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

Public Resillience using Technology to Counter Terrorism

D2.1 - Manual for vulnerability assessment

WP number and title	WP2 – Vulnerability Assessment
Lead Beneficiary	EFUS
Contributor(s)	TNO
Deliverable type	Report
Planned delivery date	28/02/2019
Last Update	14/01/2021
Dissemination level	PU

Disclaimer

The PROTECT Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Type	Country
1	Dutch Institute for Technology, Safety & Security	DITSS	NPO	NL
2	KENTRO MELETON ASFALEIAS	KEMEA	RTO	GR
3	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	TNO	RTO	NL
4	INSPECTORATUL GENERAL AL POLITIEI ROMANE	IGPR	GOV	RO
5	FORUM EUROPEEN POUR LA SECURITE URBAINE	EFUS	NPO	F
6	LIETUVOS KIBERNETINIU NUSIKALTIMU KOMPETENCIJU IR TYRIMU CENTRAS	L3CE	RTO	LT
7	GEMEENTE EINDHOVEN	Eindhoven	GOV	NL
8	AYUNTAMIENTO DE MALAGA	Malaga	GOV	SP
9	DIMOS LARISEON	DL	GOV	GR
10	VILNIAUS MIESTO SAVIVALDYBES ADMINISTRACIJA	VMSA	GOV	LT
11	MUNICIPIUL BRASOV	MUNBV	GOV	RO
12	STICHTING KATHOLIEKE UNIVERSITEIT BRABANT	JADS	RTO	NL
13	MINISTERIO DEL INTERIOR	MIR	GOV	SP

To the knowledge of the authors, no classified information is included in this deliverable

Document History

VERSION	DATE	STATUS	AUTHORS, REVIEWER	DESCRIPTION
V 0.1	15/01/2019	Draft	Efus, TNO	First draft
V 0.2	18/01/2019	Draft	Efus, TNO	Review and comments
V 0.3	25/01/2019	Draft	Efus, TNO	Review and comments
V 0.4	05/02/2019	Draft	Efus, TNO	Review and comments
V 0.5	11/02/2019	Draft	Efus, TNO	Review and comments
V 0.6	19/02/2019	Draft	Efus, TNO	Review and comments
V 0.7	22/02/2019	Draft	Efus, TNO	Review and comments
V 0.8	27/02/2019	Draft	Efus, TNO	Review and comments
V 0.9	1/03/2019	Draft	Whole consortium	Manual presentation and working groups sessions
V 1.0	7/03/2019	Draft	DITSS, Eindhoven	Review and comments
V 1.1	11/03/2019	Final	Efus	Comments integration
V 1.2	10/06/2019	Final	Efus, TNO	Adjustments after its use
V2.0	14/01/2021	Final	Efus	Change of dissemination level of the deliverable from confidential to public

Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
PRoTECT	Public Resilience suing Technology to Counter Terrorism
VAT	Vulnerability Assessment Tool
PSOI	Public Space of Interest
UAV	Unmanned Aerial Vehicle-Drone
PBIED	Person-Borne Improvised Explosive Device
IED	Improvised explosive devices
UAVIED	UAV Borne Improvised Explosive Device
VBIED	Vehicle Borne Improvised Explosive Device

Table of Contents

List of Figures

List of Tables

Executive Summary

In its effort to enhance the protection of public spaces, the European Union’s Directorate General for Migration and Home Affaires (DG HOME) has developed the EU Vulnerability Assessment Tool (VAT) (DG HOME, 2019) which main objective is to provide practical support to Member States to enhance the protection of public spaces by facilitating the conduction of an on-site vulnerability assessment (Action Plan, 2017).

As a part of the Commission’s efforts to support local and regional authorities in the protection of urban spaces, the Manual described in the present report meant to aid Municipal staff that is responsible for safety and security in public space and their stakeholders in the use of the VAT provided by the EU. This Manual support them in identifying vulnerabilities and providing awareness of soft targets against terrorism. The areas we identify as public space must be areas where regular and / or incidental masses of public come for an activity. Categories of the main sites can be transport hubs, squares, shopping areas, and places of worship, cultural -, business - or institutional venues.

The VAT Manual make part of the PRoTECT project, which objective is to strengthen Municipalities staff’ capabilities in public spaces protection by putting in place an overarching concept where tools, technology, training, and field demonstrations will lead to situational awareness and improve direct responses to secure public places before, during and after a terrorist threat. One of the project activities is to assess the EU VAT’s quality by applying the EU VAT in five European cities (Malaga, Eindhoven, Larissa, Brasov and Vilnius), aiding these cities in assessing their vulnerabilities and to give the resulting feedback about the use of the EU VAT to DG Home.

The Manual is divided in three main chapter and three appendixes. Chapter one refers to the introductory part of the Manual and gives the context of why municipalities should be considered as relevant actors in the protection of public spaces. Chapter two describes the context in which to use the EU VAT, specifically focussing on the users, the objects, how vulnerability assessments fit in the broader context of security and risk management, this section also presents the functionality of the EU VAT (format, layout etc.). Chapter three describes the steps that are needed (1) before using the tool, (2) what different steps to take and how to record it in the record template, and (3) will conclude what can be done with the results and what next steps can be taken. In the appendixes, the record template can be found as well as a scenario that can be used to explain the record template and the steps for the vulnerability assessment. The guidelines for the organization of a local workshop to conduct the vulnerability assessment as well as an overview of the different scenarios from the EU VAT are also provided in the appendixes.

1 Introduction

1.1 Background

For decades, terrorism has been a reality in many European countries and a continuous threat to a great number of European cities. It seriously threatens the safety, the values of democratic states and the rights and liberties of citizens. Acts of terrorism bring about long-term negative effects for cities and high social costs. Not only from a financial, but also from a psychological point of view in the sense of an increased feeling of insecurity among locals and visitors (Efus, 2005).

Over the years, strategies to protect public space against terrorism have strengthened and evolved, mainly focussing on protecting critical infrastructure. However, terrorist attacks are evolving as well. By adapting to new contexts and opportunities, lately public space has turned into an attractive target for terrorist attacks. To illustrate, the latest terrorist attacks in European cities such as London, Paris, Manchester, Stockholm, Berlin, Brussels, Barcelona…have occurred in public areas. These areas are considered as **"soft targets"**. This means that crowded public places including the metro, shopping centres, sports stadiums, bars, restaurants, clubs and commercial sidewalks, are easily accessible to the public and an easy target for terrorists to do great harm. These areas called soft targets, are targets because attacking them can aid terrorist organisations to obtain their goals, for instance threatening the safety of the public, the values of democratic states or the rights and liberties of citizens. These areas are called 'soft', because they are not hardened against such terrorist attacks. A crowded public space, for instance a shopping centre, can be hardened against other threats like vandalism, petty crime, or fare evasion, but not necessarily for a terrorist attack.

> *Soft target: a site that is insufficiently protected against a terrorist attack and when attacked by a terrorist organisation, will help terrorists obtain their goals.*

As stated by the European Commission in the Action Plan to support the protection of public spaces, **"local and regional authorities are also important stakeholders in the protection of public space"**. The EU Commission is thus committed to reinforce the involvement of these stakeholders by promoting dialogue and exchange between national, regional and local authorities and supporting the development of operational projects.

1.2 The EU Vulnerability Assessment Tool

In light of the above, **local authorities responsible for the safety and security of their citizens must be aware of the vulnerabilities of their public spaces in order to be able to adopt appropriate measures to prevent and mitigate terrorist attacks and their consequences** (European Commission, 2017). Therefore DG HOME has developed the EU Vulnerability Assessment Tool (VAT) (DG HOME, 2019). The EU VAT is part of the Commission's efforts to support local and regional authorities in the protection of urban spaces. The commission continues to improve it by developing macros to have a completer and more useful tool.

While some municipalities across Europe have made great progress in counterterrorism and have adopted measures to prevent and be prepared against a terrorist attack in public space, others do not consider terrorism as a threat at all. The EU VAT and this manual can help assess the vulnerability of a specific public space for cities willing to act against terrorism.

The EU VAT Manual is meant for Municipal staff that is responsible for safety and security in public space and their stakeholders. It aids them in identifying vulnerabilities in and providing awareness of soft targets against terrorism. It does not help to identify how to mitigate these vulnerabilities by itself but during the process, a collection of measures will be suggested from the tool. The areas we identify as public space have to be areas where regular and / or incidental masses of public come for an activity. Categories of the main sites can be transport hubs, squares, shopping areas, and places of worship, cultural -, business - or institutional venues. Please see Appendix B for terms and definitions.

The PRoTECT project aims to strengthen local authorities' capabilities in public spaces protection by putting in place an overarching concept where tools, technology, training, and field demonstrations will lead to situational awareness and improve direct responses to secure public places before, during and after a terrorist threat. One of the project activities is to assess the EU VAT's quality by applying the EU VAT in five European cities (Malaga, Eindhoven, Larissa, Brasov, and Vilnius), aiding these cities in assessing their vulnerabilities and to give the resulting feedback about the use of the EU VAT to DG Home. In this context, the manual for the use of the EU VAT that lies before you, has been created by TNO and Efus. This manual aids in the use of the EU VAT and helps local authorities in charge of the security in crowded places to identify the vulnerabilities to a terrorist attack. Efus as the only European network of local and regional authorities dedicated to urban security, has a mission to promote a balanced vision of urban security, combining prevention, sanctions, and social cohesion and to obtain recognition of the role of local and regional authorities in drafting and implementing national and European security policies. It has the capability to foster the exchange of experiences between authorities for the benefit of long-term security and to support local and regional authorities in the conception, implementation, and evaluation of their local security policy, as such it has added this expertise to the manual. One of the missions of TNO is to innovate for a more secure society. TNO has the capability to apply theoretical risk management knowledge in complex, practical situations and has taken up this role in creating this manual.

The manual provides the steps that must be taken by the five cities, to do a vulnerability assessment as part of the security management process. The first step is to appoint a managing body, in the case of PRoTECT the five partner cities and familiarize with the EU VAT and the manual's different sections. The second step requires to plan and prepare all the necessary resources, human and technical (who should participate, which site will be assessed, etcetera, see sections 2.4 and 3 of this Manual) and define the work method. The third step is to conduct the vulnerability assessment workshop. The final step consists of analysing the results obtained from the vulnerability assessment workshop.

If the results of the evaluation are positive, this manual should be revised for use outside the context of the PRoTECT project.

1.3 Information classification of the outcome of the vulnerability assessment

According to the guidelines provided by the European Commission (European Commission, 2016), the outcome of vulnerability assessment must be classified as EU RESTRICTED. It is the responsibility of the party that produces the vulnerability assessment to follow these guidelines.

1.4 Reader's guide

After this introduction, chapter two describes the context in which to use the EU VAT, specifically focussing on the users, the objects, how vulnerability assessments fit in the broader context of security and risk management, this section also presents the functionality of the EU VAT (format, layout etc.). Chapter three describes the steps that are needed (1) before using the tool; so all the information is gathered, the right people are prepared, how to use the tool and to decide on a work method, (2) what different steps to take and how to record it in the record template, and (3) will conclude what can be done with the results and what next steps can be taken. In the appendixes, the record template can be found as well as a scenario that can be used to explain the record template and the steps for the vulnerability assessment. The guidelines for the organization of a local workshop to conduct the vulnerability assessment as well as an overview of the different scenarios from the EU VAT are also provided in the appendixes.

2 Context for use of EU VAT

This chapter explains what the purpose of assessing vulnerabilities is and what the conditions are to use the EU VAT, as well as who should use it and for which situations. Furthermore, it is important to pay significant attention to the process of safety and security as a whole and the different steps in risk management, to understand how a vulnerability assessment fits in and what more to do.

2.1 Tool users

As mentioned in the introduction, with the EU VAT it is possible to identify vulnerabilities of specific sites against different kinds of terrorist attacks. It helps to give an overview of specific geographical areas that might be soft targets and show what areas are well mitigated against terrorism. After using the tool and identifying the vulnerabilities of a public space against terrorism, the results give the responsible agencies insights in the identified soft targets to better focus their mitigating actions. This is why it can be used by **municipal staff that are responsible for safety and security in their municipalities to identify their overall vulnerabilities in public space against terrorism.**

As management of security depends on one city to the other, it is difficult to identify the specific roles of different actors in the protection of public spaces.

