European
Forum *for*
Urban
Security

Factsheet N°3

How to use/fill in the Record template

PRoTECT

This project has received funding from the European Union's Horizon 2020
ISFP programme under grant agreement n° 815356

As stated in the factsheet N°2 "Preparing a vulnerability assessment", before carrying out the assessment the managing body must undertake the following steps:

1. Gather information about the PSOI and define relevant criteria;
2. Create a team of experts;
3. Decide on a work-method.

Having done this, the managing body and team of experts can conduct the assessment using the record template (see Annex 1).

Reminder: General procedure for preparing and conducting a vulnerability assessment by using the record template

1. **Decide which phase is relevant for the main site and each surrounding sit;.**
2. **Conceive viable attack scenarios from combinations of threat types, situations and currently existing natural and emplaced security measures;**
3. **Estimate the consequence and probability of each attack scenario following the assessment suggestions;**

The record template to conduct the vulnerability assessment is designed so that users are stimulated to use their creativity and imagination in discovering possible attack scenarios, to limit the chance that an important vulnerability is overlooked. Scenarios should be a mix of possible threat types, images, situations, questions and examples, to be used as inspiration in discussions[1]. Once the attack scenarios and levels for the consequences and probabilities have been determined, the risk levels can be established using a risk matrix. It is important that the implications, i.e. meanings, of each level of risk are clear.

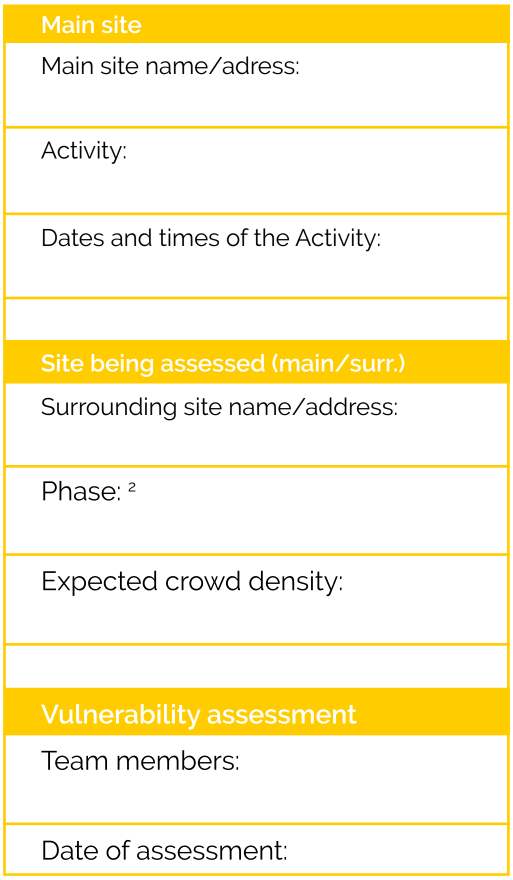
The following 5 steps are to be carried out when conducting a vulnerability assessment and filling the template:

1. Characteristics of the site;
2. Existing security measures;
3. Scenario per threat type;
4. Consequence and probability;
5. Analysis and results;

[1] The managing body should attempt to obtain more specific threat information from governmental or commercial experts. If you decide to exclude certain types of attacks, or to include others, it is important for traceability, accountability and for evaluation purposes to document your argumentation.

STEP 1: CHARACTERISTICS OF THE SITE

The first step consists of writing down the characteristics of the site that is being assessed. This is the upper left column in the record template:



Main site
Main site name/adress:
Activity:
Dates and times of the Activity:
Site being assessed (main/surr.)
Surrounding site name/address:
Phase: [2]
Expected crowd density:
Vulnerability assessment
Team members:
Date of assessment:

