CPNI
Centre for the Protection of National Infrastructure

GUIDE TO PRODUCING OPERATIONAL REQUIREMENTS FOR SECURITY MEASURES

February 2016

CPNI 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.

Contents

Introduction

An Operational Requirement (OR) is a statement of need based upon a thorough and systematic assessment of the problem to be solved and the hoped for solutions.

The aim of this Guide is to ensure that appropriate security measures are recommended to manage the risk to a level acceptable to all stakeholders. It introduces the concept of a structured methodology for determining the security requirements. Before conducting an OR you should identify the threat to your organisation or site.

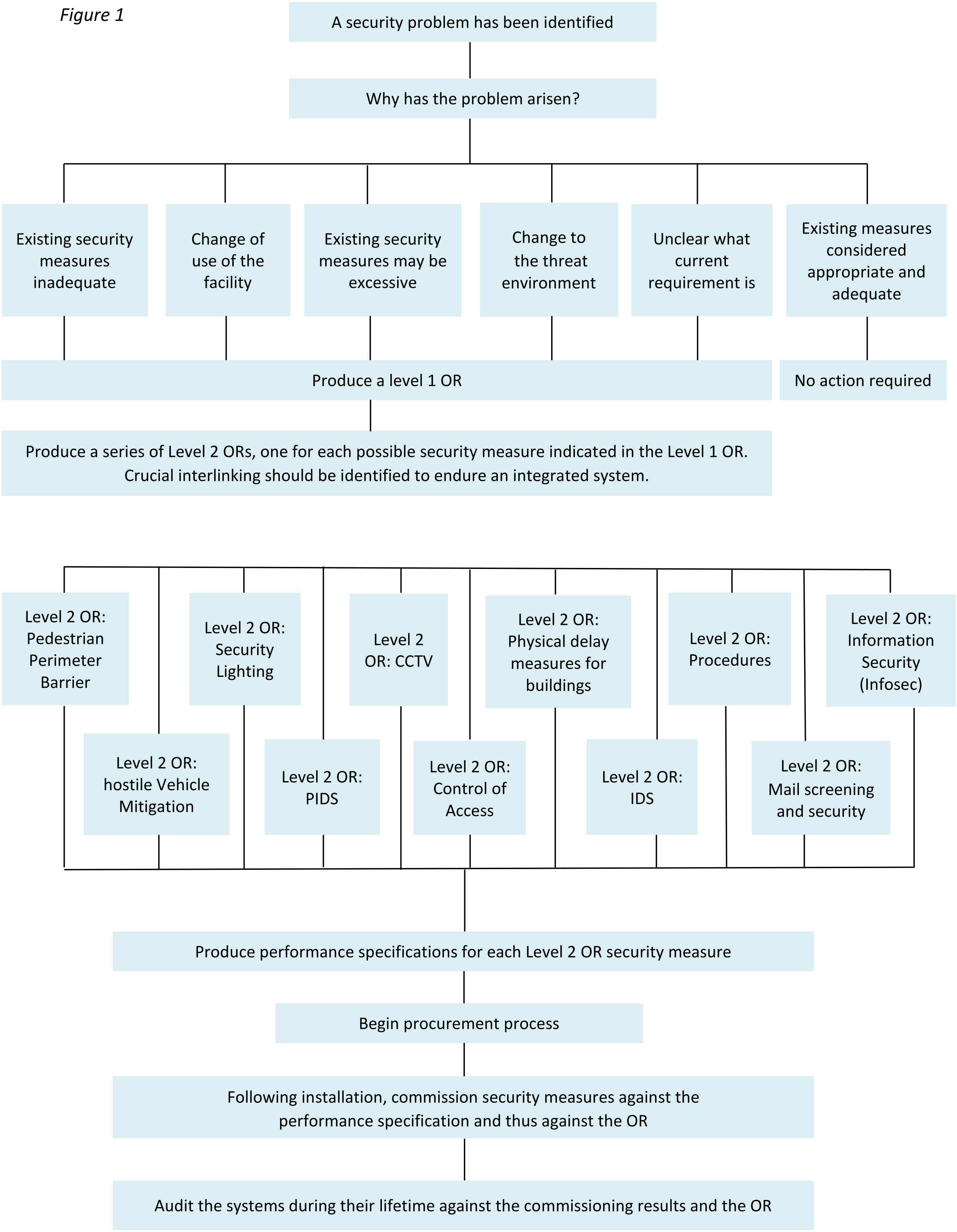
To simplify the process, the procedure has been broken down into two parts, Level 1 and Level 2 Operational Requirements.

The Level 1 OR provides a statement of the overall security need and includes the site to be considered, asset description, perceived threat, consequence of compromise, perceived vulnerabilities, and success criteria.

Level 2 ORs follow on from the completed Level 1 OR and address individual security measures (fences, CCTV, control of access etc.) in a similar fashion to the Level 1 procedure, but which together provide the basis for a fully integrated security solution. Checklists are given, in this document, for a wide range of Level 2 ORs. Not all of these will be needed for every site.

A flow chart of the entire system for producing ORs is at Figure 1.

Figure 1


A security problem has been identified
Why has the problem arisen?
Existing security measures inadequate
Change of use of the facility
Existing security measures may be excessive
Change to the threat environment
Unclear what current requirement is
Existing measures considered appropriate and adequate
Produce a level 1 OR
No action required
Produce a series of Level 2 ORs, one for each possible security measure indicated in the Level 1 OR. Crucial interlinking should be identified to endure an integrated system.
Level 2 OR: Pedestrian Perimeter Barrier
Level 2 OR: Security Lighting
Level 2 OR: CCTV
Level 2 OR: Physical delay measures for buildings
Level 2 OR: Procedures
Level 2 OR: Information Security (Infosec)
Level 2 OR: hostile Vehicle Mitigation
Level 2 OR: PIDS
Level 2 OR: Control of Access
Level 2 OR: IDS
Level 2 OR: Mail screening and security
Produce performance specifications for each Level 2 OR security measure
Begin procurement process
Following installation, commission security measures against the performance specification and thus against the OR
Audit the systems during their lifetime against the commissioning results and the OR

Level 1 Operational Requirement

A Level 1 OR assesses, evolves and justifies the actions to be taken and investments made to protect critical assets against security threats. It defines the:

- Site or building to be protected;
- Stakeholders;
- Critical asset(s);
- Threat(s) and vulnerabilities;
- Impact;
- Proposed strategic security plan;
- Organisational constraints;
- Concept of Operations;
- Implementation and integration;
- Critical dependencies;
- Costs and benefits;
- Organisational readiness.