In the following figure an overview of the main actors to be involved taking into account some examples of generic municipal structures are provided. This shows the municipal services that should be involved in the process of identifying vulnerabilities against terrorism according to their involvement in the management of public spaces.

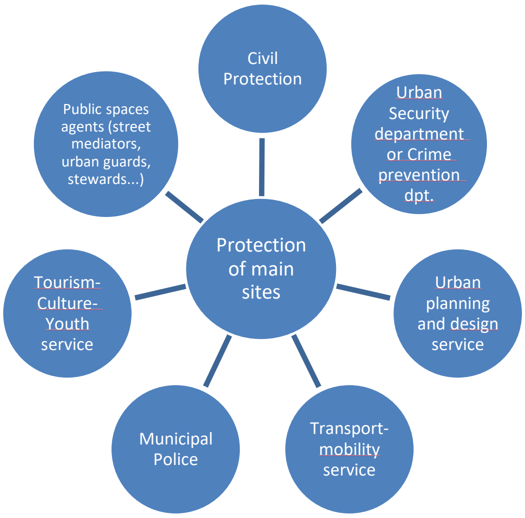

Civil Protection
Public spaces agents (street mediators, urban guards, stewards...)
Urban Security department or Crime prevention dpt.
Protection of main sites
Tourism-Culture-Youth service
Urban planning and design service
Municipal Police
Transport-mobility service

Figure 1 Municipal Services

In the EU VAT model, the implication of other stakeholders outside municipal services that have a role in the public spaces realm (whether from public or private sector) is also necessary. Some suggestions of these actors that could be involved in the process of identifying vulnerabilities against terrorism are listed in the following figure. It is important to note that this is not an exhaustive list. The objective is to provide some examples of key stakeholders to involve at some point during the process.

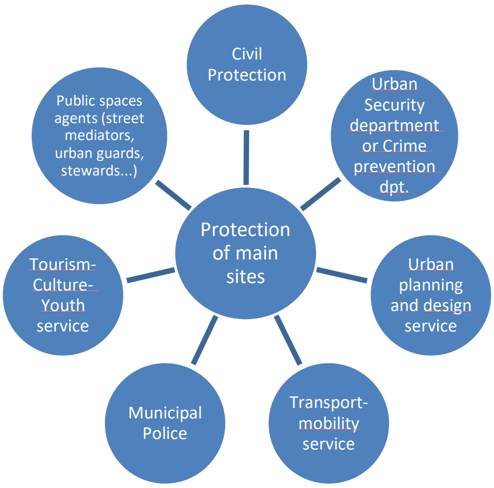
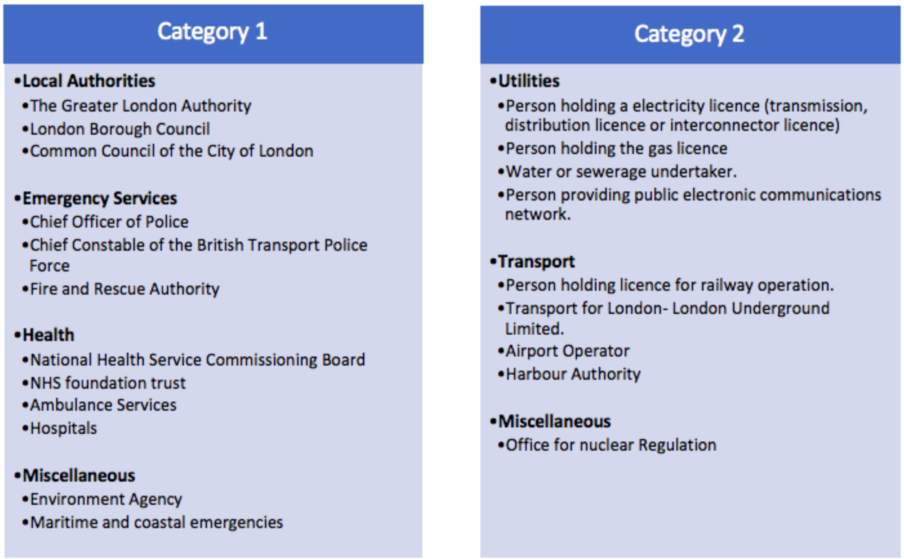

Civil Protection
Urban Security department or Crime prevention dpt.
Urban planning and design service
Transport-mobility service
Municipal Police
Tourism-Culture-Youth service
Public spaces agents (street mediators, urban guards, stewards...)
Protection of main sites

Figure 2 Key local stakeholders

Example of roles of an organization in the protection of public spaces
In the UK, Councils have a key role to play in helping make local areas safe places to live, visit and work and tackling anti-social behavior continues to be a high priority for local authorities and their partners across the country. In 2014, were introduced the Public Spaces Protection Orders (PSPOs) which aim at ensuring that public spaces can be enjoyed free from anti-social behavior providing councils with another instrument to help deal with persistent issues that are damaging their communities (Local Government Association, 2014). In case of terrorism, the Civil Contingencies Act defines local arrangements for civil protection in case of terrorist attack and as a counter-terrorism strategy. This framework guides local administrations and stakeholders to establish clear roles and responsibilities for those involved in emergency preparation and response at the local level. In cities like London, there are two types of local responders with differentiated duties. There is a distinction between 'category 1' and 'category 2' responders, please see table one for an overview. The 'category 1' responders are the organizations at the core of the response in case of emergency and that are responsible for the full set of civil protection duties such as emergency services, local authorities, and health bodies (NHS). Their main role is to assess the risk of emergencies occurring; to define, plan, inform and put in place emergency or contingency plans; to plan and put in place business continuity arrangements; make information available, warn and advice the public in the event of an emergency; they are the responsible of coordinating, co-operating and sharing information with other local responders to enhance efficiency; provide advice and assistance to business and voluntary organizations. 'Category 2' responders are the co-operating bodies mainly composed by the Health and Safety Executive, transport, and utility companies. These organizations are less likely to be involved in the heart of the planning work but will be heavily involved in incidents that affect their own sector. They have a smaller set of duties and their main responsibility is to cooperate and share relevant information with the local authorities and core responders (UK Cabinet Office, 2013).

Table 1: Category 1 and Category 2 responders.



Category 1

- **Local Authorities**
  - The Greater London Authority
  - London Borough Council
  - Common Council of the City of London
- **Emergency Services**
  - Chief Officer of Police
  - Chief Constable of the British Transport Police Force
  - Fire and Rescue Authority
- **Health**
  - National Health Service Commissioning Board
  - NHS foundation trust
  - Ambulance Services
  - Hospitals
- **Miscellaneous**
  - Environment Agency
  - Maritime and coastal emergencies

Category 2

- **Utilities**
  - Person holding a electricity licence (transmission, distribution licence or interconnector licence)
  - Person holding the gas licence
  - Water or sewerage undertaker.
  - Person providing public electronic communications network.
- **Transport**
  - Person holding licence for railway operation.
  - Transport for London- London Underground Limited.
  - Airport Operator
  - Harbour Authority
- **Miscellaneous**
  - Office for nuclear Regulation

Additionally, the city of London counter-terrorism local policies are guided by the national counter-terrorism strategy and more specifically by the "Crowded Places Guidance" (NaCTSO, 2017) which gives guidelines to local authorities and stakeholders in terms of protection and response against terrorist attacks. This guide covers the key forms of protective security: physical, personnel, cyber and personal, and gives guidance on how different sectors can act to help make their business, institutions, or organizations safer.

2.2 Public space of interest

Municipal staff from various departments are to some degree involved in and/or responsible for the safety and security of people in their municipality, especially in *public space*. Public space is generally open and accessible to members of the public, such as roads, parks, and municipal buildings. Public space includes semi-public spaces, such as train stations, and privately-owned spaces such as shopping malls.

Some areas in public space, where large crowds form, might be considered by a municipality as having a higher risk of a terrorist attack than others. These busy areas generally appear because of some specific activity in the area, such as people visiting a concert or commuters at a train station.

An activity, and the area where the activity takes place, can be managed by separate organisations/owners or just one organisation/owner. This **managing body** will also be responsible for the security of the public taking part in the activity.

The EU VAT considers the area in public space where the activity takes place as the 'main site'. The following categories of main sites can benefit from the EU VAT (see table 2):

Table 2: Categories of main sites

Category	Examples
Transport hubs	Train station, bus hub, underground metro stations, etcetera.
Squares	Squares were many events take place, are next to important buildings, have regular big markets, festivals, etcetera.
Shopping areas	Malls, main shopping street in city centre, etcetera.

Nightlife areas[1]	Area with a high density of bars, pubs and/or nightclubs, restaurants, coffee shops, small concert halls
Cultural venues	Concert hall, museum, monuments, sport events, stadiums, amusement parks, tourist sites, etcetera.
Business venues	Big hotels with meeting rooms, large offices, conference centres, etcetera.
Places of worship	Churches, mosques, etcetera.
Institutional venues	Public buildings, health buildings, education buildings, etcetera.

The activity at the main site can lead to other congested areas around the main site (e.g., an access road to a sports venue). These surrounding sites should also be taken into consideration when conceiving a security plan for the main site. **In this manual, the main site, together with the surrounding sites associated with the activity, are called the Public Space of Interest (PSOI).**

Though the EU VAT was originally developed for event-site protection (e.g., a Christmas market), it can also be used for vulnerability assessments for all the above-mentioned categories of main sites.

The EU VAT does not help in ***identifying which public spaces are public spaces of interest****. The VAT does not give clear indicators to help identify PSOI's, nor does it give indicators to help group or cluster different similar events (at the same public space). The information in the VAT suggests that crowd density is considered a highly relevant parameter, and the VAT 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.*

The scale of crowd density is probably coming from crowd-management theories, which also deal with safety problems originating from dense crowds, such as the Duisburg dance event tragedy. However, a crowd with a density that is lowest on this scale, would still be extremely vulnerable to terrorist attacks and successive panics. Because of this lack of clarity on the relevance of crowd density, we have chosen not to focus on this parameter in the manual.

Other crowd parameters than crowd density could also be relevant. The social identity of people in the crowd might be relevant to convey a political message with the attack. Crowd size could be relevant in different ways. A small crowd may be an easy target but send a less powerful message. A large crowd may easily overpower certain types of terrorist attacks, e.g., with sharp objects, making them perhaps less vulnerable than smaller crowds. Other relevant parameters could be the flow of a crowd and the level of intoxication.

2.3 Security management and assessing vulnerabilities

The PSOI will have a managing body, supported by assisting departments and various stakeholders, who will be responsible for security. The managing body may be a municipality, with for instance an event organiser, police, and retailers also as stakeholders. Or the managing body may be a venue owner with the municipality, police, and event organiser also as stakeholders. Other compositions of the stakeholders are conceivable. The stakeholders may be organised in a workgroup, partnership, committee, team of experts etc. for planning

[1] The example of urban nightlife areas was not included in the EU VAT, but it fits well in the criteria of a soft target in a public space.

and managing the site and possibly also the activities on the main site. In the case of the PRoTECT project, the managing body taking the lead is a municipality e.g., municipal staff that form a team together.

It is important to mention that the vulnerability assessment is organized by a managing body, in the case of the PRoTECT project the five municipalities and their related supporting PRoTECT partner. It is essential to involve relevant stakeholders for the security of the site to be assessed. Also, important to mention is that for the purposes of the PRoTECT project the managing body is responsible for identifying what public space to asses

To help protect the people using the PSOI from a terrorist attack, the managing body needs to have a **security plan** from the managing body itself or from one of the stakeholders. This depends on the PSOI. It is important that the security plan is developed as an integral part of planning and managing the PSOI and its activities. The security plan cannot be formed in isolation and at some point, simply delivered to the managing body, but it must be developed under the clear direction of the managing body including the shareholders, taking various aspects into consideration such as: site characteristics, characteristics of the public on the site, constraints and requirements from the various stakeholders, budget constraints, the security risks, the possibilities for risk mitigation, etc.

