CPNI
Centre for the Protection of National Infrastructure

Security Considerations Assessment

PUBLISH DATE:
June 2019

CLASSIFICATION:
Official

Security Considerations Assessment

Version number 4

Contents

Disclaimer

CPNI has taken every care in preparing this protective security advice which is informed by intelligence on the threat. However, CPNI cannot accept any liability to any person or company for any financial loss or damage arising from the use of this advice or from any failure to give advice.

Freedom of Information Act (FOIA)

This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to CPNI. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 2018.

Disclaimer

CPNI has taken every care in preparing this protective security advice which is informed by intelligence on the threat. However, CPNI cannot accept any liability to any person or company for any financial loss or damage arising from the use of this advice or from any failure to give advice.

Freedom of Information Act (FOIA)

This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to CPNI. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 2018.

Executive Summary

The Security Considerations Assessment contributes to having robust, evidence-based and documented processes relating to the identification and, where applicable, development and ongoing management of security-related vulnerabilities.

It is important to protect people, buildings, infrastructure, information, and the systems that support businesses and services, from those with hostile and malicious intent, whether they use physical and/or cyber-attack methods.

The decreasing separation between the physical and technological aspects of the environment, assets and services means that security issues can no longer be siloed as personnel, physical or cyber. Increasingly, if measures are to be effective in addressing the security risks, a multi-layered approach that includes consideration of personnel, physical or cyber security, as well as good governance, is required.

However, for any such measures to be introduced, an organisation must first appreciate and recognise that security threats, vulnerabilities and the potential resultant risks are something they need to consider and understand.

The Security Considerations Assessment (SCA) process has been developed to encourage this consideration being given across a range of activities and processes where security is not the primary focus, and, where applicable, to improve documentation of security-related decisions as well as the consistency and quality of implementation. On projects where security is the primary focus and CPNI's protective security processes are being followed, the SCA process can be used to provide a high-level overview and check of their implementation where it is felt that this will add value.

Correctly implemented, the SCA process should lead to fewer security-related changes being required at a later stage in the project or activity. It also aims to limit the re-occurrence of circumstances, decisions and actions that have previously led to a compromise of security in similar situations.

This document is intended for use by those who are accountable and responsible for the creation, planning, design, construction, manufacture, use, operation, management, modification, improvement, demolition and/or recycling of individual assets or products, or the wider built environment, as well as those involved in the provision of related services. It is also for the use of those organisations who wish to embed security-mindedness, or protect their commercial information, personal data and intellectual property, as well as organisations and teams carrying out research and development.

The Security Considerations Assessment process has been developed to encourage consideration of security threats, vulnerabilities and the potential resultant risks across a range of activities and processes where security is not the primary focus and, where applicable, to improve documentation of security-related decisions as well as the consistency and quality of their implementation.

1 Introduction

It is important to protect people, buildings, infrastructure, data and information, and the systems that support businesses and services, from those with hostile and malicious intent, whether they use physical and/or cyber-attack methods.

Robust decisions need to be made regarding when and where measures to mitigate security risks are required. The decision-making process also needs to consider the type and extent of measures that are appropriate and proportionate to the risks, factoring in the decreasing separation between the physical and technological aspects of built environments, buildings, infrastructure and services.

Technological systems are becoming ever more sophisticated with greater levels of connectivity. They also increasingly allow cyber and physical processes to be integrated, with embedded computers and networks monitoring and controlling physical processes that in turn provide feedback to alter the computations themselves. This enables assets and services to respond to changing conditions and demands in real-time and thereby improve delivery. Such processes can be applied across a wide range of disciplines but are already being utilised in traffic management, lighting, HVAC (heating, ventilation, and air conditioning), and safety (fire monitoring and evacuation) systems.

Furthermore, as society has embraced technological advances, the expectation that up-to-date information will be available, and can be obtained as soon as it is required, has grown, not only from individuals but also from business, industry and trade.

It is recognised that this ability to share data and information is important in improving: the effectiveness of service provision and delivery; the quality of decision-making and problem solving, including opportunities for innovation; and collaborative and partnership working.

In combination, these developments bring opportunities for changing the way we deliver, manage, integrate and use assets and services, improve productivity and reduce waste. However, they also bring about inherent vulnerabilities that could be used by those with hostile or malicious intent to cause harm to built environments, organisations, assets, services and/or personnel. They also increase the exposure to losses sustained through inadvertent or negligent, although non-malicious, behaviours.

As a result of this increasingly complex interplay of human, physical and technical factors, security issues can no longer be siloed as personnel, physical or cyber. Instead, if security measures are to be effective in addressing the risks, a multi-layered approach that includes consideration of each of these aspects is required.

The developments described, and the vulnerabilities that arise from these, also mean that there is a need to consider security in a broader range of fields than has traditionally been the case. These fields include:

- the planning, design, manufacture and construction of new assets (including buildings and infrastructure) and public spaces;
- the modification and improvement of existing assets and public spaces;
- the end of life of built assets (including a change in asset owner/occupier) and public spaces;
- the ongoing management and maintenance of existing assets and public spaces;
- the design, implementation and management of connected, smart and autonomous assets, including vehicles;
- data analysis and optimisation; and
- research and development.

Implementation of holistic, appropriate and proportionate security measures can, within each of these fields, assist in:

- enhancing the safety, security and resilience of assets, whether physical or digital, and thereby both individuals and services;
- enhancing the safety, security and resilience of public spaces;
- protecting the safety and security of individuals by safe-guarding personally identifiable information and information that would reveal pattern-of-life; and
- protecting valuable intellectual property and commercial information.

However, for any such measures to be introduced, an organisation must first appreciate and recognise that security threats, vulnerabilities and the potential resultant risks are something they need to consider and understand.

The Security Considerations Assessment (SCA) process has been developed to encourage this consideration being given across the range of activities and processes described, where security is not the primary focus, and, where applicable, to improve documentation of security-related decisions as well as the consistency and quality of implementation. On projects where security is the primary focus and CPNI's protective security processes are being followed, SCA can be used to provide a high-level overview and check of their implementation where it is felt that this will add value.

The aim is to provide a mechanism by which those accountable and responsible for projects, the management of assets, or the design and management of public spaces can be confident, and demonstrate through a fully documented process, that potential security-related vulnerabilities have been identified, assessed and, where necessary, addressed in a manner that is appropriate and proportionate.

