This report was funded by the European Union's Internal Security Fund — Police under grant agreement n° 815356

Public Resillience using Technology to Counter Terrorism

D4.4 - Protection of public spaces: Manual for EU

WP number and title	WP4 – Demonstrations
Lead Beneficiary	KEMEA
Contributor(s)	DITSS, TNO, IGPR, Eindhoven, Malaga, DL, VMSA, L3CE, MIR, MUNBV
Deliverable type	Report
Planned delivery date	01/06/2021
Last Update	01/04/2021
Dissemination level	Public

Disclaimer

The content of this report represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

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
V0.1	13/2/2021	Completed	KEMEA	Initial Version of TOC /
V0.2	24/03/2021	Draft	KEMEA	First draft
V0.3	01/04/2021	Draft	Partners	Updated Draft
V1.0	28/5/2021	Draft	KEMEA, EFUS, DITSS	Complete Draft Ready for Internal Review
V2.0	18/6/2021	Pre-Final	KEMEA,	Pre-final Draft
V3.0	22/6/2021	Final	KEMEA	Final Version

Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
COTS	Commercially available off-the-shelf (product)
FTGM	Field Test Guidance Methodology
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
LEAs	Law Enforcement Agencies
PDCA	Plan-Do-Check-Act
PSOI	Public Space of Interest
RF	Radio Frequency
RfI	Request for Information
SLR	Systematic Literature Review
SUS	System Usability Scale
TCA	Total Cost of Acquisition
TCO	Total Cost of ownership
TEF	Technology Evaluation Framework
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle
VA	Vulnerability Assessment
VAT	Vulnerability Assessment Tool

Table of Contents

List of Figures

List of Tables

Executive Summary

PRoTECT (funded by the European Union's ISFP, from November 2018 until June 2021) aims to raise the awareness of municipal authorities on security concepts and adaptation of technology in the protection of public spaces against terrorism and to share best practices and lessons learned to efficiently apply relevant technology concepts. It aims to build a closer, permanent collaboration between municipal authorities and law enforcement agencies via existing networks (ENLETS, EFUS).

Expected outcomes are risk mitigation and cost reduction related to the protection of public spaces for municipalities and Law Enforcement Agencies (LEAs) and the implementation of a pan European technology capability assessment methodology for cities.

To achieve this, PRoTECT methodically builds up towards the identification and selection of appropriate solutions for the protection of public spaces and "soft targets". This is done by adopting a step-by-step analytical approach which involves participants from different fields of expertise. The starting point is a Vulnerability Assessment (VA), followed by the identification of suitable solutions which will enhance the security/safety of EU public spaces, followed by live demonstrations of the identified solutions which are intended to be selected for potential adoption by the stakeholders responsible for the security of public spaces.

In the long term, it is expected that all EU local municipalities will become familiar with the vulnerability self-assessment methodology/tool and with a broad range of good practices and technology concepts and will have the incentive as well as the capability to improve the protection of their public spaces.

PRoTECT directly connects (the outcome of) EU policies to cities in EU member states all over Europe. The five cities that are directly involved with the project and where all activities will take place, are: Eindhoven (Netherlands), Brasov (Romania), Vilnius (Lithuania), Larissa (Greece) and Malaga (Spain). These local partner authorities will directly benefit from the project's actions.

The purpose of this deliverable is to provide a manual for the structured planning, organization, and execution of a process where, vulnerabilities of public spaces are assessed for which technologies and other novel solutions for the protection of public spaces and "soft targets" are identified, evaluated, selected, and tested/demonstrated. The following manual is the result of the methodologies and procedures as implemented throughout the course and under the scope of the research project "PRoTECT" for the protection of EU public spaces and "soft targets". Nevertheless, the general approach and steps presented in this document may be helpful and applicable for organizations/entities or individuals from different fields of expertise, which are interested in an analytical approach for conducting a vulnerability assessment, identifying, evaluating, selecting and adopting technological, operational or other solutions to mitigate risks or to enhance the operational capabilities of their organization in the context of protecting public spaces in the EU.

Target Audience

This deliverable is targeted towards EU municipalities and security stakeholders in general responsible for the protection of public spaces against terrorist attacks as well as the mitigation of the impact of such attacks if realized. In this regard, this document aims to provide a general procedural context, in the form of a concise manual, for facilitating all responsible entities in following a structured step-by-step approach towards securing public spaces, starting with a site selection and the corresponding Vulnerability Assessment (VA), up to the selection and field testing (demonstration) of appropriate security solutions. This process is proposed as a solid methodology for investigating/exploiting appropriate solution(s) towards addressing identified security risks, issues and increasing the sense of security.

1 Introduction

1.1 Protection of Public Spaces

For decades, terrorism has been a reality in many European countries and a continuous threat to a great number of European cities. It poses a significant threat to the safety, the values of democratic states and to 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 spaces against terrorism have strengthened and evolved, with great amounts of effort focusing on protecting critical infrastructures. However, terrorist attacks are evolving as well. By adapting to new contexts and opportunities, lately public spaces have turned into an attractive target for terrorist attacks by perpetrators that seek to maximize their impact, spread fear, and attract political and media attention. To illustrate this fact, terrorist attacks in European cities such as London (Hayden, 2017), Paris (BBC News, 2015), Manchester (Hayden, 2017), Stockholm (BBC News, 2018), Berlin (BBC News, 2016a), Brussels (BBC News, 2016b) and Barcelona (BBC News, 2017) have occurred in public areas. These areas are considered to be **"soft targets"**, meaning that they are crowded public places including metro stations, shopping centres, sports stadiums, bars, restaurants, clubs and commercial sidewalks and that they are easily accessible to the public and form an easy target for terrorists to do great harm. These areas constitute targets, because attacking them can aid terrorist organizations to obtain their goals of threatening the safety of the public, the values of democratic states or the rights and liberties of citizens and they are not hardened (with security measures) 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.*

The security of public spaces should not burden only local police agencies, since it can involve a variety of entities bearing responsibility for the security and safety of the public concentrated in an area. It should be a joint interdisciplinary effort among various security stakeholders, which should also be communicated (to) and supported by the public. 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 (PRoTECT, D2.1).

1.2 Main Stakeholders- Interoperability

In general terms, "stakeholders" include any natural or legal entities that might affect, be affected by, or perceive themselves to be affected by another entity's/organization's activities or decisions (ISO, 2018). Under the scope of security, direct stakeholders may include entities and actors that are responsible for the safety and security of a public space whether this refers to daily operations or to an emergency. The approach as presented in the Vulnerability Assessment Tool (VAT) (European Commission, 2019a) provided by DG

HOME and implemented for the purposes of PRoTECT, underlines two categories of stakeholders involved in the protection of public spaces. These categories include Municipal Services (figure 1), such as civil protection services, municipal police, urban planning and design services etc., and other key local stakeholders (figure 2) such as private security services, event organizers, health services and other.

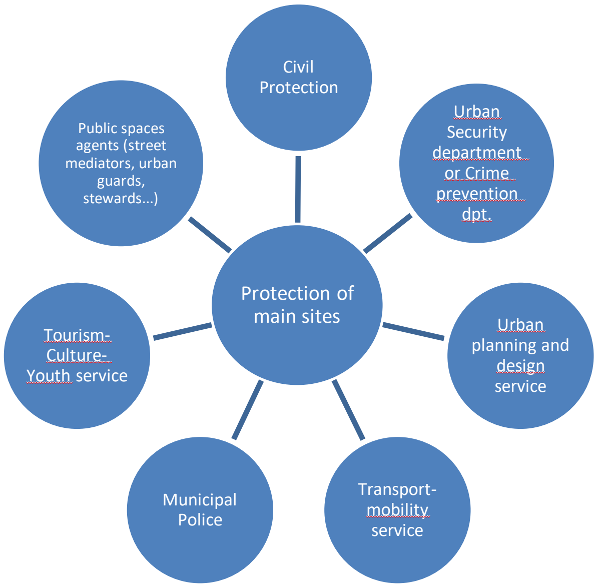

Civil Protection
Public spaces agents (street mediators, urban guards, stewards...)
Urban Security department or Crime prevention dpt.
Protection of main sites
Tourism-Culture-Youth service
Urban planning and design service
Municipal Police
Transport-mobility service

Figure 1 Municipal Services

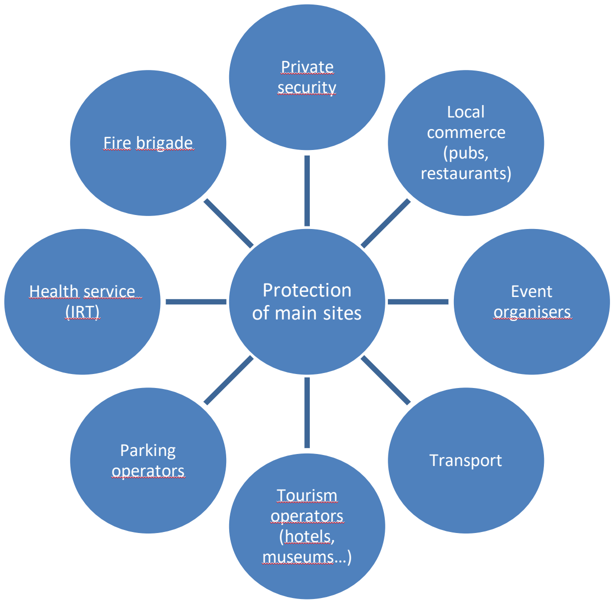


Figure 2 Key local stakeholders

The stakeholders involved in the protection of a public space, may vary per European city's/site's particular characteristics and functions, and their operational framework depends on a country's needs, national institutional structures, and the respective variety of services in place. At the stages of the design and planning of a general framework for the protection of a public space, a municipality or any other entity responsible for the protection of a public space, should identify, contact and bring together the appropriate stakeholders which will be instigated to participate in the aforementioned effort and contribute with their expertise and respective knowledge for a holistic approach towards security and safety aspects.

Since security of a public space is a matter of joint effort and responsibility shared between stakeholders from areas of different expertise, **interoperability** is one of the key aspects in determining the quality of the overall effort to protect a public site, whether this is applied on a strategic or operational level. Prerequisites for the achievement of interoperability between different agencies/parties include the initiation of interaction and discussion between them in the context of exchanging information, knowledge and best practices for the achievement of a shared understanding, common level of awareness concerning the presented issue (protection of a public space or "soft target") and a common approach for addressing the issue. This is one the main goals of PRoTECT which throughout its course and different stages, initiated multi-stakeholder workshops (physical or virtual), bringing together the scientific community, EU municipalities and services, local law enforcement agencies (LEAs), local first responders and other relevant stakeholders. The aforementioned stakeholders were brought together to undertake **Vulnerability Assessments (VAs)** of public sites in their cities against terrorist attacks, discuss solutions to mitigate those vulnerabilities, evaluate and select appropriate (as per relevant operational status) currently available Commercial Off-The-Shelf (COTS) solutions per use case for being demonstrated live in their cities.

1.3 Characteristics of Public Spaces / "Soft Targets" and challenges for the protection

Public spaces are closely linked to the people's leisure and quality of living and may carry economic, commercial, cultural, historic, religious, archaeological value or constitute a point of geographical reference with high concentration of people. These may include closed or open areas such as transport hubs, open squares, parks, shopping areas, nightlife areas, cultural venues, business venues, places of worship, or institutional venues/buildings (see table 1). Technically, some public spaces are semi-public spaces and are privately-owned or privately-operated spaces (e.g., train/ metro stations, shopping malls). Having that in mind, and in agreement with the EU's *"Action Plan to Support the Protection of Public Spaces"* approach, all the aforementioned and the examples included in Table 1 may be generally considered as public spaces due to their importance and the impact they have on the citizen's lives (Partnership on Security in Public Spaces, 2019).

Category	Examples
Transport hubs	Train station, bus hub, underground metro stations, airports, etc.
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 center, 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.

[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.

Business venues	Big hotels with meeting rooms, large offices, conference centers, etcetera.
Places of worship	Churches, mosques, etcetera.
Institutional venues	Public buildings, healthcare buildings, education buildings, etcetera.

Table 1 Categories of Main Sites

As mentioned above, Public Spaces can be categorized as “open” or “closed”, characterized by a high concentration of people, combined with inadequate or complete lack of security measures depending on the case (e.g., closed privately owned vs open public owned areas). This is understandable, given the purpose they serve for the public and their predesigned and prerequired accessibility.

Unlike privately owned buildings/areas with restricted access, the open and uncontrolled access which accompanies the functional nature of public spaces may result to looser security measures in an effort to avoid interference with a site’s aesthetics interference with a site’s intended function (e.g., free access), to avoid legislation and ethical issues, or to avoid causing a sense of fear and insecurity to the public. However, the lack of security measures may render a public site vulnerable to manmade threats such as potential terrorist attacks or regular criminal activity. To counter that effect, the identification of security gaps through systemic analysis may provide the ability to make informed decisions and to adopt proper and tailored security measures in harmony with the security, functional requirements, and the type of a specific public space of interest (PSOI), along with the restrictions and obligations which derive from the current EU and national legislation.

However, to achieve the above results and mitigate risks, a VA (see section 2.3) needs to be carried out initially for each PSOI (or main site), resulting in a full understanding of the examined public space’s operations, current protection status (security measures and policy), potential terrorist threats, security gaps against those threats, and finally identification of measures to mitigate those security gaps and threats.