All stakeholders **must** be involved in the production of the Level 1 OR to ensure that the solution is acceptable to all and that they have ownership of it.

The stakeholders are anyone who has an interest in the operational security of the site or building. These include security managers, building owners, building users' representatives, budget holders, occupants, and the operators of any technical security systems current or proposed.

The completed document can be presented to senior decision makers and budget holders to gain support for investing in security measures.

On completion of the Level 1 OR process, the Level 2 OR process should be undertaken.

The Level 2 OR is a continuation of the Level 1 OR and provides the detail required for individual security measures to be developed by project teams, and should be issued to those responsible for delivering these measures.

For more information on the Level 1 OR process refer to The Level 1 Operational Requirements Process guidance, available on the CPNI website.

Level 2 Operational Requirement

The Level 2 OR is a continuation of the Level 1 OR and is intended to focus in more detail on each area of concern and its possible solution.

The Level 1 OR would have encouraged some possible solutions. Some of these may be discounted for valid reasons, for example, operational or aesthetic. A note should be made of this. The remainder will be considered in more detail in the Level 2 OR.

The Level 1 OR will have addressed assets, threats, consequences of compromise, vulnerabilities, success criteria and possible solutions.

The Level 2 ORs now look at each of the suggested solutions and expand upon the Level 1 OR. In addition, they consider the function(s) of the possible solution, concerns, operator interfaces, risk analysis and performance requirements.

There may well be several Level 2 ORs, again some will be discounted when technical solutions are considered in detail, while the remainder will link together to provide a properly integrated solution. Some aspects may be critically linked and they should be noted where applicable, for example, a gate and pedestrian perimeter barrier.

As an example a site may have a Level 1 OR that indicates a need for pedestrian perimeter barrier with detection, this would require Level 2 ORs covering: pedestrian perimeter barrier, PIDS, lighting and CCTV surveillance. Similarly the Level 1 OR for an office block indicating a need for physical hardening and internal intruder detection would require Level 2 ORs covering the building fabric and IDS system.

Level 2 OR statement

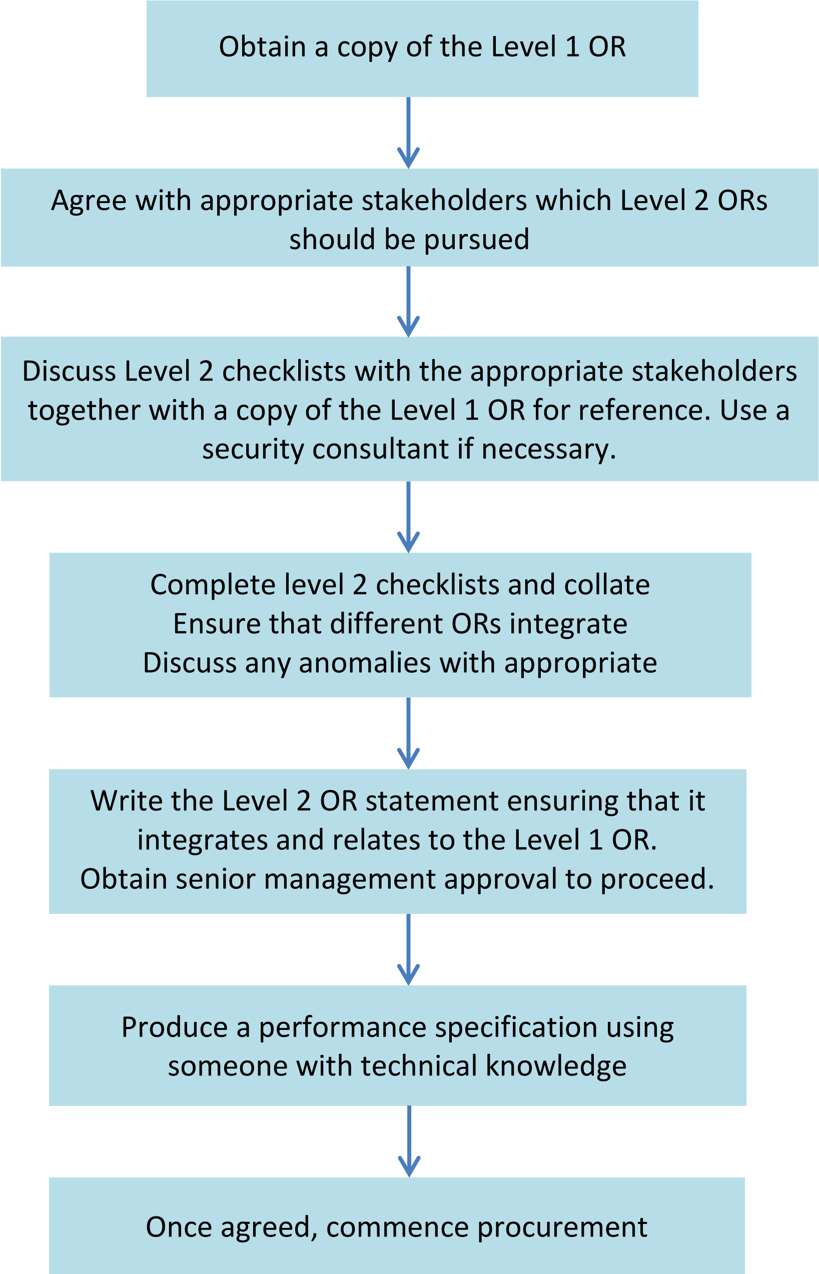
The Level 2 OR statement is a written summary of the information collated from the checklists and not a specification document. It may be supported by completed checklists if felt useful. This statement should always be accompanied by a copy of the Level 1 OR statement so that the relationship with the identified security problem is clear.

The single statement should cover all the measures considered. This is to ensure that the performance specification will address fully the integration of measures to produce an effective solution.

The Level 2 OR statement and completed checklists provide the detail for the designer to produce a performance specification covering a range of possible solutions. Performance specifications will state parameters for proposed systems that stakeholders can compare with the ORs and make an informed decision on the security risk management for their site or building before moving forward to the procurement process.

It is very important that all Level 2 solutions are integrated as appropriate.

