asset-based

An **asset-based approach** takes a bottom-up approach to risk identification. This involves inspecting critical business assets and their vulnerabilities in order to identify risk.

In an asset-based approach, all critical business assets should be captured within an asset-register prior to a risk assessment taking place. Once captured, a risk assessor will consider each of these assets in turn, exploring any gaps and weaknesses that may exist and the threats capable of exploiting these vulnerabilities.

An asset-based approach explores risk at a more granular level through the development of operational scenarios. An example operational scenario using an asset-based approach might describe a terrorist attacker exploiting a malfunctioning CCTV system to conceal and detonate an IED, resulting in mass casualties. In this case, the asset under inspection is the CCTV system.

Event-based

An **event-based** approach takes a top-down approach to identifying risk. This explores threats, events and consequences at a broader level than an asset-based approach. In an event-based approach, you are not required to complete an asset-register prior to undertaking a risk assessment as this approach concerns itself with the exploration of strategic level scenarios. An example strategic scenario might describe a terrorist attacker deploying an IED to destroy critical infrastructure.

Each approach aims to construct a scenario in order to identify and explore risk. In risk management, you will see this referred to as a **risk scenario**. This is a description of a sequence of events, leading from their initial cause to the unwanted consequence.

When you select a particular approach to identifying risk, you are essentially choosing how you wish to develop your risk scenarios and the level of detail you wish to explore risk in. Both approaches explore the same risk scenario, this is just commenced at different starting points.

In an asset-based approach, you can search upwards from the asset to a strategic scenario in order to gain insight into the broader consequences of an event. Equally, in an event-based approach, you can drill down from the strategic scenario to obtain more detail at an operational / asset level.

The level of detail you wish to explore risk in will help you decide which approach you choose. You then have the freedom to decide how far you wish to drill down or search up within this.

How do I decide between approaches?

Many organisations will employ an asset-based approach to help ensure an appropriate level of resource is allocated to protect critical assets and control risk. This can often demand the allocation of dedicated time and resource in order to ensure all assets are captured correctly as part of an asset register before the risk assessment process begins.

An asset-based approach may be a more suitable solution for your organisation if you require a more granular level of decision-making around the protection of specific assets and systems. In contrast, an event-based approach will spend less time identifying assets at a detailed level as this can be undertaken in the process of examining strategic scenarios (if required).

If you are interested in an asset-based approach to risk assessment, or believe an asset based approach would be a suitable method for your organisation, the National Protective Security Authority

(NPSA) offering of Protective Security Risk Management (PRSM) may be suitable for you. You are encouraged to review this guidance, in addition to the ProtectUK guidance, in order to determine the most appropriate approach for you organisation.

You may select any approach to identifying risk so long as this enables you to produce consistent and valid results. However, it is essential that the approach you choose is achievable with the resource you have available to you. An asset-based approach will typically require greater time and resource to complete due to the necessity of completing an asset-register prior to any risk assessment activity.

If this your first time undertaking a risk assessment, you may not yet feel comfortable selecting a particular approach. If this is the case, it is recommended that you engage with the ProtectUK Approach and guidance outlined in Section 3 before making a decision. The ProtectUK Approach pre-selects an event-based approach for your risk assessment. The guidance contained within Section 3 – Risk Assessment Process will walk you through this approach. Once you are comfortable using an event-based approach, you may wish to return to this section to explore whether an asset-based approach may be more suitable for your organisation.

Risk Assessment

What is a risk assessment?

A risk assessment enables you to analyse and evaluate risk on the basis of its potential impact and likelihood of occurrence.

For this to be possible, a **risk score** must be calculated for each risk you identify. These scores enable you to prioritise risks for treatment later in the risk assessment process.

How do I calculate risk?

A risk score can be calculated by multiplying the potential impact of a risk with its likelihood of occurrence. You may see this expressed as impact x likelihood = risk.

