

# **GUIDE TO PRODUCING OPERATIONAL REQUIREMENTS FOR SECURITY MEASURES**

OCTOBER 2007

**CPNI**

Centre for the Protection  
of National Infrastructure

### **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 1998.

### **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.

# **Guide to Producing Operational Requirements for Security Measures**

**October 2007**

Version 1.1

## 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 for specific sites.

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

A Level 1 Operational Requirement 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 Operational Requirements follow on from the completed Level 1 Operational Requirement and addresses individual security measures (fences, CCTV, access control 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 Operational Requirements. Not all of these will be needed for every site.

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

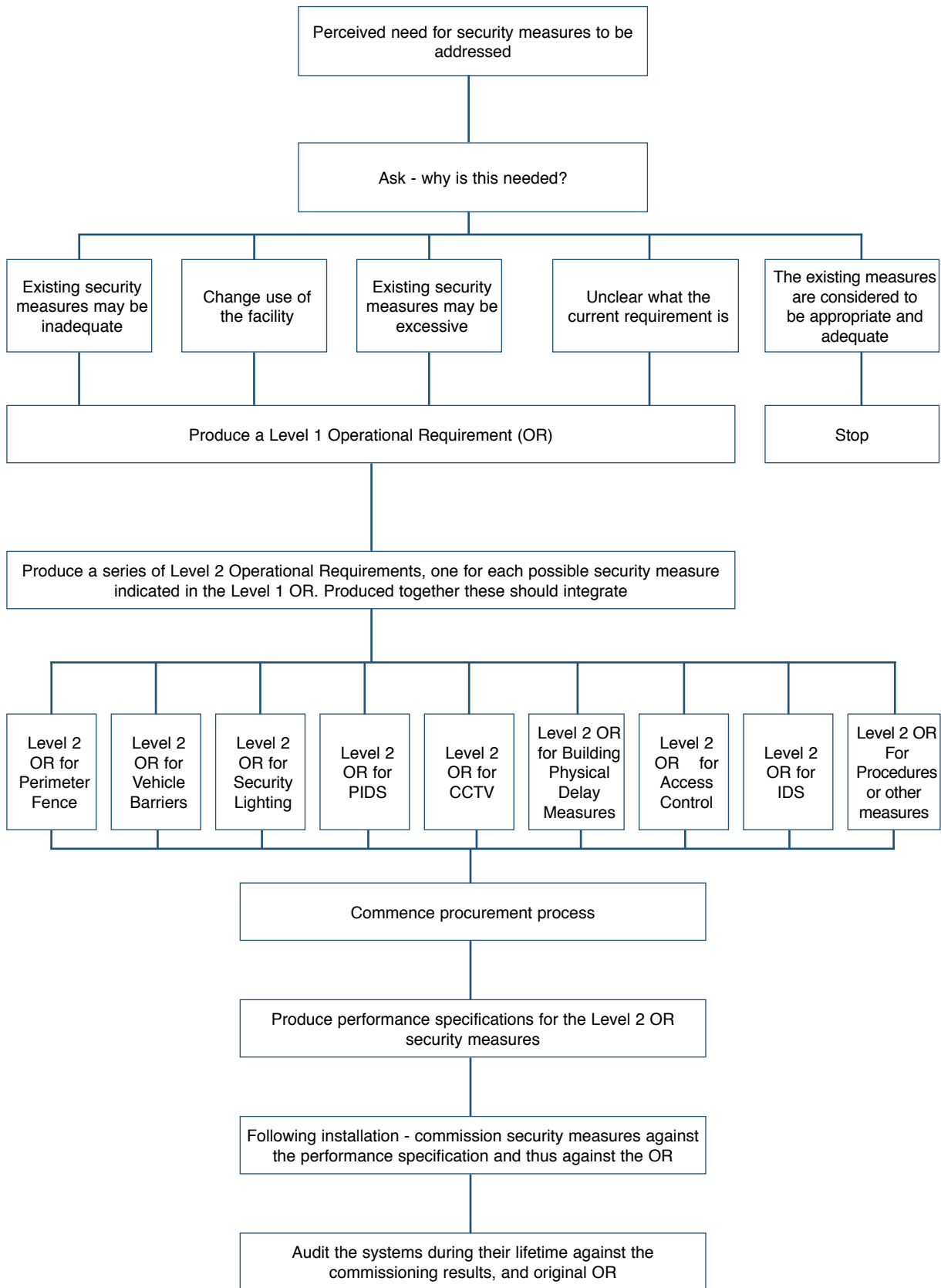


Figure 1

## Operational Requirement - Level 1

The Level 1 Operational Requirement is a statement of the overall security need.