Generally, developing a security plan is an ongoing process – threats and other circumstances change, requiring the security plan to be continually adapted as well. In the case of protecting the PSOI against terrorist attacks, it is assumed that even though a certain activity may be unique, there are some common aspects related to the PSOI: the method of planning, managing the activity and other security related aspects. As an example, consider a fairground where every year various events are held. Lessons can always be learned from each event held at the fairground, and these lessons can contribute to the development of a generic security plan for the fairground. Subsequently, the plan can be regularly reviewed and adapted to meet any changed circumstances (i.e., changes in threats, implemented measures, etc) or specific details regarding the current event.

Developing and maintaining a security plan is a cyclic process, generally involving the following steps:

1. Security audit/inspection (policy, constraints, site and activity characteristics, threats, security measures, vulnerabilities, risks, etc.);
2. Decision making (budgets, priorities, schedules, risk acceptance, go/no-go by the management body, etc.);
3. Security plan (development/adjustment, and ratification by the management body);
4. Implementation and (periodic) verification of security measures (in accordance with the security plan).

The security audit/inspection (step 1 from above) generally involves making an inventory of the following aspects:

- applicable policies, legislation, risk criteria, contracts, constraints, requirements, etc. – and those imposed by the stakeholders or others – with regard to the site or the activities to be carried out on the site;
- a survey of the site and documentation, including the site layout, access routes, already emplaced security measures, etc.;

- the activities to be conducted on site, including crowd densities, at which dates, days and times, etc.; According to the VAT, if a PSOI has between 1600-1700 people (5PPSM) this is considered as a HIGH to VEY HIGH crowded density. 1800-2000 people (1PPSM) is considered as LOW density;
- organisational structure for developing the security plan (levels and roles, responsible persons, relationship with the management, stakeholders, etc);
- calamity plans, use of emergency services, escape routes, emergency exits, etc.;
- risk assessment, including establishing threats (consulting national intelligence sources), assets (primarily people), site vulnerabilities, probabilities, and consequences of an attack, etc.

The aspect of risk assessment (mentioned above) involves three consecutive processes[2]:

1. Risk identification (identifying threats and threat scenarios)
2. Risk analysis (determining consequences, probabilities, risk levels and vulnerabilities)
3. Risk evaluation (determining priorities, risk treatment actions, risk acceptance)

The EU VAT is primarily used to establish PSOI's vulnerabilities as a result of the risk identification and risk analysis processes. A vulnerability in this context is seen as a weakness in a PSOI's security which could be exploited by a threat, specifically a terrorist organisation to attack a (soft) target, thus forming a risk.

The vulnerabilities of a PSOI and the possible risks of an attack can be identified by examining the PSOI (geographical layout, accessibility for vehicles, natural or emplaced security measures, etc) and devising viable attack scenarios. Scenarios should at least mention the threat type (e.g., shooter), the aim of the attack, with what means and how the terrorist carries out the attack. Conceiving scenarios can be an activity carried out by a team of experts from all the relevant stakeholders that is put together by the managing body. This means that to be able to carry out the assessment, different experts need to be present and gathered to go through all steps (for the exact steps, see chapter 3).

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 colour scheme.

The level of risk can be determined by using a risk matrix, which has been devised by the team to suit the purpose of the risk assessment and which is in line with the risk criteria set out by the managing body. An example of a risk matrix is given in the figure 3. (the risk level is denoted by Low/Med/High and a colour).

[2] Systematic techniques for risk assessment are described in the IEC 31010:2009 standard.

		Consequence		
		Low	Med	High
Probability	Low	Low	Med	Med
	Med	Med	Med	High
	Hi	Med	High	High

Figure 3 Example of a risk matrix

In the risk matrix above, only three levels of risk (low, medium, and high) are used, which corresponds with the EU VAT. It is important that the implications of these levels are clear, i.e., that the levels are meaningful. Are "low" levels of risk accepted? Can the managing body also deal with "high" levels of risk? It is wise to discuss this before the VAT is used. The outcome of such a discussion could be a more nuanced idea of risk, as shown in the figure below :

Negligible: risk is not considered a vulnerability. e.g., the attack can be managed by the crowd itself.

Low: risk is not considered a vulnerability. e.g., the attack can be mitigated by existing security measures.

Medium: risk is considered a vulnerability. e.g., the attack cannot be mitigated by existing security measures, and should be mitigated by managing body and its partners.

High: risk is considered a vulnerability. e.g., the risk cannot be mitigated by measures that the municipality and its partners can manage themselves.

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

Subsequently, 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.

2.4 EU VAT functionality

The EU VAT assists the user in performing a vulnerability assessment for a specific PSOI.

The tool only considers vulnerability aspects during the use of the PSOI and does not cover other stages of use, such as construction or installation activities at the site.

While writing this manual, the tool was still being updated by DG Home. For this reason, the manual will describe a method of use which – for as far as possible – allows for the tool to evolve without having to constantly update this manual.

The EU VAT is a Microsoft Excel workbook containing 6 spreadsheets (i.e., 6 tabs) and can be viewed in any current Microsoft Office environment or compatible software.

Each spreadsheet relates to a specific phase a PSOI site (i.e., main site or one of the surrounding sites) may have. Each spreadsheet denotes a 'phase' a person goes through to get to the main site (i.e., participate in the activity). The following phases (functional areas) exist:

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

Note that Phases 1 to 4 correspond to the surrounding sites. Phase 5 or phase 6 are to be used for the main site.

In Figure 4 an example is given of the 6 phases (P1 - P6) for a concert venue in a park. Phase 5 and Phase 6 are alternatives of each other, though in this example there will most likely be some form of access control. The PSOI needs to be identified in a main site and thesurrounding sites, then for every site the phase can be identified.

In the example given in Figure 4, it can be concluded that this PSOI has 1 main site and 15 surrounding sites, requiring a total of 16 site assessments using the EU VAT, whereby each assessment requires the use of a phase. The phases would thus be used as follows:

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

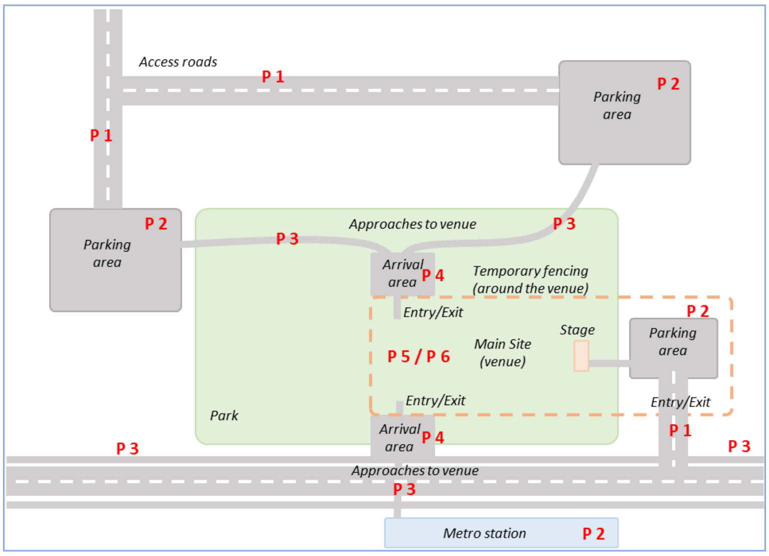


Figure 4 Example of a PSOI and EU VAT phase designation

Looking at the spreadsheet (see **Error! Reference source not found.**), each phase (i.e. tab) has the following four common parts:

Threat types	(part 1)
Situations	(part 2)
Measure Types	(part 3)
Assessment	(part 4)

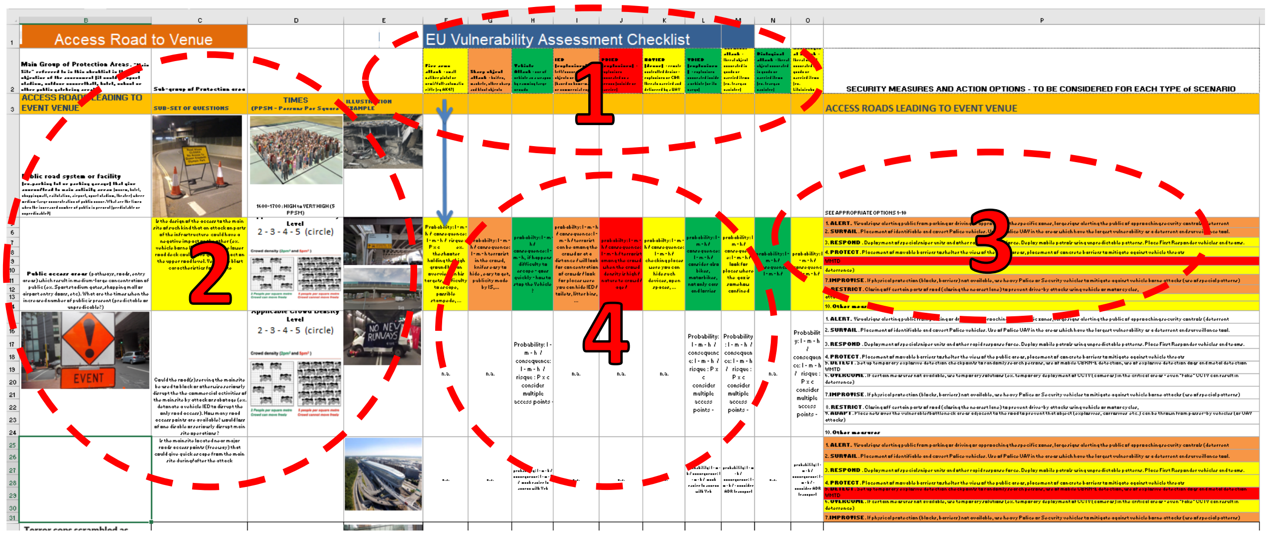

Access Road to Venue
EU Vulnerability Assessment Checklist
ACCESS ROADS LEADING TO EVENT VENUE
SUB-SET OF QUESTIONS
TIMES
ILLUSTRATION EXAMPLE
SECURITY MEASURES AND ACTION OPTIONS - TO BE CONSIDERED FOR EACH TYPE of SCENARIO
ACCESS ROADS LEADING TO EVENT VENUE
1
2
3
4
EVENT
2 - 3 - 4 - 5 (circle)
2 - 3 - 4 - 5 (circle)

Figure 5 Phase parts

The general procedure for using the EU VAT is as follows:

1. Decide which phase is relevant for the main site and each surrounding site (so the whole PSOI).
2. Conceive viable attack scenarios from combinations of threat types (part 1), situations (part 2) and currently existing natural and emplaced security measures which have been classified to the measure types (part 3).
3. Estimate the consequence and probability of each attack scenario following the assessment suggestions (part 4).

The tool is designed is such a way that users are stimulated to use their creativity and imagination in discovering possible attack scenarios, as opposed to a design whereby the user is simply asked a lot of detailed questions. The risk of the latter approach is that the right questions might not be asked, and an important vulnerability gets overlooked. Scenarios are thus presented in the tool as a mixture of possible threat types, images, situations, questions, and examples – not necessarily complete in every detail and to be taken literally, but to be used as inspiration in discussions within a team of experts.

Once the attack scenarios and levels for the consequences and probabilities have been determined, the risk levels can be established using a risk matrix (see paragraph 2.43).

This concludes the risk identification and risk analysis processes of the risk assessment step using the EU VAT. Further risk assessment and risk management actions are then carried out without using the EU VAT, for instance mitigating the threats (see paragraph 2.3).

3 Using the EU VAT

This chapter explains the steps to reveal the security vulnerabilities against terrorist attacks of your public space of interest, using the EU VAT. It describes what to do before starting, how to set up the work method to successfully identify vulnerabilities, how to use the content of the tool and how to summarize the results in the record template (see Appendix A).

> *The EU VAT can only be used to assist in risk identification and risk analysis, not within the complete progress of risk management.*

3.1 Getting started

The managing body wants to use the EU VAT to identify the vulnerabilities against terrorism of a PSOI. This manual assumes that the managing body with its relevant stakeholders have some existing security strategy regarding the main site, the surrounding sites and/or the activity taking place of the PSOI. 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 needs to be made from scratch. There is also a possibility that existing security plans have to be complemented with terrorism threats and existing policies therefore should be reviewed. e.g., a CCTV system that initially has been placed for crowd control purposes or to catch pickpockets.

Before using the EU VAT, the following actions need to be taken by the managing body of the PSOI (in this case the leading municipality).