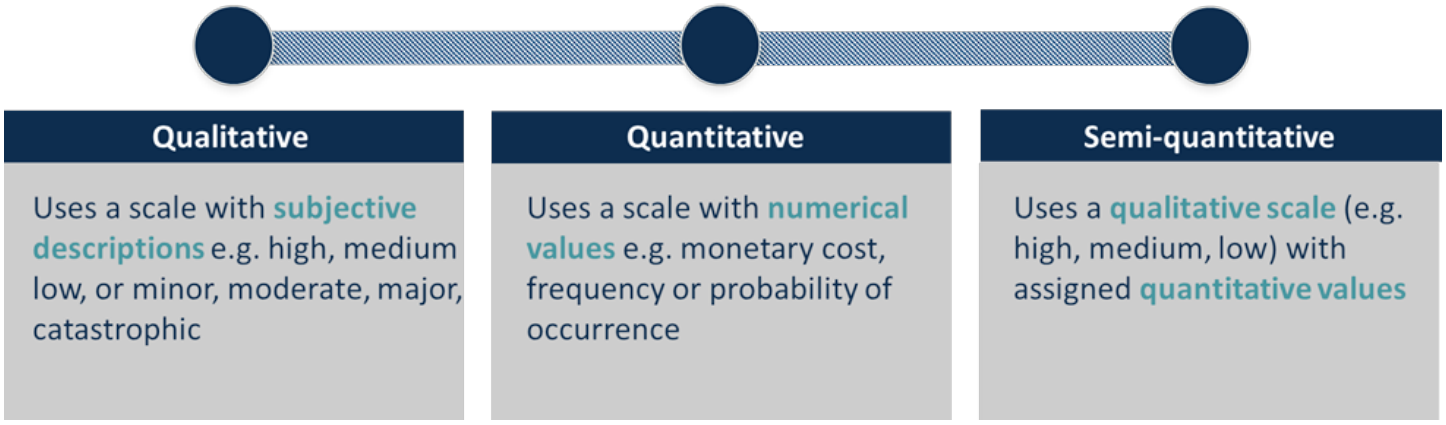
To perform this calculation, a separate rating needs to be produced for the likelihood and impact of each risk. These ratings can then be multiplied to produce an overall risk score.

Likelihood and impact ratings are typically generated using set **reference scales** that help you measure the severity of a risk and its chance of occurring.

How do I measure risk?

In risk management, it is common to use set **reference scales** to measure the likelihood and impact

of a risk. These scales may be qualitative, quantitative or semi-quantitative in nature:



Generally, reference scales will contain 4-5 levels. For impact scales, each level will capture the increasing severity of a risk. For likelihood scales, each level will capture the increasing chance of the risk occurring. The way these scales are expressed differs based on the approach you select (qualitative, quantitative, or semi-quantitative).

Some organisations require a great deal of detail when determining impact and likelihood. For example, an organisation may require a high degree of accuracy when considering the financial consequences of a risk scenario. This will generally necessitate a quantitative approach when developing scales.

While quantitative approaches have the benefit of offering greater accuracy due to their use of numerical data, this method usually requires more expertise and resource to undertake, including knowledge of statistics and access to high quality data. Without high quality input, the results you produce will lack meaning and will have little value to your organisation.

The level of accuracy offered by a quantitative approach is not always necessary to gain an adequate understanding of the risks your facing your organisation. For this reason, many organisations will opt to assess impact using qualitative methods that utilise subjective descriptions over objective detail.

Example of a quantitative impact scale

Consequence (loss)*	**Scale value**
£1,00,000	5
£10,000	4
£1,000	3
£100	2
Less than £100	1

* Monetary consequences are typically based on factors of 10 (100 to 1,000; 1,000 to 10,000)

In practice, a qualitative scales will often be the most straightforward approach to measuring and assessing risk.

Although subjective, qualitative methods often have the benefit of being easier to undertake than a quantitative approach. This enables an organisation to obtain a general indication of the severity of a risk within a more reasonable timeframe. However, due to their subjectivity, qualitative scales can be subject to inconsistent application across your organisation, particularly if they are defined ambiguously. The use of a qualitative approach should take care to define scales that are able to be interpreted clearly and consistently by all individuals concerned with the RMP. For example, by using clear definitions and objective language.

Example of qualitative likelihood scale

Rating	**Description**
Likely	A terrorist attacker will likely succeed in a method of attack.
Possible	A terrorist attacker will possibly succeed in a method of attack
Unlikely	A terrorist attacker has little chance of succeeding in a method of attack
Very unlikely	A terrorist attacker has very little chance of succeeding in method of attack

In deciding whether a qualitative or quantitative method is more appropriate, you should consider the availability and reliability of data available to you, the form of output your stakeholders are likely to expect from your assessment of risk, and the constraints on time and additional resources that may be required from adopting a particular approach, including costs, expertise and skills.

Likelihood Scales

In risk management, likelihood is used to refer to the chance of something happening. This can be described by an organisation in a variety of ways, including expected probability, frequency, or by use of descriptive terms. The scale you develop to describe likelihood is referred to as your **likelihood criteria**.

How you choose to express likelihood as part of your likelihood scale will depend on your chosen risk analysis method i.e. whether you have selected a quantitative or qualitative approach.

A quantitative approach will express likelihood mathematically when defining the expected frequency or probability of an incident, while a qualitative approach makes use of subjective terms and descriptions.