It defines:

- The site or building under consideration
- The assets to be protected
- The perceived threats against the assets, and the probability of their occurrence
- The consequences of compromise of, or damage to, the assets
- The physical areas containing the assets that give concern, and the perceived vulnerability of those areas to the threat
- Success criteria
- Possible security solutions

ALL the stakeholders MUST be involved in the production of the Level 1 Operational Requirement (OR) to ensure that the solution is acceptable to all and that they have ownership of it.

The stakeholders are everyone 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.

All stakeholders should be asked to complete a checklist so that their views and interests are considered. This checklist is neither exhaustive nor in a priority order.

On completion of the Level 1 OR, Level 2 ORs should be produced.

The Level 2 Operational Requirement is a continuation of the Level 1 OR and is intended to produce a more detailed review for each area of concern with its particular possible solution.

### **OR - Level 1 Statement**

The OR statement is a written summary of the information collated on the checklists. It may be supported by completed checklists if felt useful.

## Level 1 Operational Requirement - Flow Chart

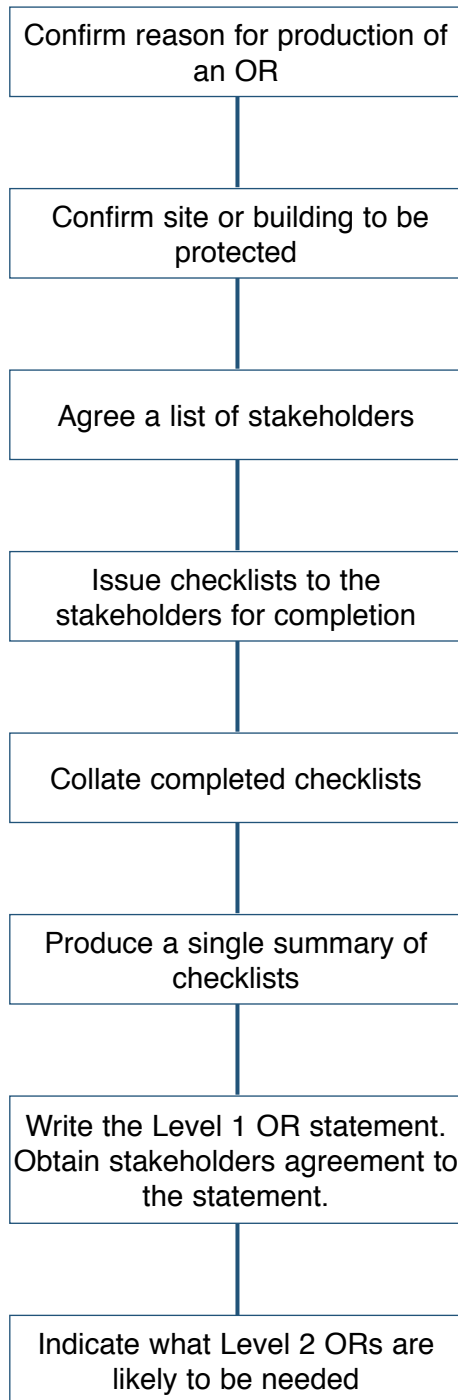


Figure 2

## Operational Requirement - Level 1 - Summary Checklists

### 1. Site or building

State the location and purpose of the site or building and any background comments on its priority or importance. State the boundaries of the site or building under consideration. This is to ensure that it is clear what land around buildings can be used for security measures.

### 2. Stakeholder

List all the stakeholders who should have an interest in the operational security of the site or building. Confirm whose priorities might be most important, and how any conflicting priorities might be resolved.

### 3. Assets to be protected

List the assets that are to be protected (human, physical, intellectual) together with their value (human, financial, operational, political).

### 4. The threat

State the perceived threat, the likely abilities of attackers, the tools they may be expected to use, and the most likely methods of attack. Try to estimate, in broad terms, the probability and frequency of the event occurring.

### 5. Consequences of compromise

State what these are in terms of financial, operational, morale and political (embarrassment) consequences. Additionally, consider how easy it would be to replace these assets. [There may be different assets on the site with different consequences - these should be recorded] Tie in the importance of each site/building to section 1 above.

**6. Areas of concern and vulnerabilities**

What are your areas of concern and vulnerabilities? For example Freedom of Information Act or Data Protection Act etc. or the areas where the assets are located (individual site or building). An attempt should be made to indicate how these sites are vulnerable to the threat. [Tie in with most likely methods of attack (section 4 above). ]  
List each defined area. Each of these will be the subject of a Level 2 OR later

--

**7. Success criteria**

What are your success criteria? For example the detection of all intruders, or preventing an intruder reaching an asset before he is intercepted by the response force, or obtaining evidence for legal purposes.  
List as many as possible.