Level 2 Operational Requirement: Flow chart



Obtain a copy of the Level 1 OR

Agree with appropriate stakeholders which Level 2 ORs should be pursued

Discuss Level 2 checklists with the appropriate stakeholders together with a copy of the Level 1 OR for reference. Use a security consultant if necessary.

Complete level 2 checklists and collate
Ensure that different ORs integrate
Discuss any anomalies with appropriate

Write the Level 2 OR statement ensuring that it integrates and relates to the Level 1 OR.
Obtain senior management approval to proceed.

Produce a performance specification using someone with technical knowledge

Once agreed, commence procurement

Level 2 Operational Requirement: Pedestrian perimeter barrier

Give title and date of the Level 1 OR to which this Level 2 OR relates:

Indicate other Level 2 ORs being produced concurrently with this one							**Date**		
Hostile Vehicle Mitigation	Security Lighting	CCTV	PIDS	Physical Delay	Control of Access	IDS	Mail screening and security	Information Security (Infosec)	Other

1. Area of concern Identify the boundary or area to be protected	
2. What is (are) the function(s) of the pedestrian perimeter barrier? • Demarcation of boundary • To deter entry into the area • To protect against climb over • To protect against cut through • To protect against vehicle intrusion • One of the above plus pedestrian access • Outer & inner fence with sterile zone to support Perimeter • Intruder Detection systems (PIDS) - to help to detect an intruder • Concealment of guards and/or activity • See through or solid	
3. Vulnerable points List features that will reduce the effectiveness of the perimeter fence (areas of cover, trees, foliage, adjacent buildings, other climbing aids.) Number of entry/exit points (e.g. doors/gates/turnstiles).	

4. External constraints • Is Local Authority Planning approval required? • Describe adjacent property • Is the type of fence topping a possible constraint? • Are there legal requirements? If so, what are they? • Height of barrier • External constraints continued • Wind, rain, snow etc. • Temperature changes • Water table – flooding • Natural lighting • Local topography	
5. Performance requirement **With Perimeter Intruder Detection Systems (PIDS)** • What is the maximum response time from detection of intruder to interception? • State desired delay against cut through • State desired delay against climb over (if double fence state for each) • State desired delay against vehicle attack (ensure this compares with any vehicle barrier) • State any other performance requirement(s) for example: to support a fence mounted PIDS. **Without PIDS** • State desired delay against cut through • State desired delay against climb over (if double fence state for each) • State desired delay against vehicle attack (ensure this compares with any vehicle barrier) • State any other performance requirement(s).	
6. Risk analysis (confirm with all stakeholders) • Is this task mandatory or covered by minimum baseline measures within your organisation's security operating procedures or plan? • Compared to the other areas of concern what is the priority for this one? • What is the likelihood of the threatening activity occurring and how often? • What are the benefits of doing this task over not doing it?	
7. What are your success criteria?	

8. Integration Confirm that the solution integrates with other level 2 ORs as appropriate. For example Hostile Vehicle Mitigation, CCTV, PIDS, security lighting etc. Which OR takes precedence?	
9. Management issues • Are audits undertaken? If yes, how many times a year? • Are there controls in place? • Are there sufficient resources to carry out the procedures?	
10. Maintenance • Do you have a maintenance contract? • Are the contractors approved by the supplier of the equipment? • Is there system documentation readily available? • Are logs kept for commissioning and subsequent performance tests? • Is there a process for fault logging and resolution? • How many times per annum are the pedestrian perimeter barriers maintained by the contractor/installer/company? • Do they look for deterioration, corrosion, degradation, vegetation, hinge fixing, screw fixings? • What maintenance should be carried out? Has this been agreed? • What is the contractors call out or response time for an emergency? Is it stated that they must resolve the problem in a given time? • Is there a maintenance log? Does it include repairs, replacements and system adjustments?	

Level 2 Operational Requirement: Hostile Vehicle Mitigation (HVM)

Give title and date of the Level 1 OR to which this Level 2 OR relates:

Indicate other Level 2 ORs being produced concurrently with this one							**Date**		
Hostile Vehicle Mitigation	Security Lighting	CCTV	PIDS	Physical Delay	Control of Access	IDS	Mail screening and security	Information Security (Infosec)	Other

1. Location of concern (NOTE: multiple locations will each require individual level 2 ORs) Identify the boundary or area to be protected: • Existing/proposed perimeter or building structure • Vehicle Access Control Point (VACP) • Emergency access control Period of concern (i.e. over what time period is the location vulnerable to vehicle borne threat?)	
2. Vulnerabilities Identify features (or lack of) that make the location vulnerable: • Vehicle approaches • Guard Force • Lines of sight • CCTV • Lighting • Location of critical services Is protection of a barrier control mechanism required?	
3. HVM measure(s) function Identify the priority function(s) of the HVM measure(s):	

• Maintain blast stand-off • Prevent encroachment • Stop penetrative attack • Control vehicle access • Enforce speed management measures	
4. Hostile vehicle/manual attack Modus Operandi (MO) How could the asset be attacked? • Parked vehicle • Encroachment (i.e. negotiating gaps in barriers without ramming; or tailgating through an active barrier system) • Penetrative (i.e. ramming) • Deception (e.g. of guard using false identification or by using a Trojan vehicle) • Duress (e.g. against guard to grant access or against legitimate driver to act as mule) • Layered attack (i.e. using more than one MO) • Surreptitious vehicle security barrier tampering	
5. Performance requirement **Under hostile vehicle attack:** • Perceived threat vehicle (e.g. car, 4x4, van, HGV, other) • Maximum vehicle impact speed and impact angle (from Vehicle Dynamic Assessment results) • Stand-off distance (i.e. placement of measure) • Blast performance (e.g. fragmentation) **Under normal operation:** • Operational traffic volume (per unit time) • Legitimate vehicle dimensions & types (e.g.. very long or wide loads vehicles) • Power requirement • Emergency access response • Override in the event of product failure	
6. Physical constraints Identify constraints that could physically restrict the use of HVM measures: • Available foundation depth • Location and depth of underground services • Overhead constraints • Topography (i.e. the contours of the land)	

