



Factsheet N°2

.....

Preparing a Vulnerability Assessment

PROTECT

The word "PROTECT" is written in large, white, bold, sans-serif capital letters. Behind the letters, there is a stylized city skyline in a lighter blue color. Yellow stars are scattered across the skyline, particularly around the letters 'O', 'T', and 'E'.

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



HOW TO PREPARE A VULNERABILITY ASSESSMENT?

- 👉 Create a **managing body**: the vulnerability assessment is organised by a managing body. It can be an individual, organisation or group of organisations that takes up the responsibility to identify and work on assessing the terrorist threat in a Public Space of Interest (PSOI). This can be a law enforcement agency, a municipality or possibly also the owner of the Main site.
- 👉 Identify the PSOI and its main and surrounding sites: the Managing body will identify the site and its surrounding sites and retrieve an accurate map of the area. In the introductory factsheet you will find the categories of main sites¹.
- 👉 Identify the phase (refer to factsheet n°1) for each site: drawing up the map of a PSOI with its main site and surroundings sites to identify the phases that need to be assessed.



BEFORE CONDUCTING A VULNERABILITY ASSESSMENT

- 👉 **First, the managing body should:**
 - Define the precise geographical boundaries of the PSOI on maps of the area;
 - Map out the several sites managed by separate organisations and security personnel of the PSOI.
 - Identify all stakeholders and their roles and responsibilities in relation to the security of the PSOI²
 - Gather project plans for events detailing timelines, deadlines, dependencies, tasks, etc;
 - Define risk evaluation criteria, **including**:
 - A **lower level** limit below which security measures are not proportional because the risk is acceptable
 - An **upper level** limit beyond which security measures are not going to be sufficient, and will require escalation measures

The manual assumes that the managing body with its relevant stakeholders has some existing security strategy regarding the main site, the surrounding sites and/or the activities taking place at the PSOI, and that the main site needs to be secured either for a new event lasting for a predetermined short period of time (e.g. a concert or fair), or continuously from now on (e.g. a train station). There could be an existing security plan which needs to be updated or one may need to be made from scratch.

¹The VAT considers crowd density a highly relevant factor to identify a PSOI, and it includes some information to help classify the crowd density on a scale from 2 to 5 (person per square meter). However, there is no other information on the relevance of this information, or on the classification scale that is provided.

²N.B If the same site is used differently over the course of a (multi-day) event, it is recommended to treat it as multiple different sites.



Second, the managing body should create a team of experts:

This team must be composed of key stakeholders who will participate during the vulnerability assessment (see the factsheet N° 1 for more details on what kind of actors to invite).


The team should have expertise in / knowledge of / access to information on:

- PSOI use: detailed information on the PSOI's activities (characteristics, times of activity, crowd movements and densities, etc.);
- PSOI sites: detailed information on the PSOI's sites (topography, i.e. maps taken from the municipal's GIS, including buildings, streets, lighting, etc);
- PSOI security: security policies, current threats (from national intelligence sources), possible threat scenarios and risk assessments, existing security plans, existing natural and emplaced measures, existing vulnerabilities, earlier assessments, safety plans and measures, available security measures (types, use, performance, etc.);
- PSOI security solution use: user needs regarding the solution to be evaluated, some technical knowledge of the solutions to be evaluated;
- Municipality public safety: the municipality's public safety regulations and procedures;
- Municipality procurement: legislation, and the municipality's procurement regulations and procedures;
- Police tasks: tactical and operational tasks and requirements of the police involved in protecting the PSOI.



Third, the managing body should collect the following information:

- How the city approaches the security of public spaces, e.g soft targets (regulation, policies, security strategies, etc.). This will be useful to determine the level of existing protection, the available resources, etc;
- Results from previously conducted Security audits (policy, constraints, site and activity characteristics, threats, security measures, vulnerabilities, risks, etc.);
- Calamity plans, use of emergency services, escape routes, emergency exits, etc.;
- Information specifically concerning the site to be assessed. This means gathering detailed knowledge of the PSOI's main site, surrounding sites and activities (topography, characteristics, and times of activity, crowd movements and densities). It is important to collect information about the specific threats identified for the selected site;
- The activities to be conducted on site, including crowd densities, at which dates and times³;
- A survey of the site and documentation, including the site layout, access routes, already emplaced security measures, etc.;
- Risk assessment, including establishing threats (consulting national intelligence sources), assets (primarily people), site vulnerabilities, probabilities and consequences of an attack, etc. This information can be provided by the national service of intelligence (in some cases this can be classified information with no access to municipalities. In this case we suggest asking an expert/consultant to help you to identify specific threats).



³ According to the VAT, if a PSOI has between 1600-1700 people (5PPSM) this is considered as a HIGH to VERY HIGH crowded density. 1800-2000 people (1PPSM) is considered as LOW density.

Fourth, they should decide on a work method:

Decide and plan how the team of experts will conduct the vulnerability assessment. There are many ways to do this; this manual suggests using a team/workgroup/workshop session to carry out a vulnerability assessment. **Please see the factsheet N°3 “Conducting a Vulnerability Assessment”** for more details.

It is estimated that the team will need at least a two-day session using the tool, depending on the number of sites comprising the PSOI, the degree of available information (i.e. threats, site characteristics, complexity, current measures, etc.), the number of stakeholders, and other factors.

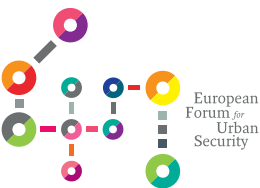
There should be an assigned **moderator** and someone filling in record templates.

Before starting a session, the team should **verify that all required information is available during the session** (e.g. site maps and boundaries, knowledge of existing natural and emplaced security measures, etc).

The team of experts should be aware that one record template (see Annex 1) needs to be filled in for each site (i.e. the main site and each surrounding site) and that each template requires the following information to be entered:

- Site details;
- Existing natural and emplaced security measures of the site;
- Possible attack scenarios per threat type;
- Consequence, probability and the assigned risk level of the attack scenario.

PROJECT PARTNERS



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