CPNI

Centre for the Protection of National Infrastructure

OPERATIONAL REQUIREMENTS

Principles of assessing and implementing effective protective security

August 2018

Contents

Operational Requirements

Executive Summary

Operational Requirements (OR) are an essential tool to enable an organisation to produce a clear, considered and high level statement of their security needs based on the risks they face.

A well-defined OR increases the likelihood of success in any security project and reduces the risk of commissioning expensive nugatory work. The involvement of key stakeholders in the OR process will increase executive buy-in for the project, simplifying any organisational change required.

Two worked examples on the CPNI website provide a guide to the production of a well-defined OR (for physical and personnel and people protective security mitigations) which is clearly linked to an organisation's security risks. Reflected within this document is the knowledge and experience collated by CPNI from a wide range of organisations across the national infrastructure and crowded places communities.

Blank Excel Templates for the OR process are available on the CPNI website.

Whilst CPNI refers to this process as Operational Requirements, other organisations may refer to similar processes, such as statement of needs, statement of requirements or statement of purpose, but they all have the same objective, which is to provide a single, high level auditable document.

Why Develop an Operational Requirement?

Before designing or implementing any security scheme or measure, security managers and practitioners should first read this guidance and understand the wider context in which it exists.

CPNI has recommended the use of an OR process for many years. The development of this process is based on observing projects where security requirements were poorly defined or developed in isolation. Where CPNI has been asked to assist in failing security projects, in almost all cases an OR process has not been followed. In many cases a comprehensive risk assessment is also absent which is why CPNI recommends completing both risk assessments and the OR process as an essential part of any security project.

Where a suitable OR process is used, projects have a significantly higher success rate and stakeholders are better engaged in the security measures implemented.

The OR process helps organisations make smarter investments in protective security measures, enabling them to implement measures which are in proportion to the risks they face. By following the process, security managers and practitioners are able to assess, develop and justify the actions their organisation needs to take, and the investments they need to make to protect against security threats.

At the end of the process an organisation will have a clear, prioritised list of protective security recommendations, which span the security disciplines[1] and where multiple measures are complementary. This interdisciplinary approach provides a more robust security outcome. A systematic and thorough assessment will help to support any business case and provide clear evidence of the need for the measures and their likelihood of success.

CPNI has received the following feedback from those using the OR process:

The design solutions are now fit for purpose, time is being saved, plus it is a more efficient way of working with project teams and all stakeholders, encouraging sites to adopt 'fit for purpose' measures through accurate identification of the problem that needs addressing and adopting pragmatic success criteria for the project once it is complete.

[1] Physical, Personnel and People, Cyber and Technical Protective Security.

Context

The OR process does not sit in isolation. It follows on from a risk assessment process and leads to the application of effective and proportionate protective security measures.

To develop a prioritised list of security risks, organisations will need to conduct a risk assessment using threat information and an understanding of their operating context and their vulnerabilities. Whilst most organisations will have their own risk assessment processes spanning a variety of the business risk areas, it is essential that security risks are adequately considered. Advice on security risk assessments is available on the CPNI website under Principles of Risk Assessment.

The OR process uses this prioritised list of security risks to develop effective protective security measures.

Operational Requirements Process

The following sections describe the OR process which will lead to a set of protective security measures assessed by the likelihood of successful application.

There are six recommended steps in the OR process, completed over two templates:

1) Splitting up a site (defining the geographical areas for consideration)
2) Defining the risks and mapping to the areas under consideration
3) Identifying and developing a suite of protective security recommendations to address the risks
4) Assessment of protective security recommendations (in terms of likelihood of success)
5) Mapping back to risks (have the risks been mitigated by the measures? Is the residual risk acceptable?)
6) Implementation of security measures (and next steps)

It is important to record as much detail as possible during the process and the use of the CPNI templates (illustrated below) will help with this. Blank templates are available on the CPNI website for you to use. It is important that an organisation clearly identifies who owns the OR process to ensure outcomes are achieved.

OR TEMPLATE: Site area, risks, recommendations and effectiveness			
Area	**Risk**	**Security Recommendations ***	**Effectiveness (mostly met/ partially met)**
Beyond the Perimeter	1)		
		Add lines if required	
	*Additional lines should be added for additional risks***		
		Add lines if required	
		Add lines if required	
		Add lines if required	
Perimeter	1)		
	Additional lines should be added for additional risks		
Within the site	1)		
	Additional lines should be added for additional risks		
Building	1)		
	Additional lines should be added for additional risks		
Asset	1)		
	Additional lines should be added for additional risks		

SECURITY RECOMMENDATIONS TEMPLATE

Use the CPNI INTERACTIVE DIAGRAM to help you identify proportional mitigations that cover physical and personnel security. Use the NCSC website for Cyber security measures. Use the NaCTSO Crowded places guidance for additional information specific to public areas

Security Layer/ Principle	Beyond the perimeter	ASSESS (RAG)	Perimeter	ASSESS (RAG)	Within the site	ASSESS (RAG)	Building	ASSESS (RAG)	Asset	ASSESS (RAG)
Deter - *stop or displace the attack*										
	Add additional lines as required									
Detect - *verify an attack, initiate the response*										
	Add additional lines as required									
Respond - *apprehend the attack and prevent further progress of the attack*										
	Add additional lines as required									
Delay - *prevent the attack from reaching the asset*										
	Add additional lines as required									
Mitigate - *minimise the consequences of an attack*										
	Add additional lines as required									

Whilst the OR process can be followed by an individual, it can be far more efficient and effective to use a stakeholder workshop(s) as a key part of the process. This will encourage buy-in from stakeholders and allow a wider range of ideas to be identified and considered. A well-structured and facilitated workshop is highly likely to provide a robust OR, in turn leading to a better protective security outcome. CPNI suggests the following personnel are considered as workshop attendees:

- Security Manager
- Security Team
- Head of Guard Force
- Human Resources
- Counter-Terrorism Security Adviser
- Facilities Manager
- Operations Manager
- Customer Relations Manager
- Union Representative
- Budget Holder
- Communications Manager
- Health and Safety Manager/Representative
- Director / Head of security/ safety / resilience / corporate risk
- Other external stakeholders – e.g. regulator, local council planning / licensing team
- For major refurbishments or new builds, representatives from the project team

Using the templates

Step 1: Splitting a Site Up

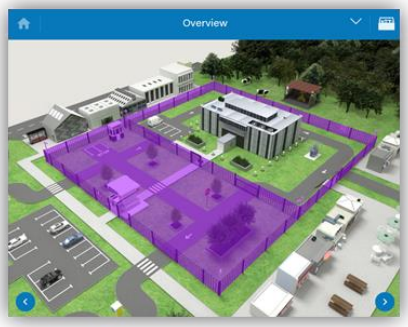
Where a site is large or complex, it can be helpful to consider different areas and/or aspects of the site in turn to allow a sufficiently detailed analysis of security requirements.

Our recommended approach – as described on the CPNI website – is to consider the five generic areas typical of many sites:

- Beyond the Perimeter
- Perimeter
- Within the Site
- Building
- Asset

However, for some sites it may be more appropriate to modify the area or description of an area to better fit the site being considered. For example, where there is public access to a building the perimeter may be the internal boundary between public and staff only areas. This description will need to be recorded on the template and communicated within the workshop to ensure that everyone has a clear definition of the areas under consideration.

Step 2: Defining the Risks



The next stage in the process is to identify, review and agree the risks for each of the areas an organisation is going to consider. If an existing risk assessment process or risk log is present then these risks should be mapped across to your site areas. It is important that any risks are defined with enough granularity to be able to identify recommendations.

This stage of the process should result in a list of the risks under the five areas, some of which will apply to multiple areas and will therefore appear more than once. Where a site has an extensive risk log it may be more manageable to consider the highest priority risks first.

Step 3: Developing Protective Security Recommendations

The CPNI website has an interactive diagram which is based on the five geographical areas mentioned in Step 1. For each area there is a 'Principles' tab at the bottom of the diagram which contains a definition of the area along with the high level security principles which are set out using the following considerations:

- Deter – stop or displace the attack
- Detect – verify an attack, initiate the response
- Delay – prevent the attack from reaching the asset
- Respond – apprehend the attack and prevent further progress of the attack
- Mitigate – minimise the consequences of an attack

These principles should be used to direct the thinking around potential security measures and are available, in more detail, on the 'Principles' tab within the interactive diagram. Consider each of the identified risks in terms of a security discipline (physical, personnel, cyber and technical) and then consider how that discipline can contribute to each of the considerations above. This will build up a range of security measures which have been carefully thought through.

As the measures are systematically assessed they should be entered on the recommendations table to confirm they are balanced across the five areas and five criteria.

Step 4: Assessment of Protective Security Measures

The next step is to prioritise these protective security measures (which may include those in place, modifications to existing measures and new measures) in terms of their likelihood of successful application. Each of the measures identified should be considered against the following criteria:

- **Resources** required (capital/operational expenditure, staffing, facilities);
- **Operational Readiness** (the ability/willingness to implement) of the organisation to implement the measure; and
- **Stakeholder Engagement** and support in making the measure work.

Resources	None (1)	Limited Availability (2)	Readily available (3)
Organisational Readiness	None (1)	Limited capability (2)	Good capability (3)
Stakeholder Engagement	None (1)	Limited engagement (2)	Good engagement (3)

The scores for resources, organisational readiness and stakeholder engagement for each recommendation should be totalled together and the final score assessed using the bands below:

Green – 8 or 9	Recommendations can be applied.
Amber 5 to 7	There will be some barriers to overcome.
Red 3 or 4	There are significant barriers to overcome.

Alternative scoring systems such as selecting the lowest score in any of the three categories could also be used. This scoring can then be used to order the list of recommendations with the one most likely to succeed at the top. In all cases this assessed list will provide the relative order of importance of the measures for that organisation, rather than a list which can be compared between organisations.

Step 5: Mapping Back to Risk

The next step in the process is to map the recommendations back to the OR Template. The recommended measures agreed upon should be entered into the 'recommendations' column. This allows an organisation to identify which risks are not mitigated or where there are limited recommendations. Where the recommendations are not deemed sufficient an organisation has to decide whether to accept and record the risk on the risk register or if further recommendation is required.

The final column in the table should be used to assess the likely effectiveness of each measure and they should be assessed as either:

- Mostly met; or
- Partially met

Whilst the assessment of effectiveness is likely to be subjective, where measure(s) are assessed as 'partially met' the residual risk should be updated/recorded on the security and/or corporate risk registers.

Step 6: Implementation of Security Measures

At the final stage in the process you will now have a set of protective security recommendations mapped out against the five geographical areas; these measures have been agreed as holistic

covering all the necessary criteria. The protective security measures will have been mapped back to the risk and the organisation will be confident the risks have been mitigated or recorded on the risk register.

The guidance material provided by CPNI can be accessed using the interactive diagram on the CPNI website. The website is structured to enable you to move from introductory pages through to specific advice and then on to detailed technical documents. Users will need to decide the appropriate level for their use and some users will engage the services of a security professional to implement the more technical aspects (commissioning/design and build).

Where protective measures identified require cyber advice, this can be found on the National Cyber Security Centre website and technical security guidance can be found on the National Authority for Counter Eavesdropping website.

Crowded places protective security advice can be found on the National Counter Terrorism Security Office website