Typically, organisations will establish a set scale across 4 – 5 levels. For example:

4 Level Likelihood Scale

Rating	Description
Likely	A terrorist attacker will likely succeed in a method of attack.
Possible	A terrorist attacker will possibly succeed in a method of attack
Unlikely	A terrorist attacker has little chance of succeeding in a method of attack
Very unlikely	A terrorist attacker has very little chance of succeeding in method of attack

The amount of levels you select will need to be consistent across your scales. For example, if you select four levels for likelihood, your impact scale should also be four levels.

It is up to the **responsible person** to decide how likelihood is expressed as part of the risk assessment process. However, a **competent person** may offer guidance and / or assist in the development of the scale.

Impact Scales

In risk management, the term impact is used to refer to the outcome of an event that affects your organisational objectives.

An impact scale helps you to measure the different types of damage or costs to your organisation caused by these events. Typically, these will be defined by organisations across 4-5 levels. The scale you develop to describe impact is referred to as your **impact criteria**.

When measuring impact, it is often not enough to rely on a general scale. For example:

Impact	Description
Catastrophic	Consequences beyond the organisation
Critical	Disastrous consequences for the organisation
Serious	Substantial consequence for the organisation
Significant	Significant but limited consequences for the organisation
Minor	Negligible consequence for the organisation

To truly measure impact, you need to consider this scale in relation to the different types of impact that may affect your organisation. Some key impacts include:

For each area of impact you identify, you will need to establish a scale of escalating consequences. This is achieved by combining the impact types you have selected with the general impact scale seen above. For example:

	Minor	Moderate	Major	Catastrophic
Operational	Loss of service <1 day	Loss of service >2 days	Loss of service > 1 week	Near total loss of service
Financial	Minor loss of business / value	Moderate loss of business / value	Major loss of business / value	Catastrophic loss of business / value
Organisational	Minor impact on key objectives	Moderate impact on key objectives	Late delivery of key objectives	Non-delivery of key objectives
Life and safety	Minor injuries to multiple people	Serious injuries to multiple people	Single loss of life	Multiple loss of life
Environmental	Minor damage to environment	Moderate damage to environment	Major damage to environment	Catastrophic damage to environment
Legal	No involvement from regulatory body	Warning from regulatory body	Exposure to fines and penalties	Exposure to prosecution
Reputational	Minor local negative publicity	Moderate local negative publicity	National negative publicity	Near total loss of public confidence

How you choose to express impact across each category will depend on your chosen risk analysis method i.e. whether you have selected a quantitative or qualitative approach.

A quantitative approach will express impact mathematically when defining the loss or damage caused by an incident, while a qualitative approach makes use of subjective terms and descriptions. The above examples utilises qualitative descriptors to capture the escalating consequences of each impact type.

Your expression of impact will also depend on your risk appetite. What one organisation considers to be catastrophic, major, moderate or minor may be different to another organisation. It is therefore important to develop your impact scale in the context of your organisation and appetite for risk. What does a minor to catastrophic impact look like for your organisation?

When considering the types of impact to include as part of your impact scale, you should include any area that you feel is relevant to your organisation. This will enable your impact criteria to reflect what is important to your organisation.

As with your likelihood criteria, it is up to the **responsible person** to decide how impact is expressed as part of the risk assessment process. However, a **competent person** may offer guidance and / or assist in the development of the scale.

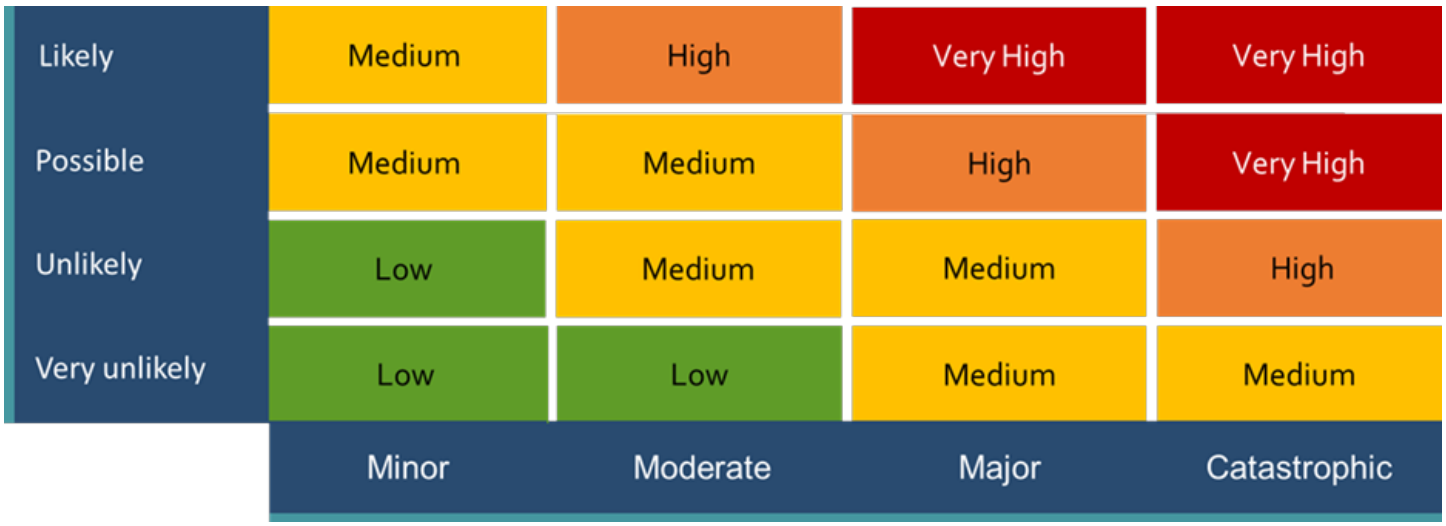
If this is your first time working with reference scales, you may wish to engage with the ProtectUK Approach before undertaking this activity. The ProtectUK Approach offers pre-established likelihood and impact scales that will help familiarise you how reference scales work in practice. Section 3 of this guidance – Risk Assessment Process will walk you through the use of these scales as part of a risk assessment step-by-step.