Considering the above, the terrorist attacks that took place in various public spaces around Europe during the recent years (e.g., in Paris- 2015[2], Berlin- 2016[3],) highlighted the security vulnerabilities of public spaces against such attacks. Terrorist attacks are a means to spread panic and fear, apply political pressure, and attract the media by causing mass casualties. In pursuit of these objectives, terrorists choose to blindly attack public spaces which are vulnerable either by nature or due to lack of protection measures, concentrate large crowds of people, and will allow them to maximize casualties and maximize the overall impact of their attack. Such public spaces are characterized as “soft targets” (Karlos, Larcher, & Solomos, 2018).

It is important to note that critical infrastructures across different sectors of the economy, including public transportation hubs such as metro stations, bus hubs and airports, or public health care and hospitals (European Commission, n.d.) also fall under the spectrum of public spaces/soft targets. Consecutively, an overlap can be observed between aspects in the protection of Public Spaces and Critical Infrastructure, meaning that a common approach, framework, and security practices could be applied, to avoid duplication of work.

[2] The 2015 attacks in Paris, refer to the coordinated terrorist attacks where suicide bombers and gunmen hit a concert hall, a major stadium, restaurants, and bars almost simultaneously, killing over a hundred people and injuring many more (BBC News, 2015).

[3] The 2016 attack in Berlin, refers to the intentional vehicle ramming attack where a lorry was driven into a crowded Christmas market, killing a dozen people and injuring many more (BBC News, 2016a).

1.3.1 Open Public Spaces

Open public spaces include recreational areas such as city squares, parks, beaches, open flea markets, event sites, large parking lots and even roads. They may be operated and managed by a public entity/ body, offering open free access to everyone. They concentrate high numbers of people especially during special events, which often result in crowd congestion, especially during Spring and Summer, due to the favorable weather conditions. As a result of their open nature, national and European regulatory (e.g., GDPR) and ethical aspects, as well as an effort by authorities and officials to avoid generating a feeling of insecurity for the public, they often lack protection measures completely or are partially but inadequately protected, especially from terrorist attacks.

Figure 3 Open Public Space- Public Square

As a response to the need for protection and a workaround to the occasional incapacity of municipalities to adopt some technological security measures (legal, ethical or operational restrictions), the concepts of Security-by-Design and Community Policing (see also 1.3.3) have gathered a lot of attention as viable alternatives or supplementary approaches. Security by Design refers to the installment of structures built and blended harmonically into the area of a public space, often presented as esthetic or functional structures. On the other hand, Community Policing relies on building ties between LEAs and the community, and the community's involvement in enforcing the protection of public spaces, for example by encouragement to actively report observed suspicious behavior or actions, which may pose a threat the public.

Furthermore, the presence of LEAs in vulnerable public space is essential for crime surveillance, prevention, deterrence, and the enhancement of feelings of security for the public in open public spaces. However, a balance in the policing/surveillance of public spaces should be kept, in order to avoid a negative impact on the feeling and perception of insecurity/safety of citizens. If LEAs presence is combined with the capacity for a well-organized, coordinated and quick response (which also includes other first responders) against security incidents, a higher level of protection of public spaces can be achieved.

Past events have demonstrated that open public spaces are especially vulnerable to attacks by vehicle-ramming [Nice - France, 2016 (BBC, 2016c)], and sharp object attacks [Turku – Finland, 2017 (Anderson, 2017)].

1.3.2 Closed Public Spaces

As opposed to open spaces, closed spaces are characterized by a high concentration of people within a specific confined area within defined boundaries. In many cases, as opposed to open public spaces, closed public spaces may have a few common security measures, such as security personnel, a CCTV system and/or alarm systems (especially when operated by private companies). However, similarly to open public spaces, due to their open access, vulnerabilities against terrorist attacks and to manmade threats in general can still be identified. Based on past events, closed public spaces can be vulnerable to bombings, firearm attacks [Bataclan- Paris, 2015 (BBC News, 2015)] and attacks with sharp objects [Hamburg – Germany, 2017 (BBC News, 2017b)].

Figure 4 Closed Public Space- Train Station

Although closed public spaces can have a higher level of protection, impose (partial) access and gateway restriction and in general restriction of movements compared to open public spaces, at the same time, they concentrate high numbers of individuals within a confined area, potentially consisting more attractive targets for terrorists or criminals whose attack can cause high impact with less effort.

1.3.3 Good Practices

Vulnerability Assessment (VA)

A VA constitutes the basis for informed decision making, the focused adoption of security measures and policy, and the design of security and crisis management plans for the protection of public spaces against antisocial behavior, illegal activity, criminal offences, and terrorist attacks. It is part of a wider risk management effort which also involves the processes of risk analysis and risk evaluation within which security vulnerabilities (of a public space), potential manmade threats (terrorist threats but also criminal activity) and their potential impact against a public space, are analyzed. The prioritization of threats and the significance of the identified vulnerabilities, allow the consideration of targeted, tailored, and effective security measures with efficient allocation of resources and cost reduction. The significance of a VA as a basis for security planning in public spaces is also highlighted in official EU documentations (European Commission, 2019a). A VA for the protection of public spaces may be implemented through the organization of multidisciplinary workshops with the participation of a PSOIs operator, LEAs, emergency responders, municipal staff and relevant potential stakeholders (depending on the case), responsible for the protection of public spaces.

The workshops provide a good opportunity for the generation of ideas, information sharing, exchange of good practices and raising the stakeholder's risk awareness. Moreover, the interaction of the different stakeholders will provide a holistic view of the issues and needs for the protection of a PSOI and can contribute towards a common language and common understanding. Additionally, it will pave the way for future communication and set the foundation for future cooperation.

Security-by-Design

Security-by-Design can be characterized as the mitigation of manmade threats (criminal offences, illegal behavior or terrorist attacks) through structural features inherent into a public space or its surrounding environment (often but not always) from its foundation phase. It can therefore be a preventative measure to protect public spaces against terrorist threats at an early stage. It is an effort to "incorporate seamlessly, wherever possible, measures for protection within the aesthetics of the urban landscape" (European Commission, 2019b). Ideally such preventive or protective elements, are part of the initial design of a building and-or area. However, they can be integrated later on as well.

Security-by-Design is a multidisciplinary approach that can involve architects, urban planners, LEAs, engineers, municipality staff, emergency services and other entities. An example is the installation of "disguised" and easy on the eye security measures in harmony with the surrounding environment (e.g., placement of trees as physical barrier), which will protect the public from a potential attack (e.g., vehicle ramming attack) as part of an area's overall design, also preserving the area's aesthetics.

An example of a physical security measure, following the principle of Security-by-Design, could be a line of consecutive concrete blocks installed at the entrance of a pedestrian street, blocking the entry of attacking vehicles that at the same time can be utilized as benches. Indicatively, other measures may include efficiently lit areas, removal of trees and vegetation that could serve as hiding spots or that can complicate the surveillance of an area and consecutive doors which delay the entry/exit of criminals into/from a building and act as deterring measures. Moreover, resilience of structures and facilities can mitigate impact and protect against multiple threats. For instance, robust structures can help avoid the progressive collapse of multiple structures (domino effects) and reduce the impact of flying fragments. Security-by-Design should be considered as a significant part of urban planning (European Commission, 2019a).Security-by-Design is also referred to as Crime Prevention Through Environmental Design (CPTED), pronounced "sep-ted" (International CPTED Association, n.d.), which also includes a component of social and management of public spaces beyond the physical conception of public spaces..

Technical Solutions

Technical solutions include technological or other appropriate and proportionate security measures and tools for the (prior) detection, deterrence, and delay of a criminal act/terrorist attack, as well as measures which could enhance the operations and response capability of LEAs and Emergency Responders. Examples of solutions include, but are not limited to the following:

Unmanned Aircraft Systems (UAS)

- Anti-shutter films (installed on glass surfaces) (against UAV loaded with explosives)
- Laminated glass to avoid shattered glass dispersion against people (buildings' glass surfaces) (against UAV loaded with explosives)
- Double glazing of glass surfaces (against UAV loaded with explosives)
- Safety net (for restricting drone access)
- UAV signal scrambler
- Anti-drone lasers
- Counter drones with nets
- Radio Frequency (RF) jammers
- GNSS (GPS) jamming
- Metal/ mesh curtains (exterior protection of buildings)
- Protection panels (exterior protection of buildings)
- Double facades (exterior protection of buildings)
- Robust (hardened) building structures

Surveillance and Detection

- Enhanced visibility (organization of the area in a manner to allow easy visibility of the entire area e.g. reduction of vegetation which favor hiding spots)
- CCTV system
- Adequate illumination of area (during night) and exterior and interior of buildings
  - Streetlights (surrounding area)
  - Lamp posts
  - Lights with motion sensors
  - Light Panel (building interior)
  - Spotlights
- Security patrols
- Alert systems
- Motion sensor alert systems

IEDs (installation and impact mitigation)

- Restriction of access to areas
- Security checks
- X-ray machines
- Metal detectors
- Anti-shutter films (installed on glass surfaces)
- Laminated glass to avoid shattered glass dispersion against people (buildings' glass surfaces)
- Double glazing of glass surfaces

- Protective walls - protection of zones via separation of areas
- Explosion vents (limitation of stress to physical structures for keeping structural integrity)
- Explosion vent roof hatches/explosion hatch (automatic unlock of hatch in the event of sudden pressure build-up)
- Robust (hardened) building structures
- Metal/ mesh curtains (exterior protection of buildings)
- Protection panels (exterior protection of buildings)
- Double facades (exterior protection of buildings)

Firearms (prevention and mitigation of impact)

- Security checks
- X-ray machines
- Metal Detectors
- Bullet proof glass/windows/doors
- Double glazing of glass surfaces (protection against bullets
- Avoidance of long queues of people within a restricted or open area (mitigation of casualties in the event of shootings)
- Physical barriers for people separation and protection in an area (in the case of shooting)
- Installation of physical obstacles to deny easy access and delay the getaway of an attacker from an area (acts also as a deterrence measure)
- Double facades (exterior protection of buildings)
- Protection panel/facades (exterior protection of buildings)

Vehicle protection (ramming and VBIEDs)

- Traffic/road signs (visual deterrence)
- Speed cushions/bumps (reduction of vehicle speed)
- Traffic control barriers
- Vehicle barriers
- Trees and vegetation (as barriers for vehicles)
- Hardened Street Furniture
- Reinforced bollards/Seat Bollards/Automatic Rising Bollards
- Decorative Fences
- Planters/Seat planters
- Fences and Walls
- Fences with Bollards
- Hardened Streetlights
- Parking lot/spots away from people concentration area
- Utilization of existing topography (altitude, natural barriers etc.)
- Multi-Level protection (division of the entire area into smaller areas protected by surrounding walls and restricting available freedom of movement)
- Window glazing
- Anti-shutter films
- Robust (hardened) building structures
- Chicanes (for reducing speed of vehicles and acceleration ability)
- Utilization or forming of ditches/trenches (for limiting access of vehicles past a specific point

The identification of proper and tailored solutions for a particular public space can be facilitated through a preceding VA and communications between the operator of the public space, technical experts, local law enforcement agencies and solution providers (bringing together the private and public sector) participating in an exchange expertise, information, experiences and good practices.

Community- Oriented Policing

A standard definition for Community Oriented Policing (COP) has not yet been established on an EU or international level (Dehbi, 2019) and different implementations with common elements have been implemented through the years by different countries across the world (Donnelly, 2013). In general, the concept of Community Oriented Policing entails the inclusion of the public and the local communities in law enforcing efforts of the police for ensuring the protection of an area (Donnelly, 2013). The involvement of the local communities and the public require (among others) the initiative by the police to engage the communities of interest, to inform them and to exchange information with them, in order to address their needs and to encourage them to participate for their own benefit, in an effort to build a secure environment to live in. This engagement can lead to the gradual build of trust and collaboration between law enforcement agencies and local communities and help in the reduction of the existing alienation between police forces and societies which characterizes many EU countries.

Consecutively, for the protection public spaces, COP can constitute a proactive approach which can help LEAs in the early detection deterrence of criminal activity rather than traditional focusing most efforts on after incident response.

In practice COP efforts which as a result will contribute to the protection of public spaces, can indicatively include the engagement of the general public and local business, engagement and information of youth groups, meetings and cooperation with other local security stakeholders and emergency responders (private or public).

Common Trainings and Joint Exercises

Common training and Joint Exercises between LEAs and other emergency responders with the involvement of the local municipalities (and other public spaces operators) responsible for the protection of a public space, may reap many benefits leading to improved communication, common understanding and cross-agency collaboration. Common training and Joint Exercises can help “tackle issues related to timely and proper response as well as task division” (European Commission, 2019a, p. 5) and may provide a good opportunity for the security stakeholders to exchange information, knowledge, experience, good practices and raise in the total level of risk awareness between them.

Trainings and exercises can be delivered through workshops, table-top exercises, simulations, demonstrations, seminars, security or response plan testing, or through realistic full-scale multi-agency exercises.

Legislation for Public Spaces Protection

The application of practices, measures, and relevant actions for the protection of public spaces must not overlook common security obligations as well as any notable legislative outline by which they are bound. The principle of proportionality should be considered in the adoption of measures and policies (especially technological solutions), to reach a balance between a secure public space, a functional and pleasant area for the public, and to ensure avoidance of legal compliance issues.

