

CPNI

Centre for the Protection
of National Infrastructure

SCA FOR

ONGOING OPERATION, MANAGEMENT AND MAINTENANCE OF EXISTING CONNECTED, SMART AND AUTONOMOUS ASSETS



MANAGING THE SCA PROCESS

A SCA can be carried out during the ongoing operation, management and maintenance of existing smart, connected and autonomous assets to look at the nature of the security-minded approach being adopted in relation to them.

A suitable individual who will be responsible for initiating and managing the associated SCA process should be nominated. The individual fulfilling this role should be employed by, or report directly to, the asset owner's 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 in the ongoing operation, management and maintenance of smart, connected and autonomous assets. It 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.

Interim 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.

Additional SCAs can be included as part of the procurement process for consultants or contractors or for the procurement of specialist contractors supplying, or with access to, sensitive assets.



STAGE 1 SCA

Timing

The Stage 1 SCA can be undertaken at any point in the ongoing operation, management and maintenance of a smart, connected or autonomous asset.

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 security 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 security risk mitigation measures are reflected in policies and processes of the operation, management and maintenance of the built asset;
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; and
6. for points 2 to 5 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. a summary of the assets and the extent of connectivity, automation and autonomy within each;
2. details of any protection measures in place;
3. documentation relating to:
 - a. the identification of those particular systems where further protection may be required, including identification of those that are deemed critical;
 - b. the identification of any data and information arising from the assets that needs to be protected for legal, commercially sensitive or security reasons;
 - c. security risk assessment and mitigation;
 - d. policies and processes for the implementation of security-related risk mitigation measures;
 - e. policies and processes for responding to security breaches and incidents; and
 - f. identification of information already in the public domain;
4. the processes for communicating security-related policies and processes to staff and other relevant third parties;
5. the policies and processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
6. the policies and processes in place for monitoring, auditing, reviewing and updating security risk management processes.

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;
 - 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 security 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 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 including the assets involved and the extent of connectivity, automation and autonomy within each;
3. any changes in, or additions to, the systems protected and/or deemed critical;
4. documentation relating to any changes in, or additions to, the data and information protected for legal, commercially sensitive or security reasons;
5. a summary of any changes to the protective security measures in place;
6. details of any changes to:
 - a. security risk assessment and mitigation documentation;
 - b. policies and processes for the implementation of security-related risk mitigation measures;
 - c. policies and processes for responding to security breaches and incidents;
7. 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
8. copies of reports from security-related monitoring and auditing undertaken.

ADDITIONAL SCAS – PROCUREMENT OF CONSULTANTS AND/OR CONTRACTORS

Timing

The first stage of this additional SCA should be undertaken prior to the issue of any tender for consultants or contractors to support the project in question. The second stage should form part of the selection and final appointment process.

Scope

Prior to the issue of tender documentation, the additional SCA should review the security requirements set out in the tender documentation against the agreed security risk mitigation measures.

During the selection and appointment process, the additional SCA should:

1. assess the completeness of the submission documentation that relates to the security requirements;
2. identify and detail any issues that have not been addressed or appear to have been addressed insufficiently;
3. assess the consultant's or contractor's ability to deliver the relevant security mitigation measures and the extent of any support needed to enable them to fulfil the security requirements; and
4. provide a high-level assessment of the consultant's or contractor's organisational readiness to implement the required security measures.

Documentation required

The portfolio of information provided should include:

1. the tender documentation; and
2. the parts of the submission documentation that relate to the security requirements set out in the tender information.

You may use or reuse this content without prior permission but must adhere to and accept the terms of the Open Government Licence for public sector information. You must acknowledge CPNI the source of the content and include a link to the Open Government Licence wherever possible. Authorisation to reproduce a third party's copyright material must be obtained from the copyright holders concerned.

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.