Correctly implemented and acted upon, it will facilitate in keeping the number and severity of security incidents to a minimum, as well as ensuring that mechanisms are in place for the early detection of any breaches or incidents. Further, it should lead to fewer security-related changes being required at a later stage and aims to limit the re-occurrence of circumstances, decisions and actions that have previously led to a compromise of security in similar situations.

This document is intended for use by those who are accountable and responsible for the creation, planning, design, construction, manufacture, use, operation, management, modification, improvement, demolition and/or recycling of individual assets or products, or the wider built environment, as well as those involved in the provision of related services. It is also for the use of those organisations who wish to embed security-mindedness, or protect their commercial information, personal data and intellectual property, as well as organisations and teams carrying out research and development. it describes the stages at which a SCA should be carried out and details of what should be considered and reviewed during each.

2 Definitions

Asset

Item, thing or entity that has potential or actual value to an organisation.

An asset may be fixed, mobile or movable. It may be an individual item of plant, a vehicle, a system of connected equipment, a space within a structure, a piece of land, an entire piece of infrastructure, an entire building, or a portfolio of assets including associated land or water. It may also comprise information in digital or in printed form.

The value of an asset might vary throughout its life and an asset might still have value at the end of its life. Value can be tangible, intangible, financial or non-financial.

Asset owner

Individual or organisation that owns the built asset and any associated asset information, is the asset operator or licensee, or is the operator of the system of which the built asset is a component.

Commissioning organisation

Organisation commissioning a SCA.

Hostile reconnaissance

Purposeful observation with the intention of collecting information to inform the planning of a hostile act against a specific target.

Neighbouring built asset

Built assets (and the services that supply them) that share a boundary (including beneath it or overhead) with the built asset under consideration, or that are in the neighbourhood of that built asset but physically separated by a public or private street, public or privately-owned open space or similar feature.

Public realm

Publicly accessible or visible spaces between buildings and civic, transportation and entertainment and leisure places with external and internal public or private land ownerships.

Sensitive data/information

Data/information, the loss, misuse or modification of which, or unauthorized access to, could:

- adversely affect the privacy, welfare or safety of an individual or individuals;
- compromise intellectual property or trade secrets of an organisation;
- cause commercial or economic harm to an organisation or country; and/or
- jeopardise the security, internal and foreign affairs of a nation.

Smart

The application of autonomous or semi-autonomous technology systems to achieve greater utilisation of resources, limiting or reducing per capita resource consumption to maintain or improve quality of life.

Threat

Potential cause of an incident which may result in harm.

Vulnerability

Weakness that can be exploited to cause harm.

3 The Security Considerations Assessment (SCA)

3.1 What is a SCA?

A SCA is a structured process for ensuring that potential security-related vulnerabilities are considered across a range of activities and processes, including the security-minded approach of organisations and supply chains, and that, where applicable, physical, personnel, cyber and cross-cutting security measures are properly embedded.

It considers:

- the process for determining the importance of people, assets, public spaces, products, services, data and information associated with any of the activities listed in 3.3;
- the understanding and analysis of the security-related threats and vulnerabilities to business, communities, individuals, service provision, data and information associated with the activity which is the subject of the SCA;
- the activity-specific security risk assessment and its alignment with any related corporate risk assessments;
- the process by which potential risk treatment options have been identified, analysed and selected;
- the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- the initial, and continued, organisational readiness relative to the security plans and requirements in place; and
- the compliance with, and consistency of the implementation of, the security-related processes by which the portfolio of agreed risk mitigation measures are delivered.

In addition, it assesses, in relation to each of the aspects listed above:

- the process for, and implementation of, monitoring, audit and review, including, when applicable, the mechanisms for implementing change; and
- the completeness and robustness of the associated documentation and the ability of that documentation to withstand scrutiny in the event of a security breach or incident.

The SCA is not a technical check of:

- physical measures intended to protect physical assets, personnel or service delivery or to respond to an incident;
- cyber measures implemented to protect data and information; or
- personnel and people security measures designed to: reduce insider risk; develop and embed a security culture; or disrupt hostile reconnaissance.

3.2 Relationship of the SCA with CPNI protective security processes

There are three CPNI protective security processes: Governance (Protective Security Management Systems); Risk Management (Protective Security Risk Management); and Operational Requirements. All three are linked together and should be used where security is the primary objective of a project as part of implementing effective protective security.

Protective Security Management Systems

Protective Security Management Systems (PSeMS) (see www.cpni.gov.uk/protective-security-management-systems-psems) support a methodical and proactive approach for assessing and managing holistic security risks for senior leadership teams and security managers, providing clear evidence to justify enablers such as additional resources and investment.

PSeMS provide the necessary organisational structure, accountabilities, policies and procedures to ensure an organisation has a systematic approach to managing security risks and effective oversight, incorporating security management into daily activities.

Protective Security Risk Management

The Protective Security Risk Management model (see www.cpni.gov.uk/rmm/protective-security-risk-management) highlights some key steps that should be taken when considering the wider process of protective security risk management.

Operational Requirements

The Operational Requirement (OR) process (see www.cpni.gov.uk/operational-requirements) is a tool which has been developed to enable an organisation to produce a clear, considered and high level statement of their security needs based on the risks they face.

The OR should be preceded by a risk assessment process that uses information about threats and the associated vulnerabilities to prioritise the security risks that an organisation faces. The OR processes uses this prioritised list to develop effective protective security measures.

The role of the SCA in relation to these security processes

The SCA does not replicate any of the processes described above, but where all of these processes have been undertaken, the SCA can be used to look at their scope, their robustness, how well they have been documented and, ultimately, how they have been acted upon or implemented.

Under the circumstances where an organisation has implemented the three protective security processes, it should determine whether also following the SCA process will add value or not. It is recommended that this decision is documented and a copy retained by the organisation.

3.3 Additional uses for a SCA

A robust, fully documented SCA process can also be used by:

- an authority as a means of demonstrating its compliance with Section 17 of the Crime and Disorder Act 1998;
- a planning authority as a means of demonstrating its compliance with paragraph 95 of the National Policy Planning Framework, both in forming planning policies and in making planning decisions; and
- a planning applicant in demonstrating that they have considered security, where applicable, in their application.