Once you are comfortable using reference scales as part of the risk assessment process, you should return to this step to consider adapting the ProtectUK scales to better suit your organisational context and risk appetite.

How do I analyse and evaluate risk?

A **risk matrix** is a common risk assessment tool used to display risks according to their impact and likelihood of occurrence. This can help you to analyse and prioritise risks for treatment.

Once you have determined a measurement of likelihood and impact for a risk, a risk matrix can be used to plot a risk and obtain an overall risk score.



Size

Risk matrices come in different sizes and can communicate different attitudes towards risk. They can be 3x3, 4x4, 5x5 etc.

The axes of the matrix correspond with the descriptors and amount of levels used for your likelihood and impact scales.

The size of the matrix you use is therefore dependent on how you have chosen to define your likelihood and impact ranges. For example, 4 level scales = 4x4 matrix, 5 level scales = 5x5 matrix.

Structure

Some matrices will use numerical values to score risks, while others will make use of qualitative descriptors. In the example shown above, qualitative descriptors have been used to score risks (low, medium, high and very high). These ratings are represented by colour coded cells.

In a numerical approach, these descriptors would be replaced by ratings valuing 1-16 to reflect the use of a 4x4 matrix. In a 3x3 matrix, you would expect to see ratings of 1-9, in a 5x5 matrix, you would expect to see ratings of 1-25.

Many organisations make use of standard risk matrices that will distribute these ratings in a balanced way. However, it is possible to create your own risk matrix, or tailor a standard risk matrix, to better suit your organisation’s risk appetite.

For example, a risk averse appetite may see you tailor a matrix to give more bias to high impact or high likelihood risks. This would be reflected in how the ratings and colour codes of the matrix cells are distributed. In this case, you would expect to see more very high (red) and high (amber) risks within the matrix to covey a low risk appetite. In contrast, a matrix skewed towards a high risk appetite will typically contain more low (green) and medium (yellow) risks.

The example matrix shown above is the risk matrix used in the ProtectUK Approach. This is a 4x4 matrix that reflects a lower risk appetite by allocating only three low risk ratings. Section 3 of this guidance will walk you through how to use this in practice.

As you become more comfortable with using risk matrices, you may wish to return to this section to consider adapting the ProtectUK Risk Matrix to better suit your organisation, or create your own risk matrix.

A risk matrix is one technique that you may consider adopting during a risk assessment. It should not be taken as the definitive technique for analysing and evaluating risk, rather it is one of many techniques that you may consider. A full list of techniques may be found in ISO 31010.