--

**8. Other Factors**

Include any constraints like planning permission, neighbouring facilities, staffing levels, response force and environmental considerations like weather and vegetation. Also include procedures and management controls. This section might state which possible solutions have been discounted and why.

--

**9. Possible security solutions**

While considering the 'areas of concern and vulnerabilities' various possible solutions will have come to mind. These thoughts should be noted, together with any constraints that may apply. Keep an open mind; this is still only the statement of needs not the final solution.

--

**Note : This list is neither prioritised nor all inclusive nor should it necessarily be completed sequentially. It acts as a guide only.**

## Operational Requirement - Level 1 - Stakeholders Checklists

### 1. Site or building

State the location and purpose of the site or building and any background comments on its priority or importance. State the boundaries of the site or building under consideration. This is to ensure that it is clear what land around buildings can be used for security measures.

### 2. Assets to be protected

List the assets that are to be protected (human, physical, intellectual) together with their value (human, financial, operational, political).

### 3. The threat

State the perceived threat, the likely abilities of attackers, the tools they may be expected to use, and the most likely methods of attack. Try to estimate, in broad terms, the probability and frequency of the event occurring.

### 4. Consequences of compromise

State what these are in terms of financial, operational, morale and political (embarrassment) consequences. Additionally, consider how easy it would be to replace these assets. [There may be different assets on the site with different consequences - these should be recorded] Tie in the importance of each site/building to section 1 above.

### 5. Areas of concern and vulnerabilities

What are your areas of concern and vulnerabilities? For example Freedom of Information Act or Data Protection Act etc. or the areas where the assets are located (individual site or building). An attempt should be made to indicate how these sites are vulnerable to the threat. [Tie in with most likely methods of attack (section 4 above). ]  
List each defined area. Each of these will be the subject of a Level 2 OR later

**6. Success criteria**

What are your success criteria? For example the detection of all intruders, or preventing an intruder reaching an asset before he is intercepted by the response force, or obtaining evidence for legal purposes.  
List as many as possible.

**7. Other Factors**

Include any constraints like planning permission, neighbouring facilities, staffing levels, response force and environmental considerations like weather and vegetation. Also include procedures and management controls. This section might state which possible solutions have been discounted and why.

**8. Possible security solutions**

While considering the 'areas of concern and vulnerabilities' various possible solutions will have come to mind. These thoughts should be noted, together with any constraints that may apply. Keep an open mind; this is still only the statement of needs not the final solution.

**Note :** This list is neither prioritised nor all inclusive nor should it necessarily be completed sequentially. It acts as a guide only.

## Operational Requirement - Level 2

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

The Level 1 OR will encourage some possible solutions to be suggested. Some of these may be quickly discounted for quite valid reasons (operational or aesthetic for example) and a note should be made of this. The remainder will be considered in more detail in this the Level 2 OR.

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

The Level 2 ORs now look at each of the suggested solutions and expand the Level 1 OR and, in addition, consider the function of the possible solution, target concerns, operator interfaces and risk analysis.

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.

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

### **OR - Level 2 Statement**

The Level 2 OR statement is a written summary of the information collated from the checklists. 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 relationship with the agreed need 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 is not a specification, it expands the Level 1 requirement statement to provide more detail to enable a designer to produce performance specifications 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