3.4 When should a SCA be undertaken?

The SCA process should carried out in relation to the following activities:

a) assessing the security-mindedness of an organisation and/or an existing supply chain;
b) the planning, design, manufacture and construction of new assets (including buildings and infrastructure) and public spaces;
c) the modification and improvement of existing assets and public spaces;
d) the end of life of built assets (including a change in asset owner/occupier) and public spaces;
e) the ongoing management and maintenance of existing assets and public spaces;
f) the design, implementation and management of new connected, smart and autonomous assets, including vehicles;
g) the management of existing connected, smart and autonomous assets;
h) a data analysis and optimisation project that will share and/or publish data or information, whether digital or physical, relating to a built asset, built environment, individuals or groups of individuals, regardless of whether it is intended that it will be anonymised; and
i) a research and development project that utilises data or information, whether digital or physical, relating to a built asset, a built environment, specific individuals or groups of individuals.

A SCA should also be undertaken as part of the procurement process for a consultant, contractor or other part of the supply chain supplying, or with access to, sensitive assets.

If the decision is made not to follow the SCA process, this should be formally recorded and this record retained as part of the project, procurement and/or asset documentation.

3.5 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.

Where the activity involves the creation, modification, improvement or end of life of a building, infrastructure or public space, the asset owner should ensure that processes are in place, and implemented, to initiate the SCA process at the start of any relevant activity. These processes should include the nomination of a suitable individual, specific to the activity being undertaken, who will be responsible for initiating and managing the associated SCA process. The individual fulfilling this role should be employed by, or report directly to, the asset owner's organisation.

Where the activity involves a data analysis and optimisation or research and development project, the project sponsor should be responsible for initiating and managing the SCA process.

When the SCA is being conducted to assess the security-mindedness of an organisation, including its requirements around an existing supply chain, the process can be initiated at any time by the senior management of that organisation.

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.

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.

3.6 The specialist(s) undertaking the SCA

Each SCA should be undertaken by an appropriately qualified and experienced specialist or small team of two or more specialists.

A specialist should:

- have an excellent understanding of the range of potential security issues affecting the business, assets, data and information, personnel and members of the public;
- appreciate the importance, and have experience in the delivery of a holistic approach to security, encompassing aspects of personnel, physical and technological 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;
- be capable of demonstrating experience at a senior level in:
    - developing a clear, comprehensive understanding and assessment of risks;
    - formulating, collating and assessing potential measures to control and minimise risks;
    - implementing of proportionate, structured and auditable management systems; and
    - undertaking audits of documentation, policies and processes; and
- know the limitations of their own knowledge and expertise and be prepared to seek specialist advice where necessary.

They should also 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 have successfully passed an appropriate level of security screening and vetting prior to commencing work.

3.7 Stages of a SCA

The SCA comprises up to 4 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. The details of each SCA Stage are set out later in this document.

Additional SCAs should be undertaken as part of any procurement of consultants and contractors who will have access to a sensitive asset, sensitive data and/or information, and/or high-profile personnel who own, lease, work in, or otherwise occupy, an asset.

The SCA process should always commence at Stage 1, even where it is being undertaken in relation to an existing built asset or portfolio of assets, or where the activity is question commenced prior to the release of this document. In the case of the latter situation, if the activity is close to, or at the end of, the planning/design phase, the Stage 1 and Stage 2 SCA can be combined.

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 initially 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. This is important in ensuring that SCA remains appropriate and proportionate to the specific nature of the activity in question.

The timing of the different SCA stages relative to the work stages within an activity involving the design, manufacture and construction of new assets (including buildings and infrastructure) and public spaces is set out in Table 1 below.

Table 1. The timing of the different SCA stages relative to the work stages of a construction project.

Work stage definitions			**SCA Stage**
RIBA 2013	**Association for Project Management**	**PAS 1192**	
0 Strategic definition	0 Strategy	0 Strategy	Stage 1
1 Preparation and brief	1 Brief	1 Brief	Additional SCA – Procurement of Consultants
2 Concept design	2 Concept	2 Concept	
3 Developed design	3 Definition	3 Definition	
4 Technical design	4 Design	4 Design	Stage 2
5 Construction	5 Build and commission	5 Build and commission	Additional SCA – Procurement of Contractors
6 Handover	6 Handover and closeout	6 Handover and closeout	Stage 3
7 In use	7 Operation and end of life	7 Operation and in use	Stage 4

An interim SCA can be undertaken if there is concern or awareness that the nature of the threats or vulnerabilities have 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 (see Appendix A to Appendix M).

As a minimum, a Stage 1 SCA should be undertaken prior to a planning application for the design, manufacture and construction of a new asset(s) or public space being made.

3.8 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, even when the SCA Report does not relate to an activity undertaken by, or on behalf of, a government department or agency, it should be marked and handled in a manner consistent with the Government Security Classifications.

3.9 The SCA Response 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. provides 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 that are implemented 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, even when the SCA Response Report does not relate to an activity undertaken by, or on behalf of, a government department or agency, it should be marked and handled in a manner consistent with the Government Security Classifications.

3.10 The shelf-life of a SCA

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.

4 The SCA Stages

4.1 Portfolio of information to be provided at each Stage

The portfolio of information required for each SCA Stage, by the type of activity to which it is being applied, is set out in Appendix A to Appendix M of this document.

Where the SCA is being undertaken in relation to a project that forms part of the Critical National Infrastructure and/or is being carried out by an organisation(s) that is exposed to national security threats, the documentation required for a Stage 1 SCA is likely to be contained within that completed in respect of an Operational Requirement (OR) process.

Where any of the documentation listed in the appendices does not exist, this should be stated within the portfolio provided, along with a brief explanation as to the reasons why that related piece of work was not considered necessary.

4.2 Stage 1 SCA

4.2.1 Timing

A Stage 1 SCA should be undertaken at the earliest stage possible in the initiation of the activity, when access to information is generally limited to a small number of people.

Ideally it should be concluded when only those involved in developing strategy associated with the activity, as well as those providing related high-level advisory services, are involved and privy to information about the activity in question. These may include specialist security advisers providing guidance in respect of relevant security threats, vulnerabilities and/or mitigations.

Whenever possible, it should also be completed prior to the release of information to any third-party other than those listed above.

