ProtectUK

Stage 5: Review

ProtectUK publication date
21/03/2024

The final stage of the risk assessment process is concerned with reviewing your actions.



This stage captures two core activities: **risk reviewing** and **risk monitoring**.

A **risk review** enables you to determine whether your risk treatment plan can be considered successful based on the reduction of risk to an acceptable level. This occurs shortly after the risk assessment has taken place.

Risk monitoring is an ongoing process that periodically verifies the status of the risks you have identified.



Risk reviews

It is often assumed that once a risk is treated that it requires no further action. However, without returning to the risk assessment, there is no way of knowing whether or not this is true.

In order to verify that the risk treatment you have implemented is effective in terms of design, operation and cost, you should return to your risk assessment to review your risks following the selection and implementation of controls.

To determine whether your treatment plan has been effective, you should consider each of your risks in turn and recalculate the level of residual risk based on your actions and measures. This will enable you to verify that the controls you have introduced have successfully reduced the impact or likelihood of risk.

It may not be possible to undertake a risk review in one sitting if you have a high number of risks. To

make this task more manageable, you may choose to stage your review process over several days, or review risks in aggregation. For example, choosing to prioritise the review of risks that have been identified as ‘very high’ and ‘high’ to ensure the most severe risks are reviewed first.

If a re-calculated risk has been reduced to an acceptable level then your risk treatment plan can be considered successful. If the risk remains at an unacceptable level then corrective action will need to be taken to address this. This requires that you revisit the controls you have implemented and introduce additional controls to help modify the risk to an acceptable level. All actions you undertake should be clearly documented in your risk treatment plan.

Risk monitoring

Risks are not fixed. The scenarios you imagine, the threats you face, and the elements that make up risk themselves can change suddenly and unexpectedly.

It is essential that you monitor risk to detect any change that may occur as a result of your organisation’s internal and external environment or the overall threat landscape. These changes may include, but are not limited to:

- changes to your legal and regulatory environment
- a change in your overall attitude toward risk and what is or is not acceptable
- new sources of risk and identified vulnerabilities
- changes in your operating environment that open up new opportunities for attack
- increase in terrorist related incidents or a change in the threat level

Major changes could produce new risks that need to be carried through the risk assessment process, or they may increase risks that you have previously assessed. This could result in risks no longer falling within the limit of acceptability that you have defined. Any risk that moves from an acceptable to unacceptable position should be treated using a treatment option outlined in Stage 3 of the risk assessment process.

As with the risk review process, any actions and decision-making around these risks should be captured in your risk assessment.

When determining when to undertake risk monitoring you should consider the level of residual risk and the risk treatment option selected. Generally, the higher a risk, the more frequently monitoring should take place. You should also be mindful of any risks you have chosen to retain or tolerate.

Risk monitoring is an ongoing process. It should be regularly repeated to confirm that the risks you have identified remain within an acceptable level and that the treatment options you have selected

are still appropriate.

You may find that following a decrease in threat level that some of the additional controls you have implemented are no longer required. For example, you may have introduced a number of enhanced controls using the Menu of Tactical Options. An active process of risk monitoring would enable you to remove these controls at the earliest opportunity rather than leaving them in place beyond your organisational requirements.

You should regularly return to risk assessment to monitor risks and set new review dates.

KEYWORDS

RISK MANAGEMENT
RISK ASSESSMENT
RISK
RESPONSE
PROTECTIVE SECURITY

PAGE CATEGORY

SECURITY RISK MANAGEMENT