• Soil conditions	
7. External constraints Identify environmental constraints that could limit the use of HVM measures: • Wind, rain, snow etc. • Temperature changes • Water table – flooding • Natural lighting Are there legal requirements? If so, what are they?	
8. Rules and regulations Identify applicable rules and regulations that could prohibit the use of certain HVM measures, e.g. • Local authority constraints • Highways issues • Planning approval • Sites of Special Scientific Interest (SSSI) • Site Operational restrictions	
9. Success criteria What are the success criteria and how are they measured? • Integration with other security measures • Integration into the public realm • Aesthetics • Budget • Reduce vulnerability level	
10. Integration Confirm that the solution integrates with other level 2 ORs as appropriate. For example, CCTV, pedestrian perimeter barrier, PIDS, security lighting etc. Which OR takes precedence?	
11. Management issues • Design and project management • Planning	

• Construction & installation (e.g. Construction Design • Management (CDM) • Testing, commissioning and handover • Ownership after commissioning • Security management procedures including manning levels • Health & safety • Training procedures and regular auditing of competency • Standard operating procedures & guard force assignment instructions	
12. Service & Maintenance considerations Service level agreements (SLAs) including tender process and competency & capability assessment of contractors. Service & Maintenance contract requirements: • Call-out response time • Breakdown repair time • Onsite spares • Number of maintenances per annum and what is to be checked and logged. Manufacturer approved service and maintenance contractor Documentation requirements, including drawings, programme listings, instructions and operation and maintenance manuals and logs. Are logs to be kept for commissioning and subsequent performance tests? Fault logging, live monitoring and auditing?	

Level 2 Operational Requirement: Security lighting

Give title and date of the Level 1 OR to which this Level 2 OR relates:

Indicate other Level 2 ORs being produced concurrently with this one							**Date**		
Hostile Vehicle Mitigation	Security Lighting	CCTV	PIDS	Physical Delay	Control of Access	IDS	Mail screening and security	Information Security (Infosec)	Other

1. Area of concern • Identify the boundary or area to be illuminated. (Where an area is large or complicated it is advisable to break it down into smaller units and to complete a separate checklist for each].) • Identify key features, buildings etc. • Include areas NOT to be illuminated, neighbours property, guard routes • Describe properties adjacent to the boundary • List all roads and railways near the boundary	
2. What is (are) the primary function(s) of the lighting system? • Deter entry into the area (state by whom) • Concealment of guards and/or activity • Aid visual observation by patrolling guards • Support CCTV surveillance • Vehicle/pedestrian access point • Assist in the searching of vehicles • Emergency lighting • Support Visual Based Detection	
3. What is (are) the secondary function(s) of the lighting system? From the list above	

4. Existing lighting • State which lighting already exists • Impact of street lighting / other lighting outside the site • Amenity and building lighting within the site • What lamp types are in use? • Column height	
5. Vulnerable points List features which will reduce the effectiveness of the lighting system (trees, areas of cover)	
6. External constraints • Weather conditions • Be aware of light pollution regulations • Consider infrared lighting • Is Local Authority planning approval needed? • Are there legal requirements? If so, what are they? • Atmospheric corrosion (sea, air, metallic salts, hydrogen sulphide) • Temperature range • Wind speed (for column loading and foundations)	
7. Operational issues • Is site blackout needed? • Are 'lowerable by one man' columns needed for maintenance? • Any particular control needs, e.g. photocell with manual override? • What are the power supply needs? Is uninterrupted power supply (UPS) required? • Strike up and restrike time (time between initiation of power to the lighting system being fully effective) • Maintenance regime proposed	
8. Performance requirement State the need from the operator's viewpoint: • Illuminate crawling intruder at xx metres from fence • Detect damage to fence fabric • Recognise vehicle colour • Reading number plates • Recognise skin tones	

9. Risk analysis (confirm with stakeholders) • Is this task mandatory or covered by minimum baseline measures within your organisations security operating procedures or plans? • Compared to the other areas of concern, what is the priority for this one? • What are the benefits of doing this task over not doing it?	
10. Success criteria What are your success criteria? Achieve minimum illumination levels defined in published guidance Not contravene statutory requirements	
11. Integration Confirm that the solution integrates with other level 2 ORs as appropriate. For example, how will the lighting work with CCTV, pedestrian perimeter barriers, vehicle security barriers etc. Which OR takes precedence?	
12. Management issues • Planning • Installation • Commissioning • Ownership after commissioning • Service level agreements • Security management procedures • Health & safety • Training procedures for health and safety issues • Standard operating procedures. Are they clear, practices and tested regularly? • Are staff performances regularly appraised? • Are audits undertaken? If yes, how many times a year?	
13. Maintenance • Do you have a maintenance contract? • Are the contractors approved by the supplier of the equipment? • Is there system documentation readily available? • Are logs kept for commissioning and subsequent	

performance tests? • Is there a process for fault logging and resolution? • How many times per annum are the systems maintained by the contractor/installer/company? • Do they look for deterioration, corrosion, degradation, hinge fixing, screw fixings, UPS? • What maintenance should be carried out? Has this been agreed? • What is the contractors call out or response time for an emergency? Is it stated that they must resolve the problem in a given time? • Is there a maintenance log? Does it include breakdowns, repairs, replacements and system adjustments?	

Level 2 Operational Requirement: Closed Circuit Television (CCTV) surveillance systems

For more details about CCTV Operation Requirements, refer to CCTV ORs 2009 publication no 28/09.

Level 2 Operational Requirement: Perimeter Intruder Detection Systems (PIDS)

Give title and date of the Level 1 OR to which this Level 2 OR relates:

Indicate other Level 2 ORs being produced concurrently with this one							**Date**		
Hostile Vehicle Mitigation	Security Lighting	CCTV	PIDS	Physical Delay	Control of Access	IDS	Mail screening and security	Information Security (Infosec)	Other

1. Area of concern Describe the area or boundary where detection is required. • What is the approximate length of the boundary? • Is there a pedestrian perimeter barrier present? • Where is the boundary non-contiguous (gates, rivers, buildings etc.)? • Is a sterile area available? If it is, how wide is it?	
2. What is the function of the PIDS? Describe the object(s) of concern (the target(s) to be detected). • What are the activities that would concern you? • Detect individual climbing • Detect individual cutting • Individual crossing restricted zone/trip wire	
3. Vulnerable points List points at the perimeter that may cause increased vulnerability • Streams, rivers etc. crossing the boundary • Vehicles ability to get close to the boundary • Areas hidden from natural/technical surveillance	
4. External constraints	