4.2.2 Scope

The Stage 1 SCA should:

1) review the documentation provided to:
    a. gain an understanding of the nature of the project and/or asset in question, as well as the organisations involved;
    b. identify any information that is missing; and
    c. identify where no explanation has been provided for the absence of any requested documentation;
2) assess the completeness of the documentation provided and identify and detail any issues that have not been addressed or appear to have been addressed insufficiently. This should include:
    a. identifying any significant potential sensitivities, threats, vulnerabilities (taking into consideration potential physical, cyber, people- or governance-related issues) and resultant risks that have not been included in the documentation provided;
    b. reviewing the proposed mitigation measures, their holistic nature and their ability to address the risks listed;
    c. assessing the rationale used in determining the risk mitigation measures to be implemented; and
    d. identifying any significant resultant risks that have not been included in the documentation provided;
3) identify and detail any gaps and inconsistencies within, and between, the documentation, policies and processes provided;
4) provide an early, high-level assessment of the organisational readiness to implement any proposed mitigation measures; and
5) provide a summary of all the issues identified and set out appropriate and proportionate recommendations for addressing each issue.

4.3 Stage 2 SCA

4.3.1 Timing

A Stage 2 SCA should be undertaken when the detailed design/planning of the project has been completed, and prior to the start of construction or project implementation.

It provides an opportunity for any security issues to be reviewed and, where necessary, re-elevated.

Where the SCA process is being undertaken in relation to the security-mindedness of an organisation, or ongoing management and maintenance of existing assets or public spaces, 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.

Under these circumstances, the Stage 2 SCA provides an early review of the implementation of the measures adopted and a re-assessment of the security risks.

4.3.2 Scope

The Stage 2 SCA should:

1) review the effectiveness of the security measures implemented to date with an examination of any security breaches or incidents, including near misses;
2) re-examine the previously identified and assessed risks to determine whether any have changed, whether for political, economic, social, technological, legal or environmental reasons;
3) assess whether any new risks have arisen in relation to the project or the asset(s) that will be created;
4) assess the potential effectiveness of the security measures it is proposed will be implemented both in the next stage of the project and, where relevant, on its completion, in order to assess the level of risk remaining. Further actions that are deemed appropriate and proportionate in order to develop and implement new or modified mitigation measures should be recommended; and
5) review the issues raised in the Stage 1 SCA Report. Any that have not been satisfactorily resolved should be identified and where these are still believed to be of importance, they should be reiterated in the Stage 2 SCA Report.

4.4 Stage 3 SCA

4.4.1 Timing

The Stage 3 SCA should be undertaken on completion of construction or when the project is substantially complete.

There is no Stage 3 SCA in relation to the security-mindedness of an organisation.

4.4.2 Scope

Where a project has created a built asset, a Stage 3 SCA should:

1) review the effectiveness of the security measures implemented to date with an examination of any security breaches or incidents, including near misses, that have occurred since the Stage 2 SCA was undertaken;
2) re-examine the previously identified and assessed risks to determine whether any have changed, whether for political, economic, social, technological, legal or environmental reasons;
3) assess whether any new risks have arisen in relation to the project or the asset(s) that has been created;
4) assess the level of risk remaining to the asset, its occupants and visitors, the services it provides and any related data and information; and
5) recommend any further actions that are deemed appropriate and proportionate in order to develop and implement new or modified security mitigation measures.

In the case of a data analysis and optimisation or research and development project, the Stage 3 SCA provides an opportunity to limit the re-occurrence of decisions and actions that have previously led to a compromise of security and potentially thereby, safety and resilience. The Stage 3 SCA should therefore:

1) review the effectiveness of the security measures implemented, with an examination of any security breaches or incidents, including near misses, that have occurred since the Stage 2 SCA was undertaken;
2) assess the residual level of security risk to the data and information generated during the course of the project;

3) recommend any further actions that are deemed appropriate and proportionate in order to mitigate any residual security risks; and
4) analyse the lessons to be taken forward to future similar projects.

4.5 Stage 4 SCA

4.5.1 Timing

A Stage 4 SCA should be undertaken 12 months after the Stage 3 SCA unless the SCA is being conducted in relation to:

- a data analysis and optimisation project; or
- a research and development project.

In these two cases, the project will have reached the end of its life at the time of, or just after, the Stage 3 SCA has been undertaken and therefore an analysis and summary of lessons to be taken forward to future similar projects will have already been completed.

Where the Stage 4 SCA is being conducted in relation to the security-mindedness of an organisation, or ongoing management and maintenance of an existing built asset or public space, it should be undertaken 12 months after the Stage 2 SCA has been completed.

In the case of built assets, public spaces, connected, smart and autonomous assets, further Stage 4 SCAs should be undertaken at regular intervals and when any security risks that impact on the asset or space, or any sensitive data and/or information associated with them, have changed for political, economic, social, technological, legal or environmental reasons.

4.5.2 Scope

The Stage 4 SCA should:

1) review the effectiveness of the security measures implemented to date with an examination of any security breaches or incidents, including near misses, that have occurred since the Stage 3 SCA was undertaken;
2) re-examine the previously identified and assessed risks to determine whether any have changed, whether for political, economic, social, technological, legal or environmental reasons;
3) assess whether any new risks have arisen in relation to the project or the asset(s) that has been created;
4) assess the level of risk remaining to the asset, its occupants and visitors, the services it provides and any related data and information;
5) recommend any further actions that are deemed appropriate and proportionate in order to develop and implement new or modified mitigation measures; and
6) analyse lessons to be taken forward to future similar projects or assets. The Stage 4 SCA provides an opportunity to limit the reoccurrence of decisions and actions that have previously led to a compromise of security.

5 Additional SCAs – Procurement of Consultants and/or Contractors

5.1 Procurement of consultants

5.1.1 Timing

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

5.1.2 Scope

The SCA should:

1) prior to the issue of tender documentation, review the security requirements set out in the tender documentation against the agreed security risk mitigation measures; and
2) during the selection and appointment process:
    a. assess the completeness of the submission documentation that relates to the security requirements and identify and detail any issues that have not been addressed or appear to have been addressed insufficiently;
    b. assess the consultant's ability to deliver the relevant security mitigation measures and the extent of any support needed to enable the consultant to fulfil the security requirements; and
    c. provide a high-level assessment of the consultant's organisational readiness to implement the required security measures.

