ProtectUK

Stage 2: Risk Assessment

ProtectUK publication date

21/03/2024

The second stage of the risk assessment process involves analysing and evaluating risk.



To achieve this, you will be using the risk criteria set by the ProtectUK Approach. This criteria will help you score each risk you have identified and evaluate its significance.

This begins with transferring the risks you identified in stage one to your ProtectUK Risk Assessment Template. You will then proceed to assess the **likelihood** and **impact** of each risk using the four level qualitative reference scales set by the ProtectUK Approach.

Once you have generated a likelihood and impact rating for each risk, you will be guided through the use of a **4x4 risk matrix**. This will include how to visually plot risks and how to apply the ProtectUK **risk acceptance criteria** to help determine which risks are acceptable to your organisation.

Finally, you will be supported in prioritising risks for treatment. This will help you to determine which risks should be addressed first in the next stage of the risk assessment process.

This stage of the risk assessment process is supported by the ProtectUK Risk Assessment Template. The process is broken down step-by-step for you below.

Step 2A: Describing Risks

Risk assessments require concise descriptions of risks. For this reason, the risk scenarios you produced at the end of stage one will need to be briefly summarised in the form of a **risk statement** before proceeding.

A risk statement provides a succinct description of an incident and its potential consequences on your organisation for ease of understanding. All risk statements generally capture the following three elements:



There are a number of ways to write a risk statement.

It is acceptable to use any format for writing your risk statements so long as you capture the key elements of the risk and these are presented unambiguously.

For example, you could use an **'if-then'** format to complete your risk statements. This presents the risk event and its outcome: **if** an event occurs **then** a specific impact will result.

Alternatively, you could use a **'cause-event-consequence'** format. This presents why the risk is happening, the risk event, and the impact of this risk being realised.

To assist you with constructing risk statements, your risk identification template has been designed to capture each individual element in the cause-event-consequence format:

Cause	Event		Consequences
Vulnerability	**Threat**	**Event**	**Consequences**
Local suppliers used for food and drink are unable to offer reassurance regarding food and drink defence	CBR attack	CBR threat compromises food supply chain to contaminate products served to the public / staff as there no procedures in place to detect tampering	Loss of life due to exposure. Existing and future customers will be reluctant to purchase our food and drinks as they will not trust our quality assurance processes, which will result in lower profits

Example Statement

A cause-event-consequence statement using the above example may look something like:

Because our suppliers lack a food defence programme (**cause**), food and drink could be

contaminated and consumed by customers in a CBR attack (**event**), resulting in loss of life and exposure to prosecution for food safety failings. This will harm our reputation, profits and ability to trade (**consequences**).

Here we have the cause – the vulnerability, our event – a description of how a threat could exploit this weakness to cause harm, and the consequences – the areas that will be negatively affected across the organisation if this risk occurs.

The cause of the risk will tell you where you need to focus your attention in terms of risk treatment later in the risk assessment process. The consequences you have identified help to communicate how severe the risk will be if it occurs.

The statements you produce should enable another reader to clearly grasp the nature of the risk and its magnitude.

A risk statement should be developed for each risk scenario you produced in stage one. This should be captured in Part I of your ProtectUK Risk Assessment Template under the ‘Risk Description’ heading.

For each risk, you should also provide a reference number for quick reference e.g. R1:

Reference	Risk Description	Threat	Existing Controls	Likelihood	Impact	Risk Score
R1	Because we lack a review process for our security procedures, our response to actual and suspected security incidents could become outdated and ineffective, resulting in loss of life and exposure to prosecution for negligence. This will harm our reputation and ability to trade by reducing customer confidence, profits and available resource					
R2	Because our IT lacks requirements for strong passwords, our systems could be hacked and sensitive customer data stolen by a cyber-attacker, resulting in fines and penalties from the ICO, which will harm our profit margins and customer confidence					
R3	Because our local suppliers lack a food defence programme, food and drink could be contaminated and consumed by customers in a CBR attack, resulting in loss of life and exposure to prosecution for food safety failings. This will harm our reputation and ability to trade, decreasing our profits					

Threats and Existing Controls

Following the development of each risk statement, the relevant threat source for each risk should be transferred to the ‘Threat’ column in your Risk Assessment Template.

Once complete, you should then look to list any existing controls you have in place to manage this risk in the ‘Existing Controls’ column.

As effective controls can reduce the likelihood of a threat exploiting a particular vulnerability, it is essential that this information is recorded in your risk assessment.

You may find it helpful to consult your original pass of existing controls against each threat type in Step 1B when completing this step. Consultation with management and staff across different business areas in your organisation may also help you to identify any relevant control measures currently in place.