• Weather conditions • Presence of wildlife in the area to be protected • Legal requirements • Trees and vegetation proximity to area to be protected • Sources of Electro Magnetic Interference (EMI)? • Sources of vibration and proximity to area to be protected. • Wildlife Is a host fence present? Is there a legal requirement? If so what is it?	
5. Performance requirement • Acceptable false alarm rates • Acceptable detection alarm rates • Tamper detection – state the areas to be protected and expected action • SEAP approved system	
6. Operational issues • When the threatening activity is detected, what will the response be? • How quickly is attendance at the point of activity needed? • Consider both verification of the event and communication with response force • Where will activity be monitored and by who? • How should the alarms be displayed and logged? • Who makes the response decision? • How is the decision arrived at? • How quickly does the operator need to respond to the activity for the response to be effective? • What back up power is required and how long should it be capable of supporting the PIDS for? • Consider what needs to be available to help the operator make the right decision • At what time of day is the activity a threat? • Visibility: Does the system need to be covert or overt?	
7. Risk analysis (confirm with all stakeholders) • Is this task mandatory or covered by minimum baseline measures within your organisations security operating procedures or plans? • Compared to the other areas of concern what is the priority for this one? • What is the likelihood of the threatening activity occurring and how often? • What are the benefits of doing this task over not	

doing it?	
8. What re your success criteria?	
9. Integration Confirm that the solution integrates with other level 2 ORs as appropriate. For example pedestrian perimeter barriers, buildings, CCTV etc. Which OR takes precedence?	
10. Management issues • Are there procedures, training, and resources in place? If yes, are procedures clear, practised and tested regularly? • Are staff performances regularly appraised? • Are there sufficient resources to carry out the procedures? • Are audits undertaken? If yes, how many times a year? • Are there controls in place? • Who should call out contractors when problems arise?	
11. Maintenance • Do you have a maintenance contract? • Are the contractors approved by the supplier of the equipment? • Is there system documentation readily available? • Are logs kept for commissioning and subsequent performance tests? • Is there a process for fault logging and resolution? • How many times per annum are the systems maintained by the contractor/installer/company? • Do they look for deterioration, corrosion, degradation, vegetation, hinge fixing, screw fixings, UPS? • What maintenance should be carried out? Has this been agreed? • What is the contractors call out or response time for an emergency? Is it stated that they must resolve the problem in a given time? • Is there a maintenance agreement (especially around PIDS)? • What maintenance tests are carried out to check performance of the PIDS? Are they repeatable? Are they in the same location of a zone?	

Level 2 Operational Requirement: physical delay measures for buildings

Give title and date of the Level 1 OR to which this Level 2 OR relates:

Indicate other Level 2 ORs being produced concurrently with this one							**Date**		
Hostile Vehicle Mitigation	Security Lighting	CCTV	PIDS	Physical Delay	Control of Access	IDS	Mail screening and security	Information Security (Infosec)	Other

1. Area of concern (existing building) • Identify the elements of the building or room that require physical delay measures • Identify where delays are required where they do not currently exist • Area of concern (new building) • Identify the elements of the building to be physically hardened against attack • Identify best locations for delay	
2. What is (are) the function(s) of the Physical Barrier(s)? • To deter entry into a building or area (state by whom) • To provide a point of detection • To provide a post detection delay • To provide proof of compromise	
3. Vulnerable points List features that are easily defeated (state by whom)	
4. External constraints • Listed Building constraints • Type of property, i.e. industrial, office etc. • Legal requirements, e.g. Health and Safety Executive (HSE)	

5. Performance requirement Minimum acceptable delay against what sort of attacker equipped with certain types of tools, e.g. undetected compromise of asset (surreptitious) or asset theft; and asset damage (forced)	
6. Operational issues • Is the site manned 24 hours a day? • Likely maximum response time from detection to reaching target area • Are attacks likely to be noisy or quiet? • Are there any services which might bridge physical measures?	
7. Risk analysis (confirm with all stakeholders) • Is this task mandatory or covered by minimum baseline measures within your organisation's security operating procedures or plans? • Compared to the other areas of concern what is the priority for this one? • What is the likelihood of the threatening activity occurring and how often? • What are the benefits of doing this task over not doing it?	
8. What are your success criteria?	
9. Integration Confirm that the solution integrates with other level 2 ORs as appropriate. For example will an IDS system be integrated with an AACS? Is it of the same security level? Which OR takes precedence?	
10. Management issues • Are there procedures, training, and resources in place? If yes, are procedures clear, practised and tested regularly? • Are staff performances regularly appraised? • Are there sufficient resources to carry out the procedures? • Are audits undertaken? If yes, how many times a year? • Are there controls in place?	

• Do the measures correspond to the response time?	
11. Maintenance • Do you have a maintenance contract? • Are the contractors approved by the supplier of the equipment? • Is there system documentation readily available? • Are logs kept for commissioning and subsequent performance tests? • Is there a process for fault logging and resolution? • How many times per annum are the systems maintained by the contractor/installer/company? • Do they look for deterioration, corrosion, degradation, hinge fixing, screw fixings, UPS? • What maintenance should be carried out? Has this been agreed? • What is the contractors call out or response time for an emergency? Is it stated that they must resolve the problem in a given time? • Is there a maintenance log? Does it include breakdowns, repairs, replacements and system adjustments?	

Level 2 Operational Requirement: Control of access

Give title and date of the Level 1 OR to which this Level 2 OR relates:

Indicate other Level 2 ORs being produced concurrently with this one							**Date**		
Hostile Vehicle Mitigation	Security Lighting	CCTV	PIDS	Physical Delay	Control of Access	IDS	Mail screening and security	Information Security (Infosec)	Other

1. Area of concern (existing building) Identify the areas, building(s) or room(s) where access is to be controlled. Is the building/site to be 'zoned'?	
2. What is the function of the control of access system? To control people, vehicles? Will it be a manual system (key and lock) or an automated access control system (AACS)? What is the threat? Is it from espionage, crime, terrorism?	
3. Vulnerable points Points where access is to be controlled All other points of entry to the areas that will need to be secure Indicate which are emergency exits	
4. External constraints Are there any Legal requirements? If so, what are they, e.g. Health & Safety or Disability & Discrimination Act (DDA)? Associated barriers to access control – what environmental weathering needs to be considered if the system is to operate outside. This could differ greatly if the site is exposed to coastal conditions.	