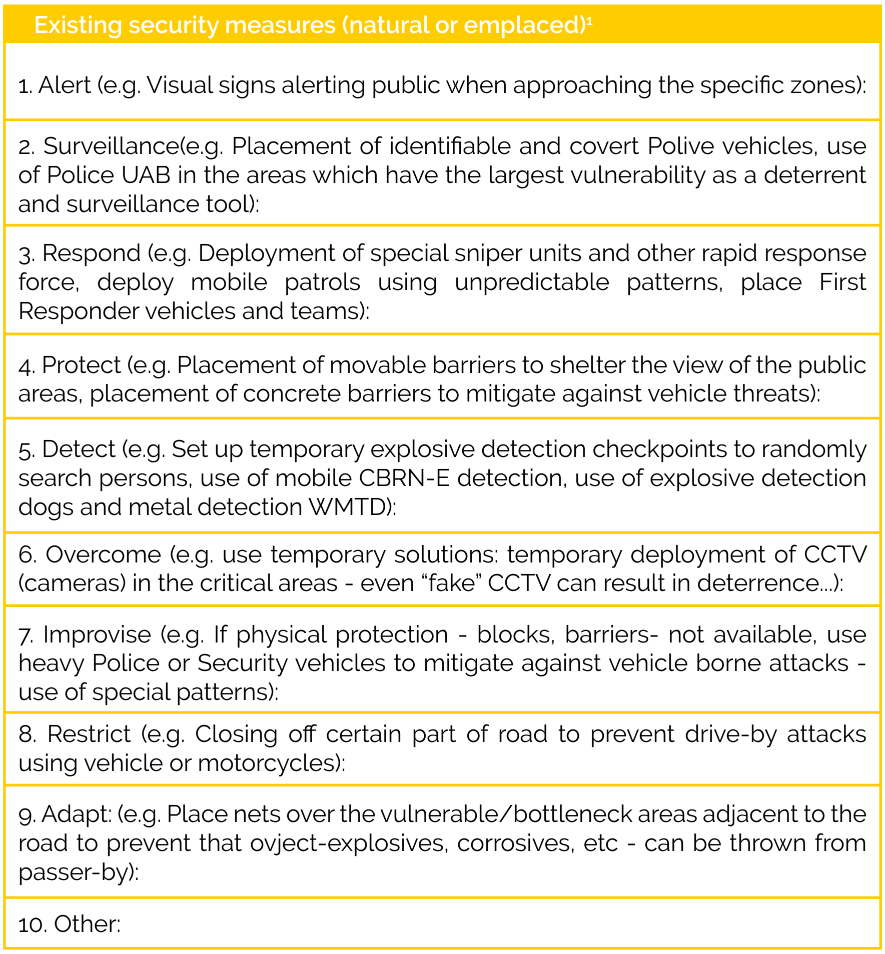
Figure 1:
Left upper column of record template; main site, site being assessed & vulnerability assessment.

- Write the necessary details like the main site's name, if there are specific activities happening (like a festival, market or something else) and when this activity occurs. The dates and times are important in order to be aware if an activity takes place regularly or if it is incidental;
- Write down the details of the site, the name and address, in which phase of the EU VAT the site fits and what the expected crowd density is (NB the crowd density could vary at specific times, please add this if relevant);
- It is also useful to add the team members and assessment date with the idea of conducting vulnerability assessments regularly to check on the PSOI's vulnerabilities.

STEP 2: EXISTING SECURITY MEASURES

- Write the existing security measures that you are aware of for the specific site in the upper right column of the record template. Based on the information collected previously (see factsheet 2), this part of the template should be filled in. It is suggested to fill in this part in advance and complete it with the expert group during the assessment;

  Some categories and examples of security measures could be:



Existing security measures (natural or emplaced)[1]
1. Alert (e.g. Visual signs alerting public when approaching the specific zones):
2. Surveillance(e.g. Placement of identifiable and covert Polive vehicles, use of Police UAB in the areas which have the largest vulnerability as a deterrent and surveillance tool):
3. Respond (e.g. Deployment of special sniper units and other rapid response force, deploy mobile patrols using unpredictable patterns, place First Responder vehicles and teams):
4. Protect (e.g. Placement of movable barriers to shelter the view of the public areas, placement of concrete barriers to mitigate against vehicle threats):
5. Detect (e.g. Set up temporary explosive detection checkpoints to randomly search persons, use of mobile CBRN-E detection, use of explosive detection dogs and metal detection WMTD):
6. Overcome (e.g. use temporary solutions: temporary deployment of CCTV (cameras) in the critical areas - even "fake" CCTV can result in deterrence...):
7. Improvise (e.g. If physical protection - blocks, barriers- not available, use heavy Police or Security vehicles to mitigate against vehicle borne attacks - use of special patterns):
8. Restrict (e.g. Closing off certain part of road to prevent drive-by attacks using vehicle or motorcycles):
9. Adapt: (e.g. Place nets over the vulnerable/bottleneck areas adjacent to the road to prevent that ovject-explosives, corrosives, etc - can be thrown from passer-by):
10. Other:

Figure 2:
Right upper column of record template; existing security measures.