Risk Bands

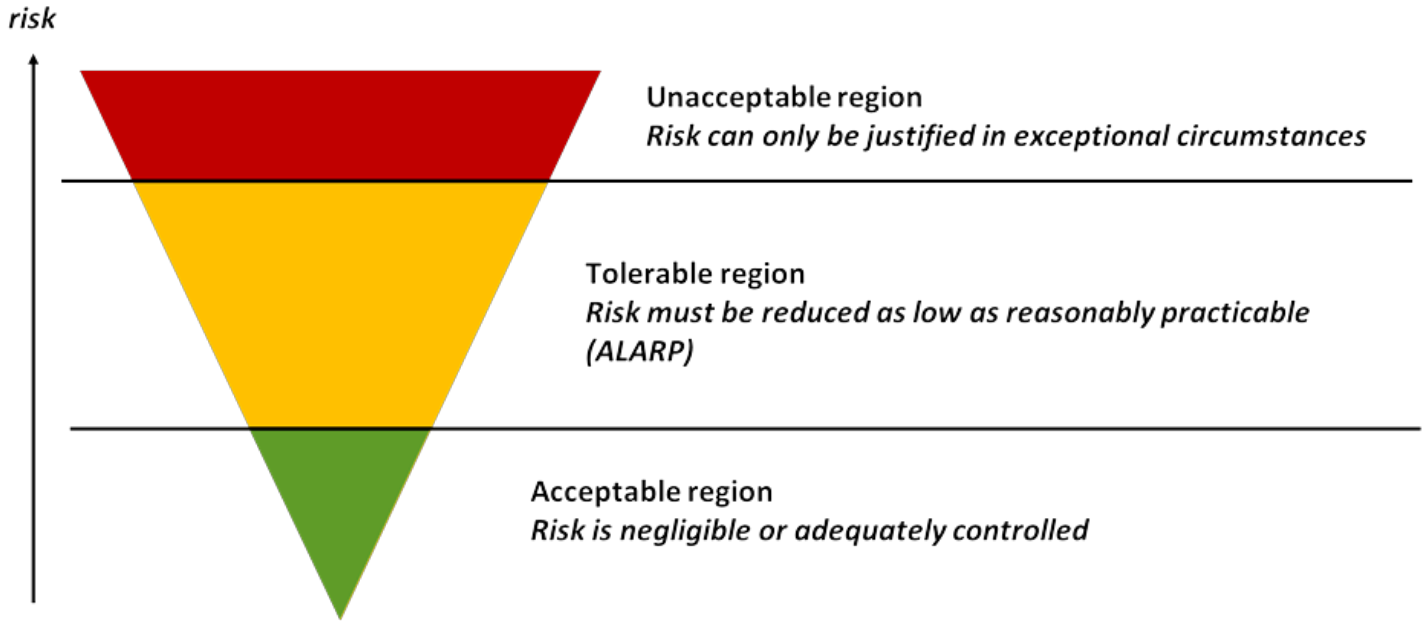
In addition to helping you plot and score risks, risk matrices can also be used to help you evaluate risk. This is achieved through the establishment of set **risk bands** that communicate particular decision rules and actions for different risk scores.

The rules you outline in each risk band are known your **risk acceptance criteria**. This sets the limits above which you will not tolerate a risk. They will usually include requirements for risk treatment or further actions.

When it comes to establishing rules around risk, a simple criteria of 'yes – accept risk' and 'no – reject risk' might seem like the most straightforward approach. In reality, this can often be too reductive to account for the context and complexity of risks.

For this reason, many organisations choose to adopt a model that divides risk acceptance into three main categories. This enables a more flexible approach than a 'yes' / 'no' criteria:

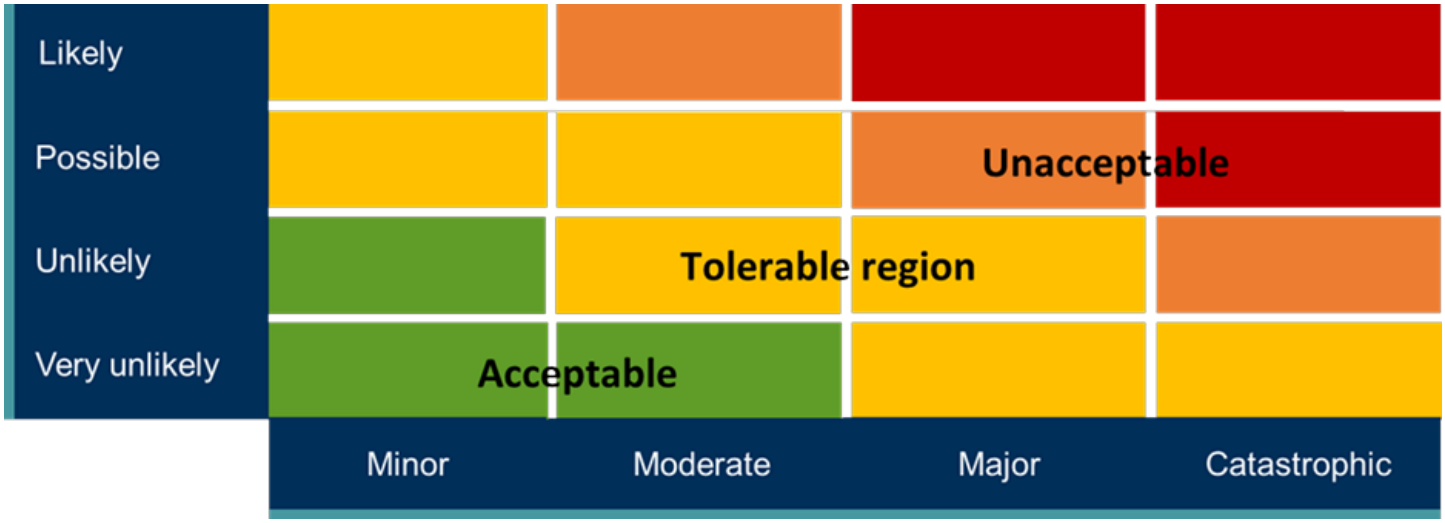
- **Unacceptable**: an intolerable risk category, where risk can only be justified in exceptional circumstances
- **Acceptable**: a broadly acceptable risk category where the risk is negligible or adequately controlled to the point where further risk reduction need not be considered (but could be implemented if practicable and reasonable)
- **Tolerable:** a region between the above two limits where further risk reduction should be implemented if the cost of reduction would exceed the improvement gained. This usually occurs by judgemental reasoning or formal cost-benefit analysis.