First, the **organisation** regarding the PSOI needs to be clear. The managing body should:

- establish the (hierarchical) organisation for creating/managing the main site with it surrounding sites and the main activities on the site (governance, operation, maintenance, safety and security, communication, etc);
- establish the place of security management within it, meaning the security policies;
- establish the geographical boundaries of the public space and its dynamics very precisely on actual maps of the area;
- establish all stakeholders and their roles and responsibilities (for instance in a Responsibility Assignment Matrix[3]);
- gather project plans for events, establish timelines, deadlines, dependencies, tasks, etc;
- establish the budget for security;
- establish risk evaluation criteria. Set a top- and a bottom-level scope of risk between which you want to be able to handle this type of risk with your security measures (see also section 2.3):
    - a lower level limit below which your security measures are not proportional because the risk is acceptable. e.g., minor material damage is acceptable, if it helps e.g., apprehend and prosecute attackers;
    - an upper limit beyond which your security measures are not going to be sufficient, and you will have to rely on escalation measures;

[3] Also known as RACI-matrix or Linear Responsibility Chart (LRC)

- map out the several sites managed by separate organisations and security personnel of the PSOI.

The EU VAT assumes that the PSOI has already been compartmentalised into "phases", i.e. types of geographical areas. For those types, it assumes a security ring model of two rings. Sites within the inner ring are called main site(s). Other sites are surrounding sites.
In concrete PSOI's, it is possible that this default ring model or the suggested phases do not reflect the concrete situation. For example, more rings may be used, or there may be a separate site for the departure of people, whereas departure is not mentioned in the VAT. In such cases, you are free to define different phases.
If the same site is used differently over the course of a (multi-day) event, then it is recommended to treat it as multiple different sites.

The EU VAT does not provide information on **how to scope the role of the municipality** and its partners in terms of risk evaluation criteria. Specifically, how to make clear that there is a lower and upper limit to the amount of risk that the managing body (typically a municipality) can help mitigate. The PRoTECT presentation in Paris (day 2) gives some theoretical background on how to approach these questions and how to scope this.

Second, the managing body should create a **team of experts** that should have (access to):

- detailed knowledge of the PSOI's sites and activities (topography (i.e., maps taken from the municipal's GIS, including buildings, streets, lighting, etc), characteristics, times of activity, crowd movements and densities, etc.;
- known (security) policies, current threats (from national intelligence sources), possible threat scenarios and assessments, existing security plans, existing natural and emplaced measures, existing vulnerabilities, earlier assessments, safety plans and measures, available security measures (types, use, performance, etc.);
- stakeholders' preconditions and requirements.

The EU VAT provides ten suggestions in part 1 for **types of attacks**. The managing body should attempt to obtain more specific threat information from governmental or commercial experts. But if no more specific information is available, then you can always work with the list provided in the EU VAT. 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.

A cyber-attack is not included in the list. Cyber-attacks are attacks targeted towards cyber assets, i.e., against (the continuity of services provided by) ICT assets. The purpose of the EU VAT is to help in the protection of physical urban spaces. In principle, this excludes the cyber domain. However, it can be imagined that this changes in the future, or that local actors have a different opinion on this matter. The VAT would need a complete redesign (regarding the phases and the existing security means) to also be applicable to assess cyber vulnerabilities in the protection of ICT assets against terrorist threats. The VAT could be used to describe a scenario where an ICT system is used to attack in the physical domain, e.g., an attack with an autonomous drone or vehicle. You are invited to use the VAT in such a way and to provide feedback on your findings.

A nuclear attack is not included in the list. DG HOME may have assessed that a nuclear threat (i.e., a nuclear bomb) is not relevant in this context. First, DG HOME may have assessed that such a threat is currently not realistic, second DG HOME may have assessed that the effects of such a threat cannot be contained with the means at the disposal of a municipality.

Third, the managing body should decide on a **work method**. Decide and plan how the team of experts will conduct the risk assessment. There are many ways to do this, but for this manual it is assumed that at some time the EU VAT will be used in a team/workgroup/workshop session to carry out a vulnerability assessment. Please look at the Appendix E of this manual 'Guidelines for the organisation of a local workshop vulnerability assessment' for the method of putting up a team of experts, gathering the right information and doing the assessment.

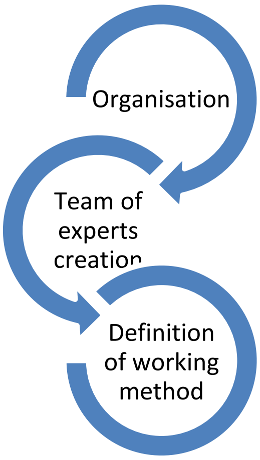


Figure 6 Steps to be taken by the managing body before using the EU VAT

The EU VAT will require a great deal of interactivity by all members of the team during the assessment. It is estimated that the team will need at least a two-day session using the tool, depending on number of sites comprising the PSOI, the degree to which information is available (i.e., threats, site characteristics and complexity, current measures, etc), the number of stakeholders (preconditions, requirements), repetitiveness, the experience of the team, and other factors.

> *The EU VAT requires a great deal of interaction between the members of the team of experts. The work session is expected to last two days depending on a number of factors.*

There should be a **moderator,** someone operating the tool (presented on a large screen) and someone filling in record templates (which could also be presented on a large screen). An example of a record template is given in Appendix A.

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 should be aware that one record template 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.

It is important to note that in our example in figure 4, this means that the main site and its surroundings sites adds up to 16 record templates that need to be filled in.

Two final notes before starting:

- It is important to know that while getting content out of the EU VAT, the colours and arrows shown in the tool can be ignored.
- It is about discovering relevant vulnerabilities from the suggestions, questions, examples, and pictures in the tool and not about literally answering the questions in tool.

3.2 Assessing the PSOI

As explained earlier, the team will put their findings in a record template, based on the template given in Appendix A.

> *It is recommended to kick-off by displaying a topographical map to the team, detailing the boundaries of the main site and surrounding sites, and describing the general function of each surrounding site in relation to the activity on the main site. When possible, organise a visit to the PSOI.*

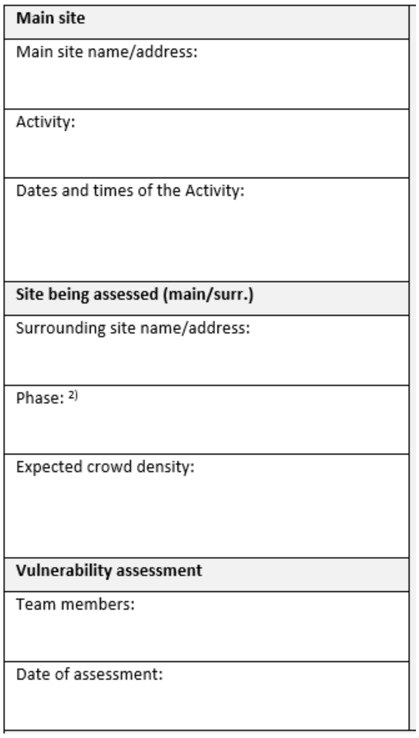
The following 5 steps are to be carried out using the EU VAT:

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

These 5 steps are detailed in the following sections.

3.2.1 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, see figure 7.



Main site
Main site name/address:
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 7 left upper column of record template; main site, site being assessed & vulnerability assessment.

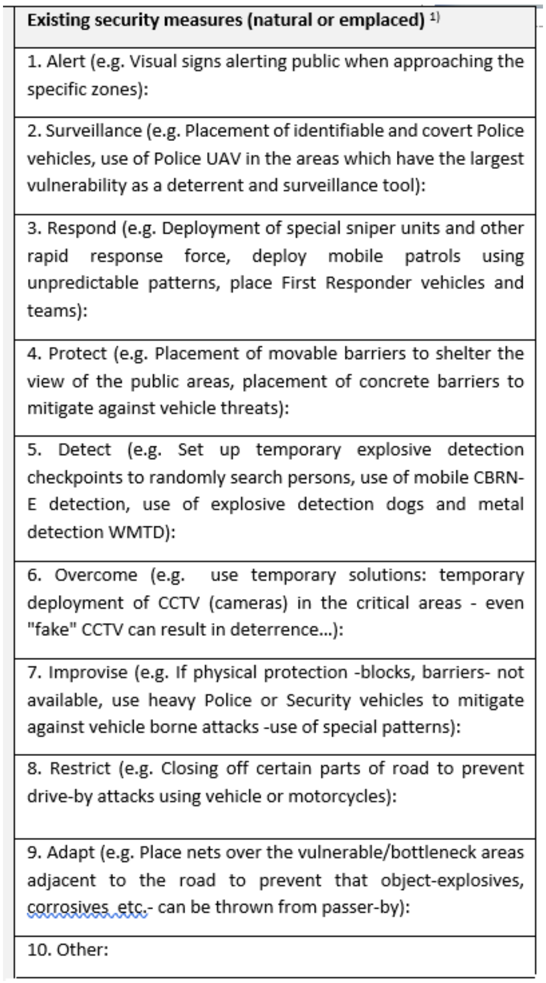
First, write the necessary details like the main site's name, if there are specific activities happening (like a festival, market, or something else) and when this activity occurs. The dates and times are important to be aware if an activity is occurring regularly or is incidental.

Second, 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. It is possible that the crowd density differs on specific times, please add this if relevant.

Finally, it is useful to fill in the team members and the date of assessment.

3.2.2 Step 2: Existing security measures

The second step is to gather, together with the team of experts, the existing security measures you are aware of regarding the specific site. This can be a natural measure, for instance a wall that can create a blockage or to hide behind, or emplaced measures, for instance surveillance police teams or roadblocks. This can be filled in in the upper right column of the record template, see figure 8. Here the nine types of measures denoted in the EU VAT are stated, to assist in discovering the measures. It can be useful to go through all the types one by one and ask yourselves if there are any measures (big or small) that fit. There is also one row where there is space to add any measures you think do not fit the types of measures.



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 Police vehicles, use of Police UAV 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 parts 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 object-explosives, corrosives, etc.- can be thrown from passer-by):
10. Other:

Figure 8 right upper column of record template; existing security measures.

> *One important note: it is about identifying existing measures that have effect on identifying vulnerabilities and not about thinking of measures that are not yet in place but that can mitigate the potential threats.*

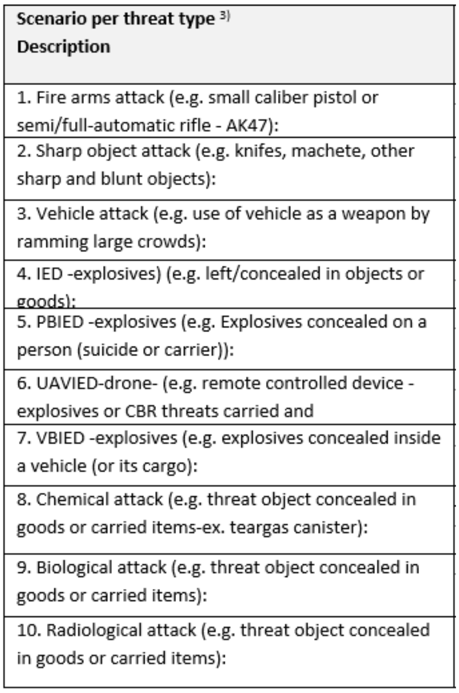
Identifying new mitigating measures is done after identifying the vulnerabilities (i.e., after using the EU VAT and out of scope for this manual).

3.2.3 Step 3: Scenario per threat type

In the third step, we ask for your creativity, expertise, and some well-argued discussions amongst each other.

Choose the EU VAT phase (i.e., Excel tab) to which the site in question belongs (determined in Step 1).

On the EU VAT phase tab, there are ten terrorist threat types identified that need to be assessed per site. Please go through every threat. The left column on the bottom of the record template gives the opportunity to write down one or more scenarios for each threat, see figure 9.



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 vehicle 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 and
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 9 right upper column of record template; existing security measures

For every threat, the EU VAT provides some information to help form a realistic scenario (see Annex D gathering the different types of scenarios in the EU VAT). Please also use any information you have gathered beforehand on known threats and current threat assessments. With an example, we will aid you in how to form a scenario and where you can find relevant information in the tool:

Example of possible scenario per threat type

Imagine there is a medium sized festival, with a large viaduct adjacent to the main site. The viaduct normal traffic (vehicles) going over it, including the arriving and departing festival goers. The viaduct was designated a Phase 1 site.