5.2 Procurement of contractors

5.2.1 Timing

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

5.2.2 Scope

This SCA should:

1) prior to the issue of tender documentation, review the security requirements set out in the tender documentation against the agreed security risk mitigation measures; and
2) during the selection and appointment process:
    a. assess the completeness of the submission documentation that relates to the security requirements and identify and detail any issues that have not been addressed or appear to have been addressed insufficiently;
    b. assess the contractor's ability to deliver the relevant security mitigation measures and the extent of any support needed to enable the consultant to fulfil the security requirements; and
    c. provide a high-level assessment of the contractor's organisational readiness to implement the required security measures.

Appendix A – Organisational security-mindedness

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- details of the arrangements for the governance, accountability and responsibility for security within the organisation and/or relevant parts of its supply chain;
- the policies and processes for identifying, reviewing and updating critical, including sensitive/high risk/value, sites and assets, including information;
- the process for identifying, reviewing and updating threats to the organisation, its assets and/or the services it provides;
- the process for identifying, reviewing and updating the security risks arising from those threats;
- the process for identifying, reviewing and updating security mitigation measures that are appropriate and proportionate to the identified risks;
- the policies and processes in place to implement, monitor and audit the security mitigation measures;
- the process for identifying, reviewing and updating the security requirements on the supply chain;
- the policies and processes for communicating security requirements to the supply chain, for assessing its ability to successfully implement those security requirements and to identify where additional support may be required;
- the policies and processes for monitoring and auditing the supply chain's implementation of the security requirements;
- the policies and processes for dealing with security breaches and incidents, including the requirements placed on the supply chain; and
- the process for developing, implementing, reviewing and updating a Business Continuity Plan.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- documentation relating to any changes in, or additions to, the documentation listed under A.1.1.1 above; and
- 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.

Stage 3

There is no Stage 3 SCA in respect of the security-mindedness of an organisation.

Stage 4

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- documentation relating to any changes in, or additions to, the documentation listed under A.1.1.1 above; and
- 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**.**

Appendix B - Design, manufacture and construction of a new built asset

Examples of new built assets include: a railway; an office block; a hospital; a school; a military facility; a research facility etc.

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the project being undertaken, initial plans for location, layout, occupation, utilisation and accessibility to members of the public;
- a summary of any neighbouring built assets, highlighting any that are considered sensitive;
- documentation relating to:
    - whether the built asset is considered sensitive, whether in whole or in part;
    - the identification of those particular assets that will need to be protected, including those that are deemed critical;
    - the identification of project-, organisation- and asset-related threats and the project- and built asset-related vulnerabilities that the respective threat actors may seek to exploit;
    - the risk assessment process undertaken in relation to these threats;
    - the identification of risk mitigation options and the selection of measures to be implemented; and
    - any other relevant security corporate risk assessments and risk mitigation option identification and selection;
- where digital engineering techniques are going to be used in the built asset's design, construction and/or management, documentation relating to:
    - the security risk assessment processes undertaken; and
    - the identification of risk mitigation options and the selection of measures to be implemented;
- details of the security-related processes for the implementation of all selected security-related risk mitigation measures;
- the processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes to the project since the Stage 1 SCA, including those relating to the built asset's intended location, layout, occupation, utilisation or accessibility to members of the public;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
    - any changes in the identified threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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

- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes to the project since the Stage 2 SCA, including those relating to the built asset's intended use, layout, occupation or utilisation plans and accessibility to members of the public;
- a summary of all protective security measures implemented;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1 and 2 SCA, documentation relating to:
    - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 4

The portfolio of information provided should include:

- the Stage 1, Stage 2 and Stage 3 SCA Reports and respective SCA Response Reports;
- a summary of any changes since the Stage 3 SCA to the built asset, including those relating to its use, layout, occupation, utilisation and accessibility to members of the public;
- a summary of all protective security measures in place;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1, 2 and 3 SCA, documentation relating to:
    - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Appendix C - Design, manufacture and/or construction of a new public space

Examples of a public space include: a street; a public square/pedestrianised area etc.

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the type of public space being created, including its intended use, any initial plans of layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any proposed vehicular access to the area including by members of the public;
- documentation relating to:
  - the identification of any areas of the public space where protection is required;
  - the identification of threats and environmental vulnerabilities that the respective threat actors may seek to exploit;
  - the risk assessment process undertaken in relation to those threats; and
  - the identification of risk mitigation options and the selection of measures to be implemented;
- where digital engineering techniques are going to be used in the area's design and/or construction, documentation relating to:
  - the security risk assessment process undertaken; and
  - the identification of risk mitigation options and the selection of measures to be implemented;
- the security-related processes for the implementation of all selected mitigation measures;
- the processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- the processes in place for monitoring, auditing, reviewing and updating security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes to the project being undertaken since the Stage 1 SCA, including the type of public space being created, its intended use, layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any proposed vehicular access to the area by members of the public;
- documentation relating to any changes in, or additions to, areas of the public space where protection is required/will be undertaken;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
  - any changes in the identified threats and/or vulnerabilities that the respective threat actors may seek to exploit;
  - any reviews of the risk assessments in place; and
  - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes, since the Stage 2 SCA, to the public space created, including its intended use, layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any vehicular access to the area by members of the public;
- a summary of all protective security measures implemented;
- in relation to each of the security risk management processes reviewed in the Stage 1 and 2 SCA, documentation relating to:
    - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 4

The portfolio of information provided should include:

- the Stage 1, Stage 2 and Stage 3 SCA Reports and respective SCA Response Reports;
- a summary of any changes since the Stage 3 SCA to the public space, including the type of public space created, its use, layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any vehicular access to the area, including that by members of the public;
- a summary of all protective security measures in place;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1, 2 and 3 SCA, documentation relating to:
    - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Appendix D - Modification or improvement of an existing built asset

Examples of existing built assets include: a railway; an office block; a hospital; a school; a military facility; a research facility etc.