This includes European and national legislation which shape the options of operations and measures adopted by the stakeholders responsible for the protection of a PSOI. In recent years, a lot of attention has been awarded to the protection of personal data and privacy, especially with regard to the application of ICT systems and their technical specifications and operations at a PSOI (security solutions in public spaces attract public scrutiny). Current legislation such as the General Data Protection Regulation (GDPR) (European Parliament, European Council, 2016a) for the protection of natural persons regarding personal data collection and processing, and the Directive on Security of Network and Information Systems (NIS Directive) (European Parliament, Council of the EU, 2016b) or any other legislation applying or overseen the protection of public spaces, may dictate restrictions and obligations but also guidance in the implementation of security practices and application of measures.

A typical example are the restrictions and limits of options in the application of available advanced technological solutions and practices for the protection of public spaces posed by GDPR. Many technological solutions of today as advanced and cutting-edge as they are, cannot be applied due to GDPR compliance issues. For Internet of Things (IoT) manufacturers specifically, these privacy regulations set a strict framework of security requirements on devices that collect and transmit private data, and legal ramifications if hackers access those data. Support for compliance with EU laws is available from the European Union Agency for Network and Information Security (ENISA).

In respect to the above, current European and national legislation should always be taken into consideration in the adoption of security plans, security assessments or the selection of security solutions to ensure a feasible and valid approach.

1.4 Methodological roadmap for investigation of mitigation actions

Figure 5 depicts the steps of a proposed methodological roadmap which can be considered for the effective protection of a public space, starting with the analyses of a specific site, and concluding with the choice of appropriate security solutions based on informed decision making.

The proposed methodology starts with the VA of a designated Public Space of Interest (PSOI). The VA allows the prioritization of threats and identification of vulnerabilities for each PSOI which serve as the basis for the consideration of potential solutions to mitigate the identified security threats and vulnerabilities. Following the VA, the search for solutions is subsequently realized through a Systematic Literature Review (SLR) as an initiating action. The last aims to gather information on good practices and solutions which could be exploited, as well as to potentially narrow down the scope of the search leading to a Request for Information (RfI), and to gain insight on the latest available Commercial Off-The-Shelf (COTS) solutions.

To enhance the effectiveness of the above mentioned RfI (considering any SLR results), in case of absence of specific functional requirements, a Test Scenario shall be designed / incorporated for the respective PSOI, which may include the initiation and progression of hypothetical attacks at the PSOI based on the previously identified threats and its current status. The developed scenarios which shall be included within the RfI document for the guidance of the RfI solution providers, may take into account different categories of threats, and in this context may provide the operational and security context towards which the desired solutions are aimed.

Upon participation of a number of applicable solutions, these are subsequently assessed by the entity responsible for the PSOI’s protection based on a mechanism that is encompassed by the Technology Evaluation Framework (TEF) presented later in the document (developed by the consortium of PRoTECT). TEF incorporates the mechanism of evaluating all the solutions provided via the Request for Information (RfI) and sorting out the most suitable solutions available for the city of interest, based on its current protection status, needs and the desired level of protection which is to be achieved.

The final step of the methodological roadmap consists of the live demonstrations of the higher ranked solutions as evaluated by the PSOI’s operator/manager and stakeholders and are selected (for demonstration/validation purposes) as more suitable for the PSOI. The design, organization and realization of the demonstrations (or field tests in general) can be based on the structured step-by-step approach which is called the Field Test Guidance Methodology (FTGM) and will be presented in chapter 8 “Phase 3” of this document which includes the Design of Pilots, Phase 1- Preparation of Pilots, Phase 2- Supervision, and Phase 4- Evaluation as seen in Figure 5.

The above constitutes a short overview of the entire process that will be presented and analyzed further within the document. It should be taken in consideration that the sequence of steps as described above and that is graphically depicted in the following figure, does not include a step that corresponds to a potential procurement of a solution. However, this could be perceived as a fourth step that would take into consideration all the knowledge generated as part of the proceeding process and advance to all procedural actions regulated by the applicable European and national legislation.

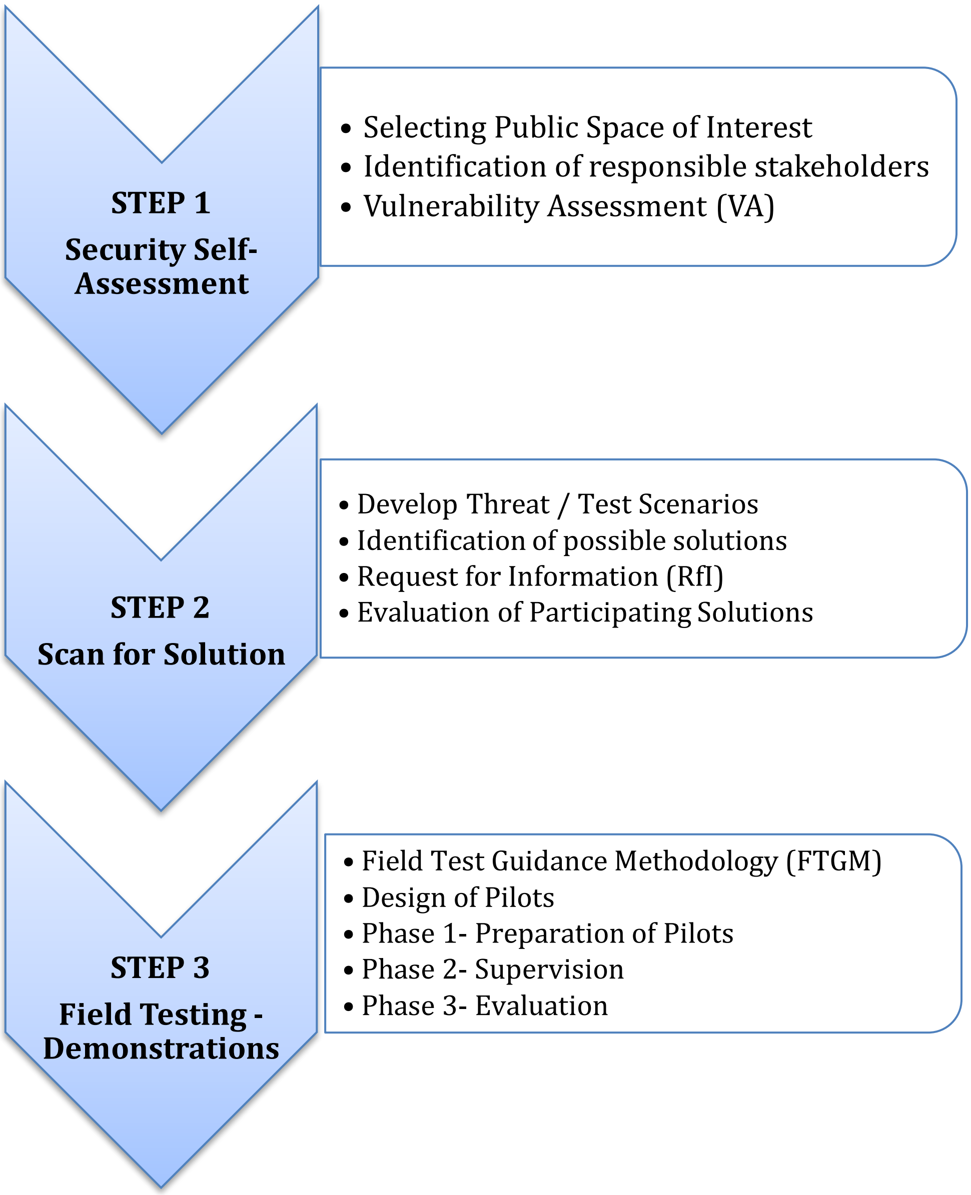

STEP 1
Security Self-Assessment
Selecting Public Space of Interest
Identification of responsible stakeholders
Vulnerability Assessment (VA)
STEP 2
Scan for Solution
Develop Threat / Test Scenarios
Identification of possible solutions
Request for Information (RfI)
Evaluation of Participating Solutions
STEP 3
Field Testing - Demonstrations
Field Test Guidance Methodology (FTGM)
Design of Pilots
Phase 1- Preparation of Pilots
Phase 2- Supervision
Phase 3- Evaluation

Figure 5 PRoTECT methodology for identification of risk mitigation solutions

2 Step 1. Security self-assessment

To achieve the effective protection of a site, it is essential to adopt tailor-made security measures and policies. A general approach for the protection of public spaces may be followed, but at the same time, each PSOI has its own unique characteristics and operations. Accordingly, before designing a security plan and empirically adopting any security measures, it is important that each different PSOI should primarily undergo a security assessment consisting of several steps, which all together result in an analysis of the general function and current protection status of the PSOI, the potential threats against the PSOI, its vulnerability types and levels against those threats, and that it altogether provides the necessary information for informed decision making and effective security measures while avoiding waste of resources. The process of this analysis is presented below, starting with the selection of a PSOI to be examined and concluding with the results of the VA. Responsible for carrying out the VA of a PSOI is the entity responsible for its operation and management. In most cases, this entity is a municipality, and since the VA is not sub-contracted to a private company, or generally an external entity, the VA may be characterized as a self-assessment.

2.1 Selecting Public Space of Interest (PSOI)

The public space of interest (PSOI) may refer to any public space which is generally of open access to the public. Some public spaces, where large crowds form, might be considered by a municipality as areas of higher risk against a terrorist attack than others. These busy areas are in general the result of a particular activity in the area, such as people visiting a concert or commuters at a train station (TNO & EFUS, 2019). As mentioned in section 1.3, the selection of a PSOI may include open or closed spaces, such as roads, parks, squares, libraries, metro stations, municipal buildings and others, with low or high concentration of people, whether this occurs on daily basis or due to a specific event.

The selection of a PSOI which will undergo a security/vulnerability assessment is based on a few specific criteria which are related to its value at a municipal or national level, its features, and its main function. These criteria are presented in more detail below:

- Economic value - Based on the daily or situational generation of financial income for a site's respective city or nation.
- Cultural value - The cultural or historic value which a site may hold for the municipality or a nation.
- Religious value - The religious value of the site at a local and national level.
- Concentration of people - The level of people concentration daily or during a specific event.
- Location of site - Where the site of interest is located within a city and if the site is located nearby critical infrastructures or other sites with a high concentration of people or high levels of traffic.
- Existing Protection measures - How protected is a site based on its existing security measures against man-made threats. It might be preferable to assess and protect a busy site which is currently vulnerable to terrorist attacks, given its total lack of security measures, rather than to assess a busy site which is already protected by fully or partially implemented security measures.

The above mentioned selection criteria contribute towards the overall importance of a site which may guide the choice of a municipality to prioritize it above others and carry out a VA targeted towards its protection against man-made attacks or other malicious acts. At the same time, the criteria above may also contribute towards a site's attractiveness as a target for terrorist attacks and criminal or illegal activity.

2.2 Identification of responsible stakeholders

Following the selection of the PSOI to be assessed, the next step before reaching the stage of the VA, should be the identification of stakeholders which are directly or indirectly responsible for the security of the PSOI or actors which may be involved with the management and response to an emergency incident at the PSOI. Such stakeholders include the body (or bodies), public or private, responsible for the management and/or the operation (daily or per case) of the PSOI, the respective municipality, Law Enforcement Agencies (LEAs), emergency services, private security companies, civil protection, public transportation services and other relevant actors. Besides co-designing the protection of a PSOI and responding to incidents, the various stakeholders are required to actively participate in the VA via workshops where they will have the chance to exchange information based on their operational practices/expertise and contribute to the actual assessment of the PSOI. Given the above, proper identification of stakeholders will be beneficial for the collection and exchange of crucial information during the process of the VA, the risk awareness and risk communication among them, and will affect the quality of the input and output of the assessment.

In the case of PRoTECT, the participants of the VA workshops mainly consisted of Municipality staff (including staff originating from municipal police and civil protection departments), LEAs and emergency services (health services and fire brigade) as well as other local critical infrastructure representatives. An indication of the stakeholders that could per case be proposed, is depicted in figure 5. During the workshops, (as mentioned) they engaged in discussions that revolved around the existing security measures, the operational status and the potentially feasible threats against the PSOI to conclude in a list of specific potential threats against each PSOI with different risk ratings and prioritization for mitigation of each threat.