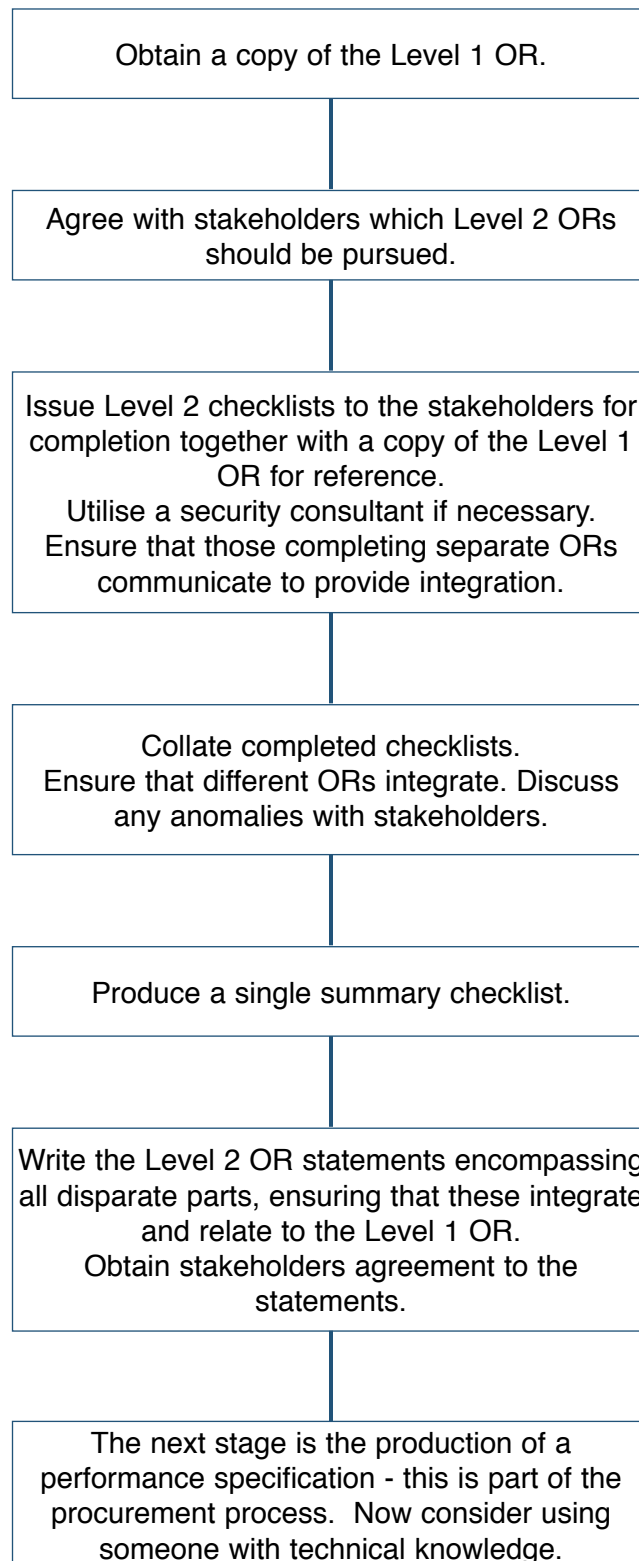


Figure 3

## Level 2 Operational Requirement for a Perimeter Fence

Give title and date of the Level 1 OR to which this Level 2 OR relates:							Date			
Indicate other Level 2 ORs being produced concurrently with this one:	Vehicle barriers	Perimeter fence	Security lighting	CCTV	PIDS	Physical delay	Access control	IDS	Other?	

<p><b>1. Area of concern</b></p> <p>Identify the boundary or area to be protected</p>	
<p><b>2. What is (are) the function(s) of the perimeter fence?</b></p> <p>Demarcation of boundary                      To deter entry into the area<sup>1</sup>                      To protect against climb over<sup>1</sup>                      To protect against cut through<sup>1</sup>                      To protect against vehicle intrusion                      Outer &amp; inner fence with sterile zone to support PIDS - to help to detect an intruder                      Concealment of guards and/or activity</p>	
<p><b>3. Vulnerable points</b></p> <p>List features that will reduce the effectiveness of the perimeter fence (areas of cover, trees, adjacent buildings, other climbing aids.)</p>	
<p><b>4. Environmental considerations</b></p> <p>Is Local Authority Planning approval required?                      Describe adjacent property                      Is the type of fence topping a possible constraint?                      Legal Requirements.</p>	

<sup>1</sup> Define by whom

<p><b>5. Performance requirement</b></p> <p><b>WITH PIDS</b>          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.</p> <p><b>WITHOUT PIDS</b>          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).</p>	
<p><b>6. Risk analysis (confirm with all stakeholders)</b></p> <p>Is this task mandatory or covered by minimum baseline measures?</p> <p>Compared to the other areas of concern what is the priority for this one?</p> <p>What is the likelihood of the threatening activity occurring and how often?</p> <p>What are the benefits of doing this task over not doing it?</p>	
<p><b>7. Success criteria</b>          What are your success criteria?          List as many as possible.</p>	
<p><b>8. Integration</b>          Confirm that the solution integrates with other ORs as appropriate</p>	
<p><b>9. Management Issues</b>          Are there procedures, training, resources in place?          If yes, are procedures clear and practised 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?</p>	

## Level 2 Operational Requirement for Vehicle Barriers

<b>Give title and date of the Level 1 OR to which this Level 2 OR relates:</b>							<b>Date</b>		
<b>Indicate other Level 2 ORs being produced concurrently with this one:</b>	Vehicle barriers	Perimeter fence	Security lighting	CCTV	PIDS	Physical delay	Access control	IDS	Other?

