ProtectUK

Stage 3: Risk Treatment

ProtectUK publication date

21/03/2024

The third stage of the risk assessment process involves treating risk.

To achieve this, you will be using your professional judgement to select a risk treatment option and appropriate control measures.

A control is any measure or action that maintains or modifies risk.

Once you have decided on a risk treatment option, you will then calculate a new risk score. This score will based on the controls and further actions you have planned and implemented. This is known as your **residual risk score**.

Residual risk is the level of risk that remains after additional controls have been applied. This is calculated in the same way as inherent risk i.e. likelihood x impact = risk. Calculating residual risk enables you to see the effect of the control measures you have implemented to manage risk.

Finally, you will assign a risk owner and review date to each risk to ensure that the actions you generate are completed within a reasonable time-frame by an individual you deem competent.

This stage of the risk assessment process is supported by Part II of the ProtectUK Risk Assessment Template. The ProtectUK Control List and Menu of Tactical Options (MoTO) also act as additional supporting resources.

Step 3A: Selecting Treatment Options

For each risk listed in your risk treatment plan you will need to determine an appropriate treatment option.

There are four main options for treating risk that you will need to consider:

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 considering the transfer of sensitive information to a new cloud service provider 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 share the entire amount of risk.

Risk sharing involves delegating the responsibility of implementing a 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.

Deciding Between Options

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

The ProtectUK Approach utilises judgemental reasoning to make such assessments. This is based on the understanding you have gained from assessing each risk and the risk treatment options available to you.

As you become more familiar with the risk assessment process, you may choose to utilise other

techniques to help you decide between options. For example, formal cost / benefit analysis or decision trees. Some additional techniques are also provided in ISO 31010 which you may also wish to consult.

You should consider alterative techniques for helping you decide between options once you are confident with the process below. Further information on risk management techniques can be found in Section 2 of this guidance.

When deciding between treatment options, you may find it helpful to work through the following questions:

- What impact does each option have on your business objectives?
- What are the expected benefits of each option?
- Which options align best with your appetite for risk, risk acceptance criteria and stakeholder expectations?
- What disadvantages are associated with each option?

Once you have selected an appropriate risk treatment option for each risk, you should record this in your template under the ‘Treatment’ heading. You should also outline your rationale for your selected option under the ‘Rationale’ heading:

Your output at this stage should be: a list of prioritised risks identified by their reference number with a risk treatment option selected

Step 3B: Determining Appropriate Controls

The next activity in the risk treatment stage requires you to select the control measures that will help you reduce risk to an acceptable level in your organisation. These controls may be **physical** or **active:**

- **Physical controls** relate to building and infrastructure, equipment and technology.
- **Active controls** are procedural and concerned with what people do on site and how they do it.

You will need to determine the most appropriate control measures for each risk based on the risk treatment option you have selected.

One or more controls should be applied to each risk listed in your risk treatment plan.The controls you select may be new to your organisation, or they could be controls that already exist.

When selecting controls, you may choose from a control list, such as the ProtectUK Control List or Menu of Tactical Options. You are also free to use ‘custom’ controls that sit outside of these control lists. If selecting a ‘custom’ control for implementation, the description used to capture the control should clearly communicate what the control is and how it is working to control risk. If using a control from the ProtectUK Control List or MoTO, you may reference the particular control reference in your template.

Example MoTO Controls

Remember, a control includes any action or measure that maintains or modifies risk. This could be a control measure selected from an appropriate source or a particular form of action that you are taking

to modify or maintain risk. For example, monitoring a risk to ensure it remains at an acceptable level.

To help you avoid duplicating a control that is already working to control risk, you should refer to the existing controls identified in your Risk Assessment Template when completing this step.

Each control you select should be checked to determine if it is necessary by considering the effect it has on the likelihood or impact of a risk and the overall risk level. A necessary control is one that has more than a negligible effect on the risk being considered.

When determining the controls necessary to treat risk, you will need to decide the balance between the cost of investment and accepting the consequences that may follow if the risk is actualised. You should consider these costs in relation to individual risks and across your risk treatment plan as a whole.

As with other stages of the RMP, you may find it helpful to consult with management and staff, security specialists / experts, local and national bodies, and your wider community support networks (neighbouring businesses, sectors etc.) when considering controls. These individuals may be able to provide you with additional advice or information that can help you in your selection of appropriate controls.

Describing Controls

The controls you select should be recorded in your template under the ‘Further Actions’ column. These descriptions should include the following:

- A clear description of the control(s) you have selected
- How you intend to implement the control(s) and when, including details of those responsible for the implementation

- The resource required and any constraints
- When the actions are expected to be completed

Your output at this stage should be: a list of prioritised risks identified by their reference number, a selected risk treatment option, and a description of further actions, including selected controls.