5. Operational issues

Fire Officer’s requirements:

- Release on emergency
- Muster points
- Need for occupation reports by number and location (Impacts on anti-tailgating, anti-passback and swipe in/out)
- What are the requirements for disabled access?
- When will the system be operational? (i.e. during a working day or out of office hours only)
- Have you a dual door system whereby the outer door or barrier is mechanically locked out of hours?
- What is your expected throughput/footfall?

Minimum security requirements

- Areas requiring minimum occupation
- Anti-tailgating?
- Anti-passback?
- By-passing barrier?

How will access by controlled for:

- Disabled Visitors
- Other non pass holders
- Contractors

Is there a control of passed or keys? Who is responsible? Who issues them or collects them?

How will deliveries be controlled?

Where will data entry and monitoring of alarm activity take place?

How will data for entry or modification be gathered?

How will security clearances be processed?

Associated control barriers – What throughput time is required and how often are the barriers going to be used? This will have a bearing on the material, hardware and cost.

6. Performance requirement

Consider token options:

- Proximity, proximity plus PIN
- Swipe, swipe plus PIN
- Enrolment/removal of users on system
- Level of security requirement. It is a SEAP approved system?
- Is it commensurate with other barriers and systems (see also 9)
- Zoning
- Alarm for forced entry and/or door open sensor

7. Risk analysis (confirm with all stakeholders) • Is this task mandatory or covered by minimum baseline measures within your organisation’s security operating procedures or plans? • Compared to the other areas of concern what is the priority for this one? • What is the likelihood of the threatening activity occurring and how often? • What are the benefits of doing this task over not doing it?	
8. What are your success criteria?	
9. Integration Confirm that the solution integrates with other ORs as appropriate. For example vehicle security barriers, pedestrian perimeter barriers, CCTV, IDS, procedures plus others. Which OR takes precedence?	
10. Management issues • Are there procedures, training, and resources in place? If yes, are procedures clear, practised and tested regularly? • Are there sufficient resources to carry out the procedures? • Are audits undertaken? If yes, how many times a year? • Are there controls in place? • Is the access control associated barrier going to be monitored?	
11. Barriers associated with access control Is the system automatic or manned? (This will have a bearing on the type of barrier and particularly the type of locking used.) Barriers for use on the perimeter may be required to do a different function to those at the building line. Do perimeter barriers need to be commensurate with the fence line? What are your required delay times? Think about what the asset is; is the threat from espionage, crime, terrorism?	

12. Maintenance • Do you have a maintenance contract? • Are the contractors approved by the supplier of the equipment? • Is there system documentation readily available? • Are logs kept for commissioning and subsequent performance tests? • Is there a process for fault logging and resolution? • How many times per annum are the systems maintained by the contractor/installer/company? • Do they look for deterioration, corrosion, degradation, vegetation, hinge fixing, screw fixings, uninterrupted power supply (UPS)? • What maintenance should be carried out? Has this been agreed? • What is the contractors call out or response time for an emergency? Is it stated that they must resolve the problem in a given time? • Is there a maintenance log? Does it include breakdowns, repairs, replacements and system adjustments? Is there a site maintenance agreement?	

Level 2 Operational Requirement: Intruder Detection Systems (IDS)

Give title and date of the Level 1 OR to which this Level 2 OR relates:

Indicate other Level 2 ORs being produced concurrently with this one							**Date**		
Hostile Vehicle Mitigation	Security Lighting	CCTV	PIDS	Physical Delay	Control of Access	IDS	Mail screening and security	Information Security (Infosec)	Other

1. Area of concern • Identify the building or room(s) to be covered • Possible routes through the building	
2. What are the functions of IDS? • Describe the object(s) of concern • Describe the activity that is a threat to the assets	
3. Vulnerable points List the possible points of entry to the area of concern (doors, windows, walls, roof, ducts etc.)	
4. External constraints To ensure IDS components can be selected that are appropriate to the service environment list the following: • Building heating • Air conditioning • Sources of vibration (e.g. heavy traffic, machinery, railway line) • Sources of radio frequency interference (i.e. close proximity of radio masts/antenna etc.) • Conditions of building fabrics, doors, windows etc. Are there any legal requirements? If so, what are they?	

5. Performance requirement • Acceptable false alarm rates • Acceptable probability of detection • Tamper Detection • SEAP Approval of System	
6. Operational issues • At what time of day is the activity a threat? • When the threatening activity is detected what will the response be? • How quickly is attendance at the point of activity needed? • Consider both verification and communication with response force • Where will activity be monitored and by whom? • Who makes the response decision? • How is the decision arrived at? • How quickly does the operator need to respond to the activity for the response to be effective? • Consider what needs to be available to help the operator make the right decision • Will authorised persons be present during periods when the IDS is operational? • Consider where and how authorised personnel/IDS users will interact with the IDS (i.e. preferred method of setting and unsetting the system) • Is there a preferred type of response force? • Who will have authority to issue/change access codes? • Does the system need to satisfy Association of Police Officers (ACPO) requirements	
7. Risk analysis (confirm with all stakeholders) • Is this task mandatory or covered by minimum baseline measures within your organisation's security operating procedures or plans? • Compared to the other areas of concern what is the priority for this one? • What is the likelihood of the threatening activity occurring and how often? • What are the benefits of doing this task over not doing it?	
8. What are your success criteria?	

9. Integration State how the solution integrates with other ORs as appropriate. For example, building fabrics, control of access, procedures. Which OR takes precedence?	
10. Management issues • Are there procedures, training, and resources in place? If yes, are procedures clear, practised and tested regularly? • Are staff performances regularly appraised? • Are there sufficient resources to carry out the procedures? • Are audits undertaken? If yes, how many times a year? • Are there controls in place?	
11. Maintenance • Do you have a maintenance contract? • Are the contractors approved by the supplier of the equipment? • Is there system documentation readily available? • Are logs kept for commissioning and subsequent performance tests? • Is there a process for fault logging and resolution? • How many times per annum are the systems maintained by the contractor/installer/company? • Do they look for deterioration, corrosion, degradation, hinge fixing, screw fixings, uninterrupted power supply (UPS)? • What maintenance should be carried out? Has this been agreed? • What is the contractors call out or response time for an emergency? Is it stated that they must resolve the problem in a given time? • Is there a maintenance log? Does it include breakdowns, repairs, replacements and system adjustments? • Is there a site maintenance agreement (especially around IDS)? • What maintenance tests are carried out to check performance of the IDS? Is it repeatable? Is it in the same location of a zone?	