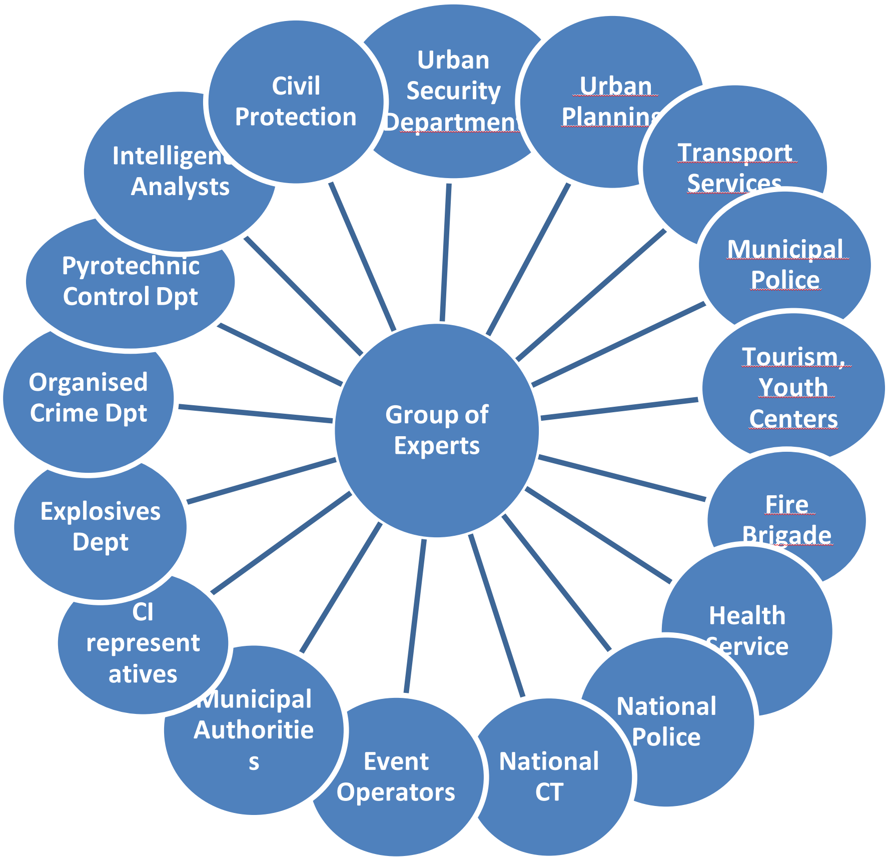


Figure 6 PRoTECT Workshops Stakeholders

2.3 Vulnerability Assessment

A Vulnerability Assessment (VA) constitutes the basis for informed decision making, the focused adoption of security measures and policy, and the design of security and crisis management plans for the protection of public spaces against antisocial behavior, illegal activity, criminal offences, and terrorist attacks. It is applied under the wider scope of risk management to support proactive efforts against security threats.

It can be implemented as part of a risk assessment (ISO, 2018) where the "vulnerabilities a PSOI are established as a result of risk identification and risk analysis" (TNO & EFUS, 2019, p. 17). It is a structured step-by-step process of analysis involving multidisciplinary stakeholders, which enables public spaces' stakeholders to identify potential threats against a public space/soft target and raises awareness regarding the current protection status of a public space against potential security issues. It leads to a targeted effort of protection, more efficient allocation of resources and selection of proper/tailored solutions for threat mitigation.

A VA typically includes (at least) the following content:

- Understanding of the selected site's physical characteristics and operations
- Examination of a site's surrounding environment
- Identification of currently applied security measures and policy
- Identification of potential security threats
- Analysis of potential threats per their probability of occurrence and their impact - in relation to the current security measures and policy (vulnerabilities)

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). An important factor to have in mind is that adopted measures to mitigate a terrorist attack may also serve the mitigation of daily threats such as petty crime and criminal activities independently of the purpose and the risk source.

After having selected a specific PSOI and having identified the relevant security and safety stakeholders, the goal is to collect the details of the site and to gather all the necessary information which will be utilized during the process of the VA. In this regard it shall be taken into consideration that a security assessment or more specifically, a VA is not a "one size fits all" type of assessment. It consists of a tailored examination which takes into consideration a site's distinct characteristics as listed below.

- Type of function and operations
- Stakeholders involved (security and other stakeholders)
- Critical assets to be protected
- Surrounding environment
- Area size
- Concentration of people
- Nearby Critical Infrastructures (CIs)
- Existing security measures (and usually applied measures in case of events)

Type of function and operations

Understanding the type of operation and how a site functions is important to identify relevant stakeholders, critical assets which need to be protected, the site's operations protocol, person peak hours (elevated risk levels) and other important parameters to be considered within the analysis of the site.

Stakeholders involved (safety, security, and other stakeholders)

For the purpose of the VA, all stakeholders which are responsible or are in any way involved in the security /safety of a public space, should be encouraged to participate in the process. Their contribution lies in the information sharing regarding their operations, challenges, needs, past experiences and generally their expertise, and they are expected to engage in the exchange of information and best practices with other stakeholders. Furthermore, the identified stakeholders will be required at some point in time to actively contribute to the security of the selected site based on the results of the VA.

Critical assets to be protected

Critical assets of an infrastructure typically include tangible and intangible assets which are critical to the operation of an infrastructure (including its human resources). In the case of a public space, "critical assets" primarily refer to the people (visitors or staff) located at a site and then technical assets and critical structures that need to be protected.

Surrounding environment

The protection of a space of interest can be greatly affected by the sites and structures located in the surrounding environment. For instance, trees planted in the perimeter of a site may provide a natural guard against vehicle ramming attacks, while at the same time they provide cover for perpetrators/attackers and can make their identification difficult. Tall buildings surrounding a site may provide convenient spots for active shooters.

Additionally, an event taking place at a main site (e.g. public square of interest), may cause congestion at the area surrounding the main site (e.g. access roads, nearby metro station etc.)

Area size

The size of the area affects the surface of surveillance, the amount of people it can accommodate, the amount of security staff needed, a potential perpetrators freedom of movement and other security and protection related factors.

Concentration of people (crowd density)

The larger the concentration of people, the higher the impact of a potential terrorist attack, and the more difficult emergency response effort becomes. The concentration of people is by itself an important indicator of a public space in need of protection.

Nearby Critical Infrastructures

When a site is surrounded by Critical Infrastructures, such as public transportation infrastructure or an energy infrastructure, it requires a high level of protection, since an attack against the site, may have a domino effect onto the critical infrastructures located in its proximity.

Existing Security measures.

It is only logical, upon the initiation of security assessment, to identify the current security measures and policies in place. During the stage of the risk analysis, inadequate (or complete lack of) security measures and policies will reveal the weaknesses (vulnerabilities) of a PSOI against specific threats. The overall vulnerability of a public space against an attack, is proportional to the security measures already in place. The existing security measures may affect the likelihood of some threats occurring and their potential impact. Additionally, the protection of the PSOI may be based on the upgrade, improvement, and update of the existing system.

In consideration of the above, and within the scope of PRoTECT, VA workshops were held in the Municipalities of Larissa, Brasov, Vilnius, Eindhoven, and Malaga (members of the PRoTECT Consortium), where the five cites implemented and tested the EU VAT, developed and provided by DG HOME. The tool was accompanied by a user manual, which was developed for the purpose of PRoTECT under Work Package 2 (WP2), facilitating the provision of context to the end users and the implementation of the VA by the municipalities and the respective LEAs, Emergency Services and other stakeholders. The process resulted in the identification of potential security man-made threats with focus on terrorist attacks, and the identification and analysis of vulnerabilities of each city's selected PSOI, in relation to the threats identified.

The results of the VA were of great importance, as they narrowed down a few feasible threats with higher risk level and provided the opportunity for a focused effort for the identification of the needed type of technologies to be adopted for the mitigation of these threats[4].

[4] The presented points above, reflect only a brief description a VA's structure. To see the complete process of the VA followed by PRoTECT, provided that you are eligible to access the document, please refer to Deliverable 2.1 (D2.1) – Manual for Vulnerability Assessment.

3 Step 2. Scan for solution

3.1 Elaboration of an accurate problem statement / Test Scenario

The identification of solutions (see 3.2 below) is a reaction and a logical next step to the prior establishment and articulation of security gaps (vulnerabilities), which have been identified during the VA and require respective risk mitigation and improvement actions. Choosing appropriate and proportionate solutions to mitigate identified threats and cover security gaps is not a one-fits-all process and should be adjusted to a particular PSOI accordingly. The scanning of appropriate novel solutions can be carried out based on different approaches such as Systematic Literature Review (SLR- see section 3.2), experts' opinion, an RfI, a triangulation of these three, or based on entirely different methods. However, successful research always requires clear requirements, objectives, and criteria. These parameters can be analyzed, clarified and communicated through the formulation of elaborate hypothetical threat scenarios, which will underline the assets that need to be protected (*what*), the stakeholders responsible for their protection (*who*), the location and the characteristics of the area that surrounds the assets and is required to be secured (*where*), and will allow the identification and testing of possible solutions (*how*) for achieving the required level of protection.

In general, the hypothetical threat scenarios will present the realization of specific threats (identified and prioritized threats from the VA) at (an) imaginary location(s), that shares common attributes with the real PSOI that is the subject of the initial security assessment effort. The imaginary location(s) shall resemble (approximately) the geographic, structural, functional, operational characteristics (daily or eventual) of the PSOI and share its security gaps.

It must be taken in consideration that it may be the case that the increase of security level against a given threat/vulnerability may not be mapped to a single known solution. As such the elaboration of specific technical specifications describing a known solution will not be possible. Moreover, local governments may not have the internal capacity for proceeding to accurately specifying a desired (technological) solution before procuring it. As such there is always the danger in being engaged in a complex binding process that could lead to exploiting an expensive solution that does not fit entirely within the purpose of the given problem. In this regard, the use of a detailed scenario may largely help all organizations to describe what they would like to be protected against and leave space to the industry to respond with a wide spectrum of available solutions.

Moreover, the formulation of appropriate scenarios is not only significant for the scanning of solutions in general, but at the same time it greatly supports other processes, such as an RfI (see section 3.3), as it facilitates the communication of risk to solutions providers (responders to the RfI), it provides the necessary overall context in which the solution is required to function, it clarifies the security objectives set by the operator of a PSOI and set the limits within which a solution is acceptable by the operator.

The provision of threat scenarios in a simulated setting such as described above, ensures that sensitive information specific to the security of the PSOI is not revealed and its anonymity is preserves, while the consideration of potential solutions for mitigating the security gaps (vulnerabilities) of the real PSOI is made possible through the application of realistic parameters to the imaginary PSOI described in the scenario.

The realism of the scenarios should be emphasized to the point that it allows the imaginary scenarios to examine and at a later stage test the real PSOI's identified security gaps in correlation with the PSOI's current emergency response mechanism and risk tolerance/acceptance.

In light of the context discussed above, the elaboration of the desired demonstration scenarios is based on the segmentation of the PSOI's background information will be exploited for the derivation/description of a realistic operational scenario. The aim is to achieve a deeper level of analysis as to who does what and when (per scenario), how, where, and what is the current room for improvement given the valid operational context.

The segmentation of the necessary information will allow the formulation (in a structured manner) of a scenario revolving around realistic identified threat(s) that an entity wants to investigate given the identified vulnerabilities. A proposed approach with respect to the mentioned segmentation of information, includes the following six steps:

Step 1: Identification of applicable regulatory framework

The initial step consists the identification of the underlying legislation that governs the operations of the stakeholders in performing tasks in case of an event taking place within the scenario. The legislation framework in force, should also be considered by the security solution providers for any restrictions and compliance risk, along with the total inability of their solution's application at a PSOI. Legislation, along with current security norm should be examined at a local, national and European level.

Step 2: Identification of Pilot site attributes

The second step includes the identification and description of the primary characteristics (attributes) of the demonstration site which will be investigated. The demonstration site described within this step resembles an imaginary site within the city of interest, which shares common characteristics with the real PSOI. Such characteristics include access routes, a similar surrounding environment, expected crowd density, security measures in place and other similarities.

Step 3: Involved stakeholders and pilot actors

This step focuses on the identification and listing in detail of all the different stakeholders that are normally engaged in an event such as the event considered by each scenario individually, along with their distinct responsibilities. This includes any potential operational particularities applicable for the operators (e.g. the municipality) of the public space described. Consequently, a tailored set of stakeholders will be formed for any scenario designed and adjusted to the needs of the respective demonstration. Additionally, a realistic operational environment will be formed to provide a proof of concept against enhancing effectiveness and increasing the offered level of security. This will facilitate the efforts of the solution demonstrators by offering a complete sense of the context and the environment that the solution will be demonstrated in.

Step 4: Considered vulnerabilities and threats

This step includes the description of the vulnerabilities that each corresponding scenario will try to exploit. The vulnerabilities which are previously identified during the VA and chosen by the PSOI operator to be prioritized, will be the focal point of the demonstration solutions which will aim to mitigate it.

Step 5: Scenario unfolding

During this step, the onset of an attack is being described in detail. This description, on the basis of confidentiality of the actual information, will have to consider a hypothetical site of the city resembling the desired characteristics of the real PSOI. In this context - specific attention should be paid to devising a demo case scenario that will exploit the full set of important threats/vulnerabilities as identified by each participating PSOI operator falling within scope of investigation.

Provided the above, the said description referring to a specific incident at the hypothetical PSOI must incorporate at least the following dimensions:

- **Risk Source:** strategic pre-positioning (influence), sabotage – destruction, ideological – agitation – propaganda (hacktivists, cyber-terrorists), spying – intelligence, fraud lucrative (mafias, gangs), malice vengeance (angry employees, disloyal competitors), non-human
- **Attacker (Opponent) Objective:** psychological impact on population and discredit public authorities (terrorist), get a competitive advantage (competitor), rally many people to his cause (hacktivist)

- **Consequences (Impact/Severity):** Negligible (overcome the impacts without difficulty), Limited (overcome the impacts despite some difficulties), Important: (overcome the impacts with serious difficulties), Critical (the organization will not overcome the impacts, its survival is threatened)
- **Asset:** Vital for the municipality activity (if applicable)

Step 6: Deployment of innovative technological solutions

Having established the prerequisite knowledge base, decomposed in the aforementioned steps, step 6 is mainly concerned with the listing of foreseeable solution(s) and how these could be used for preventing and /or strengthening the response capacity of the PSOI operators (municipalities in the case of PRoTECT) in a corresponding incident. This section will provide the potential participant with a non-exhaustive indication of the underlying operational context that is envisaged using such a solution(s). In a wider sense, this step provides an approach that adoption of such a solution could be incorporated into the existing practices of the stakeholders.