<p><b>1. Area of concern</b></p> <p>Identify the boundary or area to be protected.</p>	
<p><b>2. What is the function of the Vehicle Barrier?</b></p> <p>Perimeter protection          Local permanent closure          To support access control measures          To provide a vehicle access control point          To slow or stop attacking vehicles          To maintain suitable stand off from buildings.</p>	
<p><b>3. Vulnerable points</b></p> <p>List features that will reduce the effectiveness of the perimeter as a vehicle barrier (eg approach routes, wide range and volume of vehicles that need to use the access point)          Identify those parts of the site that can be approached by vehicles particularly at speed.</p>	
<p><b>4. Environmental considerations</b></p> <p>Is Local Authority Planning approval needed?          Is there a high water table?          Are there a lot of services just below the surface?          What use can be made of natural features such as trees, banks and ditches?          Will a traffic management plan be needed?          Consider safety changes in traffic flow and the operational capability to react to changes in security levels.</p>	

<p><b>5. Performance requirement</b></p> <p>What are the likely size and types of vehicles and their likely approach speeds at the barrier? Is there a requirement to allow vehicle access through the barrier, if so, how many per hour?</p>	
<p><b>6. Risk analysis (confirm with all stakeholders)</b></p> <p>Is this task mandatory or covered by minimum baseline measures?</p> <p>Compared to the other areas of concern what is the priority for this one?</p> <p>What is the likelihood of the threatening activity occurring and how often?</p> <p>What are the benefits of doing this task over not doing it?</p>	
<p><b>7. Success criteria</b></p> <p>What are your success criteria? List as many as possible.</p>	
<p><b>8. Integration</b></p> <p>Confirm that the solution integrates with other ORs as appropriate (note that the vehicle barrier and fence should have similar vehicle resistance).</p>	
<p><b>9. Management Issues</b></p> <p>Are there procedures, training, resources in place?</p> <p>If yes, are procedures clear and practiced regularly?</p> <p>Are there sufficient resources to carry out the procedures?</p> <p>Are audits undertaken?</p> <p>If yes, how many times a year?</p> <p>Are there controls in place?</p>	

## Level 2 Operational Requirement for Security Lighting

Give title and date of the Level 1 OR to which this Level 2 OR relates:							Date			
Indicate other Level 2 ORs being produced concurrently with this one:	Vehicle barriers	Perimeter fence	Security lighting	CCTV	PIDS	Physical delay	Access control	IDS	Other?	

<p><b>1. Area of concern</b></p> <p>Identify the boundary or area to be protected. [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].</p>	
<p><b>2. What is (are) the primary function(s) of the lighting system?</b></p> <p>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.</p>	
<p><b>3. What is (are) the secondary function(s) of the lighting system?</b></p> <p>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.</p>	
<p><b>4. Existing lighting</b></p> <p>State what lighting already exists Street lighting outside the site Amenity and building lighting within the site What lamp types are in use?</p>	
<p><b>5. Vulnerable points</b></p> <p>List features that will reduce the effectiveness of the lighting system. (trees, areas of cover).</p>	
<p><b>6. Environmental considerations</b></p> <p>Weather conditions Be aware of light pollution regulations Consider infrared lighting Is Local Authority planning approval needed? Describe properties adjacent to the boundary. List all roads and railways near the boundary.</p>	

<p><b>7. Operational issues</b></p> <p>Is site blackout needed?          Are de-mountable columns needed for maintenance?          Any particular control needs, e.g. Photocell with manual override?          What are the power supply needs?          Is uninterrupted power supply required?          Strike up and restrike time (time between initiation of power to the lighting system being fully effective).</p>	
<p><b>8. Performance requirement</b></p> <p>State the need from the operator's viewpoint, e.g.:          See crawling intruder at xx metres from fence          Detect damage to fence fabric          Recognise vehicle colour          Reading number plates          Recognise skin tones.</p>	
<p><b>9. Risk analysis (confirm with all stakeholders)</b></p> <p>Is this task mandatory or covered by minimum baseline measures?          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?</p>	
<p><b>10. Success criteria</b></p> <p>What are your success criteria?          List as many as possible.</p>	
<p><b>11. Integration</b></p> <p>Confirm that the solution integrates with other ORs as appropriate.</p> <p>How will the lighting work with CCTV?</p>	
<p><b>12. Management Issues</b></p> <p>Are there procedures, training, resources in place?          If yes, are procedures clear and practiced 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?</p>	

## Level 2 Operational Requirement for CCTV Surveillance Systems

<b>Give title and date of the Level 1 OR to which this Level 2 OR relates:</b>							<b>Date</b>			
<b>Indicate other Level 2 ORs being produced concurrently with this one:</b>	Vehicle barriers	Perimeter fence	Security lighting	CCTV	PIDS	Physical delay	Access control	IDS	Other?	

