CPNI
Centre for the Protection
of National Infrastructure

INTRODUCTION TO

SECURITY CONSIDERATIONS ASSESSMENT

THE ROLE OF THE SECURITY CONSIDERATIONS ASSESSMENT (SCA)

It is important to protect people, buildings, infrastructure, information, and supporting systems from those with hostile and malicious intent.

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

This can assist in:

- enhancing the safety, security and resilience of buildings, infrastructure, environments and services;
- protecting the safety and security of individuals by safeguarding personally identifiable information and information that would reveal pattern-of-life; and
- protecting valuable intellectual property and commercial information.

What is A SCA?

The SCA is a structured process for ensuring that potential security-related vulnerabilities are considered across a range of activities and processes. It helps to improves 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.

The aim is to provide a mechanism by which organisations 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, 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 reoccurrence of circumstances, decisions and actions that have previously led to a compromise of security in similar situations.

WHAT DOES THE SCA LOOK AT?

A SCA examines:

- the process for determining what may need protecting;
- the understanding and analysis of security-related threats and vulnerabilities;
- the robustness of the security risk assessment;
- the process by which potential risk mitigation measures have been identified, analysed andselected, for example, CPNI operational requirements;
- the processes in place for identifying, and responding to, security breaches and incidents, including near misses;
- the compliance with, and consistency of, implementation of security policies and processes;
- 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 the actual personnel, physical and/or cyber security measures implemented.

In other words, SCA looks at the ‘why’,not the ‘what’.

A robust, fully documented SCA process can 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.

RELATIONSHIP OF THE SCA TO 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 bysenior 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

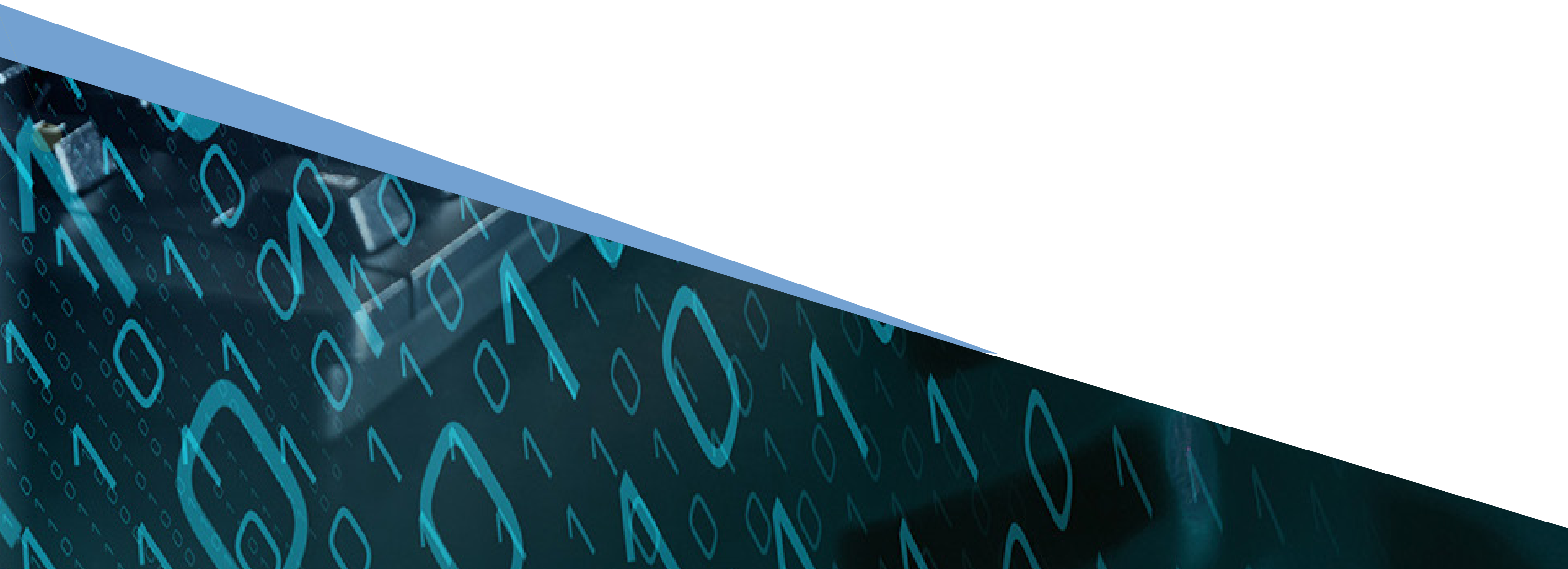
The operational requirement (OR) process (see www.cpni.gov.uk/operational-requirements) is a tool which has been developed to enable an organisation to produce a clear, considered and high level statement of their security needs based on the risks they face.

The OR should be preceded by a risk assessment process that uses information about threats and 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.



Disclaimer

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

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

CPNI
Centre for the Protection
of National Infrastructure