CPNI

Centre for the Protection of National Infrastructure

UNDERTAKING A SECURITY CONSIDERATIONS ASSESSMENT

MANAGING THE SCA PROCESS

The responsibility for initiating, and subsequently managing, the SCA process will depend on the type of activity that is being undertaken.

It is essential that each stage of the SCA is initiated at the correct point in the activity and that there is sufficient opportunity for:

- the SCA to be carried out;
- both the SCA report and SCA response report to be completed; and
- accepted recommendations to be incorporated into the activity.

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. This may be a team of in-house specialists or external consultants.

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 SPECIALIST(S) UNDERTAKING THE SCA

A specialist should:

- have an excellent understanding of the range of potential security issues;
- understand the relationship and interdependencies between personnel, physical and cyber security;
- understand the nature of different threats and the vulnerabilities that the respective threat actors may seek to exploit;
- be experienced in undertaking, and have had responsibility for, risk management at a senior level, including:
  - » developing a clear, comprehensive understanding and assessment of risks;
  - » formulating, assessing, implementing and managing appropriate and proportionate risk mitigation measures;
  - » undertaking audits of documentation, policies and processes;
- know the limitations of their own knowledge and expertise and be prepared to seek specialist advice where necessary; and
- be able to evidence that they have kept their skills up-to-date through suitable continuing professional development.

Where the activity in question has particular sensitivities for national security reasons, the individual appointed to undertake the SCA should hold an appropriate level of security clearance prior to commencing work.

STAGES OF A SCA

The SCA comprises up to four distinct stages:

- **Stage 1** – undertaken at the earliest stage possible in the initiation of an activity;
- **Stage 2** – undertaken immediately on completion of detailed planning and prior to any form of implementation work being undertaken;
- **Stage 3** – undertaken when the implementation of an activity has been fully completed; and
- **Stage 4** – monitoring of an ongoing activity.

The nature of the activity to which it is being applied will determine precisely what each stage will consider. More information on this is available in the activity-specific guidance documentation.

If neither the asset owner/project lead nor the specialist(s) undertaking the Stage 1 SCA identify any security risks that exceed the relevant organisation(s) risk appetite, the subsequent stages of the SCA should focus on whether there has been a significant change in the nature of the activity or the threat landscape that would alter this. Where no change is found to have occurred, this should be documented in the relevant stage SCA report. Under such circumstances, this will complete that stage of the SCA process.

An interim SCA 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 next SCA stage due should be provided.

THE SCA REPORT

A written report should be produced from each stage of the SCA process.

The report should contain:

1. details of the specialist(s) undertaking the SCA;
2. a record of when the SCA was carried out and the state of the activity at the time of the SCA;
3. a list of all the documentation provided by the commissioning organisation;
4. a list of any individuals/teams consulted during the process;
5. details of any other documentation, correctly referenced, relied upon by the specialist(s) as part of the SCA process;
6. a section on each issue identified that sets out:
    a. a summary of the issue identified;
    b. the nature of potential problems that may arise from that issue with an assessment of their severity and likelihood; and
    c. associated proportionate and viable recommendations to remove or mitigate the issue.

The use of the word ‘must’ should be avoided in the recommendations contained within the report.

A draft version of the report should be submitted to the commissioning organisation to allow for an opportunity for any issues and recommendations to be discussed and, where necessary, clarified with the specialist(s). Where the specialist(s) feels that it is right to amend the SCA report in light of these discussions, this should be done prior to the report being finalised and issued.

A record of the outcome of any such discussions should be made, agreed, signed and dated by the participants, and added as an appendix to the SCA response report.

It is recommended that the SCA report be marked in line with the individual organisation’s classification and handling caveats.

HOW LONG IS SCA VALID?

The SCA response report is produced by the commissioning organisation in response to the recommendations contained in the SCA report.

The SCA response report should include:

1. details of the representatives from the commissioning organisation who produced the SCA response report;
2. the stage of the SCA, the document reference and date of the SCA report that the response report considers;
3. a section on each issue and associated recommendations raised in the SCA report that sets out:
    a. whether the issue is accepted or not;
    b. whether the recommendations made by the SCA report to remove or mitigate the issue are accepted;
    c. details of any alternative recommendations for consideration; and
    d. appropriate reasoning where the issue and/or recommendations are rejected.

An issue highlighted by the SCA report might not be accepted if the commissioning organisation believes that the issue is:

- insignificant; or
- outside the scope of the SCA.

A suggested mitigation measure might be rejected by the commissioning organisation if it is believed to be:

- not suitable (for example for economic, contractual, legal, ethical or environmental reasons); or
- technically not feasible.

The commissioning organisation is responsible for ensuring that any SCA recommendations do not compromise any statutory or regulatory requirements prior to their implementation.

The commissioning organisation should issue a draft of the SCA response report to the specialist(s) who wrote the SCA report to allow for an opportunity for any points of disagreement to be discussed and, where possible, resolved to the satisfaction of both parties. A record of the outcome of any such discussions should be made, agreed, signed and dated by the participants, and added as an appendix to the SCA response report.

Once completed, the SCA response report should be issued to, and signed off by, the senior management team/project director.

It is recommended that the SCA response report be marked in line with the individual organisation's classification and handling caveats.

THE SCA RESPONSE REPORT

A SCA will be valid for as long a period of time as the risks are perceived to remain the same, and/or the related risk mitigation measures remain unchanged.

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