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the built asset's current use, including layout, occupation, utilisation and accessibility to members of the public;
- a summary of the project being undertaken, including any changes to current use, layout, occupation, utilisation, or accessibility to members of the public;
- details of any protection measures already in place, whether personnel, physical or cyber;
- documentation relating to:
    - the identification of any change in those assets that will need to be protected or the level of protection required, including identification of those that are deemed critical;
    - the identification of any project-related threats and the vulnerabilities that the respective threat actors may seek to exploit;
    - the risk assessment processes undertaken in relation to any new and pre-existing threats and vulnerabilities;
    - the identification of risk mitigation options and the selection of measures to be implemented;
    - identification of information already in the public domain; and
    - any other relevant security corporate risk assessments;
- where digital engineering techniques are going to be used in the built asset's modification or improvement, documentation relating to:
    - the security risk assessment process undertaken; and
    - the identification of risk mitigation options and the selection of measures to be implemented;
- the security-related policies and processes for the implementation of the selected mitigation measures;
- the processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- the processes in place for monitoring, auditing, reviewing and updating security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes to the project being undertaken since the Stage 1 SCA, including any changes to planned layout, occupation, utilisation, or accessibility to members of the public;
- documentation relating to any changes in, or additions to, protection measures already in place, whether personnel, physical or cyber;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
    - any changes in the identified threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any additional documentation found to already be in the public domain;

- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes, since the Stage 2 SCA, to the project including those relating to the built asset's intended use, layout, occupation or utilisation plans and accessibility to members of the public;
- a summary of all protective security measures implemented;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1 and 2 SCA, documentation relating to:
    - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 4

The portfolio of information provided should include:

- the Stage 1, Stage 2 and Stage 3 SCA Reports and respective SCA Response Reports;
- a summary of any changes since the Stage 3 SCA to the built asset, including those relating to its use, layout, occupation, utilisation and accessibility to members of the public;
- a summary of all protective security measures in place;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1, 2 and 3 SCA, documentation relating to:
    - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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

- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Appendix E - Modification or improvement of an existing public space

Examples of a public space include: a street; a public square/pedestrianised area etc.

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the public space's current use, including layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any vehicular access to the area including by members of the public;
- a summary of the project being undertaken, including any changes to current use, layout, nature of the surrounding area, and vehicular access to members of the public;
- details of any protection measures already in place;
- documentation relating to:
    - the identification of any change in the level of protection required;
    - the identification of any change in the threats and/or environmental vulnerabilities that the respective threat actors may seek to exploit;
    - the risk assessment processes undertaken in relation to any new and pre-existing threats and vulnerabilities; and
    - the identification of risk mitigation options and the selection of measures to be implemented;
- where digital engineering techniques are going to be used in the area's modification or improvement, documentation relating to:
    - the security risk assessment process undertaken; and
    - the identification of risk mitigation options and the selection of measures to be implemented;
- the security-related processes for the implementation of the selected mitigation measures;
- the processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- the processes in place for monitoring, audit, review and update of security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes to the public space's current use, including layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any vehicular access to the area by members of the public;
- documentation relating to any changes in, or additions to, protection measures already in place;
- a summary of any changes to the project being undertaken, including any changes to planned use, layout and vehicular access to members of the public;
- documentation relating to any changes in, or additions to, areas of the public space where protection is required/will be undertaken;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
    - any changes in the identified threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;

- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes, since the Stage 2 SCA, to the public space created, including its intended use, layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any vehicular access to the area by members of the public;
- a summary of all protective security measures implemented;
- in relation to each of the security risk management processes reviewed in the Stage 1 and 2 SCA, documentation relating to:
    - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 4

The portfolio of information provided should include:

- the Stage 1, Stage 2 and Stage 3 SCA Reports and respective SCA Response Reports;
- a summary of any changes since the Stage 3 SCA to the public space, including the type of public space created, its use, layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any vehicular access to the area, including that by members of the public;
- a summary of all protective security measures in place;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1, 2 and 3 SCA, documentation relating to:
    - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Appendix F - End of life of a built asset, including a change in asset owner/occupier

At the end of life of a built asset a SCA should be undertaken where failure to take appropriate measures could result in precise details about risks and mitigation methods being revealed.

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the built asset's current use, including layout, occupation, utilisation and accessibility to members of the public;
- details of any protection measures in place;
- a summary of the project being undertaken;
- details of any protection measures already in place, whether personnel, physical or cyber;
- documentation relating to:
  - the identification of any sensitive assets that will need to be removed and/or asset information that will need to be protected;
  - the identification of any project-related threats and the vulnerabilities that the respective threat actors may seek to exploit;
  - the risk assessment processes undertaken in relation to any new and pre-existing threats and vulnerabilities;
  - the identification of risk mitigation options and the selection of measures to be implemented;
  - identification of information already in the public domain; and
  - any other relevant security corporate risk assessments;
- where digital engineering techniques are going to be used in the built asset's end of life, documentation relating to:
  - the security risk assessment process undertaken; and
  - the identification of risk mitigation options and the selection of measures to be implemented;
- the security-related processes for the implementation of the selected mitigation measures;
- the processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- the processes in place for monitoring, auditing, reviewing and updating security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes to the project being undertaken since the Stage 1 SCA;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
  - any changes in the identified threats and/or vulnerabilities that the respective threat actors may seek to exploit;
  - any reviews of the risk assessments in place; and
  - any changes in the risk mitigation options and/or selection of measures implemented;
  - details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;

- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes, since the Stage 2 SCA, to the project including those relating to the built asset's intended use, layout, occupation or utilisation plans and accessibility to members of the public;
- a summary of all protective security measures implemented; and
- 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.

Stage 4

There is no Stage 4 SCA in respect of the end of life of a public space.

Appendix G - End of life of a public space

At the end of life of a public space, a SCA should be undertaken where failure to take appropriate measures could result in precise details about risks and mitigation methods being revealed.

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the public space's current use, including layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any vehicular access to the area by members of the public;
- a summary of the project being undertaken;
- details of any protection measures in place;
- documentation relating to:
    - the identification of any change in the level of protection required;
    - the identification of any change in the threats and/or environmental vulnerabilities that the associated threat actors may seek to exploit;
    - the risk assessment processes undertaken in relation to any new and pre-existing threats and vulnerabilities; and
    - the identification of risk mitigation options and the selection of measures to be implemented;
- where digital engineering techniques are going to be used, documentation relating to:
    - the security risk assessment process undertaken; and
    - the identification of risk mitigation options and the selection of measures to be implemented;
- the security-related processes for the implementation of the selected mitigation measures;
- the processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- the processes in place for monitoring, audit, review and update of security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes to the project being undertaken since the Stage 1 SCA;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
    - any changes in the identified threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes, since the Stage 2 SCA, to the project including those relating to the built asset's intended use, layout, occupation or utilisation plans and accessibility to members of the public;
- a summary of all protective security measures implemented; and
- 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.