Step 3D: Calculating Residual Risk

Residual risk refers to the risk remaining after risk treatment.

The calculation of residual risk enables you assess the effectiveness of the treatment you have put in place. This will help you decide whether the remaining risk is acceptable or not to your organisation.

In order to determine residual risk, you should consider the likelihood and impact of each risk in light

of the existing controls you have in place and the new controls you are looking to introduce.

Following this calculation, you will then need to decide whether the residual risk that remains is acceptable to your organisation, or whether further risk treatment is required.

Your residual risk score is calculated in the same way as your inherent risk score i.e. likelihood x impact = risk. This requires you to return to your reference scales and risk matrix in order to generate your new score. The results of this new calculation should then be compared with the ProtectUK risk acceptance criteria in order to determine acceptability.

Where a risk remains at an unacceptable level – either because all treatment options have been exhausted, or because the financial cost of treatment is too great compared to the expected loss or harm – then the residual risk will need to be accepted. However, these risks should still be subject to ongoing monitoring.

You should make note of your newly assessed likelihood and impact scores and your residual risk score in your template.

Example Rating

Let’s consider how the residual risk score has been determined for risk R1. This risk is concerned with a potential attack from all terrorist threat types:

Reference	Treatment	Rationale	Further Action	Likelihood	Impact	Residual Risk	Risk Owner	Review Date
R1	Reduce	Beyond level of risk acceptance	• Implement PUK Control A3 & A5 • Review procedure to be established and cascaded to senior leaders by store manager	Very Unlikely	Major	Medium		

In the case of R1, there has been a reduction in likelihood from ‘possible’ to ‘very unlikely’. There has also been a reduction in impact from ‘catastrophic’ to ‘medium’.

These new scores have been generated in light of the control measures introduced by the organisation. This includes ProtectUK control A3, which introduces a measure to review policies, and ProtectUK control A5, which introduces a similar measure to review procedures.

As these control measures directly address the vulnerability identified i.e. a lack of review procedures, there has been a reduction in both the likelihood and impact scores assigned.

Of course, there is still a possibility that a gap or weakness could emerge outside of the review times set by the organisation. However, as the organisation has taken the necessary steps to ensure that up to date policies and procedures are in place, this is no longer expected to cause catastrophic levels of impact.

With these new scores, R1 has now been reduced to a ‘medium’ level risk:

In line with the ProtectUK risk acceptance criteria above, this risk would be acceptable to the

organisation if there are no further controls that could be implemented to reduce this score. The improvement gained from implementing any additional controls would need to exceed the cost of the measures introduced in order to be considered necessary.

It is not always possible to treat a risk further, particularly when the costs outweigh the expected benefits. In the case of R1, the organisation may decide that additional controls are unnecessary as these would not bring any significant improvement. As such, the organisation would look to accept the residual risk.

Your output at this stage should be: a list of prioritised risks identified by their reference number, a selected risk treatment option, a description of further actions, including selected controls, and a residual risk score.

Step 3D: Assigning a Risk Owner and Review Date

To complete your risk treatment plan, you will need to designate an overall risk owner for each risk and a suitable review date. This will help to ensure accountability for the implementation of your risk treatment plan and the risk management process as a whole.

Assigning a risk owner

A risk owner is a person or entity with the accountability and authority to manage risk. The owner you assign may be a member of the senior management team or an individual who has expertise and

oversight over a particular area of business. You may also assign yourself as a risk owner (where relevant).

If assigning a risk owner other than yourself, all expected actions and timelines for delivery should be clearly communicated to the risk owner. This includes exchanging and sharing information about the results of the risk assessment and risk treatment plan. Risk owners should also understand the risk management process as a whole and their roles and responsibilities within this.

Assigning a review date

For each risk in your risk treatment plan, you should assign an appropriate date for review. This decision may be based on the severity of the risk and/or the risk treatment option selected.

Reviewing your risks is an essential part of the risk management process. This action enables you to verify that the actions and controls in your risk treatment plan have been successful. Further information on reviewing risk will be discussed the next stage of this guidance.

The risk owners and review dates you assign should be clearly recorded in your risk treatment plan:

This completes the risk treatment stage of the RMP. You have successfully developed a risk treatment plan for the risks facing your organisation. The importance of recording your actions will now be discussed in the next stage of the process: Record the Risks.

Your output at this stage should be: a list of prioritised risks identified by their reference number, a selected risk treatment option, a description of further actions, including selected controls, a residual risk score, and an assigned risk owner and review date.

KEYWORDS

RISK MANAGEMENT

RISK ASSESSMENT

RISK

RESPONSE

PROTECTIVE SECURITY