Reference	Risk Description	Threat	Existing Controls	Likelihood	Impact	Risk Score
R1	Because we lack a review process for our security procedures, our response to actual and suspected security incidents could become outdated and ineffective, resulting in loss of life and exposure to prosecution for negligence. This will harm our reputation and ability to trade by reducing customer confidence, profits and available resource	All Threats	• None			
R2	Because our IT lacks requirements for strong passwords, our systems could be hacked and sensitive customer data stolen by a cyber-attacker, resulting in fines and penalties from the ICO, which will harm our profit margins and customer confidence	Cyber	• Passwords for log on • Staff briefed on basic information security • ACT e-learning			
R3	Because our local suppliers lack a food defence programme, food and drink could be contaminated and consumed by customers in a CBR attack, resulting in loss of life and exposure to prosecution for food safety failings. This will harm our reputation and ability to trade, decreasing our profits	CBR	• Staff trained in food safety, including contamination • Regular inventory checks undertaken to detect damage and tampering			

Your output at this stage should be: a list of risk statements with corresponding threats and existing control measures

Step 2B: Assessing Likelihood

With your risk statements complete, the risk assessment process now turns to the assessment of likelihood.

In risk management, likelihood refers to the chance of something happening. In order to provide a likelihood score, you will need to be able to measure the increasing chance of an incident occurring in your organisation.

This can be achieved by the use of a **likelihood reference scale**.

The ProtectUK Approach utilises a qualitative, four point scale to measure likelihood:

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 a method of attack

As you become more familiar with the risk assessment process, you may choose to define these levels differently, or use a quantitative or semi-quantitative approach to measuring likelihood. The way you choose to define and measure likelihood is known formally as your **likelihood criteria**.

You should consider alternative approaches to measuring likelihood once you are confident with the process below. Further information on adapting your likelihood criteria can be found in Section 2 of this guidance.

For each identified risk, you will need to determine a likelihood rating according to the above scale and record this in your template.

Reference	Risk Description	Threat	Existing Controls	Likelihood	Impact	Risk Score
R1	Because we lack a review process for our security procedures, our response to actual and suspected security incidents could become outdated and ineffective, resulting in loss of life and exposure to prosecution for negligence. This will harm our reputation and ability to trade by reducing customer confidence, profits and available resource	All Threats	• None	Possible		
R2	Because our IT lacks requirements for strong passwords, our systems could be hacked and sensitive customer data stolen by a cyber-attacker, resulting in fines and penalties from the ICO, which will harm our profit margins and customer confidence	Cyber	• Passwords for log on • Staff briefed on basic information security • ACT e-learning	Possible		
R3	Because our local suppliers lack a food defence programme, food and drink could be contaminated and consumed by customers in a CBR attack, resulting in loss of life and exposure to prosecution for food safety failings. This will harm our reputation and ability to trade, decreasing our profits	CBR	• Staff trained in food safety, including contamination • Regular inventory checks undertaken to detect damage and tampering	Very Unlikely		

The rating you generate should factor in the following:

- The effectiveness of any existing controls you currently have in place
- The motivation, capabilities and resources available to the identified threat
- The perception of attractiveness and vulnerability of your organisation to attack
- The vulnerabilities that exist across your organisation individually and in aggregation

The ProtectUK Approach encourages you to use your best judgement to provide likelihood ratings across risks. This takes account of the understanding you have generated of the risk so far and your knowledge of the existing controls you already have in place to manage that risk.

The ratings you generate should reflect the chance of an incident occurring **with** current controls in place to enable you to establish the likelihood of each scenario in the current context of your organisation.

As it is difficult to predict exactly when an event might occur, the assessment of likelihood should be considered an exercise that generates a meaningful estimate as opposed to a value with total accuracy. However, this should still be evidence-based and you should consider engaging with

various evidence sources before making your judgement.

You may find it helpful to consult with members of your team, such as management, HR, IT and security staff when carrying out this activity. These individuals will be well placed to inform you if your current controls are working effectively to reduce likelihood and if any controls require review. The data you collected and reviewed as part of your initial threat assessment may also be useful to consult here when considering threat motivators and target attractiveness.

You may also wish to consult with security specialists and experts for additional insight.

Example Rating

Let’s consider how a ‘very unlikely’ score may have been determined for risk **R3**. This risk is concerned with a potential CBR attack:



While there is a chance that R3 could occur - it has been recognised that there is a gap in the supplier’s efforts to protect food from contamination – you can see from the template above that there are other controls in place that are currently working to reduce this risk. This includes staff being trained in food safety and regular inventory checks to detect damage and tampering.