You may be familiar with this approach in a health and safety context, where the principle, 'as low as

reasonably practicable' (ALARP), is used to decide whether a risk should be treated.

When establishing risk bands in a matrix, colour codes are used that broadly correlate with the above three categories of risk. For example, you will often see red and orange used to signify very high and high risks, yellow used for tolerable risks, and green used for acceptable risks.



These colour codes enable different zones to be established in the matrix that communicate different forms of action via a risk band. Further colours can be used to communicate more decision rules:

Rating	Description
Very High	Unacceptable risk. Requires urgent treatment.
High	Unacceptable risk. Action to be taken as soon as possible.
Medium	Tolerable only if the cost of reduction exceeds the improvement gained.
Low	Acceptable with periodic review

It is up to the **responsible person** to decide how each risk band is set and defined within a risk matrix. This includes the amount of bands established and the rules applied within this. If you are using a standard risk matrix, these bands may be pre-established. You would then need to decide whether to adapt these to better suit your organisation. Alternatively, you could create your own boundaries and set your own rules.

When setting risk bands and outlining further actions, you should be mindful of your organisational context and risk appetite. For example, if you had a risk averse appetite, you would likely set rules to treat any ‘very high’ or ‘high’ risks as soon as possible as these would be unacceptable to your organisation.

You could also take your risk acceptance criteria further by establishing different levels of acceptance across different risk types. If you recall some of the key types of impact from earlier – life and safety, finance, reputation – you may find that you are less willing to accept risk in some of these areas than others.

To account for this, you could establish a separate risk appetite per each impact type to help guide your decision-making around accepting risk in particular areas. This adds a greater degree of complexity into the risk evaluation stage, but may be a useful next step for you once you have built confidence with the risk management process.

You can find more information on producing individual risk appetite statements in the UK Government’s Orange Book – Risk Appetite Guidance, which covers risk appetite and risk appetite statements in more detail.

If this is your first time using a risk matrix, you may find it helpful to work through the guidance in Section 3 – Risk Assessment Process before developing your own approach. Within this step-by-step guidance, you will be presented with the ProtectUK Matrix, a pre-set 4x4 matrix with 4 risk bands, which will help familiarise you with how to apply this technique in practice.

Once you are comfortable using a risk matrix as part of the risk assessment process, you should return to this step to consider adapting the ProtectUK Matrix, or developing your own matrix and / or decision rules.

Risk Criteria

When brought together, your likelihood, impact and risk acceptance criteria are known collectively as your **risk criteria**.

Risk criteria outlines the terms of reference against which the significance of a risk is evaluated during the risk assessment process. Essentially, this criteria helps determine how risks are scored and the actions that should follow from the result of that score.

Your risk criteria should be established prior to undertaking your risk assessment. However, it is important to regularly review the scales and rules you set in order to ensure that they continue to reflect your attitude toward risk and your organisational context.

Risk Treatment

What is risk treatment?

Risk treatment is the process of modifying risk to an acceptable level for your organisation. This takes place after your risk scores have been generated.

The actions you take to treat risk are referred to as **controls**. A control is any measure or action that maintains or modifies risk. These actions are recorded in a **risk treatment plan**, which outlines how you intend to implement and monitor your chosen treatment option.

Each risk you identify requires a form of risk treatment to be selected and applied. There are four main approaches for treating risk:

Avoid	Decide not to start or continue with the activity that gives rise to the risk
Share	Split responsibilities for risk with other parties (internally or externally)
Modify	Introduce, remove or alter controls to change the likelihood or impact of the risk
Retain	Retain the risk by informed choice (no change)

- **Avoid**
  Risk avoidance asks you to consider whether the activity giving rise to risk can be ceased if already commenced, or not started at all if yet to be commenced. For example, if an organisation were considering the transfer of sensitive information to a new cloud service provider, and it had been identified that this would place the organisation's information at an increased risk of cyber-attack, then this particular project could be terminated.