<p><b>1. Area of concern</b></p> <p>Identify the area(s) to be covered. (Where the area to be covered is large or complicated it is advisable to break the area down into smaller units and to complete a separate checklist for each.)</p>	
<p><b>2. What is (are) the purpose of the CCTV surveillance system?</b></p> <p>Describe the activity that is a threat to the assets. [This might be covert entry into vulnerable areas, attacking an asset or vehicle ram raiding] Describe the object(s) of concern and the target(s) to be viewed. List the specific areas to be covered with the observation criteria for each one. These criteria are monitoring detection, recognition or identification of the target (including any evidential requirement) Where perimeter detection systems are to be viewed consider the zone lengths and locations.</p>	
<p><b>3. Vulnerable points</b></p> <p>List the features that will reduce the effectiveness of the CCTV surveillance systems (trees, adjacent buildings, areas of cover).</p>	
<p><b>4. Environmental considerations</b></p> <p>Is Local Authority planning approval needed? Weather conditions Legal requirements eg DPA (Data Protection Act).</p>	
<p><b>5. Performance requirements</b></p> <p>Verify alarm activation within xxx seconds. Monitoring and intruder (ie able to confirm recognition of target reading number plates/ vehicle colours).</p>	

<p><b>6. Operational Issues</b></p> <p>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 of the event 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 to make the right decision.          Is there an uninterrupted power supply (UPS)?</p>	
<p><b>7. Risk analysis (confirm with all stakeholders)</b></p> <p>Is this task mandatory or covered by minimum baseline measures?          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?</p>	
<p><b>8. Success criteria</b></p> <p>What are your success criteria?          List as many as possible.</p>	
<p><b>9. Integration</b></p> <p>Confirm that the solution integrates with other ORs as appropriate. PIDS fences, AACS, lighting, procedures for response force.</p>	
<p><b>10. Management Issues</b></p> <p>Are there procedures, training, resources in place?          If yes, are procedures clear and practised 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?</p>	

## Level 2 Operational Requirement for Perimeter Intruder Detection Systems (PIDS)

<b>Give title and date of the Level 1 OR to which this Level 2 OR relates:</b>							<b>Date</b>			
<b>Indicate other Level 2 ORs being produced concurrently with this one:</b>	Vehicle barriers	Perimeter fence	Security lighting	CCTV	PIDS	Physical delay	Access control	IDS	Other?	

<p><b>1. Area of concern</b></p> <p>Describe the area or boundary where detection is required.</p> <p>What is the approximate length of the boundary?</p> <p>Where is the boundary non-contiguous (gates, rivers, buildings etc)?</p> <p>Is a sterile area available? If it is, how wide is it?</p>	
<p><b>2. What is the function of the PIDS?</b></p> <p>Describe the object(s) of concern (the target(s) to be detected).</p> <p>Detect activity at the perimeter. What are activities that would concern you?</p> <ul style="list-style-type: none"> <li>-Detect activity</li> <li>-Detect individual climbing</li> <li>-Detect individual cutting</li> <li>-Detect individual digging under.</li> <li>-Individual crossing restricted zone/trip wire</li> <li>-Vehicle crossing restricted zone/trip wire</li> </ul>	
<p><b>3. Vulnerable points</b></p> <p>List points at the perimeter that may cause increased vulnerability.</p> <p>Streams, rivers etc crossing the boundary.</p> <p>Vehicles ability to get close to the boundary.</p>	
<p><b>4. Environmental conditions</b></p> <p>At what time of day is the activity a threat?</p> <p>Weather conditions</p> <p>Legal requirements</p>	
<p><b>5. Performance requirement</b></p> <p>Acceptable false alarm rates</p> <p>Acceptable detection alarm rates</p> <p>Acceptable zone lengths.</p>	

<p><b>6. Operational Issues</b></p> <p>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.          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?</p> <p>Consider what needs to be available to help the operator make the right decision.</p>	
<p><b>7. Risk Analysis (confirm with all stakeholders)</b></p> <p>Is this task mandatory or covered by minimum baseline measures?</p> <p>Compared to the other areas of concern what is the priority for this one?</p> <p>What is the likelihood of the threatening activity occurring and how often?</p> <p>What are the benefits of doing this task over not doing it?</p>	
<p><b>8. Success criteria</b></p> <p>What are your success criteria?          List as many as possible</p>	
<p><b>9. Integration</b></p> <p>Confirm that the solution integrates with other ORs as appropriate.          Is an IDs system to be installed to the measure or AACS?</p>	
<p><b>10. Management Issues</b></p> <p>Are there procedures, training, resources in place?          If yes, are procedures clear and practised 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?</p>	

## Level 2 Operational Requirement for Physical Delay Measures.

<b>Give title and date of the Level 1 OR to which this Level 2 OR relates:</b>							<b>Date</b>			
<b>Indicate other Level 2 ORs being produced concurrently with this one:</b>	Vehicle barriers	Perimeter fence	Security lighting	CCTV	PIDS	Physical delay	Access control	IDS	Other?	