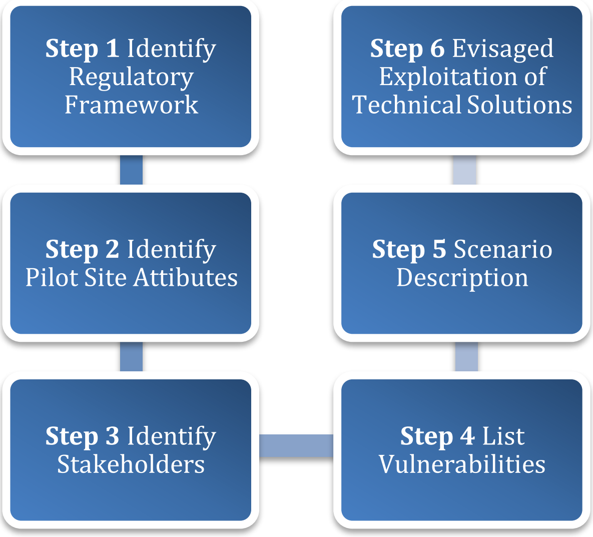

Step 1 Identify Regulatory Framework
Step 2 Identify Pilot Site Attibutes
Step 3 Identify Stakeholders
Step 4 List Vulnerabilities
Step 5 Scenario Description
Step 6 Evisaged Exploitation of Technical Solutions

Figure 7 Scenarios Derivation Methodology

3.2 Identification of technological/thematical context of possible solutions

Harnessing technological solutions can result into great benefits for the protection of public spaces. Some of those include quick provision of information for early threat detection, the availability of necessary information for better informed and timely decision making (European Commission, 2020), risk communication and situational awareness.

The starting point for initiating a process of identification of appropriate novel technological solutions to mitigate security threats at a PSOI, is the output and the findings of a previously implemented VA. The information derived from the assessment will provide a holistic view on the security/safety vulnerabilities of a PSOI and the current needs for improving its protection, thus enabling the design of parameters on which the research of solutions will be based. Moreover, the experts who participate in the workshops of a VA, via the exchange of information, best practices, and brainstorming, might be able to identify and suggest novel solutions they are familiar with, and that will be suitable to the respective PSOI which is analyzed.

In addition, an SLR using open or restricted sources can unveil a variety of useful solutions which may be applicable for the protection of a specific PSOI. Moreover, an SLR can provide a general idea with the types of solutions currently available, for further targeted research. Another method for obtaining further information on novel solutions, which can be benefited from prior literature review, is an RfI. An RfI is a non-legally binding document, through which an interest party can require and obtain information about products or services and their specifications by a provider.

As it was applied in the case of PRoTECT, an SLR aims to identify types of solutions which could possibly be relevant to the security vulnerabilities identified at the PSOI of each city through the VA. The subsequent step following the SLR may consist of the design of a market scanning process that could reveal additional detail/opportunities to address the highlighted problem (security gap). As such, an RfI process seems to be a very efficient approach for a public entity (public space operator) to investigate existing solutions. The process constitutes a structured approach to gathering targeted information about security solutions directly from various providers, without the need to procure for basing any later strategic decisions (including procurement). In this context, the benefit of the previously applied literature review (based on the actual VA) is the potential to increase the possibility that the solutions presented by the providers through the RfI (see section 3.3 below) would have a high chance of relevance to the actual needs for a PSOIs protection (as also approached by PRoTECT). In this regard, the RfI as designed for PRoTECT, was active for a specific period of time and addressed to any technological solution provider, given the provider has Commercial Off-The-Shelf (COTS) products available, which served the purpose (mitigation of identified vulnerabilities) of the PSOIs' protection described within the RfI.

Based on the general description of the identified solutions within the RfI, the technological providers presented (via an online platform custom-designed for PRoTECT) a plethora of solutions which covered the categories of planning and management, intelligence gathering, access control, threat deterrence, threat detection, threat response, attack detection and attack response within the scope of security/safety, were presented.

Following the completion of the RfI and the creation of a registry with the provided solutions, the solutions were evaluated during workshops kept in each city to decide which of those would be chosen by the end-users for live demonstrations. The solutions were evaluated by the PSOI stakeholders per their perceived suitability and added value regarding each PSOI's improvement of protection. To serve that exact purpose and as prerequisite deriving from PRoTECT's expected actions, a Technological Evaluation Framework (TEF) for technological solutions was developed under Work Package 3 (WP3). The TEF contributed to the identification of suitable solutions with output towards the RfI and was used during workshops at each participating city, where the municipalities and their respective stakeholders evaluated the identified solutions, based on specifically designed threat scenarios with imaginary locations that simulated their real PSOIs.

The processes of the RfI and the TEF will be described in the following sections in more detail. It should be taken in consideration that both the RFI and TEF aspects as described, are fully customizable as per the individualities/particularities of each case and can/should be adjusted accordingly for facilitating all different cases in the best possible manner.

3.3 Request for Information (RfI)

3.3.1 General

An RfI is a business process used by customers (or interested parties in general) to gather information about providers' various products and services. It allows a customer to make informed decisions before a product/service is purchased and to gain insight to the various products and services currently available on the market.

An RfI document typically contains information such as the requirements, needs of the customer, the scope and purpose of the required solution(s), and provides the context within which a solution will be applied, to be considered by the providers. It does not constitute a procurement in the sense that it is a non-legally binding document, it is not accompanied by a contract, and it is conducted just for the purpose of information gathering.

The result of an RfI is a register of possible solutions (products or services), including the description of their purpose, functions, technical details and cost of purchase and maintenance. When, an adequate number of providers have showed interest and replied to the RfI, the customer can rank the available solutions, evaluate them and select whether or not to proceed with the purchase a solution by directly contacting the provider.

Given the inherent flexibility that this approach presents, provided also that procurement was out of scope, it has been selected for exploitation within PRoTECT project for reasons of (among others) scanning a broad spectrum of market available solutions that were not specifically known to responsible security stakeholders of considered sites. The following section provides the details of this approach.

3.3.2 PRoTECT RfI

The RfI for PRoTECT, consisted of a document designed by the project's consortium, specifically targeted towards gathering information on available novel solutions oriented in protecting public spaces (or "soft targets") from terrorist attacks and managing the effects if such attacks were to occur. In this context, the RfI document aims at addressing the industry/research community towards expressing their interest in participating in a process (of selection) as candidates to provide a demonstration of their solution to PRoTECT's beneficiary municipalities. Considering the aforementioned, the document was published via an online open call to providers aimed towards the identification of technological and procedural solutions for the protection of the public spaces of the five partner municipalities in relation to their respective vulnerabilities.

The primary objectives of the municipalities benefiting by the RfI's results were:

- To safeguard the security of the public.
- To adopt cost – effective measures and improve the LEAs' and Emergency Services' response capability against attacks.
- To mitigate specific identified vulnerabilities and select the best suited solutions for demonstration, or to conduct a proof-of-concept trial, or to ascertain the overall existence of solutions to an identified vulnerability.

As per its content, the document focused on the following:

- To provide the context and details of the process that the interested parties should comply with, to be eligible for participation.
- To provide a clear picture of the operational context where the providers' solution(s) could be applicable and suited and could enhance the end users' operational capacity.
- Describing the mechanism that will later be used by the responsible stakeholders (end-users) for the evaluation of the participating solutions as per the envisaged relevance for accommodating specific operational instances and end-user's designated objectives.

To assist the potential providers with understanding the concept of protection and suggest suitable solutions, the RfI included a hypothetical attack scenario for each of the five cities (participating in PRoTECT), taking place at a hypothetical public space, similar to the ones previously assessed in each city (during the VA), which included the appearance of various threats and examples of several security vulnerabilities. The purpose of this was to guide the providers to suggest suitable solutions and eliminate irrelevant suggestions. The providers were asked in the RfI to match the relevance of their solution to one of the five scenarios included in the RfI and indicate what kind of threat type (from a provided list of relevant threats) their solution addresses. Moreover, the providers where requested to match their solutions with a capability which they are meant to accommodate e.g. planning and management, threat detection, intelligence gathering, methodology, etc. Lastly, the providers where required to describe their solution's technology category use from a predetermined set of technology categories and security operational uses, and to provide information on their solution's technical specifications.

Aside from the focus on the technical aspects of the solutions, the evaluation process following the completion of the submission of application was also described, which involved an evaluation workshop in each of the five PRoTECT cities under the responsibility of the municipalities, with the participation of relevant stakeholders.

The RfI was addressed towards various enterprises, research centers, universities, and organizations to gain insight into the overall functionality, implementation costs and capabilities of security solutions.

After the RfI's deadline was met, a workshop was held in each PRoTECT participating municipality where the RfI deriving solutions were evaluated per city case, with the active participation of each municipality and relevant stakeholders, based on a Technology Evaluation Framework, designed by the project's consortium specifically for that purpose. Following the overall evaluation of the solutions (see also section 3.4), the preferred (by the end-users) solutions that were validated and designated by the municipalities during a consortium online workshop (due to COVID- 19) - were invited to provide (by the end of the project) a demonstration (proof of concept) at specific city sites that constitute potential "soft targets" and were selected by PRoTECT's participating municipalities.

The demonstrations will be based on the threat scenarios designed and previously utilized at the solutions evaluation workshops, which will be adjusted to match the needs of the demonstrations (see also section 4). The demonstrations will provide an opportunity for the end-users to assess the cost- effectiveness of the offered solutions.

Disclaimer: The selection of solutions to be demonstrated in no case implied or led to the purchase of a solution as part of PRoTECT's procedures.

3.4 Evaluation of Participating Solutions

3.4.1 General

The evaluation process serves the assessment of solutions which will facilitate the mitigation of specific security/safety vulnerabilities (in the case of PRoTECT) or accommodate a specific need for improvement. The evaluation of a solution is based on a specific set of criteria regarding the technical characteristics and its suitability to mitigate vulnerabilities that may have been identified as part of the VA.

Achieving a holistic and efficient evaluation of security/safety solutions is based on many different variables. As a first step, the objectives of the evaluation procedure should be established. The end users may aim towards various goals when scouting for a solution. In the case of PRoTECT, this is the security and safety of public spaces and the end users are (among others) European municipalities and security stakeholders. It is very important to clarify and be specific about these goals, e.g. the mitigation of a specific vulnerability.

After the general context has been outlined, the evaluation shall be based on a specific set of parameters. These parameters reflect the variety of the currently available solutions on the market and their capabilities, but also on the technical minimum and maximum specifications. Consequently, these leads to the determination of a set of functional and technical requirements which accommodate the needs of the end users, and requirements involving the solution provider and its capability to deliver. Lastly, specific criteria should be set, which will determine, according to the individual process objectives, the quality of a solution in comparison to the other solutions available on the market, and its suitability per use case.

For facilitating the effort of all responsible stakeholders during an evaluation process in reaching an objective outcome, some generic criteria are proposed, which are easily comprehensible by all evaluators from different operational fields/backgrounds and will allow them to evaluate the solutions (TNO, 2019, p. 26). Such criteria could include:

- Cost of solution
    - Total Cost of Acquisition (TCA)
    - Total Cost of Ownership (TOC)

- Benefits
    - Physical characteristics (e.g. volume, weight, length, height, robustness/tolerance to physical damage and visual prominence)
    - Compliance with existing legislation (Privacy, Security, Safety, Ethics)
    - Performance [reliability, accuracy, timelines (e.g. processing times), capacity (e.g. processing throughput)
    - Environmental (e.g. protection against rain, dust, water etc., emissions)
    - Operability (e.g. usability, staff needed, deployment time)
    - Interoperability with other systems (e.g. information, interfacing)
    - Maintainability [e.g. availability (time to repair), support (availability of service)]
    - Training (e.g. education for use required, experience)
    - Maturity [e.g. Technology Readiness Level (TRL), availability (development, time to produce), roadmap (expected short-term improvements)]
    - Other miscellaneous advantages and disadvantages

3.4.2 PRoTECT Technology Evaluation Framework (TEF)

A **Technology Evaluation Framework** (TEF) has been developed to evaluate potential technological and social security solutions for the purpose of demonstration and potentially for future improvement of public space security in the five cities of PRoTECT consortium. The TEF was developed on the basis of previous EU H2020 projects, information gathered from the five municipalities, results from using the EU VAT in PRoTECT, feedback from the municipalities and other consortium partners, and expertise from TNO and KEMEA (TNO, 2019, p. 11).

TEF was development to be applied by the participating municipalities in PRoTECT and the relevant stakeholders including LEAs (municipal police, crime prevention agencies etc.), Emergency Response Services (Health Services, Fire Brigade, Civil Protection), Urban planners, Tourism and Transport Operators and others, who are directly or indirectly responsible for the protection of public spaces and "soft targets". TEF is meant to enable the users to obtain information on potentially appropriate solutions and evaluate them based on their ability to address a users' PSOI's security/safety (specific) vulnerabilities, thus improving the physical protection of the public space.

As it can be observed in figure 8 TEF is interconnected with the other processes described in sections 2.3, 3.2 & 3.3, and they all together contribute towards shaping the selection of solutions for proceeding to further actions (if any - including the provision of a proof of concept). TEF relies on the vulnerabilities identified via the EU VAT, receives input from Systematic Literature Review (SLR), exchanges information with the RfI and finally, its output after the evaluation and rating of potential solutions, allows the selection of the most suitable ones for field demonstrations/testing.