- **Share**
  If it is not possible to terminate the risk, you will need to decide whether the risk can be shared – either internally, or externally with a third party. In some cases, it may not be possible to transfer or share the entire amount of risk.

  Risk sharing involves delegating the responsibility of implementing the control to another party. This can help to modify the likelihood or impact of risk. However, risk sharing does not

absolve you, as the responsible person, from accountability. When sharing risk with another party, the responsibility for the risk itself will remain with your organisation, even if the implementation of the control is transferred.

Using the above example of information transfer, an organisation may choose to place its information with a third party provider as opposed to storing this information on its own servers. If this provider is subject to a cyber-attack, the responsibility for any harm resulting from a data breach would remain with the organisation, including any fines or penalties incurred.

- **Modify**
  Risk modification asks whether the risk can be reduced or modified through the implementation of controls that reduce the impact or likelihood of something happening, or a combination of both. An example of risk reduction may be the introduction of a food defence programme to reduce the likelihood of product contamination. This would strengthen the organisation's efforts to prevent a CBR attack, reducing the likelihood of this attack method being successful. However, this would need to be balanced against the cost of implementing this programme of work and providing ongoing support and resource.

- **Retain**
  The final treatment option for consideration is to retain the risk. This option is typically selected when a risk is too costly to treat or when further risk treatment is not possible. Risk retention may also be selected where risk is required to be accepted on a temporary basis.

  It is important to note that when a risk is chosen to be retained, it is not chosen to be ignored. Accepted risks should be documented and reviewed periodically in case the level of risk changes, or there is sudden change in the threat level that may result in an increase in likelihood. When this happens, you may decide that the cost of acceptance is beyond the organisation, leading you to select another treatment option.

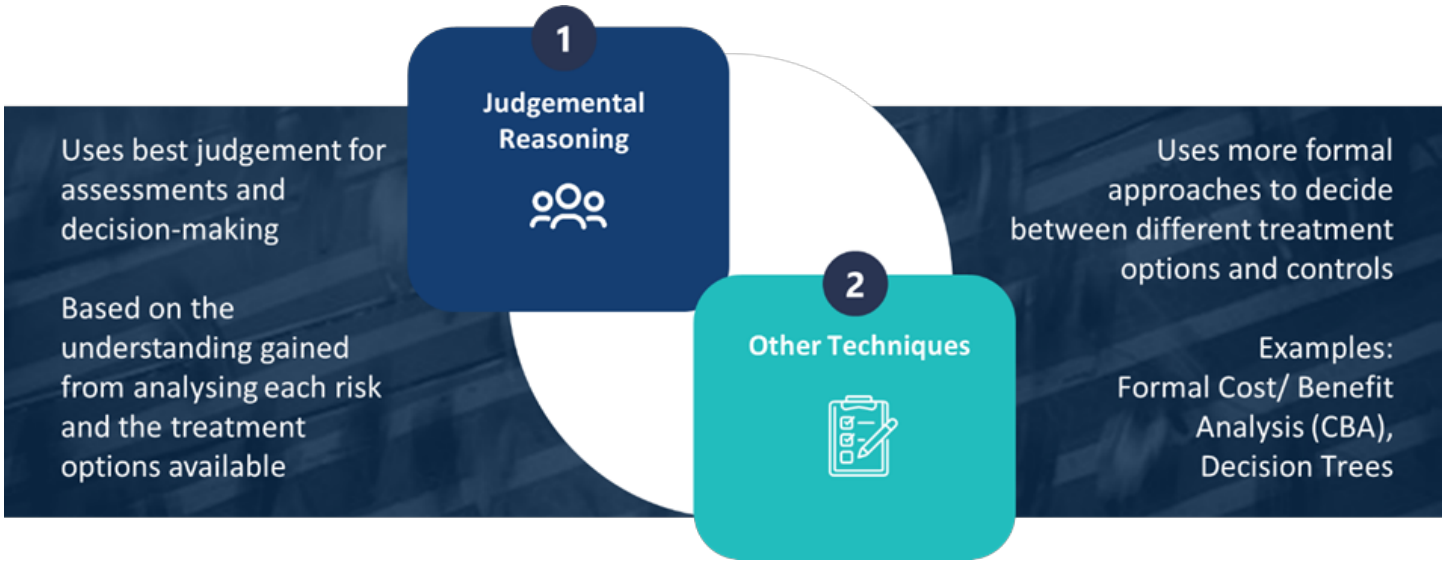
The above options set the approach for treating risk at a strategic level. They do not treat risk in and by themselves. The selection of individual controls to directly treat risk is discussed in further detail in Section 3 of this guidance – Risk Assessment Process.