We start with assessing the first threat: **a firearms attack**. There are many forms of a firearms attack, which is why it is important to look at the EU VAT and use your creativity to form a realistic scenario of a firearms attack on or from the viaduct.

Please look **at section 2 of the EU VAT** phase tab (see chapter 2) or look at Appendix D where all relevant scenario building information from the EU VAT is stated per phase. Here, different images, situations and questions are placed, that might help you create a realistic situation and scenario for a specific threat. So, within the "phase 1 tab" look at section 2 for the different situations that are at stake regarding the different threats. Look for the situations regarding a firearm attack for instance.

In our example, **there might be two relevant scenarios**. One might be that there is a shooter that will walk on the viaduct or get out of the car and shoot festival goers on the main site from this high vantage point. Another scenario might be that the terrorist walks on the viaduct when the traffic on the viaduct becomes congested and then starts shooting people in the cars.

As a team, you need to decide on possible scenarios and write down what happens. It is important to consider relevant measures you have identified earlier and consider any deficiencies in these measures in your scenario. For instance, maybe you do not allow people to walk on the viaduct and you have a surveillance team monitoring this. If this is the case, the scenario of someone walking on the viaduct and then potentially shooting the festival goers, is not likely as you can easily detect and stop people walking on the viaduct. On the other hand, you might not have the ability to check all the traffic on the viaduct, so the potential of someone getting out of a car on the viaduct and start shooting people might be a viable scenario.

When conceiving attack scenarios for this site, also consider combinations of existing measures for this site with existing measures and weaknesses on other sites belonging to this 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. For the purposes of the vulnerability assessment exercise, the team of experts need to search for realistic and probable scenarios taking into account the characteristics of the PSOI and all relevant information collected for the preparation of the assessment.

> *One important note: it might be that for a specific site you only identify two potential threat scenarios. The ten threats are there just to stimulate discussions and search for scenarios. Non-viable scenarios can be disregarded. One should only assess scenarios that the team decides are realistic and everyone feels the urge to know how vulnerable the site is for such a scenario.*

3.2.4 Step 4: Consequence and probability

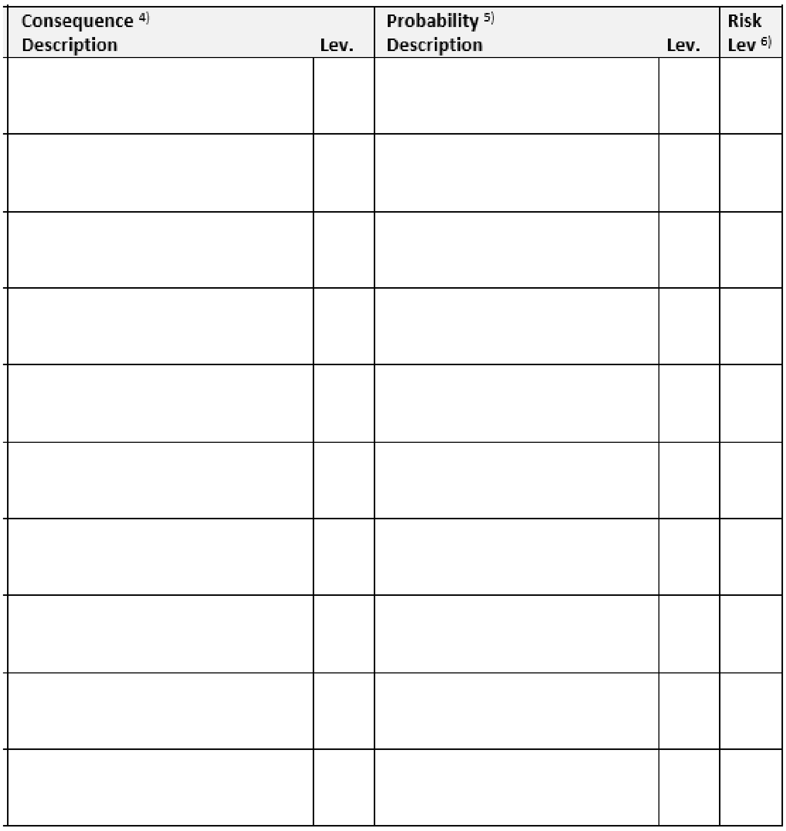
In the previous step, the devised scenario regarding a threat has been written down and agreed on by all the team members. Now in this step, this scenario can be assessed by determining the consequence of the attack and the probability that this actually happens.

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 level of probability of a scenario (see figure 10).

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 of low consequence and again, 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 easy a potential terrorist can reach the site, what surrounds the site, what means do you already have, and which factors influence the probability. Together you decide if the attack has a high, medium, or low probability. Please try to describe your motivation to choose the given probability level.

Please view appendix C with a created scenario and a filled in record template with the information provided by the scenario to give even more understanding of how to do this vulnerability assessment.



Consequence [4]		Probability [5]		Risk
Description	Lev.	Description	Lev.	Lev [6]

Figure 10 bottom right column of record template; consequence, probability and risk level.

3.2.5 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 level of risk for each scenario, for instance by using a risk matrix (see paragraph 2.3 Figure 3 - Example of a risk matrix) and note it 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 score of High, Medium, or Low (see table 3).

Table 3 Overview of vulnerabilities of each site regarding each terrorist threat[4]

	Fire arms attack	Sharp object attack	Vehicle attack	IED attack	PBIED attack	UAVIED attack	VBIED 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 is done.

3.3 What's next

Once an overall insight into the vulnerabilities of the PSOI is available, follow-up actions can be taken such as:

- The security experts' team can suggest mitigation options for some or all of the attack scenarios to the management body;
- Using the results from using the EU VAT, the managing body can evaluate the risks, deciding which risks to mitigate and how (in part based on the options provided by the security team) and which risks to accept;
- Getting the measures implemented;
- Informing and involving the stakeholders.

[4] Please, if it is the case that for a specific terrorist threat you have assessed multiple scenarios, be creative by using the example of creating an overview of your vulnerabilities.

4 Conclusions

This report has provided an operational Manual which objective is to help local authorities use the tool developed by the European Union's Directorate General Home Affairs to assess the vulnerabilities of urban public spaces specifically their soft targets, titled Vulnerability Assessment Tool (VAT). This tool can be used on site to evaluate a public space.

In addition, several tools have been designed to facilitate the implementation of a vulnerability assessment. These tools suggest group work methodologies that can be carried out during the assessment as well as practical exercises to become familiar with the working methodology and the tool.

This document reports the first activity of WP2 and constitutes a starting point for the partner cities of the project to test the EU VAT tool using the Manual and to identify the vulnerabilities of a chosen public space of interest. A time of two months has been foreseen to carry out the process of identification of these vulnerabilities in each municipality. The WP 2 staff will support the municipalities in each phases of the process.

The Manual is considered to be an ongoing document, as it will receive feedback from each municipality when conducting their assessment, in terms of obstacles and recommendations for the improvement. At the end of the different assessments the manual will be updated including the different lessons learned from the municipality and included in the final report recommendations for the improvement of the VAT tool addressed to the DG Home that will enrich their commitment to involve local stakeholders in the protection of public spaces.

5 References

[1] DG HOME. (2019). Site assessment checklist master enlet1. Version January 2019.

[2] Efus. (2005). Secucities: Cities against Terrorism-Training Local Representatives in Facing Terrorism. Last visited on 19-02-2019 : https://issuu.com/efus/docs/cities_against_terrorism

[3] European Commission (2018). EU Grant Agreement 815356-PRoTECT. ISFP-2017-AG-PROTECT. Version October 2018

[4] European Commission. (2017). Action Plan to support the protection of public spaces. Last visited on 19-02-2019: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_action_plan_to_improve_the_protection_of_public_spaces_en.pdf.

[5] European Commission (2016). General Secretariat, Corporate policies, Classified information assurance. Last visited on 7-02-2019https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/

[6] ISO standard 31000:2018 series.

[7] Local Government Association. (2014). Public Spaces Protection Orders Guidance for councils. Last visited on 19-02-2019: https://www.local.gov.uk/sites/default/files/documents/10.21%20PSPO%20guidance_06_1.pdf

[8] Ministère de l'Intérieur (2018). Guide des bonnes pratiques de sécurisation d'un évènement de voie publique. Last visited on 20-02-2019 https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Securisation-des-evenements-de-voie-publique

[9] National Counter-Terrorism Security Office (NaCTSO). (2017). Crowded Places Guidance. Last visited on 19-02-2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701910/170614_crowded-places-guidance_v1a.pdf

[10]UK Cabinet Office. (2013). The Civil Contingencies Act. Last visited on 19-02-2019: https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others.

[11]Word Café Method Last visited on 19-02-2019 http://www.theworldcafe.com/key-concepts-resources/world-cafe-method/

[12]5D Methodology (Appreciative Inquiry) Last visited on 27-02-2019 http://www.kstoolkit.org/Appreciative+Inquiry

Appendix A - Vulnerability assessment record template

This appendix contains an example format for recording the vulnerabilities and their assessments as determined by the team of experts. This template could be constructed in Microsoft Word document or Excel spreadsheet.

The template is given on the next page; footnotes accompanying the template are given on the page thereafter.

The parts of the EU VAT correspond to the parts of the template as follows:

- “Scenario per threat type” combines threat types (part 1) and situations (part 2).
- “Existing measures” is based on measure types (part 3)
- “Assessment” is based on part 4.

Main site	**Existing security measures (natural or emplaced)** [1]
Main site name/address:	1. Alert:
Activity:	2. Surveillance:
Dates and times of the Activity:	3. Respond:
	4. Protect:
Site being assessed (main/surr.)	
Surrounding site name/address:	5. Detect:
Phase: [2]	6. Overcome:
Expected crowd density:	7. Improvise:
	8. Restrict:
Vulnerability assessment	
Team members:	9. Adapt:
Date of assessment:	10. Other:

Scenario per threat type [3]	**Consequence** [4]	**C.Lev.**	**Probability** [5]	**P.Lev.**
1. Fire arms attack:				
2. Sharp object attack:				
3. Vehicle attack:				
4. IED (explosives):				
5. PBIED (explosives):				
6. UAVIED (drone):				
7. VBIED (explosives):				
8. Chemical attack:				
9. Biological attack:				
10. Radiological attack:				

Footnotes accompanying the record template:

1) The type of area (as given in the EU VAT, e.g., Phase 1 - Access roads to venue, Phase 2- parking and transport, etc).
2) A description of the exiting measures on the site (natural or emplaced)
3) A description and examples of the threat types are given on the Phase tab and a scenario description based on a vulnerability (lacking or insufficient existing measure); if not applicable, describe why; if applicable, describe what the threat does to what/whom and how this is achieved (name the exploited weakness); if more than one viable scenario is imaginable for a threat type, add extra lines under the threat type.
4) A description of the estimated consequence(s) of the scenario (impact, e.g. delays, damage, deaths) and dependences, and the allocated severity level (e.g. Low/Medium/High).
5) A description of influences on the probability of the scenario unfolding (likelihood/chance), and the allocated probability level (e.g., Low/Medium/High).
6) The risk level as determined from a risk matrix (e.g., Low/Medium/High).

Appendix B – Terms and definitions

This manual adopts the terminology of the EU VAT. This appendix describes the most relevant terms. Sometimes, the terminology of the VAT is not clear. In those cases, an additional remark is made here, and at the first point the respective term is introduced in the manual itself.

Activity A common or collective action performed by a large group of people. For example, people in a concert hall, commuting at a train station or people present at a festival.

Attack An act of physical violence.

Main Site A confined area in *Public Space*, where a specific *Activity* takes place, and for which the municipality deems protection against terrorist attacks necessary. The main site can have various *Surrounding Sites* which support the activity at the main site.

Managing Body The managing body is an individual, organisation or group of organisations that takes up the responsibility to identify and work on counter terrorism regarding *PSOI's*. This can be a law enforcement agency, a municipality or possibly also the owner of the *Main site*. The management will most likely involve various stakeholders in decisions concerning site security, such as local government, emergency services, retailers, etc. In the case of the PRoTECT project, the managing bodies are the 5 municipalities that will identify their *vulnerabilities* against various terrorist attacks and identify their *soft targets*.