If these controls are functioning as intended, you would expect the likelihood of a CBR attacker successfully exploiting this weakness to be lower than if no controls were in place. The effectiveness of the controls put in place by the organisation has therefore reduced the likelihood of the risk occurring. In light of this, a ‘very unlikely’ rating has been assigned to this risk.

Your output at this stage should be: a list of risk statements with corresponding threats, existing control measures and likelihood ratings

Step 2C: Assessing Impact

The risk assessment process now turns to the assessment of impact.

In risk management, an impact is the adverse result of a threat taking advantage of a gap or weakness in your organisation. In order to determine impact, you need to be able to identify what kind of harm could occur and the extent to which that harm might affect your organisation.

This is achieved by the use of an **impact reference scale**.

The ProtectUK Approach utilises a qualitative, four point scale to measure impact:



To help determine impact more specifically, this scale is combined with seven pre-selected key impact areas to produce the **ProtectUK Impact Criteria**:





As you become more familiar with the risk assessment process, you may choose to define the levels of your impact scale differently, or use a quantitative or semi-quantitative approach to measuring impact. Equally, you may decide to include more or less impact areas, or select entirely different impact areas to rate. How you choose to define and measure impact is known formally as your **impact criteria**.

You should consider adjusting your approach to measuring impact once you are confident with the process below. Further information on adapting your impact criteria can be found in Section 2 of this guidance.

For each identified risk, you will need to determine an impact rating across the seven impact areas included in the ProtectUK Impact Criteria. The highest rating you generate for each risk will form your overall impact score. Not all impact areas will be relevant to each risk. You should rate only those you consider to be relevant.

You are encouraged to make use of the impact scoring card included with your Risk Assessment Template when completing this step:

Risk Ref	Operational	Financial	Organisational	Life and Safety	Environmental	Legal	Reputational	Highest Rating
R1								
R2								
R3								

When using the scoring card, you should individually rate each impact area according to the ProtectUK Impact Criteria. Your ‘Highest Rating’ will be the highest impact score you assign across each of these areas. For example:



Once complete, you should transfer your ‘Highest Rating’ for each risk to your Risk Assessment Template:



The ratings you generate for each area should factor in the following:

- The effectiveness of any existing controls you currently have in place
- The motivation, capabilities and resources available to the identified threat
- Whether the potential consequences will be short-term or long-term, or both
- The vulnerabilities that exist across your organisation individually and in aggregation

The ProtectUK Approach encourages you to use your best judgement to provide impact ratings across risks. This takes account of the understanding you have generated of the risk so far and your knowledge of the existing controls you already have in place to manage that risk.

The ratings you generate should reflect the level of impact experienced by your organisation **with** current controls in place to enable you to establish the severity of each scenario in the current context of your organisation.

As with the assessment of likelihood, your impact ratings should be informed by the best available evidence. You should consider engaging with various evidence sources before making your judgement. Some typical evidence sources include:

- **Staff, stakeholders and support networks**

Staff working at both a strategic and operational level can offer valuable insight into the damage that may follow a security incident, including the impact that this may have on day to day activities. Particular departments and / or roles may also be able to provide insight across different impact type e.g. HR departments, Legal, Finance, IT and security teams.

- **Research literature and open research sources**

Academic publications, journal articles and open government sources provide a general evidence base on the impact / consequences of security incidents. These resources can be utilised to inform your decision-making.

- **Table-top exercises and scenario-based tools**
  Table-top exercises and scenario based tools can help your organisation evaluate the outcomes of different incident scenarios, including how and when different impacts might occur. This is achieved by generating different scenarios that you can use to test and practice your response to a variety of attacks. These tools can also help to identify vulnerabilities and events.

Example Rating

Let's consider how a 'major' score may have been determined for risk **R3**. This risk is concerned with a potential CBR attack:

Reference	Risk Description	Threat	Existing Controls	Likelihood	Impact	Risk Score
R3	Because our local suppliers lack a food defence programme, food and drink could be contaminated and consumed by customers in a CBR attack, resulting in loss of life and exposure to prosecution for food safety failings. This will harm our reputation and ability to trade, decreasing our profits	CBR	• Staff trained in food safety, including contamination • Regular inventory checks undertaken to detect damage and tampering	Very unlikely	Major	

The consequences previously identified for R3 include loss of life and exposure to prosecution for food safety failings. This was seen to expose the organisation to reputational damage and decreasing profits.

The consequences explored during the risk identification phase provide an indication of the impact that this risk will have on the organisation. However, in order to determine an overall impact rating, R3 needs to be measured against the different impact types included in the ProtectUK Impact Criteria. This will help determine the severity of loss or harm that may be caused by this risk being actualised. These ratings will also need to take account of the effectiveness of any existing control measures.