<p><b>1. Area of concern (existing building)</b></p> <p>Identify the elements of the building or room that require physical delay measures. Identify where delays are required where they do not currently exist.</p> <p><b>Area of concern (new building)</b></p> <p>Identify the elements of the building to be physically hardened against attack. Identify best locations for delay.</p>	
<p><b>2. What is (are) the function(s) of the Physical Barrier(s)?</b></p> <p>To deter entry into a building or area (state by whom)                  To provide a point of detection                  To provide a "post detection delay".</p>	
<p><b>3. Vulnerable points.</b></p> <p>List features that are easily defeated (state by whom).</p>	
<p><b>4. Environmental considerations</b></p> <p>Listed Building constraints                  Type of property i.e. industrial, office etc.                  Legal requirements e.g. HSE.</p>	
<p><b>5. Performance requirement</b></p> <p>Minimum acceptable delay against what sort of attacker equipped with certain types of tools.</p>	
<p><b>6. Operational issues</b></p> <p>Is the site manned 24 hrs 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?</p>	

<p><b>7. Risk analysis (confirm with all stakeholders)</b></p> <p>Is this task mandatory or covered by minimum baseline measures?</p> <p>Compared to the other areas of concern what is the priority for this one?</p> <p>What is the likelihood of the threatening activity occurring and how often?</p> <p>What are the benefits of doing this task over not doing it?</p>	
<p><b>8. Success criteria</b></p> <p>What are your success criteria? List as many as possible.</p>	
<p><b>9. Integration</b></p> <p>Confirm that the solution integrates with other ORs as appropriate. Is an IDS system to be installed to the measure or AACS</p>	
<p><b>10. Management Issues</b></p> <p>Are there procedures, training, resources in place? If yes, are procedures clear and practised 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?</p>	

## Level 2 Operational Requirement for Control of Access.

Give title and date of the Level 1 OR to which this Level 2 OR relates:							Date			
Indicate other Level 2 ORs being produced concurrently with this one:	Vehicle barriers	Perimeter fence	Security lighting	CCTV	PIDS	Physical delay	Access control	IDS	Other?	

<p><b>1. Area of concern</b></p> <p>Identify the areas, building(s) or room(s) where access is to be controlled. Is the building/site to be 'zoned'?</p>	
<p><b>2. What is the function of the access control system?</b></p> <p>To control people, vehicles?</p>	
<p><b>3. Vulnerable points</b></p> <p>Points where access is to be controlled</p> <p>All other points of entry to the areas that will need to be secured.</p> <p>Indicate which are emergency exits.</p>	
<p><b>4. Environmental considerations</b></p> <p>Legal Health &amp; Safety Disability &amp; Discrimination Act (DDA).</p>	
<p><b>5. Operational Issues</b></p> <p><b>Fire Officers' requirements</b> Release on emergency Muster points Need for occupation reports by number and location (Impacts on anti-tailgating, anti-passback and swipe in/out) Are there control of passes?</p> <p>What are the requirements for disabled access?</p> <p><b>Minimum security requirements</b> Areas requiring minimum occupation Anti-tailgating? Anti-passback? By-passing barrier?</p> <p><b>How will access for:</b> Disabled Visitors Other non pass holders Contractors be controlled?</p> <p>Are there control of passes?</p> <p>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?</p> <p>How will security clearances be processed?</p>	

<p><b>6. Performance requirement</b></p> <p>Consider token options: Proximity, proximity plus PIN.</p> <p>Swipe, swipe plus PIN.</p> <p>Level of security requirement</p> <p>Zoning.</p>	
<p><b>7. Risk analysis (confirm with all stakeholders)</b></p> <p>Is this task mandatory or covered by minimum baseline measures?</p> <p>Compared to the other areas of concern what is the priority for this one?</p> <p>What is the likelihood of an unauthorised attempt at access occurring and how often?</p> <p>What are the benefits of doing this task over not doing it?</p>	
<p><b>8. What are your success criteria?</b></p> <p>List as many as possible.</p>	
<p><b>9. Integration</b></p> <p>Confirm that the solution integrates with other ORs as appropriate. For example barriers, CCTV procedures plus others.</p>	
<p><b>10. Management Issues</b></p> <p>Are there procedures, training, resources in place?</p> <p>If yes, are procedures clear and practiced regularly?</p> <p>Are there sufficient resources to carry out the procedures?</p> <p>Are audits undertaken?</p> <p>If yes, how many times a year?</p> <p>Are there controls in place?</p>	

## Level 2 Operational Requirement Checklist for Intruder Detection Systems (IDS).

<b>Give title and date of the Level 1 OR to which this Level 2 OR relates:</b>							<b>Date</b>			
<b>Indicate other Level 2 ORs being produced concurrently with this one:</b>	Vehicle barriers	Perimeter fence	Security lighting	CCTV	PIDS	Physical delay	Access control	IDS	Other?	