Phase VAT defines a phase as a type of geographical site that is part of a PSOI. The VAT defines six phases. **Remark 1**: the term phase is related to time, not to geography. This can lead to confusion. For example, the same site can be used for arrival and for departure of people, but that does not have to be the case. **Remark 2**: The six phases are implicitly derived from a security ring model consisting of two rings. Concrete (events in) PSOI's can use a different number of security rings.

Public space A place that is generally open and accessible to members of the public, such as roads, parks, and municipality buildings. Public space includes semi-public spaces, such as train stations, and privately-owned spaces such as shopping malls.

PSOI A Public Space of Interest (PSOI) is the *Main Site* and the associated *Surrounding Sites*. A vulnerability assessment is made for a PSOI.

Soft target A site that is insufficiently protected against a terrorist attack and when attacked by a terrorist organisation, will help terrorists obtain their goals. In the context of recent terrorist attacks, the soft target specifically is the members of the public that are present at that site[5]. The EU VAT requires a soft target as input to the process. It is then called a *Main Site* or one of the associated *Surrounding Sites.*

Surrounding Site A confined area in *Public Space* where a large number of people congregate in connection with the *Activity* at the *Main Site* (e.g. an access road, a parking area). The municipality deems protection against terrorist attacks necessary for a surrounding site.

[5] A soft target can also be something else than people. For example, an unprotected symbolic object such as a monument.

Appendix C – PSOI scenario example

A scenario for the use of Vulnerability assessment Manual by local authorities

This is the story of City X. It is a fictional scenario aimed at illustrating the use of the EU Vulnerability Assessment Tool Manual for the identification of vulnerabilities of soft targets in case of a terrorist attack. This scenario is inspired from the scenario built in the framework of the project SURVEILLE on the use of security and surveillance technologies Deliverable 2.3. While the story and all names are fictional, they are based on real world analogies.

Using a scenario serves several purposes. Firstly, it provides users of the manual with an overview of a plausible situation that might be confronted to. Secondly, although not exhaustive, the scenario of city X provides insights on operational procedures and stakeholders at the municipal level involved in the protection of public spaces. Third, it facilitates the understanding of the manual and the use of the tool and give municipal actors the possibility to conduct a vulnerability assessment in a real site.

As mentioned in the Manual the EU VAT was meant for European law enforcement agencies. However, since the competences of local authorities differ from those of law enforcement agencies, this scenario intends to illustrate the roles and competencies that these local actors have in the protection of soft target.

The story of city X.

City characteristics:

- Every year a music festival is organized hosting 5000 participants (locals and visitors)
- The festive gathering is planned in 6 months.
- The event will take place in the central park of the city center
- The event will start on a Saturday at 6pm and it will end at midnight.
- Night transport in city X runs until 1:30 am on weekends.
- The city has a vibrant nightlife (restaurants, bars, theatres and clubs located in the city centre attracting large crowds) this poses some risk to public order, but the city manages quite well thanks to its municipal supervision center lead by Tomas M. which cooperates with different departments and categories of personnel (from municipal, civil services, transport and mobility service, police officers to street mediators), and thanks to its cooperation with the police.
- Moreover, the city increased its knowledge base and prospective capacity through a closer partnership with the tourism office, and with transport, parking operators and hotel companies.
- Even while the city has been hosting this event for the past 9 years, the current security challenges require an adaptation or revision of their operational procedures to reduce vulnerabilities.
- Even though organizers have carefully planned the event in the past editions, and have their own security squad, Thomas worries about groups of extremists and other violent troublemakers.
- In the previous edition of the festival, the city hosted around 5000 participants. This year, in occasion of the 10th anniversary of the event, special activities are planned and therefore a larger number of people is expected.
- Last year, the municipality decided to put roadblocks to avoid trucks from accessing the surrounding areas. This measure reduced the participants’ rate and gathered complaints from the retailers due to the highly negative impact on the urban landscape, it also had a highly negative impact on people’s feeling of security.
- This year, the municipality appointed 300 municipal officers to police the area, they are deployed in the arrival areas and approaches to venue zones. The festival operator has assigned 5 private security guards to control access points.
- Thomas knows that to protect participants from any danger requires a special preparation considering the current threat level and the high number of expected participants this year.

- In the previous editions the team of experts led by the council staff included: event organizers, private security team, municipal police, civil protection...
- In preparation of the event, Thomas has identified 4 access roads to the venue (Normally two will be blocked during the event), 1 parking, 1 transport area, 2 approaches to venue, 2 entry/ exit zones.
- In this edition Thomas plan to have access control points in every arrival area.
- This year, apart from the permanent bars and restaurants that are located in the west side of the parks, there will also be some food & drinks areas inside the event. Until now the municipality has not vetted the suppliers of goods for events and no control of areas used to store goods in the permanent shops is done.
- In the area around, there are some small and medium hotels, with a 50-person capacity each. Following the regulations of the city concerning commercial activities, building in this area might not have more than 3 floors.
- In the past editions, the square where the festival took place started filling up with people from 2pm increasing the traffic going in the direction of the city Centre.
- Thanks to radio frequency identification, chips in transport tickets allow to identify an unusual number of passengers. By 4pm, large crowds have gathered not only in the streets and on the sidewalks, but also in the public transport system: subway lines, tramways and buses were packed.
- The festival ends at midnight. From 11:30 to 00:30, areas leading to the metro station are very crowded.
- In summertime the park is open 24/7. Security starts from 6.00 am to 9.00 pm. The rest of the time there is any security patrols, the cameras present in the park are not sufficiently technological to capture night images.

City equipment:

- local crime observatory[6]
- In order to monitor events and maintain public order the city has an urban supervision center which receives and requests live footage from the local CCTV system.
- The municipality has installed 5 fixed cameras around the area from the municipality, retailers surrounding the venue also put cameras in the entrance of their shops. In case of an emergency, all the CCTV systems can be connected.
- Police units on the ground can also receive information on mobile devices and provide footage with mobile cameras.
- The latest tool of city X are its two drones, which can deliver life footage to the supervision centre
- The city has a local security and prevention strategy including the protection of public space.
- At the national level, the Minister of Interior has developed a guidebook for the protection of events and public spaces[7]
- There is also an evacuation plan of the venue detailing use of emergency services, escape routes and emergency exits.

Please see below a filled in record template according to this scenario as an example.

[6] There are local, regional and national crime observatories. National observatories sometimes provide local authorities with local statistics and crime maps such as the CartoCrime project of the French government http://www.cartocrime.net/Cartocrime2/index.jsf

[7] Here some concrete examples of national guidelines https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Securisation-des-evenements-de-voie-publique https://www.gov.uk/government/publications/crowded-places-guidance

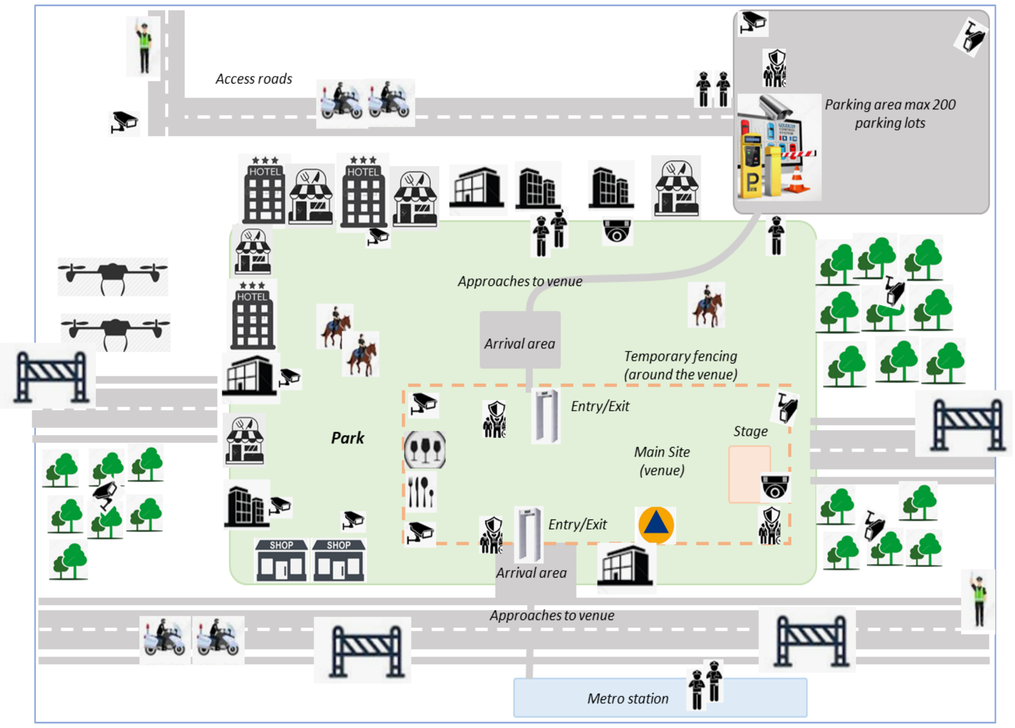
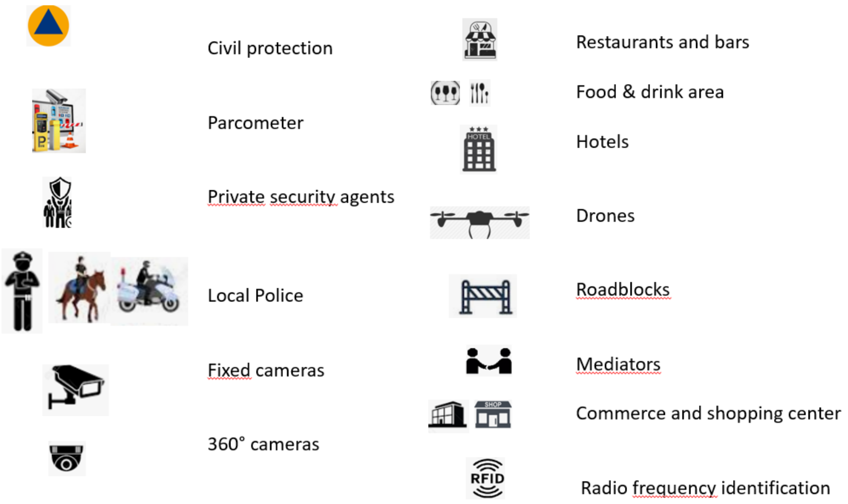


Figure 11 Example of a PSOI and EU VAT phase designation[8]



Civil protection

Parcometer

Private security agents

Local Police

Fixed cameras

360° cameras

Restaurants and bars

Food & drink area

Hotels

Drones

Roadblocks

Mediators

Commerce and shopping center

Radio frequency identification

[8] This is just an illustrative example to visualize and map out the site, it is not meant to be used for the scenario exercise, during the actual workshop the managing body will be providing an accurate map of the site to be assessed and participants will draw their own map of all the phases/sites surrounding the main site

Appendix D – Scenarios from EU VAT

Phase 1 Access Road to Venue

Main Group of Protection Areas	Sub-group of Protection area
Public road system or facility (ex. parking lot or parking garage) that give access/lead to main activity areas (museum, hotel, shopping mall, rail station, airport, sport stadium, theatre) where medium-large concentration of public occurs. What are the times when the increased number of public is present (predictable or unpredictable?)	
Public access areas (pathways, roads, entry areas) which result in medium-large concentration of public (ex. Sport stadium gates, shopping mall or airport entry doors, etc.). What are the times when the increased number of public is present (predictable or unpredictable?)	Is the design of the access to the main site of such kind that an attack on parts of the infrastructure could have a negative impact on the other (Ex. Vehicle borne IED attack on the lower road deck could have grave impact on the upper road level. Verify the blast characteristics for the site
	Could the road(s) serving the main site be used to block or otherwise seriously disrupt the commercial activities of the main site by attack or sabotage (ex. detonate a vehicle IED to disrupt the only road access). How many road access points are available? Would loss of one disable or seriously disrupt main site operations?
	Is the main site located near major roads access points (freeway) that could give quick escape from the main site during/after the attack
	Does the road access allow for a large and heavy vehicle to potentially access the areas where concentration of public is present, could the use of vehicle as a sole means of attack be sufficiently dangerous? (Could a vehicle containing Dangerous Chemicals or other substances be used to achieve the terrorist goals?) Could a military style vehicle be used?
	Could the garage or other public complexes be used to attack either the arriving public or the complex itself (ex. Madrid airport parking garage attack). Could such attack seriously disrupt the commercial activities of the main site?