In the case of R3, each one of these impact types has been deemed relevant to the risk being explored, so a score has been provided for each area.

You will see from the completed scoring card that a 'major' rating has been assigned under a number of impact types. These scores have been assigned in recognition of the organisation's existing control measures. These are currently considered to be working effectively to control the severity of the risk. For example, the regular inventory checks and training undertaken by staff are considered to help limit the potential for contaminated food to be consumed by customers. As staff are trained to identify and respond to potential contaminants, the organisation does not expect

multiple loss of life to occur. As such, catastrophic levels of disruption and harm are not expected across the organisation. This rationale is reflected in the ‘major’ scores assigned across each of the impact types.

If no controls were in place, you would expect to see a catastrophic rating applied across the majority of these impact areas as nothing is working to reduce the severity of loss or harm.

As the ‘major’ rating is the highest assigned score, this has been noted in the ‘Highest Rating’ column in the scoring card and has been transferred to the Risk Assessment Template ‘Impact’ column.

Your output at this stage should be: a list of risk statements with corresponding threats, existing control measures and likelihood and impact ratings

Step 2D: Analysing and Evaluating Risk

With your impact and likelihood ratings recorded, you are now in a position to analyse and evaluate the risks facing your organisation.

This requires you to combine the likelihood and impact scores you have generated produce an overall risk rating. This is an **inherent risk score**. Inherent risk is the current risk level with existing controls in place.

Using the ProtectUK Approach, this step is carried out with the use of a 4x4 Risk Matrix. This will help you plot risks according to their likelihood and impact scores. The axis of this matrix reflect the four point scales used to measure likelihood and impact in previous steps:

Likely	Medium	High	Very High	Critical
Possible	Medium	Medium	High	Very High
Unlikely	Low	Medium	Medium	High
Very unlikely	Low	Low	Medium	Medium
	Minor	Moderate	Major	Catastrophic

The structure of the ProtectUK Risk Matrix reflects a minimalist risk appetite – the preference is for very safe options regarding risk. As such, there are only three low risks included in this matrix.

In order to determine whether a risk is acceptable, the ProtectUK Matrix establishes four risk bands with specific decision rules. These decision rules correlate with the colour codes used with the

ProtectUK Matrix:

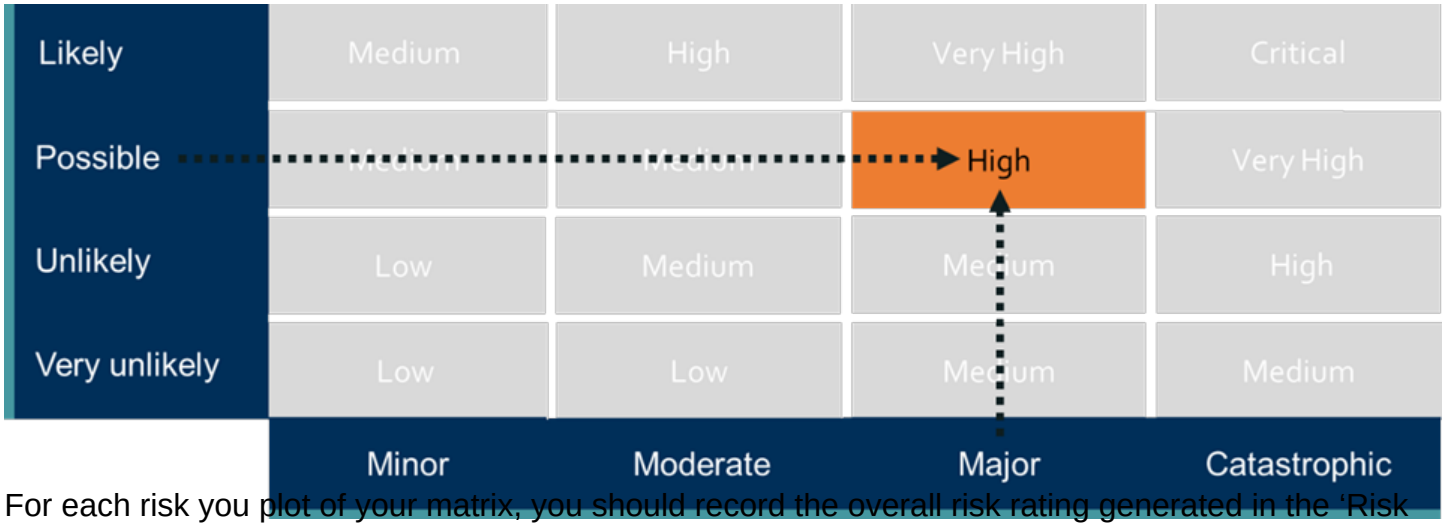
Rating	Description
Very High	Unacceptable risk. Requires urgent treatment.
High	Unacceptable risk. Action to be taken as soon as possible.
Medium	Tolerable only if the cost of reduction exceeds the improvement gained.
Low	Acceptable with periodic review