Setting criteria and requirements, can be enriched from a prior SLR through which, current novel solutions and their capabilities can be identified. This will assist the design of an evaluation framework and technicalities about the solutions which need to be considered or included in the framework. Additionally, an evaluation framework may receive information from an RfI as input which will assist in the framework's improvement and completion. However, the evaluation framework can also provide output towards designing an RfI by provided parameters and criteria which need to be included or described for the solution providers in the RfI. The interconnection between the different processes can be seen in figure 8 below.

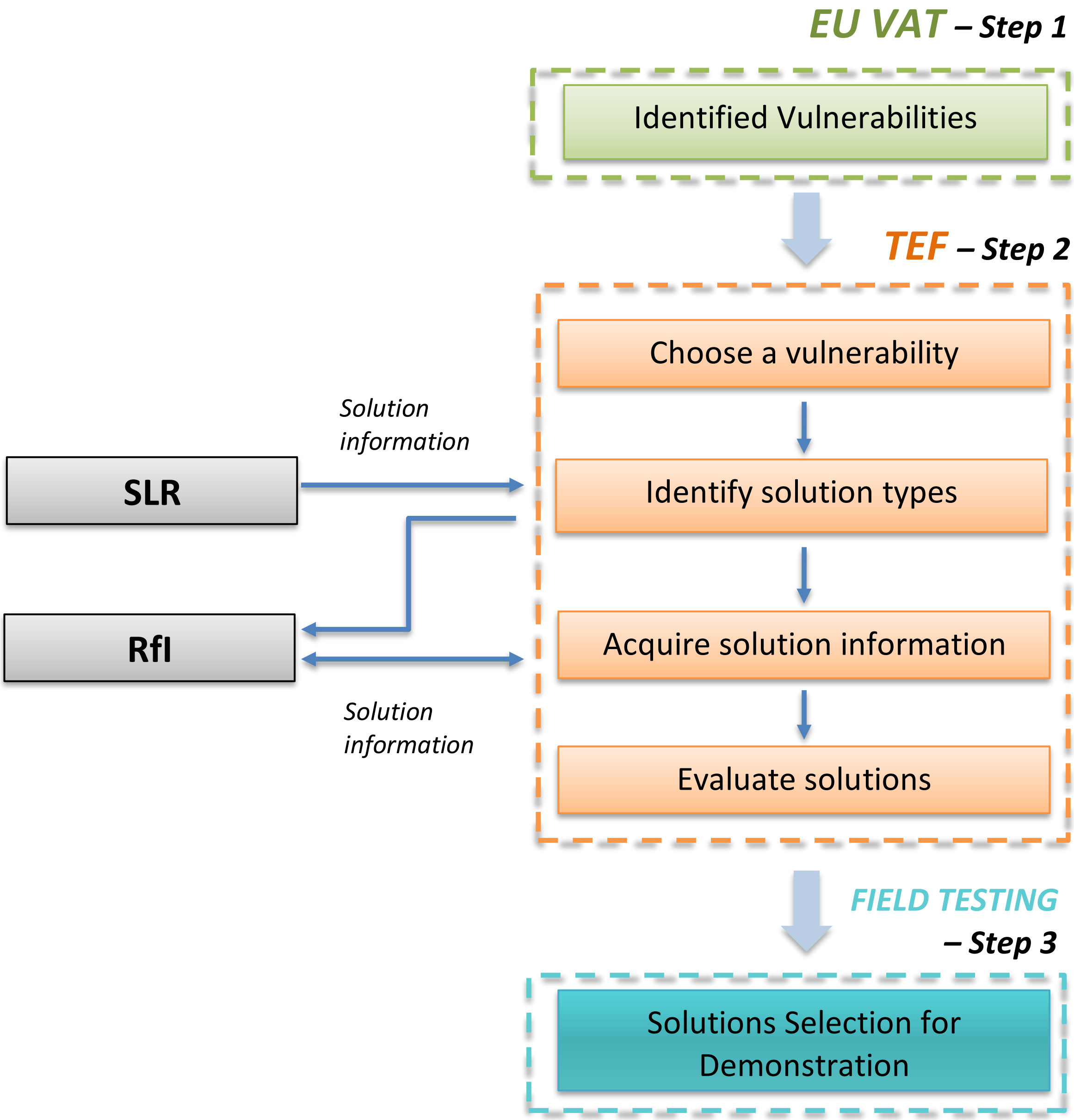


Figure 8 TEF inputs-outputs – in line with methodology for identification of risk mitigation solutions

For the case of protect, the evaluation framework presented above was provided to each municipality of the five PRoTECT cities with the intention to form evaluation committees and evaluate the security/safety solution which derived from the RfI, based on specific threat scenarios designed for each city. This was done via the realization of five respective workshops, one in each city, where the solutions deriving from the RfI were evaluated, giving way to the final selection of solutions for live demonstrations.

Generally, in the case of emergency or general inability to hold physical meetings, such as the times during the COVID 19 pandemic, evaluation workshops may be held virtually via online video conference platforms.

3.5 Public Procurement

Besides the processes of the RfI and the technology evaluation (indicated above), in the case of a public authority willing to procure a suited solution (product or service) for a specific purpose, a procurement process may be necessary to be carried out, which will be open to competition among relevant economic operators. In this context "Public procurement" refers to the process by which public authorities, such as government departments or local authorities, purchase work, goods or services from the industry[5].

Similarly, to the RFI, a procurement procedure may entail market analysis for gaining prior knowledge and understanding of the potential solutions available to satisfy specifically designated needs (European Commission, 2018). However, the procurement process is not restricted only to market and solution scanning, but it involves the publication, submission and evaluation of tenders for awarding/signing of a contract between the winning economic operators/I.e. suppliers of solutions and the public (contracting) authority (buyer) for the purchase of the actual solution.

The preparation, planning and execution of the whole process of procurement, demands the involvement of stakeholder sand/or experts (internal or external) and the forming of technical committees for evaluating tenders and ensuring quality of procured goods and services. The involved stakeholders' expertise highly depends on the nature of the procurement objectives. As such the process may require individuals specialized in the subject matter (e.g. protecting public spaces) and could require civil engineers, architects, IT specialists, lawyers, economists, and others who are familiar with process and have participated in such a process in the past (European Commission, 2018). Similarly, the choice of solution(s) to be purchased will be based on various and more specific than the RFI set of technical criteria, to ensure the operational suitability and financial justification of the solution purchase.

The procurement, according to the goods and/or services being procured, as well as the level of the relevant budget, may rely on a set of different approaches. The main types of types of EU public procurement procedures may be summarized in the following manner along with their main characteristic/requirements.

Procedures Types	Procedures Specific requirements for using the procedure
Open	In an open procedure all economic operators interested in the contract can submit tenders. All tenders must be considered without any prior selection process. The selection and evaluation is carried out after the tenders have been submitted.
Restricted	The restricted procedure is a two-stage process where only pre-selected tenderers may submit tenders.

[5] https://ec.europa.eu/growth/single-market/public-procurement_en

Procedures Types	Procedures Specific requirements for using the procedure
Competitive procedure with negotiation	The competitive procedure with negotiation, like the competitive dialogue, is a process that can be used in exceptional circumstances. It involves shortlisting at least three candidates who are invited to submit an initial tender and then negotiate, on the basis of the initial tenders, while the evaluation will con-sider the final version of the tenders on the basis of the most economically advantageous tender criteria.
Competitive dialogue	This procedure can be used by a contracting authority with the aim of proposing a method of addressing a need defined by the contracting authority. At least three economic operators are shortlist-ed based on their capacity to perform the contract (as with the competitive procedure with negotiation). During the competitive dialogue phase, all aspects of the project can be discussed with the economic operators. Once the contracting authority is confident that it will receive satisfactory proposals, it invites the economic operators to submit their tenders which will be evaluated on the basis of the most economically advantageous tender criteria.
Negotiated procedure without prior publication	When using the negotiated procedure without prior publication, contracting authorities negotiate, with-out advertising, the terms of the contract directly with one or more economic operators. The negotiated procedure without prior publication can be used only in exceptional circumstances which must be duly justified.
Innovation partnership	This procedure may be used when there is a need to purchase a good or service that is still unavailable on the market. A number of companies may participate throughout the process. An innovation partnership is implemented through a three-stage procurement process (prequalification, negotiation, delivery). The contracting authority buys both R&D services to develop an innovative solution and the resulting innovative products, services or works.
Design contest	This procedure is used to obtain an idea for a design. A design contest is a competitive procedure which enables contracting authorities to purchase a plan or a design mainly in the fields of spatial planning, architecture, civil engineering or data processing.
Pre-commercial procurement	The existing open procurement procedure to procure R&D services is been used, in a way that uses competitive development in phases, and shares intellectual property rights and related risks and benefits between the contracting authority and participating tenderers.

Table 2 Types of EU public procurement procedures

In choosing which procedure to use, contracting authorities need to weigh a range of factors, including: ā the specific requirements and purpose of each procedure; the benefits of full open competition; the advantages of restricting competition; the administrative burden entailed by each procedure; the likely risk of complaints and remedies often linked to corruption and collusion risks; and ā the incentive for innovative or tailored solutions to a specific need.[6] The most often encountered process, refers to the Open Process. This may be graphically summarised in the following manner:

[6] European Commission “PUBLIC PROCUREMENT GUIDANCE FOR PRACTITIONERS”, February 20218

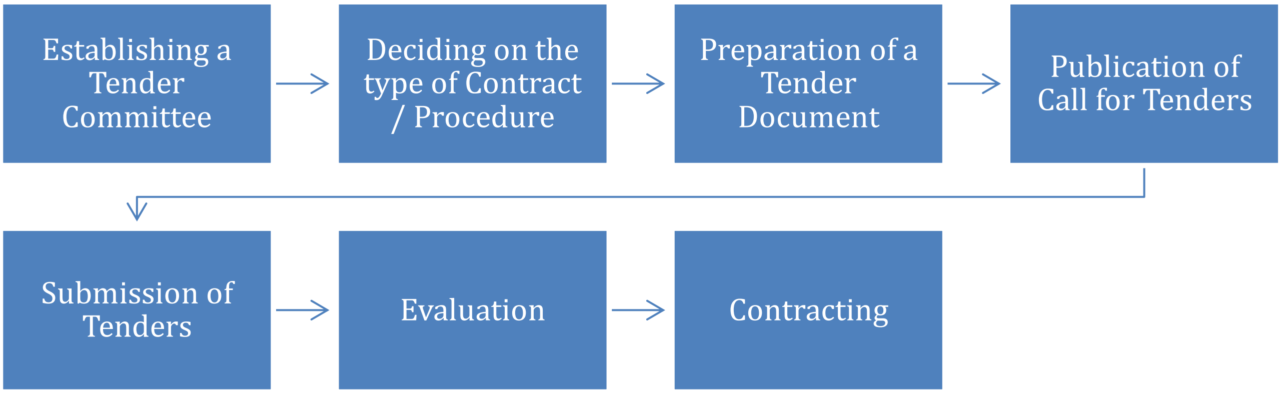

Establishing a Tender Committee
Deciding on the type of Contract / Procedure
Preparation of a Tender Document
Publication of Call for Tenders
Submission of Tenders
Evaluation
Contracting

Figure 9 Tendering Process Outline (Open Procedure)

Provided the above, it has to be taken in consideration that the above processes are highly dependent on the applicable national legislation that presents considerable procedural diversity across the EU member states and has to be taken into account when designing the relevant process. Provided the above, there is an overarching EU framework that sets the outline for all EU member states about public procurement process that is can be primarily found in the EU Directive 2014/24[7].

[7] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0024

4 Step 3. Field Testing – Demonstrations

4.1 Field Test- Demonstrations

The final evaluation, understanding and observation of the selected solutions which are called to contribute to the improvement of the protection of public spaces can be realized through field testing/ live demonstrations. Live demonstrations allow the end-users to experience the proposed solution functioning in a real-world environment, to interact up-close with the solution (in case of a product) and its provider and to grasp a better understanding of the theoretical functions of a product, or procedures of a service, through practical application. During this interaction, the end-users are provided with the chance to communicate with providers, pose direct questions to them and increase get a better understanding of a solution's technicalities and operational context (Alqahtani, Al- Jewair, Albarakati, & ALkodife, 2015).

Live demonstrations of products or services can be experienced in a simulated environment and be presented as they would be implemented in real conditions. Live demonstrations are used in various fields of expertise for training purpose, one of them being dental procedure training. (Alqahtani, Al- Jewair, Albarakati, & ALkodife, 2015).

Considering the above, live demonstrations have the ability to captivate and engage the end-user, enhance the communication between the participants, and facilitate discussion for knowledge exchange and better understanding of a concept. On the other hand, live demonstrations and field testing as opposed to online presentations are costly, require on site resources, availability of facilities, and require proportionate number of staff to support the procedures and to accommodate the demonstration participants.

Alternatively, products and services can be demonstrated and explained virtual, via "training videos" or online/ digital presentations. These methods can be less costly, since they require mobilization of less people, and can be restricted to teaching sessions with standard premade material. They also give more freedom to the solution provider, who can adjust the material beforehand and will not be forced to carry equipment or have concerns about functionality and performance uncertainties, necessary participants, necessary infrastructure, and facilities for a live demonstration.

Under task 4.3 (Demonstrations) of PRoTECT and following previous actions such as the RfI and the evaluation and selection of solutions by PRoTECT's municipalities, various solutions were invited to perform a demonstration in the form of a live (onsite) application in the PSOIs.