For now, you should note that these are the main options that you will need to consider regarding risk treatment.

How do I decide between options?

Selecting the most appropriate form of risk treatment will usually involve weighing up the potential advantages and disadvantages of each risk treatment option. This includes any uncertainties around potential outcomes and costs.

To make your decision, you can use your professional judgement, or opt to use more formal techniques.



Judgemental reasoning involves you making decisions around risk treatment based on the understanding you have gained from analysing each risk and the options available to you. The decisions you make should take account of your risk appetite, the potential benefits and risks associated with each treatment option, your organisational objectives, and the views and expectations of your stakeholders.

If you require further insight into the potential advantages and disadvantages of each option, or the cost / resource implications that may be associated with particular treatments, then you may choose to use more formal techniques to help you decide between options.

For example, you may find it worthwhile to undertake a formal qualitative or quantitative cost / benefit analysis (CBA) when weighing up risk treatment options. This would enable you to more precisely cost any investments in time and resource and determine any expected benefits.

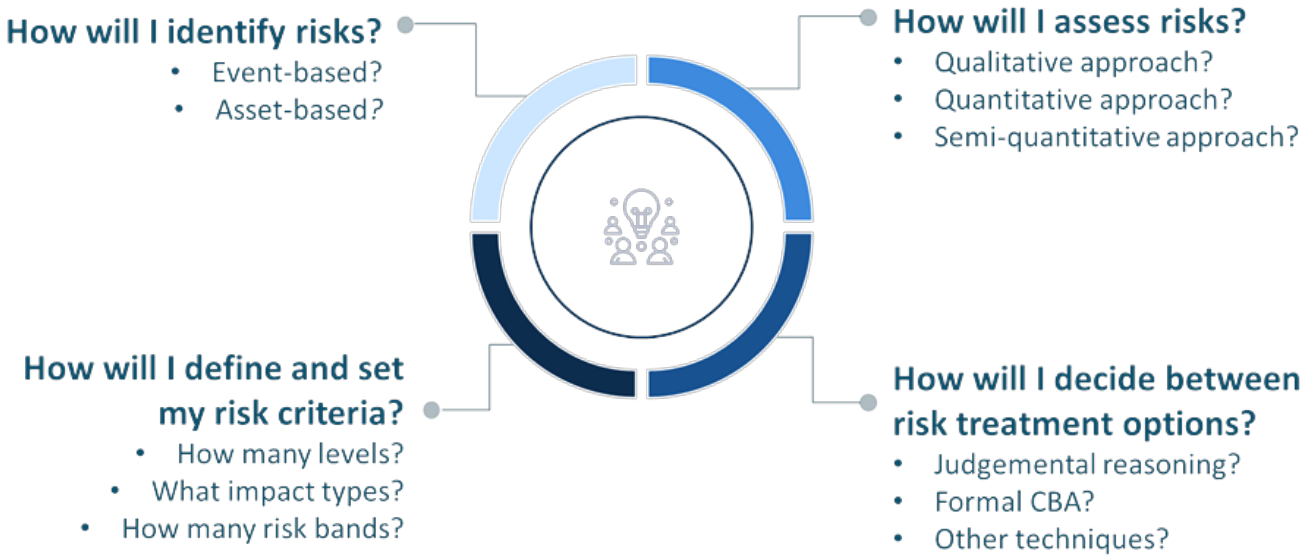
There are many other techniques available for deciding between options that you may also wish to consider. Some further examples can be found in ISO 31010.

It is up to the **responsible person** to decide how risk treatment options are selected. If you opt to use more formal techniques, such as formal CBA, you should ensure that those responsible for performing this analysis have the expertise required to do so.

Key Considerations

It is clear that a risk assessment goes far beyond the completion of a simple template.

To ensure risks are managed well in the context of your organisation, it is necessary to think carefully about your approach and the techniques and methods you opt to use. The decisions you make should take into account your risk appetite and the expectations of your stakeholders.



The aim of the ProtectUK Risk Management Guidance is to build your confidence and maturity with risk management so that you can eventually feel comfortable making these decision for yourself.

This guidance now turns to a step-by-step breakdown of the risk assessment process using the ProtectUK Approach. This will support first time assessors in completing their first terrorist risk assessment by offering a pre-established approach to assessing risk.

Once you are comfortable with the guidance in Section 3, you should return to this section to consider where you could adapt the ProtectUK Approach, or establish an entirely new approach, that best suits your organisation’s context and needs.

KEYWORDS
RISK MANAGEMENT
RISK ASSESSMENT
RISK
RESPONSE
PROTECTIVE SECURITY