Stage 4

There is no Stage 4 SCA in respect of the end of life of a public space.

Appendix H - Ongoing management and maintenance of an existing built asset

Examples of existing built assets include: a railway; an office block; a hospital; a school; a military facility; a research facility etc.

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the built asset's current use, including layout, occupation, utilisation and accessibility to members of the public;
- details of any protection measures in place;
- documentation relating to:
  - the identification of those particular assets that will need to be protected, including identification of those that are deemed critical;
  - the identification of built asset- or organisation-related threats and vulnerabilities that the respective threat actors may seek to exploit;
  - the risk assessment process undertaken in relation to these threats and vulnerabilities;
  - the identification of risk mitigation options and the selection of measures implemented;
  - identification of information already in the public domain; and
  - any other relevant security corporate risk assessments and risk mitigation option identification and selection;
- where digital engineering techniques are used in the built asset's maintenance and/or operation, documentation relating to:
  - the security risk assessment process undertaken; and
  - the identification of risk mitigation options and the selection of measures to be implemented;
- details of the security-related processes for the implementation of all selected risk mitigation measures;
- the processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes to the built asset's current layout, occupation, utilisation or accessibility to members of the public;
- documentation relating to any changes in, or additions to, protection measures already in place, whether personnel, physical or cyber;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
  - any changes in the identified project- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
  - any reviews of the risk assessments in place; and
  - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any additional documentation found to already be in the public domain;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;

- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

There is no Stage 3 SCA in respect of the ongoing management and maintenance of an existing asset.

Stage 4

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes since the Stage 2 SCA to the built asset, including those relating to its use, layout, occupation, utilisation and accessibility to members of the public;
- a summary of all protective security measures in place;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1 and Stage 2 SCA, documentation relating to:
  - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
  - any reviews of the risk assessments in place; and
  - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Appendix I - Ongoing management of an existing public space

Examples of a public space include: a street; a public square/pedestrianised area etc.

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the public space's current use, including layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any vehicular access to the area by members of the public;
- details of any protection measures in place;
- documentation relating to:
    - the identification of any areas of the public space where protection could be required;
    - the identification of threats and the environmental vulnerabilities that the respective threat actors may seek to exploit;
    - the risk assessment process undertaken in relation to those threats; and
    - the identification of risk mitigation options and the selection of measures implemented;
- where digital engineering techniques are going to be used in the area's design and/or construction, documentation relating to:
    - the security risk assessment process undertaken; and
    - the identification of risk mitigation options and the selection of measures to be implemented;
- the security-related processes for the implementation of all selected mitigation measures;
- the processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- the processes in place for monitoring, auditing, reviewing and updating security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes to the public space's current use, including layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any vehicular access to the area by members of the public;
- documentation relating to any changes in, or additions to, protection measures already in place;
- documentation relating to any changes in, or additions to, areas of the public space where protection is required/will be undertaken;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
    - any changes in the identified threats and/or environmental vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

There is no Stage 3 SCA in respect of the ongoing management and maintenance of an existing public space.

Stage 4

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes since the Stage 2 SCA to the public space, including the type of public space created, its use, layout, the use and nature of the surrounding area including buildings and public highways, and the nature of any vehicular access to the area, including that by members of the public;
- a summary of all protective security measures in place;
- documentation relating to any changes in, or additions to, the assets that are regarded as sensitive, including those that are deemed critical;
- in relation to each of the security risk management processes reviewed in the Stage 1 and Stage 2 SCAs, documentation relating to:
    - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Appendix J - Design and implementation of new connected, smart and autonomous assets

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the project being undertaken, including the assets involved and the extent of connectivity, automation and autonomy within each;
- documentation relating to:
    - the identification of those particular systems that will need to be protected, including identification of those that are deemed critical;
    - the identification of any data and information that needs to be protected for legal, commercially sensitive or security reasons;
    - the identification of project- and asset-related threats and vulnerabilities that the respective threat actors may seek to exploit;
    - the risk assessment process;
    - the identification of risk mitigation options and the selection of measures to be implemented; and
    - any other relevant security corporate risk assessments;
- security-related processes for the implementation of the selected mitigation measures;
- processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- processes in place for monitoring, audit, review and update of security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes to the project being undertaken, including the assets involved and/or the extent of connectivity, automation and autonomy within each;
- documentation relating to any changes in, or additions to, the systems that need to be protected and/or are deemed critical;
- documentation relating to any changes in, or additions to, the data and information that needs to be protected for legal, commercially sensitive or security reasons;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
    - any changes in the project- and/ asset-related threats and vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes, since the Stage 2 SCA, to the project including the assets involved and the extent of connectivity, automation and autonomy within each;
- documentation relating to any changes in, or additions to, the systems protected and/or deemed critical;
- documentation relating to any changes in, or additions to, the data and information protected for legal, commercially sensitive or security reasons;
- a summary of all protective security measures implemented;
- in relation to each of the security risk management processes reviewed in the Stage 1 and Stage 2 SCA, documentation relating to:
    - any changes in the asset-related threats and vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 4

The portfolio of information provided should include:

- the Stage 1, Stage 2 and Stage 3 SCA Reports and respective SCA Response Reports;
- a summary of any changes since the Stage 3 SCA, including the assets involved and the extent of connectivity, automation and autonomy within each;
- documentation relating to any changes in, or additions to, the systems protected and/or deemed critical;
- documentation relating to any changes in, or additions to, the data and information protected for legal, commercially sensitive or security reasons;
- a summary of all protective security measures in place;
- in relation to each of the security risk management processes reviewed in the Stage 1, 2 and 3 SCA, documentation relating to:
    - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Appendix K - Ongoing management of existing connected, smart and autonomous assets

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the assets and the extent of connectivity, automation and autonomy within each;
- a summary of the protection already in place;
- documentation relating to:
  - the identification of those particular systems where further protection may be required, including identification of those that are deemed critical;
  - the identification of any data and information arising from the assets that needs to be protected for legal, commercially sensitive or security reasons;
  - the identification of asset-related threats and vulnerabilities that those threat actors may seek to exploit;
  - the risk assessment process undertaken in relation to those threats;
  - the identification of risk mitigation options and the selection of measures to be implemented; and
  - any other relevant security corporate risk assessments;
- security-related processes for the implementation of the selected mitigation measures;
- processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- processes in place for monitoring, audit, review and update of security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes since the Stage 1 SCA, including the assets involved and the extent of connectivity, automation and autonomy within each;
- documentation relating to any changes in, or additions to, the systems protected and/or deemed critical;
- documentation relating to any changes in, or additions to, the data and information protected for legal, commercially sensitive or security reasons;
- a summary of all protective security measures in place;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
  - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
  - any reviews of the risk assessments in place; and
  - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

There is no Stage 3 SCA in respect of the ongoing management of existing smart, connected or autonomous assets.