Unfortunately, the implementation of demonstrations can be susceptible to various risks, many of which can be mitigated through proactive and effective management, and foreseen mitigation measures. Examples of such risks can include unavailability of chosen demonstration site, lack of necessary infrastructure, unfavorable sudden weather conditions (in open spaces) sudden unavailability of personnel, failure of equipment and other. COVID 19 pandemic was an unexpected long-lasting occurrence, which forced many European research project to adjust the timeline of their events, due to restrictions in movement and transportation around Europe. In the case of PRoTECT, an initially proposed alternative as mitigation action to potential hindrances such as COVID 19, which would allow the actualization of live demonstrations, was the organization of a technology show for providing a proof of concept against the test case and scenarios derived from the actions described in the previous sections of the document.

In light of the above, the solutions are aimed to be demonstrated in the context of providing the widest spectrum of available input in what technology and operational frameworks have to offer in mitigating potential threats in public spaces. The results of the solutions which will be demonstrated and the related technologies that will be tested in the five pilot cities of the project will be thoroughly presented in a detailed report along with relative conclusions drawn by the cities' stakeholders, as part of the overall Field Test Guidance Methodology presented below.

4.2 PRoTECT Field Test Guidance Methodology

The framework on which the design, preparation, supervision, and evaluation of the demos were based, relies on the custom project management Field Test Guidance Methodology (FTGM). FTGM's approach adopts many elements from the Trial Guidance Methodology (TGM), designed by the EU DRIVER+ project for assessing solutions related to crisis management (DRIVER+, 2020). It was tailored to accommodate the needs of PRoTECT in respect to field testing/demonstrations under the scope of the project. It is a step-by-step cyclic structured process for assisting the coordinator of demonstration or other similar project to break down the design, preparation, supervision and evaluation stages of a demo, keep track of each specific necessary subprocess and tasks and identify any limitation or potential issues that need to be resolved. The FTGM wheel made for PRoTECT is presented in Figure 10 PRoTECT - Field Test Guidance Methodology (FTGM).

For the purpose of facilitating PRoTECT's demonstrations organizers, a dedicated document (Demonstration Plan) has been prepared for providing a concise "pocket guide" proposing a set of necessary actions towards planning, delivering and evaluating demonstrations in an efficient/timely manner (as per applicable circumstances) (KEMEA, 2020).

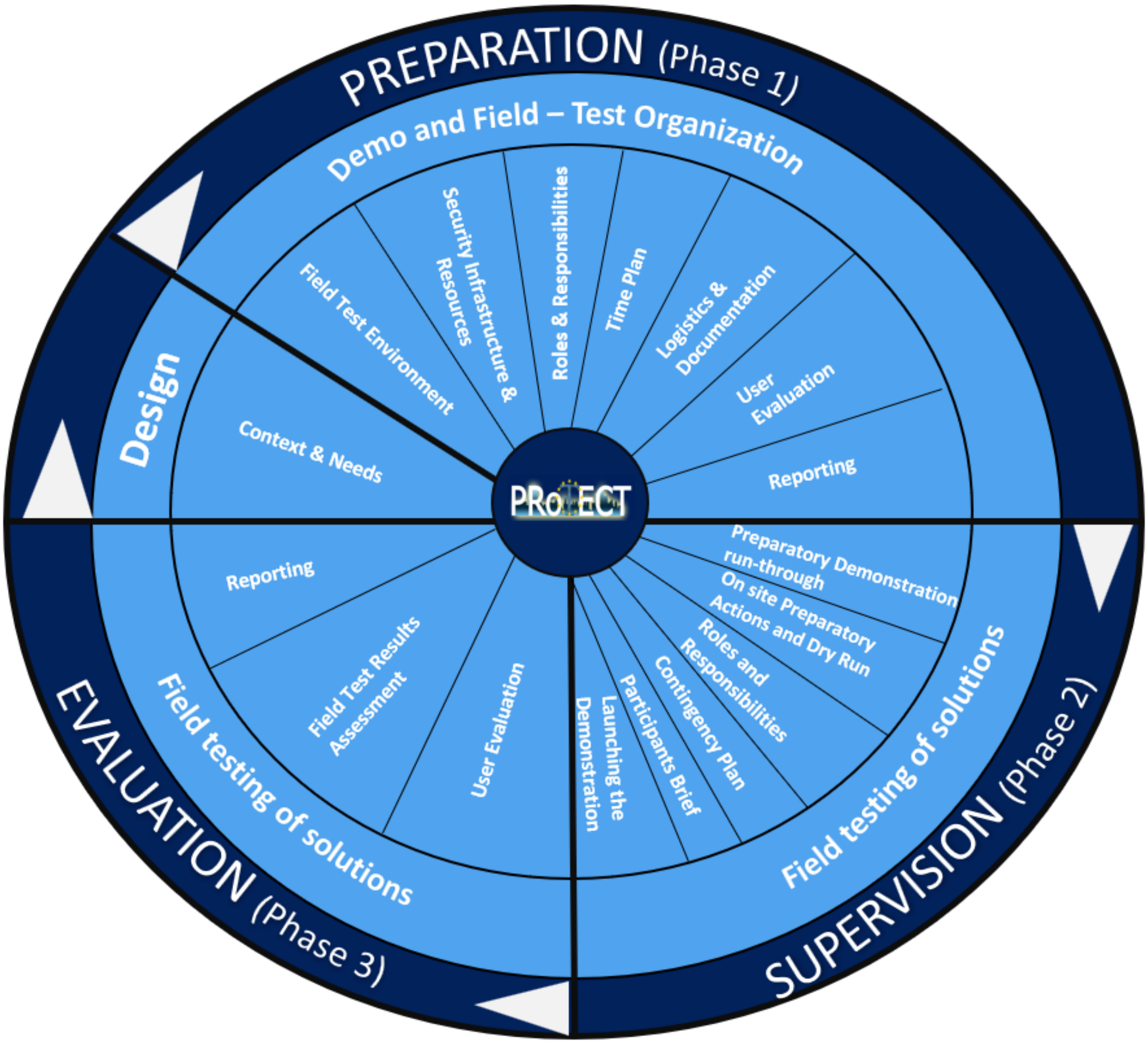

PREPARATION (Phase 1)
Demo and Field – Test Organization
Field Test Environment
Security Infrastructure & Resources
Roles & Responsibilities
Time Plan
Logistics & Documentation
User Evaluation
Reporting
Design
Context & Needs
PRoTECT
SUPERVISION (Phase 2)
Field testing of solutions
Preparatory Demonstration run-through
On site Preparatory Actions and Dry Run
Roles and Responsibilities
Contingency Plan
Participants Brief
Launching the Demonstration
EVALUATION (Phase 3)
Field testing of solutions
Reporting
Field Test Results Assessment
User Evaluation

Figure 10 PRoTECT - Field Test Guidance Methodology (FTGM)

FTGM starts with the Design of the demonstrations pilot(s) and continues with the three main phases of the Preparation, Supervision and Evaluation of the demonstrations. All the phases of FTGM are broken down and described in the following chapters.

5 DESIGN of Pilots

5.1 Context & Needs

Prior to the performance of a solution field test (hereby demonstration as is the case in PRoTECT), the presentation of the overall demonstration and operational context will provide the informational background needed for a common understanding between the demonstration organizer/host, the stakeholders and the solutions providers, including but not limited to the scope and objectives of the test/demo, the formulation of research questions, the operational environment in which a solution is meant to be incorporated and its respective security stakeholders, the final choice of security threats that the solutions are expected to address, the operational gaps (capacity needs) which the solutions are expected to cover, and the expected function(s) of the solution(s) itself. Following the extensive research framework presented in this document, most of these elements derive from, or have been addressed and analyzed in previous steps such as the Security self-assessment (section 2), the Scan for solutions (section 3).

Aside from a common understanding, describing the context of the demonstration will assist the actual end – users at a later stage, to assess if the initial objectives of the event were met. Additionally, it will be beneficial in the later evaluation of the solutions' performance and add value compared to its original purpose, its expected capabilities, and its suitability to the end – users' needs. End- user operational needs may in include aspects such as:

- Increases visibility at the PSOI
- Enhanced situational awareness
- Population count in the PSOI at a given time
- Alert systems
- Enhanced communications between security stakeholders
- Communication capability with the population at the PSOI
- Monitoring of the PSOI
- Enhanced emergency response capacity

End-user technical needs regarding the solutions may include aspects such as:

- Ease of use
- Ease of learning
- Fast performance and responsiveness
- Low operational and sustainability cost
- Ease of integration to existing systems
- Compliance with existing legislation

Moreover, the context of a demonstration should be thoroughly described to contribute to a concrete, and organized plan which is easy to monitor. This includes description of the field test environment (location, physical space and general daily operation), general description of required technical and security infrastructure, and available resources to accommodate the demonstration and provider's needs, description of the participating entities (the organizer/host and its personnel) and their purpose, listing of the relevant stakeholders (participants), and the providers, and finally, the description of any training that might be required.

Last but not least, the purpose of a field test/demonstration in the first place, is the validation and/or evaluation of selected technical solutions based on the threat scenarios developed and tailored to the demonstration site, utilized by previous processes such as the RfI (see section 3.1). Threat scenarios consist a major element of a demonstration's context, since they highlight the operational context of a PSOI, the vulnerabilities of a PSOI, potential threats against it and the needs that the security solutions are required to address. Based on the threat scenarios, simulation scenarios must be developed for a demonstration, which be tested as realistically as possible in a controlled environment.

6 PREPARATION- Demo / Field Test Organization (Phase 1)

6.1 Field Test Environment

The organizing entity in close collaboration with the local security stakeholders shall undergo a consultation process in order to identify the physical site that best suits the demonstration purposes, taking in consideration all experienced circumstances/limitations (including COVID 19). Hence, it should be taken in consideration that the actual site may differ from the one initially defined at the beginning of the project and the scenarios, based on the applicable restrictions. However, care shall be taken in order to retain the main characteristics of the original site and assumptions made during the threat/attack scenarios elaboration process for reaching accurate conclusions as to the applicability of technology for the specific case studies (KEMEA, 2020, p. 18).

In the preparation stage, the demonstration site should be described along with its surrounding environment. This should include the type of the site (e.g. open or closed public space), the site's main function (e.g. library or public square), type of area (commercial city, rural area etc.), the concentration of people in general and on the day of the demonstration, its similarities or not to the real PSOI which need to be protected, the site's significance (at a local or national level), and other important infrastructure or public spaces in close proximity to the site of demonstration.

6.2 Security Infrastructure & Resources

The security infrastructure and resources should be described in twofold. First, the existing security infrastructure and resources available to be utilized for the demonstration should be listed and described, to provide a clear picture to everyone involved with the organization of the demonstration. This will also reveal any limitations in the current security infrastructure and existing resources for further improvement. Secondly, the infrastructure and resources required for carrying out the demonstration should be listed and described to ensure a clear understanding between the organizer of the demonstration and the providers who will demonstrate their solutions, along with the availability of all necessary resources on time.

Special attention should be given in case of integration and compatibility of the providers' systems with system located at the demonstration site. This should be checked and tested early enough before the live demonstration to ensure that in case of issues there is still time available for configurations and adjustments.

6.3 Roles & Responsibilities

The organizer of the demonstration is responsible for assigning different roles and responsibilities to the member of its personnel. These can be divided between different teams or individuals depending on the scale of the event, the available personnel and the project management framework which is adopted by the organizer. The roles and responsibilities of the personnel may also be distinguished into different categories such as coordination of the event, logistics and budget, preparation and management of resources, external communications (with guest or external individuals participating in the event), legal and ethical issues, evaluation of the demonstration, technical assistance, hosting and others.

Moreover, if external participants and experts are to be involved in the processes prior or during the demonstration, their roles and responsibilities (if any) should also be described within the demonstration plan and communicated to them and the rest of the personnel. A list of these participants should be held and invitations to all relevant experts should be sent, taking into consideration the achievement of a fair balance of expertise among participants.

It is highly recommended that the demonstration organizer, will hold a briefing/training session to inform the assigned personnel of their duties and provide any clarification to issues that may be identified.

6.4 Time Plan

An achievable and clear time plan should be set with specific dates of the start and completion of each process, from the initial planning of the demonstration, until review of the results and findings following the demonstration. This could be presented as a GANTT diagram. The timeline should consider all organizational aspects such as the definition of the demonstration time and place, estimation of budget and identification/invitation of participants, installation, integration and testing of necessary equipment. Additionally, it should consider all the in-between processes and break down of all the pending procedures to provide a clear and holistic picture to the organizers of the demonstration, of their responsibilities and tasks to be completed. Consequently, the project will be managed more effectively, the decided schedule is more likely to be followed and potential delays can be easier to identify.

6.5 Logistics & Documentation

A logistics team should be appointed to gather and be responsible for all the provisions, materials, equipment, services, and facilities necessary for the demonstration (European Center for Disease Prevention and Control, 2014, p. 14) to facilitate the efforts of the solution providers and accommodate the needs of the end-users/participants. The responsibilities regarding logistics may include but not be limited to, facilities and rooms, registration, food and refreshments, manuals, informational flyers/documents, videotaping, role players (if any are needed), badges and identification.

The demonstration organizer is responsible for the production of all printed material following a throughout review process to avoid mistakes potentially causing procedural inconvenience. Printed material may include information flyers, posters, manuals, demonstration scenarios, evaluation questionnaires, consent forms and other.

Last but not least, logistics should involve budgetary planning and coverage. It is advised that the organizer carries out the necessary administrative processes, in preparation of participants' (e.g. the developers of the solutions to be demonstrated) compensation for eligible demonstration costs.