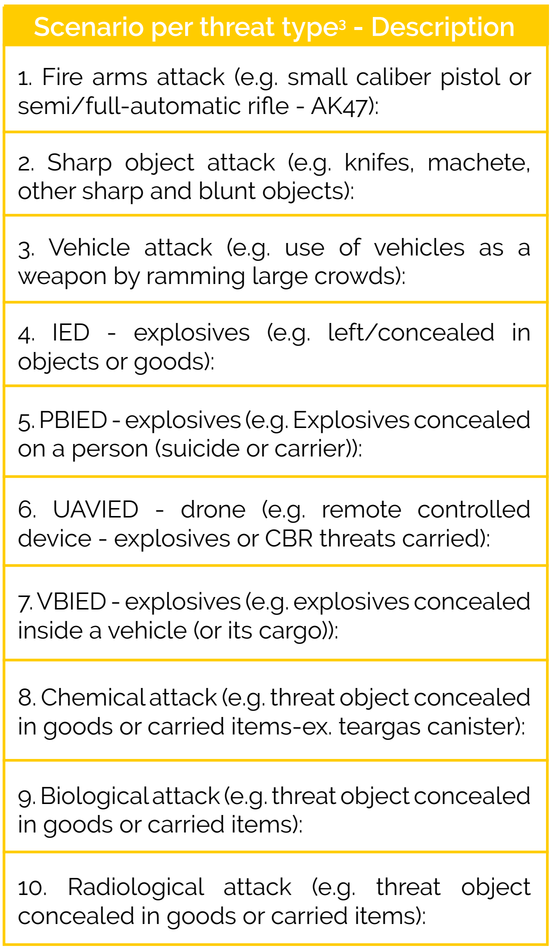
- The measures can be natural e.g a wall to hide behind, or emplaced e.g roadblocks;
- It can be useful to go through all the types one at a time and ask yourselves if there are any measures that fit;
- NB this exercise is to identify existing measures that have an effect on identifying vulnerabilities, not to think of measures that are not yet in place but that may mitigate potential threats.

STEP 3: SCENARIO PER THREAT TYPE

Choose the phase[2] to which the site in question belongs (determined in Step 1). The phases that a person goes through to get to the main site (i.e. participate in the activity) of the PSOI are as follows:

- Phase 1: Access to the Venue
- Phase 2: Parking and Transport
- Phase 3: Approach to Venue
- Phase 4: Arrival at Venue
- Phase 5: Venue Security – No Access Control
- Phase 6: Venue Security – With Access Control

On the record template there are ten terrorist threat types that need to be assessed for each site; please go through every threat. You can write down scenarios for each threat in left column at the bottom of the record template:



Scenario per threat type[3] - Description
1. Fire arms attack (e.g. small caliber pistol or semi/full-automatic rifle - AK47):
2. Sharp object attack (e.g. knifes, machete, other sharp and blunt objects):
3. Vehicle attack (e.g. use of vehicles as a weapon by ramming large crowds):
4. IED - explosives (e.g. left/concealed in objects or goods):
5. PBIED - explosives (e.g. Explosives concealed on a person (suicide or carrier)):
6. UAVIED - drone (e.g. remote controlled device - explosives or CBR threats carried):
7. VBIED - explosives (e.g. explosives concealed inside a vehicle (or its cargo)):
8. Chemical attack (e.g. threat object concealed in goods or carried items-ex. teargas canister):
9. Biological attack (e.g. threat object concealed in goods or carried items):
10. Radiological attack (e.g. threat object concealed in goods or carried items):