<p><b>1. Area of concern</b></p> <p>Identify the building or room(s) to be covered.</p>	
<p><b>2. What are the functions of IDS?</b></p> <p>Describe the object(s) of concern</p> <p>Describe the activity that is a threat to the assets.</p>	
<p><b>3. Vulnerable points</b></p> <p>List the possible points of entry to the area of concern (doors, windows, walls, roof, ducts etc.)</p>	
<p><b>4. Environmental considerations</b></p> <p>Weather conditions</p> <p>Bulding heating</p> <p>Legal Issues</p> <p>Air conditioning.</p>	
<p><b>5. Performance requirements</b></p> <p>PIDS</p> <p>False alarm rates</p> <p>Detected alarm rates.</p>	

<p><b>6. Operational Issues</b></p> <p>At what time of day is the activity a threat?</p> <p>When the threatening activity is detected what will the response be?</p> <p>How quickly is attendance at the point of activity needed?</p> <p>Consider both verification and communication with response force.</p> <p>Where will activity be monitored and by whom?</p> <p>Who makes the response decision?</p> <p>How is the decision arrived at?</p> <p>How quickly does the operator need to respond to the activity for the response to be effective?</p> <p>Consider what needs to be available to help the operator make the right decision.</p>	
<p><b>7. Risk analysis (confirm with all stakeholders)</b></p> <p>Is this task mandatory or covered by minimum baseline measures?</p> <p>Compared to the other areas of concern what is the priority for this one?</p> <p>What is the likelihood of the threatening activity occurring and how often?</p> <p>What are the benefits of doing this task over not doing it?</p>	
<p><b>8. Success criteria</b></p> <p>How are your success criteria?</p> <p>List as many as possible.</p>	
<p><b>9. Integration</b></p> <p>Confirm that the solution integrates with other ORS as appropriate. Building fabrics, AACS, procedures.</p>	
<p><b>10. Management Issues</b></p> <p>Are there procedures, training, resources in place?</p> <p>If yes, are procedures clear and practiced regularly?</p> <p>Are there sufficient resources to carry out the procedures?</p> <p>Are audits undertaken?</p> <p>If yes, how many times a year?</p> <p>Are there controls in place?</p>	

## Level 2 Operational Requirement for Procedures

<b>Give title and date of the Level 1 OR to which this Level 2 OR relates:</b>								<b>Date</b>	
<b>Indicate other Level 2 ORs being produced concurrently with this one:</b>	Vehicle barriers	Perimeter fence	Security lighting	CCTV	PIDS	Physical delay	Access control	IDS	Other?

<p><b>1. Area of concern</b></p> <p>Identify the area or site.</p>	
<p><b>2. What are the functions of procedures?</b></p> <p>Describe the duties of any good guard force:          Monitor CCTV          Patrolling          Access control          Searching visitors/staff          Response to alarms or attack          Escorting visitors          Logging visitors on and off sites          Miscellaneous administrative duties.</p>	
<p><b>3. Vulnerable points</b></p> <p>Identify any elements of the site that are particularly vulnerable to attack or where protective measures can be defeated.</p>	
<p><b>4. Environmental considerations</b></p> <p>At what time of day is the activity a threat?</p> <p>Weather conditions</p> <p>Legal requirements.</p>	
<p><b>5. Performance requirements</b></p> <p>Response times to any intrusion/alarm.</p> <p>Quantify any duties proposed in para 2.</p>	
<p><b>6. Operational Issues</b></p> <p>Are all elements of the guard force required 24hrs a day?</p> <p>Is the guard force required for 24hrs a day?</p> <p>Does the guard force provide a response ability? If so what?</p> <p>Is the response arrived?</p>	

<p><b>7. Risk analysis (confirm with all stakeholders)</b></p> <p>Are these tasks mandatory or covered by minimum baseline measures?</p> <p>Compared to the other areas of concern what is the priority for this one?</p> <p>What is the likelihood of the threatening activity occurring and how often?</p> <p>What are the benefits of doing this task over not doing it?</p>	
<p><b>8. Success criteria</b></p> <p>How are your success criteria?</p> <p>List as many as possible.</p>	
<p><b>9. Integration</b></p> <p>Confirm that the procedures integrates with other ORs as appropriate. Building fabrics, AACS, procedures.</p>	
<p><b>10. Management Issues</b></p> <p>Are there procedures, training, resources in place?</p> <p>If yes, are procedures clear and practiced regularly?</p> <p>Are there sufficient resources to carry out the procedures?</p> <p>Are audits undertaken?</p> <p>If yes, how many times a year?</p> <p>Are there controls in place?</p>	

## Notes

## Notes

## Notes