	If public transport system is closely supporting the public access to the main site, could attack on such public transport seriously impact on the operation of the main site. Question of predictability of the times most people arriving et departing (just after the event: large crowds waiting in front of the station or in the station)

Phase 2 Parking and Transport Facilities

Main Group of Protection Areas	**Sub-group of Protection area**
Public access areas used for parking or gathering places with connection to local transport which result in medium-large concentration of public	Are any roads that lead to the entry of the Main Site (example between the parking lot and the site) that may offer more exposure to sudden attacks. Is pedestrian traffic forced to pass a tunnel or other confined space before arriving at the main venue (ex. Shopping mall, hotel, sport stadium, train etc.)
Public road system or facility (Ex. parking lot or parking garage) that give access/lead to main activity areas (museum, hotel, shopping mall, rail station, airport, sport stadium, theater) where medium-large concentration of public occurs. What are the times when the increased number of public is present (predictable or unpredictable?)	Could transport parking and other facilities be used to launch attacks against public utilizing such areas, are the crowd concentration index high.
	Could the hotels, public/private buildings/garages or other public complexes be used to attack either the arriving public or the complex itself (ex. Las Vegas attack, Madrid airport parking garage attack). Could such attack seriously disrupt the commercial activities of the main site.
	If public transport system is closely supporting the public access to the main site, could attack on such public transport seriously impact on the operation of the main site. Could the attack be carried on the transport system itself due to the vulnerability created at the transport point in order to protect the main site? Question of predictability of the times most people arriving and departing (just after the event: large crowds waiting in front of the station or in the station)
	Parking garages. Does the garage locations give direct access to the main site (or are located under the main site) and which could be exploited to strike at the main site (ex. 1993 World Trade Center Garage attack)

Phase 3 Approach to Venues

Main Group of Protection Areas	**Sub-group of Protection area**

Public road system or facility (Ex. parking lot or parking garage) that give access/lead to main activity areas (museum, hotel, shopping mall, rail station, airport, sport stadium, theatre) where medium-large concentration of public occurs. What are the times when the increased number of public is present (predictable or unpredictable?)	Are any r**oads that lead to the entry of the Main Site** (example between the parking lot and the site) that may offer more exposure to sudden attacks. Is pedestrian traffic forced to pass a tunnel or other confined space before arriving at the main venue (ex. Shopping mall, hotel, sport stadium, train etc.)
	Is the design of the access to the main site of such kind that an attack on parts of the infrastructure could have a negative impact on the other (Ex. Vehicle borne IED attack on the lower road deck could have grave impact on the upper road level. Verify the blast characteristics for the site
	Does the road access allow for a large and heavy vehicle to potentially access the areas where concentration of public is high, could the use of vehicle as a sole means of attack be sufficiently dangerous? (Could a vehicle containing Dangerous Chemicals or other substances be used to achieve the terrorist goals?) Could a military style vehicle be used?
	Could the hotels, public/private buildings/garages or other public complexes be used to attack either the arriving public or the complex itself (ex. Las Vegas attack, Madrid airport parking garage attack). Could such attack seriously disrupt the commercial activities of the main site?
	If public transport system is closely supporting the public access to the main site, could attack on such public transport seriously impact on the operation of the main site. Could the attack be carried on the transport system itself due to the vulnerability created at the transport point in order to protect the main site? Question of predictability of the times most people arriving and departing (just after the event: large crowds waiting in front of the station or in the station)

Phase 4 Arrival at Venue Points

Main Group of Protection Areas	Sub-group of Protection area
Arrival points at the venue - used for entry or exit. **Public access areas** (pathways, roads, entry areas) which result in medium-large concentration of public (ex. Sport stadium gates, shopping mall or airport entry doors, etc.). What are the times when the increased number of public is	Are any r**oads that lead to the entry of the Main Site** (example between the parking lot and the site) that may offer more exposure to sudden attacks. Is pedestrian traffic forced to pass a tunnel or other confined space before arriving at the main venue (ex. Shopping mall, hotel, sport stadium, train etc.)

present (predictable or unpredictable?)	
	Could any type of attack be carried out near or at the access points to the main site (without accessing the site) with great loss of life? Could a suicide attack be the potential mode?
	Are the public transport merge points giving access to the venue resulting in high density crowd, are the injection points resulting high/medium or low concentration

Phase 5 Venue Security- no access ctrl

Main Group of Protection Areas	**Sub-group of Protection area**
Public access areas (pathways, roads, entry areas) which result in medium-large concentration of public (ex. Sport stadium gates, shopping mall or airport entry doors, etc). What are the times when the increased number of public is present (predictable or unpredictable?)	Are any r**oads that lead to the entry of the Main Site** (example between the parking lot and the site) that may offer more exposure to sudden attacks. Is pedestrian traffic forced to pass a tunnel or other confined space before arriving at the main venue (ex. Shopping mall, hotel, sport stadium, train etc.)
Public main activity areas with No Access Control (schools, hotel, shopping mall, rail station, airport, hospital, house of worship/church) where medium-large concentration of public occur. What are the times when the increased number of public is present (predictable or unpredictable?)	Are the main site construction materials of such design or product (ex. glass) that impact on such design could result in harm to the public? (Ex. Glass ceiling collapsing on the public?)
	Does the main site offer many exists that could be used in the event of an attack, could such exits be blocked by the attackers and create a larger public escape point which could be targeted? (Ex. Blocking exit by a burning rubbish bins and directing escaping public to other point where attackers are positioned?

Phase 6 Venue Security with access ctrl

Main Group of Protection Areas	**Sub-group of Protection area**
Public access areas (pathways, roads, entry areas) which result in medium-large concentration of public (ex. Sport stadium gates, shopping mall or airport entry doors, etc). What are the times when the increased number of public is present (predictable or unpredictable?)	Are any r**oads that lead to the entry of the Main Site** (example between the parking lot and the site) that may offer more exposure to sudden attacks. Is pedestrian traffic forced to pass a tunnel or other confined space before arriving at the main venue (ex. Shopping mall, hotel, sport stadium, train etc)

	Could any type of attack be carried out near or at the access points to the main site (without accessing the site) with great loss of life? Could a suicide attack be the potential mode?
Restricted public access areas with Access Control (ex. access granted to ticket holders: museums, entertainment parks, sport stadium, theatre, train/maritime hubs) which result in medium-large concentration of public. What are the times when the increased number of public is present (predictable or unpredictable?)	Does the main site create a congestion that could be exploited by attackers? Are the security controls spaced so that the crowd density is not resulting in high concentration?
	How many access points which could be used during entry or exit, are the emergence exit points the same? Could emergency exit point be blocked by unlawful ways?
	Does the main site operate public elevators which create limited space and can such elevators be targeted from outside (ex. Elevators with glass windows)
	Could the areas be breached and entered with relative ease and allow to carry out an attack. ex. fence can be climbed or cut and allow access.

Phase 6 Security controls inside venue

Main Group of Protection Areas	**Sub-group of Protection area**
Security controls inside venue	Could an attack be perpetrated inside the event, or facility aided by insiders (ex. Staff may allow attackers to enter via staff/service entry points)
	Are there any areas which could be used to store threat objects that could be previously carried by outsiders
	Are there any areas which could be used to store threat objects that could be previously introduced by insiders or staff preparing the venue for event or otherwise who has access to the venue
	Are the suppliers of different goods conveyed to the critical areas, known by the operator of the venue? Are these suppliers vetted by authorities (job history check is not considered vetting)
	Are such suppliers subject to any security regime (ex. does they have any security programme or security principles they follow) Could such vendor supplies be used to conceal

	different threats? could the vendor staff themselves be potentially capable to carry out an attack (see past insider threat attack cases)
	Are all supplier using own staff or is the supplier using subcontracted staff, is the staff subject to any vetting or background verification such as job history or code of conduct (Police check), Could such staff be able to carry out attack on the venue or the public?
	During the event, or operations, is the supplier deliveries subject of any controls (for signs of tampering or introduction of potential threat objects), are the deliveries performed by staff recorded and known to the supplier. Could goods conceal certain types of threats to the public which could be activated via an automated or remote triggering mechanism?
	Are all the security measures known to the public (and staff), assess the potential impact of insiders to carry in threat objects in-between the security controls (ex. before the event, Are the goods to be used at the venue protected or supervised during the storage period to ensure that no unauthorized threat objects can be inserted after the security controls have been carried out? Which goods could be exploited to conceal threats?
	Does the operator have any internal quality control programme which measures the effectiveness of operator's security measures or regime, is the frequency of any quality control measures undertaken according to a planned and known pattern to the employees (ex. once or twice annually), are the quality control methods effectively monitoring the full range of different threats or are the QC measures limited to certain core activities? Which are these methods?

Appendix E – Guidelines for the organization of a local workshop – Vulnerability assessment

As mentioned in the Manual of the EU VAT, the vulnerability assessment of the soft targets in case of a terrorist threat is a process necessitating different steps.

1. PSOI (Public Space of Interest) identification.

You as the "Managing body" (Municipality representative and supporting organisation) in this case will identify the site and its surrounding sites and will retrieve an accurate map of the area[9]. For the purpose of the pilots on the use of the Manual, it is suggested to choose a site close to the venue where the workshop will take place, in order to be able to organize a visit. Ideally, if this site organizes an upcoming event that will bring together a significant number of people or if in everyday life the site presents moments of massive use, the site will be considered a PSOI to conduct the vulnerability assessment.

In page 8 you will find the categories of main sites.

Table 4. Managing body per Municipality

Managing body per Municipality	
Vilnius	Security municipal representative L3CE
Larisa	Security municipal representative KEMEA
Malaga	Security municipal representative Ministry of the Interior
Brasov	Security municipal representative National Police of Romania
Eindhoven	Security municipal representative DITSS

2. Constitution of the team of experts:

Representatives from the cities and supporting organisations have been trained to the use of the Manual and the EU tool during the workshop in Paris (partners meeting PRoTECT and on the 1st of March). These persons should identify two groups of people to participate in the different moments of the process:

[9] For the purposes of the exercise, it is important to have an accurate map of the area drawing the exact boundaries, the distance between buildings, roads etc., the number and location of street furniture etc. This map can be taken from the municipal archives and/or from the Municipal GIS (Geographic Information System).

2.1 Managing body members: Municipal actors to be involved in the vulnerability assessment (6 to 7 in total). These persons need to be familiarised with the Manual and have prior security knowledge. We suggest organising a one day meeting (reproducing the session in Paris) in which these municipal actors understand the tool and their role during the assessment. They will have a main role in the moderation of the VA session (workshop).

2.2 Key stakeholders who will integrate the team of experts during the vulnerability assessment (See section 2.1 Tool users for more details on what kind of actors to invite). These persons will be invited to participate to the workshop in which the VA will be implemented. No more than 25 persons should take part in the assessment.

3. Collecting useful information:

Information about how the city approaches the security of public spaces, for instance soft targets (regulation, policies, security strategies, etc.). This information will be useful to determine the level of existing protection, the available resources, etc. More elements to be gathered can be found on sections 2.3 and 3.1.

Also collect 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). Important to collect information about the specific threats identified for the selected site. 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 associating an expert/ consultant to help you to identify specific threats).

4. Phases identification:

Another step here is drawing up the map of PSOI with its main site and surroundings sites to identify the phases of the tool that need to be assessed.

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

More information on section 3.1 Getting started.

5. Preparation of the local workshop:

5.1 Methodological issues:

The local workshop will have different moments, site visit, work in small groups, plenary sessions… it is important that during the assessment the participation of all actors is ensured. Keep in mind that time may be limited, and sessions may become too cumbersome. It is therefore necessary to define an iterative and varied working methodology.

Here are some suggestions meant to support each partner in organising his workshop:

- *World café:*

“The "World Café" is a structured conversational process intended to facilitate open and intimate discussion, and link ideas within a larger group to access the "collective intelligence" or collective wisdom in the room. Participants move between a series of tables where they continue the discussion in response to a set of questions, which are predetermined and focused on the specific goals of each World Café”.