Stage 4

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes since the Stage 2 SCA, including the assets involved and the extent of connectivity, automation and autonomy within each;
- documentation relating to any changes in, or additions to, the systems protected and/or deemed critical;
- documentation relating to any changes in, or additions to, the data and information protected for legal, commercially sensitive or security reasons;
- a summary of all protective security measures in place;
- in relation to each of the security risk management processes reviewed in the Stage 1 and Stage 2 SCA, documentation relating to:
    - any changes in the asset- or organisation-related threats and/or vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Appendix L - Data analysis and optimisation project

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the project being undertaken, including the intended purpose, scope, outcome and consumer;
- the data and/or information being utilised and its source;
- a summary of any terms under which any data and/or information from third parties has been provided;
- documentation relating to:
    - the identification of any data and information that needs to be protected for legal, commercially sensitive or security reasons;
    - the identification of project-related threats and vulnerabilities that the respective threat actors may seek to exploit;
    - where the project will be publishing or sharing data and information, the identification of any existing data and information sets that have already been shared or published and that, when aggregated, would allow a third party to draw inferences or create unplanned associations;
    - where the project will be publishing or sharing geographically tagged data and information, the identification of any additional risks created by allowing relationships, patterns and trends to be more easily analysed;
    - the identification of risk mitigation options and the selection of measures to be implemented, including any data and information sharing agreements; and
    - any other relevant security corporate risk assessments;
- the security-related processes for the implementation of the selected mitigation measures;
- the processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- the processes in place for monitoring, audit, review and update of security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes to the project being undertaken, including the intended purpose, scope, outcome and consumer;
- a summary of any changes to the data and/or information being utilised and its source;
- a summary of any terms under which any new data and/or information from third parties has been provided;
- documentation relating to any changes in, or additions to, the data and information that needs to be protected for legal, commercially sensitive or security reasons;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
    - any changes in the project- and asset-related threats and vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented, including any data and information sharing agreements;
- details of any additional relevant data and information sets found to already be published or shared;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;

- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes, since the Stage 2 SCA, to the project including the purpose, scope, outcome and consumer;
- documentation relating to any changes to the data and/or information utilised and its source;
- a summary of any terms under which any new data and/or information from third parties has been provided;
- documentation relating to any changes in, or additions to, the data and information protected for legal, commercially sensitive or security reasons;
- a summary of all protective security measures implemented;
- in relation to each of the security risk management processes reviewed in the Stage 1 and Stage 2 SCA, documentation relating to:
    - any changes in the project- and asset-related threats and vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented, including any data and information sharing agreements;
- details of any additional relevant data and information sets found to already be published or shared;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 4

There is no Stage 4 SCA in respect of a data analysis and optimisation project.

Appendix M - Research and development project

Portfolio of information required for each stage of the SCA process

Stage 1

The portfolio of information provided should include:

- a summary of the project being undertaken, including the intended purpose, scope and outcome;
- a summary of the data and/or information being utilised and its source;
- a summary of any terms under which any data and/or information from third parties has been provided;
- documentation relating to:
  - the identification of any data and information that needs to be protected for legal, commercially sensitive or security reasons;
  - the identification of risk mitigation options and the selection of measures to be implemented; and
  - any other relevant security corporate risk assessments;
- security-related processes for the implementation of the selected mitigation measures;
- processes in place for identifying, and responding to, security breaches and incidents, including near misses; and
- processes in place for monitoring, audit, review and update of security risk management processes.

Stage 2

The portfolio of information provided should include:

- the Stage 1 SCA Report and SCA Response Report;
- a summary of any changes to the project being undertaken, including the intended purpose, scope and outcome;
- a summary of any changes to the data and/or information being utilised and its source;
- a summary of any terms under which any new data and/or information from third parties has been provided;
- documentation relating to any changes in, or additions to, the data and information that needs to be protected for legal, commercially sensitive or security reasons;
- in relation to each of the security risk management processes reviewed in the Stage 1 SCA, documentation relating to:
  - any changes in the project-related threats and vulnerabilities that the respective threat actors may seek to exploit;
  - any reviews of the risk assessments in place; and
  - any changes in the risk mitigation options and/or selection of measures implemented, including any data and information sharing agreements;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 3

The portfolio of information provided should include:

- the Stage 1 and Stage 2 SCA Reports and respective SCA Response Reports;
- a summary of any changes, since the Stage 2 SCA, to the project including the purpose, scope and outcome;
- documentation relating to any changes to the data and/or information utilised and its source;
- a summary of any terms under which any new data and/or information from third parties has been provided;
- documentation relating to any changes in, or additions to, the data and information protected for legal, commercially sensitive or security reasons;
- a summary of all protective security measures implemented;
- in relation to each of the security risk management processes reviewed in the Stage 1 and Stage 2 SCA, documentation relating to:
    - any changes in the project-related threats and vulnerabilities that the respective threat actors may seek to exploit;
    - any reviews of the risk assessments in place; and
    - any changes in the risk mitigation options and/or selection of measures implemented, including any data and information sharing agreements;
- details of any additional relevant data and information sets found to already be published or shared;
- details of any changes to the security-related processes for the implementation of the selected risk mitigation measures;
- details of any changes to the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- 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
- details of any changes to the processes in place for monitoring, auditing, reviewing and updating all security risk management processes.

Stage 4

There is no Stage 4 SCA in respect of a research and development project.