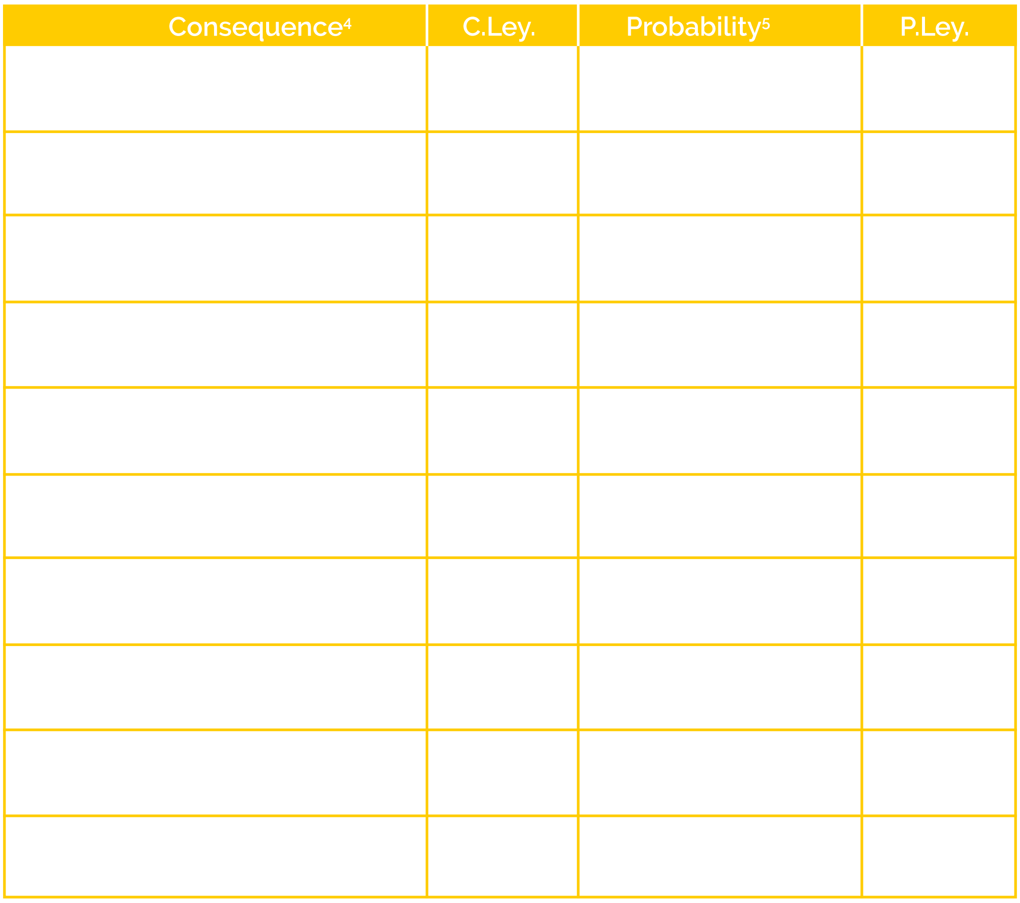
Figure 3:
Bottom left column of record template; scenario per threat type

- For every threat, Annex 3 provides an example to help form a realistic scenario. Please also use any information you have gathered beforehand on known threats and current threat assessments (see the factsheet 2 "Preparing a vulnerability assessment" for examples/more details);
- When conceiving attack scenarios for a site, also consider combinations of existing measures for the site with existing measures and weaknesses on other sites belonging to the PSOI. Please also take into account the current threat level or your own previous threat assessment regarding this specific attack if you have this information;
- Only assess scenarios that the team decides are realistic and feels the urge to know how vulnerable the site is to such a scenario;
- If you decide to exclude certain types of attacks, or to include others, it is important for traceability, accountability and for evaluation purposes to document your reasoning.

[2] The VAT defines a phase as a type of geographical site that is part of a PSOI. The VAT defines six phases. The term phase is related to time, the moment a person goes through to get to the main site, not to geography; for example the same site can be used for arrival and for departure of people, but that does not have to be the case. The six phases are implicitly derived from a security ring model consisting of two rings.The protection ring system is a concept derived from computer science, where hierarchical protection domains often called protection rings, are mechanisms to protect data and functionality from faults and malicious behavior. Concrete (events in) PSOI's can use a different number of security rings ranging from most privileged (most secured, usually numbered zero) to least privileged (least secured, usually with the highest ring number).

