CPNI
Centre for the Protection of National Infrastructure

SCA FOR

ORGANISATIONAL SECURITY MINDEDNESS

MANAGING THE SCA PROCESS

A SCA can be undertaken to understand how well security mindedness is embedded and implemented across an organisation.

The individual responsible for initiating and managing the SCA process on behalf of the commissioning organisation should ensure that an appropriately qualified and experienced specialist or small team of two or more specialists is appointed to undertake a SCA (see 'Undertaking a Security Considerations Assessment').

It is important that sufficient notice of when a SCA will be required is given, with each of the relevant parties agreeing a timeframe for completion.

THE SCA STAGES

The Stage 1 SCA can be undertaken at any point and provides an opportunity to review the nature, and implementation, of the security-minded approach already in place or the potential need for such an approach to be adopted.

A Stage 2 SCA should be undertaken if recommendations to address issues identified in the Stage 1 SCA have been made and subsequently adopted, whether in whole or in part, by the commissioning organisation.

There is no Stage 3 SCA for this type of activity.

The Stage 4 SCA allows the implementation of the security-minded approach adopted to be reviewed and relevant improvements to be made.

Additional SCAs can be undertaken if there is concern or awareness that the nature of the threats or vulnerabilities has altered since the last SCA was undertaken. Under these circumstances, the list of documentation that would be provided for the Stage 4 SCA should be provided.

STAGE 1 SCA

Timing

A Stage 1 SCA can be undertaken at any time in an organisation's life when there is desire to understand the extent to which security mindedness is embedded and implemented across an organisation.

Scope

The Stage 1 SCA should:

1. list the information provided and record the information that is not available, noting the reason for this where provided;
2. review the risk assessment documentation to identify any potential weaknesses in the process, in particular:
    a. any threats, vulnerabilities or risks which it would be appropriate and proportionate to include; and
    b. whether the documentation provides a robust record of the risk assessment process and outcome;
3. consider how risk mitigation measures are reflected in policies and processes;
4. identify and detail any gaps and inconsistencies within, and between, the documentation, policies and processes provided;
5. assess how policies and processes are being conveyed to those who need to follow them;
6. review the effectiveness of the security measures implemented with an examination of any security breaches or incidents, including near misses;
7. examine the consistency of implementation of security mitigation measures;
8. review security-related monitoring and auditing activities undertaken; and
9. for points 2 to 8 above, provide a summary of all the issues identified and set out appropriate and proportionate recommendations for addressing each issue.

Documentation required

The portfolio of information provided should include:

1. risk assessment and mitigation documentation;
2. details of the security-related processes for the implementation of security-related risk mitigation measures;
3. the policies and processes in place for identifying, and responding to, security breaches and incidents, including near misses;
4. the policies and processes in place for monitoring, auditing, reviewing and updating all security risk management processes;
5. details of any occurrences of security incidents and/or breaches and the actions taken at the time of, and subsequent to, the breach or incident; and
6. copies of reports from security-related monitoring and auditing undertaken.

STAGE 2 SCA (WHERE BEING CONDUCTED)

Timing

A Stage 2 SCA should be conducted once changes made in light of the recommendations from the Stage 1 SCA have been fully implemented.

Scope

The Stage 2 SCA should:

1. list the information provided and record the information that is not available, noting the reason for this where provided;
2. review changes to the security risk assessment and mitigation documentation;
3. consider how changes to security risk mitigation measures are reflected in policies and processes;
4. consider how changes to security-related policies and processes have been communicated to staff and other relevant parties;
5. examine early implementation of the changes.

Documentation required

The portfolio of information provided should include, in addition to the documentation provided in the previous SCA:

1. the previous SCA and SCA response reports;
2. details of changes to:
    a. security risk assessment and mitigation documentation;
    b. policies and processes for the implementation of security-related risk mitigation measures; and
    c. policies and processes for responding to security breaches and incidents;
3. details of how changes to the policies and processes have been communicated to staff and other relevant parties.

STAGE 4 SCA

Timing

A Stage 4 SCA should be undertaken 12 months after the Stage 1 SCA and then at regular intervals thereafter, at a frequency considered appropriate by the commissioning organisation.

Scope

The Stage 4 SCA should:

1. re-examine the previously identified and assessed risks to determine whether there have been any changes, whether for political, economic, social, technological, legal or environmental reasons;
2. review the effectiveness of the security measures implemented to date with an examination of any security breaches or incidents, including near misses;
3. examine the consistency of implementation of security mitigation measures;
4. review security-related monitoring and auditing activities undertaken;
5. review the issues raised in the previous report and reiterate any that have not been satisfactorily resolved and are still believed to be of importance.

Documentation required

The portfolio of information provided for each SCA stage should include, in addition to the documentation provided in the previous SCA:

1. the previous SCA and SCA response reports;
2. a summary of any significant changes to the organisation since the previous SCA that could impact on security requirements;
3. details of any changes to:
    a. those aspects of the organisation that are considered to be sensitive;
    b. risk assessment and mitigation documentation;
    c. policies and processes for the implementation of security-related risk mitigation measures;
    d. policies and processes for responding to security breaches and incidents;
4. details of any occurrences of security incidents and/or breaches and the actions taken at the time of, and subsequent to, the breach or incident; and
5. copies of reports from security-related monitoring and auditing undertaken.

Disclaimer

This guide has been prepared by CPNI and is intended to assist in undertaking a Security Considerations Assessment. This document is provided on an information basis only, and whilst CPNI has used all reasonable care in producing it, CPNI provides no warranty as to its accuracy or completeness.

To the fullest extent permitted by law, CPNI accepts no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using the document. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

CPNI
Centre for the Protection of National Infrastructure