Level 2 Operational Requirement: Information Security (INFOSEC)

Note: This OR is drafted as part of a document set for non-technical high level purposes for use by physical security personnel. A more detailed technical OR documents should also be drafted by specialist INFOSEC personnel for their purposes.

Give title and date of the Level 1 OR to which this Level 2 OR relates:

Indicate other Level 2 ORs being produced concurrently with this one							**Date**		
Hostile Vehicle Mitigation	Security Lighting	CCTV	PIDS	Physical Delay	Control of Access	IDS	Mail screening and security	Information Security (Infosec)	Other

1. System function(s) Office automation, Supervisory Control and Data Acquisition (SCADA), security system, management information system	
2. Area and equipment of concern Identify the site, buildings, rooms where system equipment and cabling is located	
3. Physical, logical and personnel controls Define the system access controls, e.g. local and remote user system access, user area, equipment and server rooms, media libraries, cabling infrastructure	
4. Threat to the system(s) Intrusion, remote or internal user access, malware, hacking, denial of service, theft, system misuse, external support personnel or contractors	

5. Consequences of a system compromise In terms of, for example, confidentiality, integrity, availability, data or intellectual property loss, potential criminal activity or national security issues	
6. External constraints Heating, lighting, water, sewage, fire or power issues that may impact on the security of the information system	
7. Performance requirements System performance issues that may impact on system security	
8. Operational issues Issues that may create security problems, e.g. 24/7 operation, remote access, contractor support	
9. Vulnerable points Potential vulnerable points that need further assessment from a physical, personal, document or electronic perspective	
10. Integration Confirm that the solution integrates with other ORs as appropriate. For example, control of access. Which one takes precedence?	
11. Management issues • Supporting policies and procedures available? • Agreed by senior management? • Who maintains them? • When they were last reviewed? • User awareness campaign?	
12. What are your success criteria?	

Level 2 Operational Requirement: Mail screening and security

This OR outlines the key issues to consider when identifying requirements for mail screening and security measures. Extensive guidance on this subject is available in PAS97:2009 – A Specification for Mail Screening and Security, published by BSI in collaboration with CPNI. It is strongly recommended that the PAS is used in the process of an OR development.

Note: Before commencing a Level 2 OR for mail screening and security, it is important to have completed a Level 1 OR with due consideration of postal threats and their potential impact.

NB: This OR focuses on screening mail, but similar considerations and measures can be applied to the screening of bulk deliveries such as catering, cleaning and office supplies.

Give title and date of the Level 1 OR to which this Level 2 OR relates:

Indicate other Level 2 ORs being produced concurrently with this one							**Date**		
Hostile Vehicle Mitigation	Security Lighting	CCTV	PIDS	Physical Delay	Control of Access	IDS	Mail screening and security	Information Security (Infosec)	Other

1. Identify stakeholder requirements and constraints • Understand all mail streams into the organisation, including approximate numbers and types of items, and any seasonal variations • Understand business drivers and other organisational constraints on its mail handling and screening processes, e.g. time available for screening, priorities associated with particular mail streams	
2. Assess the risk the organisation faces from postal threats • Understand the ways in which items of mail may cause concern, disruption or harm • Assess the extent to which the organisation is a target • Understand the risk profiles of the organisation's various mail streams • Assess the vulnerability of the organisation to, and the	

impact on the organisation of, suspicious or hazardous mail • Understand the significance to the organisation of valuable items and sensitive information that may be sent or received by post	
3. Identify appropriate screening processes commensurate with the risk Screening processes intended to detect explosive devices, blades, and other more conventional hazards. Likelihood of organisation being targeted in this way Screening process intended to detect “white powder” chemical, biological or radiological materials. Likelihood of organisation being targeted in this way	
4. Identify appropriate physical protective measures for the mail room/screening facility • Basic physical security measures, e.g. control of access, intruder detection systems • Blast-hardening • Basic measures to reduce the impact of containment releases e.g. design and construction that facilitates cleaning, design of ventilation system so air tends to flow into mail facility from rest of building • More advanced measures to reduce the impact of contaminant releases, such as specialist ventilation system	
5. What are your success criteria?	
6. Integration • Confirm that the solution integrates with other security measures (and respective ORs) as appropriate • Pay particular attention to physical measures such as control of access and intruder detection systems for mail screening facilities and any other locations where mail may be sorted	
7. Management issues • Need clear incident response measures, which are part of the organisation’s wider emergency response procedures • Health and safety considerations; are mail screening/handling staff adequately protected given the risks they may face? • Review screening facilities and measures regularly, and	

following any incidents, changes to the threat etc. • Is there management commitment at all levels to achieving a robust screening capability? Or do other, e.g. throughput, targets compete with screening in practice? • Are staff highly motivated? (Task rotation, to prevent prolonged work on a single activity, may help.) • Are staff adequately trained in: identification of postal threats, use of any screening equipment and responding safely to incidents? • Do staff receive regular refresher training? • Is staff performance monitored?	

Level 2 Operational Requirement: Procedures

Give title and date of the Level 1 OR to which this Level 2 OR relates:

Indicate other Level 2 ORs being produced concurrently with this one							**Date**		
Hostile Vehicle Mitigation	Security Lighting	CCTV	PIDS	Physical Delay	Control of Access	IDS	Mail screening and security	Information Security (Infosec)	Other

1. Area of concern - Identify the area or site	
2. What are the functions of procedures? • Describe the duties of any good guard force • Monitor CCTV • Patrolling • Control of Access • Searching visitors/staff • Response to alarms or attack (undetected compromise of asset (surreptitious) or asset theft; and asset damage (forced) • Escorting of visitors • Logging visitors on and off sites • Miscellaneous administrative duties • Breaches	
3. Vulnerable points Identify any elements of the site that are particularly vulnerable to attack or where current protective measures can be defeated	
4. External constraints • At what time of day is the activity a threat? • Weather conditions • Are there any legal requirements? If so, what are they? • Do you share a tenancy? • Is there a landlord?	