STEP 4: CONSEQUENCE AND PROBABILITY

- In the bottom right columns of the record template, there is room to write down influences, assumptions, preconditions and uncertainties associated with determining the level of consequence and the probability of a scenario occurring;



Consequence[4]	C.Ley.	Probability[5]	P.Ley.

Figure 4:
Bottom right column of record template; consequence, probability and risk level.

- Discuss what the consequences of the attack could be. Consider the possible damage to buildings and other structures, how many wounded or dead people can be expected, and influencing factors such as how long does it take to respond or rescue, etcetera. It is important to take the crowd density into account. Please decide if the attack has a high, medium or low consequence and try to describe what the reasons are for choosing the consequence level;

- Discuss how probable the scenario, having the established consequence(s), is and thus how probable the threat is. It is important to think of how easily a potential terrorist can reach the site, what surrounds the site, what means you already possess, and which factors influence the probability of an attack occurring. Together decide if the attack has a high, medium or low probability. Please try to describe your reasoning for choosing the given probability level.

- In the risk analysis process, the consequences (i.e. impact, severity) and probability (i.e. likelihood, chance) of each attack scenario are determined by the team of experts, considering all factors of influence. The consequence and probability are expressed as a level, e.g. 1...5, Negligible/¬Minor/-Moderate/¬Severe, Low/¬Medium/¬High, or a color scheme, as presented in the matrix (Figure 5).
- The managing body should determine which risk matrix will be used to suit the purpose of the risk assessment and which is in line with the risk criteria set out by the managing body.

Probability		Very likely	Likely	Unlikely	Highly unlikely
Consequences	Fatality	High	High	High	Medium
	Major injuries	High	High	Medium	Medium
	Minor injuries	High	Medium	Medium	Low
	Negligible injuries	Medium	Medium	Low	Negligible

Figure 5:
Example of a risk matrix

- The risk evaluation process can be carried out by the managing body, supported by the team of experts and possibly the other stakeholders. Based on the earlier established risk criteria, the management body decides how to treat each risk, considering all risk mitigation options and possibly deciding to accept some risks or degree of risk.

STEP 5: ANALYSIS AND RESULTS

- When all consequences and probabilities have been determined for a site, check for any inconsistencies or dependencies among the scenarios, consequences and probabilities, and make adjustments where necessary. Possibly repeat this activity once all record templates for all sites have been completed;
- Determine the level of risk for each scenario, for instance by using a risk matrix, and add a note in the record template;.
- To create an overview of the vulnerabilities for the PSOI, consider making a table as shown below. This can be done by cross referencing the sites and the attack types and adding the scores of High, Medium or Low.

Table 1:
Overview of vulnerabilities of each site regarding each terrorist threat

	Fire arms attacks	Sharp object attack	Vehicle attack	IED[4] attack	PBIED[5] attack	UAVIED[6] attack	VBIED[7] attack	Chemical attack	Biological attack	Radiological attack
Site 1										
Site 2										
Site 3										
Site 4										

- With this overview and the filled in record templates with the reasoning behind identifying the vulnerabilities, the vulnerability assessment has been completed.

[4] Improvised explosive device
[5] Person-Borne Improvised Explosive Devices
[6] Drones or unmanned aerial vehicles
[7] Vehicle-borne improvised explosive device

PROJECT PARTNERS

PRoTECT

CITY OF VILNIUS

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

EINDHOVEN

European Forum *for* Urban Security

Stichting DITSS Dutch Institute for Technology Safety & Security

PRIMARIA MUNICIPIULUI BRAŞOV

Ayuntamiento de Málaga Policía Local

L3CE Lithuanian Cybercrime Center of Excellence for Training, Research & Education

TNO innovation for life

JADS Jheronimus Academy of Data Science

KEMEA

ΔΗΜΟΣ ΛΑΡΙΣΑΙΩΝ MUNICIPALITY OF LARISSA

This project has received funding from the European Union's Horizon 2020 ISFP programme under grant agreement n˚ 815356