“Small groups of four or five participants sit around a table and discuss an open-ended question for a structured amount of time. Notes and drawings are often made by participants on the paper tablecloths used in most events. Individuals switch tables after the agreed upon amount of time, where (if they are being used) a "table host" at the new table briefly welcomes people and fills them in on highlights of the previous discussion”[10].

How to use during the assessment?

Once having identified the phases - meaning the PSOI’s main site and surroundings sites linked to the phases of the EU VAT - that are relevant for the selected site, participants should be equally distributed into groups, each group needs to have a person that is familiar with the tool and the manual. Ideally this person should be from the Managing body and have a role in each group. Each group should analyse a specific phase of those identified. After 40-50 minutes of discussion on each of the phases, people must change tables. Each working group should appoint a person that will fill in the record template. When using the Vulnerability assessment record template, we suggest following the sequence proposed in the manual (Section 3.2.1, step 1 to 4, step 4 will be discussed in plenary session):

Step 1. Characteristics of the site

Step 2. Existing security measures

Example: the site has a CCTV system of 5 fixed cameras belonging to the Municipality

Step 3. Scenario per threat type

Examples of possible scenarios per phase: Venue security with access control

- Could any type of attack be carried out near the access point to the main site (without accessing the site) with great loss of life? Could a suicide attack be the potential *modus operandi*?
- Does the mains site create a congestion that could be exploited by attackers?
- Are the security controls spaced so that the crowd density is not resulting in high concentration?

While not all scenarios will be realistic for all kinds of terrorist attacks, it is suggested to go through every type of threat, think of scenarios and select the ones you want to assess while skipping the others. Sometimes there could be multiple scenarios for a terrorist attack, you

[10] http://www.theworldcafe.com/key-concepts-resources/world-cafe-method/

then can choose to assess all, or decide on the ones you find most likely or to have the most impact and assess them. See other examples in Annex D. Nevertheless, keep in mind that these examples are not exhaustive, therefore the creativity of the group is necessary to the success of the session.

The moderator will suggest different scenarios and together with the team choose which scenario regarding the terrorist attacks to assess. The moderator will guide participants through the VA tool.

Step 4. Consequence and probability

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 of low consequence and again, try to describe what the reasons are for choosing the consequence level. More details on section 3.2 of the Manual.

Step 5. Analysis and results (will be developed in plenary session)

How to set up the working groups?

As mentioned in the Manual, the number of phases to be analysed depends on the number of sites identified, i.e., there can be more than one site attributed to one phase. This can hinder or lengthen the working session as this methodology calls for participants to change and participate in different phases (that we call rounds). However, we propose the following method to organize the groups.

For example, if you have 15 sites to analyse:

Table 5 Illustration of working groups set up-World Café

		World Café			
		Round 1	**Round 2**	**Round 3**	**Round 4**
Phase	**Number of site per phase**	**Working table**	**Working table**	**Working table**	**Working table**
Phase 1	2	1			
Phase 1			1		
Phase 2	3	2			
Phase 2			2		
Phase 2				2	
Phase 3	4	3			
Phase 3			3		
Phase 3				3	
Phase 3					3
Phase 4		4			
Phase 4	4		4		

Phase 4				4	
Phase 4					4
Phase 5	2	5			
Phase 5			5		
Participants per table	**15**	**6**	**6**	**10**	**15**

According to the table above, to analyse 15 sites requires 4 rounds. The number of participants in each group in each round depends on the number of phases. Note that for round 4 two groups of 15 people are required.

- *5-D model*

  The 5-D model is an applied method based on the appreciative inquiry theory of Cooperrider. It intends to help people (from different backgrounds) to collaboratively create a future ideal picture, and hence build a plan to get there. It is a positive driven approach building on what is the best[11]. The model is widely applied for creating self-directed organizational change and program assessment, monitoring and evaluation. Picturing a collaborative goal and formulating what is needed to get there might be interesting for PRoTECT.

  Note: swapping tables during the workshop, like done at the World Café method is less suitable for this method, since the group formulates and work on 'their' own analysis during all phases of the method.

  How to use during the assessment?

  For the use of the 5D methodology, it is necessary to define a goal, which for this case would be the identification of the vulnerabilities of the selected site. It is suggested that the session is divided into 5 moments.

  I. Definition: establishing the focus and scope of the inquiry.

  Example: assessment of phase 2 of main site.

  II. Discovery: identifying all of existing measures implemented that contribute to the protection of the site.

  Example: the site has a CCTV system of 5 fixed cameras belonging to the Municipality.

  III. Dystopia: collecting the wisdom and imagining what might happen- (normally this phase includes a visualization of the desired future) for purposes of the project in this phase we suggest to visualise the possible scenarios that can put at risk the security of the site).

  Examples of possible scenarios per phase: Venue security with access control

[11] http://www.kstoolkit.org/Appreciative+Inquiry

- Could any type of attack be carried out near the access point to the main site (without accessing the site) with great loss of life? Could a suicide attack be the potential modus operandi?
- Does the mains site crate a congestion that could be exploited by attackers?
- Are the security controls spaced so that the crowd density is not resulting in high concentration?

See other examples in Annex D

IV. Destiny: Consequence and probability

V. Design: bridges to the future based on the best of the past and the present - in this part groups work to use assets discovered in the second phase to number the category of measures to be taken. (Plenary session)

How to set up the working groups?

As mentioned before swapping tables during the workshop, is less suitable for this method, participants will be distributed per phase and they will analyse all sites identified in each phase.

For example, according to the table below, to analyse 15 sites requires 5 working groups (one for each phase). There is no switch of working group among the participants; they will always work with the same ones. However, it is necessary to make some breaks at the end of the assessment for each site.

This methodology is interesting when there are specific competencies in the team of experts linked to a particular phase.

Table 6 Illustration of working groups set up-5D

	5D	
Phase	**Number of site per phase**	**Working table**
Phase 1	2	1
Phase 1		
Phase 2	3	2
Phase 2		
Phase 2		
Phase 3	4	3
Phase 3		
Phase 3		
Phase 3		
Phase 4		4
Phase 4	4	
Phase 4		

Phase 4		
Phase 5	2	5
Phase 5		
Participants per table	**15**	**6**

In both working methodologies, right after the working groups phase, moderators and reporters meet to identify the main takeaways of the sessions and present them to all participants in order to continue with step 5 (Analysis and results). The objective is to commonly create an overview of the vulnerabilities for the PSOI. We suggest using the table providing an “Overview of vulnerabilities of each site regarding each terrorist threat” in section 3.2 of the Manual.

At this point, filling all the records and following all the steps the identification of the vulnerabilities is done. The last part of the session consists in undertaking a reflection on the type of actions that can be taken with the emerged information during the assessment. Although the tool does not intend to list the actions that should be taken, since this depends on various dependencies, competencies and hierarchies, suggested measures can be formulated according to the short, medium, and long term.

5.2 Logistical issues

- Send the invitations to the team of experts and the agenda of the two days (an invitation model in the workshop kit available in the PRoTECT project platform).
- Coffee break and lunch organisation
- Name tags for participants
- Participant’s folder
- Information File: File to collect all the information (we suggest you use a word form to fill in during the assessment, see Appendix A of the Manual or put the content of the record template in an excel sheet to have more of an overview), map of the site to be assessed, agenda of the day...

6. During the workshop:

The people who participate in the workshop, the so-called team of experts, must have prior knowledge of the objectives of the workshop, of what is expected of them (active participation) and the expected results (identification of site vulnerabilities to terrorist attacks).

We suggest the development of the session in the following way:

Day 1:
9.00-11.00 PSOI visit: to fix a meeting point to start the visit of the site and the area to assess. Take 10 minutes to explain the objectives of the visit and to set the route. Prior to the visit, the managing body will have an exact map of the site and the identified phases- meaning the PSOI’s main site and surroundings sites linked to the phases of the EU VAT.
11.00-11.30 Coffee break at workshop venue

11.30-12.30 starting of the workshop
Begin by presenting the objectives of the session within the framework of the project, explain the development of the day, explain the content of each participant's folder, the role of each moderator and the workshop methodology. As mentioned in the Manual section 3.1 There should be a moderator (in this case the managing body) and a reporter (someone filling in record templates). We suggest selecting from the team of experts, one person who fulfills the role of reporter in each working group, in the case of World café this person will stay with the moderator.
Present the site that you have visited, why the selection of the site and the previous documentation analysis.
12-30.-13.30 Lunch
13.30-14-30 Discussion on phases identification: this session is intended to have participants finalize and analyze whether the phases previously identified by the managing body are in line with the field visit and understood by everyone.
14.30-17.00 Working groups session part 1 according to the selected methodology. If World Café: first X rounds in function of the sites identified for each phase. If 5D, distribute participants into groups per phase.
Day 2:
9.00-11.00 Working groups session part 2 according to the selected methodology. If World Café: phases left (be aware that the number of phases varies in function of the selected PSOI)
11.00-11.30 Coffee Break. In parallel: moderators meeting to gather main takeaways from each working group session.
11.30-12.30 Plenary session: working groups results sharing
12.30-13.30 Lunch
13.30-15.30 Step 5. Analysis and results
15.30-17.00 Next steps
17.00 Closing remarks and end of the workshop

7. Post: Reporting

For the purposes of the WP 2, no information on the outcome of the assessments[12] is needed. However, it is important to receive feedback from the 5 pilot cities on the use of the VA Manual and VA Tool assessing: 1. operationality, 2. efficacy (if the tool responds to the needs of municipalities), 3. Adaptability to the local security strategy.

1. *Workshop review:*

- Type of site assessed (general category)
- Activities of the site:
- Number of phases identified and assessed:
- Number of participants and affiliation
- Categories of vulnerabilities identified

[12] As mentioned in the manual, section 1.3, the vulnerability assessment may have to be RESTREINT UE/EU RESTRICTED. Municipalities are responsible for the information classification. There are some consequences of this classification level, which are introduced here: https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/ . This includes encryption of data, screening of staff, etc

2. *Vulnerability assessment review:*

1. Operationality

a. Was the Manual helpful to understand and use the VAT?

b. Were the tools provided (Manual, VAT, workshop methodology and logistics kit) sufficient to conduct the vulnerability assessment in the PSOI? Which other element would you consider necessary to successfully conduct a vulnerability assessment?

c. Do you consider that the vulnerability assessment record template provided by the Manual is complete enough to moderate the working sessions? Which kind of improvements could be included?

d. Was the scenario provided helpful to get you familiarized with the manual and the site assessment? What kind of additional tool do you consider could be developed?

2. Efficacy

a. Did the assessment allow you to identify the existing measures, resources, and the vulnerabilities per type of threat of your PSOI?

b. After using the tool, do you feel able to conduct a vulnerability assessment of another PSOI in your city?

c. Did the working sessions with the team of experts help you in identifying potential mitigation measures to be taken?

3. Adaptability & sustainability

a. Will you include this tool as part the municipal risk assessment cycle?

b. What types of measure do you considered that can be taken on the medium and long terms after the analysis of results? (structural, operational, technological)

c. Any suggestions for the improvement of the VAT for the European Commission and future projects?

During the whole implementation process of the vulnerability assessment on the five partner cities, it is important to record all useful information about the different remarks and challenges on the use of the VAT. A feedback document has been created to collect this useful information that will nourish the final report of WP 2 in which recommendations to DG Home will elaborated.
Partners are encouraged to access the following link and include their own suggestions.

VAT feedback document

8. Workshops organisation

Table 7: Planning Local workshops

Timeline	weeks							
	1	2	3	4	5	6	7	8
1.PSOI (Public Space of Interest) identification	X							
2.Constitution of the team of experts	X							

2.1 Managing body members (Manual familiarization meeting)		X						
2.2 Identification of Key stakeholders who will integrate the team of experts		X						
3. Collection and analysis of useful information	X	X	X					
4.Visit to the PSOI and Phases identification			X					
5.Preparation of the local workshop:								
5.1 Methodology selection				X				
5.2 Logistical issues								
• Send the invitations to the team of experts and the agenda of the two days				X				
• Coffee break and lunch organisation					X			
• Name tags						X		
• Participants folders						X		
6. Workshop							X	
7.Reporting								X