As you become more familiar with the risk assessment process, you may choose to adopt a matrix of a different size or structure. You may also choose to adapt your risk bands by including more or less levels, or by outlining different forms of action. How you choose to define your risk bands is known formally as your **risk acceptance criteria.**

You should consider adjusting your approach to analysing and evaluating risk once you are confident with the process below. Further information on risk matrices and adapting your risk acceptance criteria can be found in Section 2 of this guidance.

In order to generate an overall risk rating for each risk, you should combine the likelihood rating with the impact rating in the ProtectUK Risk Matrix.

For example, a risk that has been rated with a ‘possible’ likelihood and a ‘major’ impact would generate a ‘high’ risk rating:



For each risk you plot of your matrix, you should record the overall risk rating generated in the ‘Risk

Score' column of your template:

Reference	Risk Description	Threat	Existing Controls	Likelihood	Impact	Risk Score
R1	Because we lack a review process for our security procedures, our response to actual and suspected security incidents could become outdated and ineffective, resulting in loss of life and exposure to prosecution for negligence. This will harm our reputation and ability to trade by reducing customer confidence, profits and available resource	All Threats	• None	Possible	Catastrophic	Very High
R2	Because our IT lacks requirements for strong passwords, our systems could be hacked and sensitive customer data stolen by a cyber-attacker, resulting in fines and penalties from the ICO, which will harm our profit margins and customer confidence	Cyber	• Passwords for log on • Staff briefed on basic information security • ACT e-learning	Possible	Major	High
R3	Because our local suppliers lack a food defence programme, food and drink could be contaminated and consumed by customers in a CBR attack, resulting in loss of life and exposure to prosecution for food safety failings. This will harm our reputation and ability to trade, decreasing our profits.	CBR	• Staff trained in food safety, including contamination • Regular inventory checks undertaken to detect damage and tampering	Very unlikely	Major	Medium

Your output at this stage should be: a list of risk statements with corresponding threats, existing control measures, likelihood and impact ratings, and an overall risk score.

Step 2E: Prioritising Risks

The final activity in this stage of the risk assessment process requires the establishment of a prioritised list of risks for treatment. This list should be contained within a **risk treatment plan.**

A risk treatment plan specifies the order in which risks should be treated and how the chosen treatment option for each risk will be implemented and monitored.

Your risk treatment plan is contained within Part II of the ProtectUK Risk Assessment Template. You will be working with this section of the template for the remaining steps in the risk assessment process:

Reference	Treatment	Rationale	Further Action	Likelihood	Impact	Residual Risk	Risk Owner	Review Date

Before proceeding to select how you will treat risk, you must first bring together your prioritised list. To avoid duplicating the first part of your risk assessment, you should record the relevant risk reference number only when placing your risks in order of priority:

Reference	Treatment	Rationale	Further Action	Likelihood	Impact	Residual Risk	Risk Owner	Review Date
R1								
R2								
R3								

Using the ProtectUK Approach, the risks you will typically prioritise will be those that have been assigned a ‘very high’ or ‘high’ rating. These have been determined as unacceptable against the ProtectUK Risk Criteria. In general, this means that the higher the level of risk, the sooner any action relating to risk treatment will need to take place. In the template above, R1 will receive priority for treatment as this carries a ‘very high’ risk score. This is followed by R2 with a ‘high’ risk score and R3 with a ‘medium’ risk score.

Any risks that have fallen within an acceptable range i.e. ‘low’ risks are still required to be listed in your risk treatment plan. Although these risks may not require treatment, they will still need to be periodically reviewed to ensure they remain at an acceptable level.

This action completes the risk assessment stage of the RMP. You have successfully analysed and evaluated the risks facing your organisation. This has enabled you to generate a prioritised list of risks for treatment. You will now look to develop and action your risk treatment plan in the next stage of the process: Treat the Risks.

Your output at this stage should be: a list of prioritised risks identified by their risk reference numbers.

KEYWORDS

RISK MANAGEMENT
RISK ASSESSMENT
RISK
RESPONSE
PROTECTIVE SECURITY

PAGE CATEGORY

SECURITY RISK MANAGEMENT