• What is the site/building design or configuration?	
5. Performance requirement • Response times to any intrusion/alarm • Quantify any duties proposed in section 2	
6. Operational issues • Are all elements of the guard force required 24 hrs a day? • Is the guard force required for 24 hrs a day? • Does the guard force provide a response capability? • If so, what? Is the response arrived?	
7. Risk analysis (confirm with all stakeholders) • Are these tasks mandatory or covered by minimum baseline measures within your organisation's security operating procedures or plan? • Compared to the other areas of concern what is the priority for this one? • What is the likelihood of the threatening activity occurring and how often? • What are the benefits of doing this task over not doing it?	
8. What are your success criteria?	
9. Integration Confirm that the procedures integrate with other level 2 ORs as appropriate.	
10. Management issues • Are there procedures, training, and resources in place? If yes, are procedures clear, practised and tested regularly? • Are staff performances regularly appraised? • Are there sufficient resources to carry out the procedures? • Are audits undertaken? If yes, how many times a year? • Are there controls in place?	

Level 2 Operational Requirement: Guard hut

Give title and date of the Level 1 OR to which this Level 2 OR relates:

Indicate where this OR integrates with additional Level 2 OR							**Date**			
Pedestrian Perimeter Barrier	Security Lighting	CCTV	PIDS	Physical Delay	Control of Access	IDS	Mail screening and security	Information Security (Infosec)	Guard Hut	Other

1. Location of the guard hut (NB. multiple locations will each require individual level 2 ORs) Identify the boundary or area where the guard hut will be located. • Vehicle check point • Pedestrian access/control point • Existing/proposed perimeter security • Inside or outside the perimeter security, e.g. near the asset. Integrated or standalone system (i.e. integrated with existing perimeter security or infrastructure.) Period of concern (i.e. what time length is the guard hut expected to be required for?) Occupancy period (how long will the guard hut be occupied for?)	
2. Guard hut function Who will be using the guard hut? (e.g. civilian or armed guards?) Identify the priority function(s) of the guard hut: • Provide shelter from the environment for guards • An observation post • Provide an area to retreat to for protection against defined threats • A fighting position • Communication point • Barrier control point for exit and/or entrances	

3. Vulnerability Identify features that make the location of the guard hut vulnerable: • Vehicle approaches • Pedestrian approaches • Lines of sight • Stand off from protected area	
4. Guard hut attack The asset is likely to be the main target of an attack, with a guard hut located on the perimeter viewed as a barrier to overcome. In cases where there is limited stand-off between the asset and a guard hut, the impact of the primary attack on the asset should be considered. Consider how the asset may be attacked. • VBIED (i.e. dynamic impact, blast and fragmentation effects) • PBIED (i.e. blast and fragmentation effects) • Small arms attack • Indirect fire attack Consider how the guard hut may be attacked. • Suppression of the guard hut to gain access to the asset or exit the protective area (i.e. concealed IED, small arms attack, indirect fire attack) • Penetrative attack to gain access to the asset or exit the protected area (i.e. ramming of vehicle) • Effects from an attack on the asset or on the guard hut (i.e. blast effects from VBIED, PBIED, indirect fire attack) Are there any secondary effects which need to be considered? (e.g. secondary fragmentation)	

5. Performance requirement **Under hostile attack:** • Maximum vehicle impact speed and impact angle (from Vehicle Dynamic assessment results) • Ballistic performance from small arms and indirect fire • Blast performance • Access requirement • Communication requirement • Barrier control requirement **Under normal operation:** • Power requirement • Lighting requirement • Temperature requirement • Communication requirement • Barrier control requirement and location, e.g. internal and external • Access requirement • Occupancy levels • Observation requirement	
6. Physical constraints Identify physical constraints which could affect the use or design of the guard hut: • Proposed/available space • Access to site, in particular width and height restrictions • Weight of unit(s) and lifting capacity/arc of lifting equipment • Ground conditions and topography • Underground services	
7. External constraints Identify external constraints which could affect the use or design of the guard hut: • Available services • Wind, rain, snow etc. • Temperature changes Are there legal requirements, e.g. Health and Safety at Work Act? If so, what are they?	

8. Rules and regulations Identify applicable rules and regulations that could prohibit or influence the installation or appearance of a guard hut: ● Local authority constraints ● Planning approval ● Site operational restrictions	
9. Success criteria What are the success criteria and how are they measured? ● Integration with other security measures ● Aesthetics ● Budget ● Reduce vulnerability level ● Physical presence / public perception	
10. Integration Confirm that the solution integrates with other level 2 ORs as appropriate. For example, fence, hostile vehicle barriers, CCTV, security lighting etc. Which OR takes precedence?	
11. Management issues ● Design and project management ● Planning, considering the need for an alternative access point during construction/installation if required. ● Construction and installation ● Quality and product assurance ● Testing, commissioning and handover ● Operational and Maintenance manuals ● Ownership after commissioning ● Security management procedures including manning levels ● Health and safety ● Standard operating procedures & guard force assignment instructions ● Leasing agreement	

12. Service & Maintenance contract requirements: • Documentation requirements, including drawings, programme listings, instructions and operation and maintenance manuals and logs; • Identify what needs to be included in the yearly routine maintenance. Service and maintenance arrangements, e.g. contractor or in-house. If the guard huts are going to be re-deployable, who will be responsible for delivery, management and storage of the stock? What is the design life of the guard hut and how long is it guaranteed for? How will the protection level be assessed during the service life, how often and by whom?	

Additional guidance/References

For further guidance or reference material, please refer to CPNI's Extranet for the following:

Pedestrian Perimeter Barrier
Policy & Good Practice Guidance>Physical Security>Pedestrian barriers and security containers

Hostile Vehicle Mitigation (HVM)
Policy & Good Practice Guidance>Physical Security>Hostile Vehicle Mitigation (HVM)

Security Lighting
Policy & Good Practice Guidance>Physical Security>Electronic and Imaging Systems (EIS)

Closed Circuit Television (CCTV)
Policy & Good Practice Guidance>Physical Security>Electronic and Imaging Systems (EIS)

Perimeter Intruder Detection Systems (PIDS)
Policy & Good Practice Guidance>Physical Security> Electronic and Imaging Systems (EIS)

Physical Delay Measures for Buildings
Policy & Good Practice Guidance>Physical Security>Pedestrian barriers and security containers

Control of Access
Policy & Good Practice Guidance>Physical Security>Electronic and Imaging Systems (EIS)

Intruder Detection Systems (IDS)
Policy & Good Practice Guidance>Physical Security>Electronic and Imaging Systems (EIS)

Information Security (INFOSEC)
Policy & Good Practice Guidance>Information Security

Mail Screening and Security
Policy & Good Practice Guidance>Physical Security>Explosives Research Group>Explosives and Weapons Search and Detection>Screening and Mail Deliveries