6.6 User Evaluation

A consistent evaluation of a demonstration and its presented solution requires a concrete framework, based on which the participants and/or the coordinator of the demonstration will assess the overall implementation of the event and the demonstrated solution. The coordinator of the event is responsible for the choice of framework to be used. This can consist of checklists, questionnaires for the participants or interviews (see section 8 for more details on evaluation methods).

6.7 Reporting

Reporting must be documented and based on a predesigned template. It should include all the information on the processes prior to the demonstration, the demonstrations itself and its outcome. Within this context, descriptive details should be provided on:

- the scope and objectives of the demonstration

- the date and location of its implementation
- all the participants (providers, coordination team and organizational members, guests, all end – users)
- the roles and actions of the participants
- the function of the solution(s) presented
- the solutions(s) objective in relation the end-user's security needs
- any issues that occurred during the demo (technical or otherwise)
- the reception of the demonstration and the solution by the end-users and the participants
- the evaluation results
- the identification of issues and gaps organizational, technical or otherwise
- suggestions for further improvements

7 SUPERVISION- Field Testing of Solutions (Phase 2)

7.1 Preparatory Demonstration run-through

After the demonstration preparation processes (presented in section 6) have been defined and organized, Phase 2 is initiated, where the demonstration of the chosen solution(s) will be reviewed and carried out.

As a first step, the preparatory run-through aims to bring together the organizers and the stakeholders of the demonstration, with the purpose of making sure that everyone is on the same page in terms of the way that the demonstration will be implemented, the demonstration's scope, its content, and that all the necessary conditions (technical and organizational) are met.

This can be done by organizing a physical or if not possible due to restrictions (e.g., COVID 19), an online meeting where the Demonstration Plan will be presented and discussed between the organizers of the demonstration and the rest of the stakeholders.

The purpose of this, is the presentation of the demonstration's scope, the description of its outcome and benefits for the stakeholders, the confirmation that necessary resources for the demonstration are available (including availability of demonstration site), the description of the Execution processes, the data collection methods that will be followed and finally, the description of the evaluation process which takes place in phase 3.

A benefit of the discussion is that possible risks (disrupting events/issues) which might affect the demonstration can be detected to be dealt with, stakeholder needs can be reviewed and opportunities for adjustments or improvements before the demonstration can be highlighted. The risk identified during the run-through should be listed for inclusion in the contingency plan (see 7.3).

7.2 On site Preparatory Actions and Dry Run

During the week before the demonstration, the demonstration organizer should procced to the deployment/installation of all supporting equipment. Systems and planned actions can be mock tested to ensure readiness for the demonstration.

During this task, all supporting infrastructure shall be installed and tested as per the demo requirements that have been previously dictated by each invited solution provider.

Additionally, a designated day before the demonstration should be dedicated for a Dry Run (DRIVER+, 2020) which will ensure that all necessary technical adaptations, installations, and integrations have been achieved and the systems are ready to be used, demonstrated, and evaluated. Depending on the scale of the demonstration, more than one day can be dedicated for testing the integration and functionality of systems and resolving potential issues which may be identified.

The Dry Run entails the testing of the prerequired systems at the demonstration site integrated with the systems of the demonstrators (technical solution providers). A Dry Run presents a good opportunity for the demonstration organizer, the stakeholders, and the technical solution providers, to understand each other needs, gain a holistic understanding of the demonstration processes and to identify and resolve/address any remaining issues/gaps.

7.3 Roles and responsibilities

Roles and responsibilities should be documented and presented as a list of all the participants, roles, and responsibilities, prior and during the demonstration (final preparatory and execution activities). This may refer to stakeholders responsible for communications with demonstration participants (guests, experts, or solution suppliers), ensuring the provision of amenities for the participants (efficient hosting), the availability of resources and necessary infrastructure for the execution of the demonstration, and any other roles or responsibilities for the facilitation of the demonstration's execution. Depending on the type of the demonstration, actors appointed by the organizer to participate in demonstration scenarios should be listed and their roles should be described.

As mentioned in section 6.3, depending on the type of demonstration and needs, the actors can be divided into various categories. Indicative examples include:

- Communications team
- Technical staff
- Logistics team
- Evaluation team/Committee
- Coordination team
- Demonstration actors
- Event hosting team

The roles and responsibilities of each team should be described thoroughly, with the inclusion of a list of all the participants in each team.

7.4 Contingency Plan

A contingency plan refers to planned actions aimed at the mitigation of previously identified risks, the occurrence of which, could disrupt the demonstration processes. Such risks can vary from simple things such as parts of necessary equipment which a supplier of a solution missed to bring along for the demonstration, to unstable wi-fi connection, missing informational material, sudden power outage, last minute unavailability of space, sudden shortage of staff, inability of solution suppliers to attend (e.g., due to COVID 19).

All the risks and mitigation measures should be documented descriptively and communicated between all members responsible for the organization and execution of the demonstration.

7.5 Participants briefing

Prior to the launch of the demonstration, all the participants should be informed on the context and content of the demonstrations, the schedule and/ or timeline of the demonstration, unresolved minor issues, and potential last-minute changes in the execution of the demonstration. The participants briefing is a good opportunity for last minute notifications and changes. During the briefing, the final availability of personnel with assigned tasks should be ensured, along with the understanding of all required tasks by each participant.

7.6 Launching the Demonstration

This is the final step of the execution process which takes place on the Demonstration day(s). Depending on the type of demonstration and the number of solutions to be presented, the actual demonstrations may be carried through several difference days.

Throughout the demonstration(s), observations about the effectiveness of the event and its shortcoming, along with feedback from the participants and end-users should be documented. This will contribute towards the later evaluation of the event's success and recommendation for future improvements.

A recommended set of actions which need to be considered for the actual day of a demonstration is listed below. The presented actions aim to facilitate the demonstration organizer to ensure the seamless delivery of the demonstration process (KEMEA, 2020).

Before/During the demonstration:

- Sign all the prepared informational, participation, ethics and legal forms related to participants, data gathering, handling and storage processes and other related topics. These -among other- may include forms such as a participant list and consent forms, research participation instructions with description of process, questionnaires and interviews related to participants (can be integrated to the consent forms) and others.
- Provide information on security and confidentiality issues (e.g. restrictions related to unauthorized filming and photography, disclosure of operational procedures).
- Include a briefing session where all the demonstrations details will be presented to the participants, including the demonstration scenarios and provide an opportunity for further details to be discussed
- Involved actors should be coached according to their role in the pilot (if applicable) in order to be able to respond to a security incident based on the details of each scenario.

After the demonstration

- All participants should be requested to fill out the designed questionnaires (see unit 8.1) and selected participants (given their consent) should be interviewed.
- The data and feedback gathered through questionnaires, interviews and observations during the demonstration should be processed and then analyzed.

8 EVALUATION- Field Testing of Solutions (Phase 3)

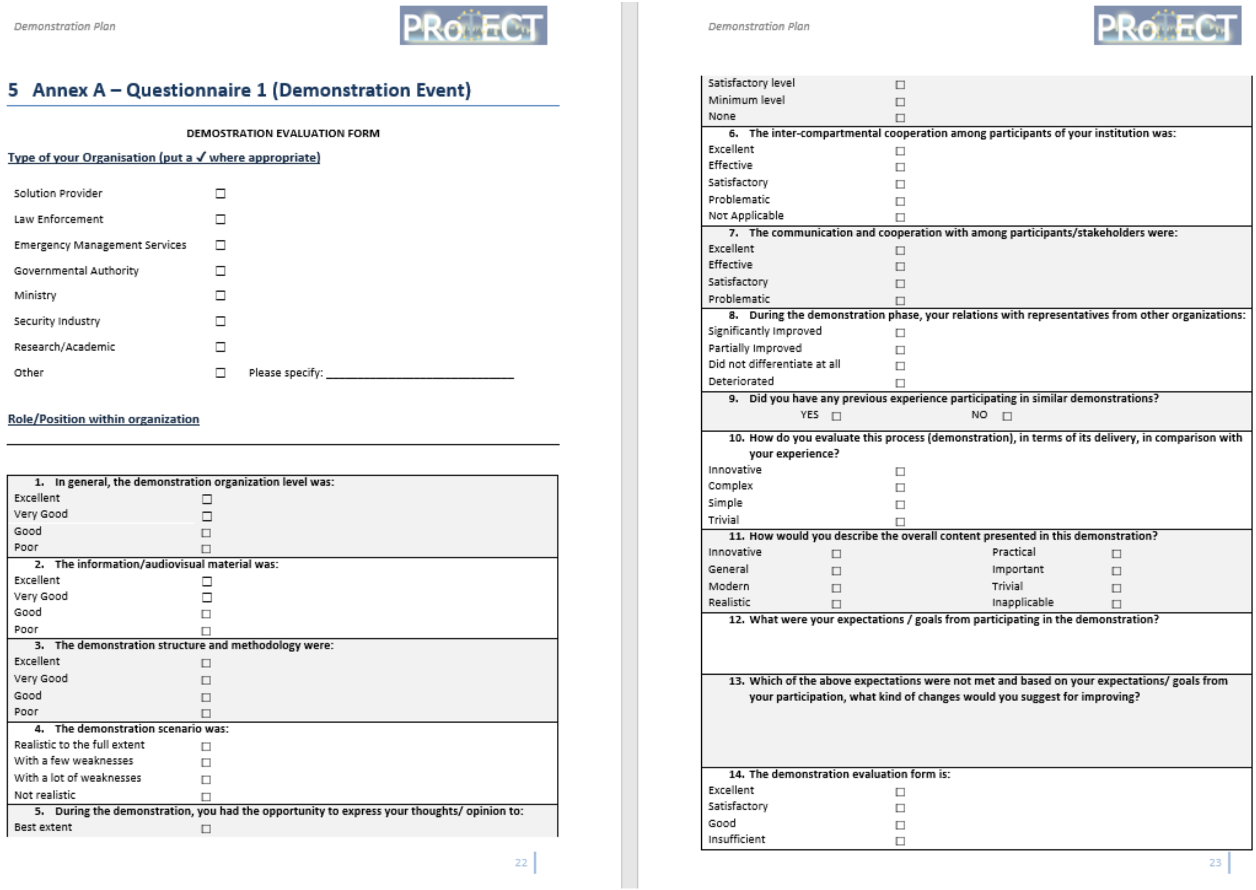
8.1 User Evaluation

A user evaluation can focus around two aspects. First, the demonstration as per its organization, its implementation, effectiveness and relevance of the demonstration scenario, information provision, effectiveness, the absence or active participation of stakeholders and the end – user satisfaction level regarding the overall process. The second focal point of an evaluation refers to the presented solution itself. The solution can be evaluated per its capability to meet the security objectives set by the end – users for a PSOI, its ability to mitigate a specific vulnerability(ies), its practicality (deployability, ease of use, level of required expertise) and its overall added value for the security stakeholders.

The points above can all be integrated into a structured questionnaire, which will be answered by the security /safety stakeholders participating at the demonstration and are responsible for the protection of a PSOI, namely a municipality, an operator of a PSOI, LEAs, emergency response services and others.

Alternatively, or supplementarily to the questionnaires, interviews (with individuals or in groups) can be held after the demonstration with the participants, where they can answer all the points mentioned above and can expand on them, providing information that might not have been considered and can further contribute to the evaluation process.

The assessment tools which were made especially for the evaluation of the demonstrations that took place during PRoTECT, and which can be used in similar contexts, consisted of two questionnaires. The first was generic and focused on assessing the organizational aspects of the process. It included questions about the organization level of the demonstration, information/audiovisual material provided to the participants, the structure and methodology which was based on, the scenario which it was based on, participation of stakeholders, cooperation between participating stakeholders, and others.



Demonstration Plan

5 Annex A – Questionnaire 1 (Demonstration Event)

DEMOSTRATION EVALUATION FORM

Type of your Organisation (put a ✓ where appropriate)

Solution Provider □
Law Enforcement □
Emergency Management Services □
Governmental Authority □
Ministry □
Security Industry □
Research/Academic □
Other □ Please specify: ______________________

Role/Position within organization

____

1. In general, the demonstration organization level was:
Excellent □
Very Good □
Good □
Poor □

2. The information/audiovisual material was:
Excellent □
Very Good □
Good □
Poor □

3. The demonstration structure and methodology were:
Excellent □
Very Good □
Good □
Poor □

4. The demonstration scenario was:
Realistic to the full extent □
With a few weaknesses □
With a lot of weaknesses □
Not realistic □

5. During the demonstration, you had the opportunity to express your thoughts/ opinion to:
Best extent □

22

Demonstration Plan

Satisfactory level □
Minimum level □
None □

6. The inter-compartmental cooperation among participants of your institution was:
Excellent □
Effective □
Satisfactory □
Problematic □
Not Applicable □

7. The communication and cooperation with among participants/stakeholders were:
Excellent □
Effective □
Satisfactory □
Problematic □

8. During the demonstration phase, your relations with representatives from other organizations:
Significantly Improved □
Partially Improved □
Did not differentiate at all □
Deteriorated □

9. Did you have any previous experience participating in similar demonstrations?
YES □ NO □

10. How do you evaluate this process (demonstration), in terms of its delivery, in comparison with your experience?
Innovative □
Complex □
Simple □
Trivial □

11. How would you describe the overall content presented in this demonstration?

Innovative	□	Practical	□
General	□	Important	□
Modern	□	Trivial	□
Realistic	□	Inapplicable	□

12. What were your expectations / goals from participating in the demonstration?

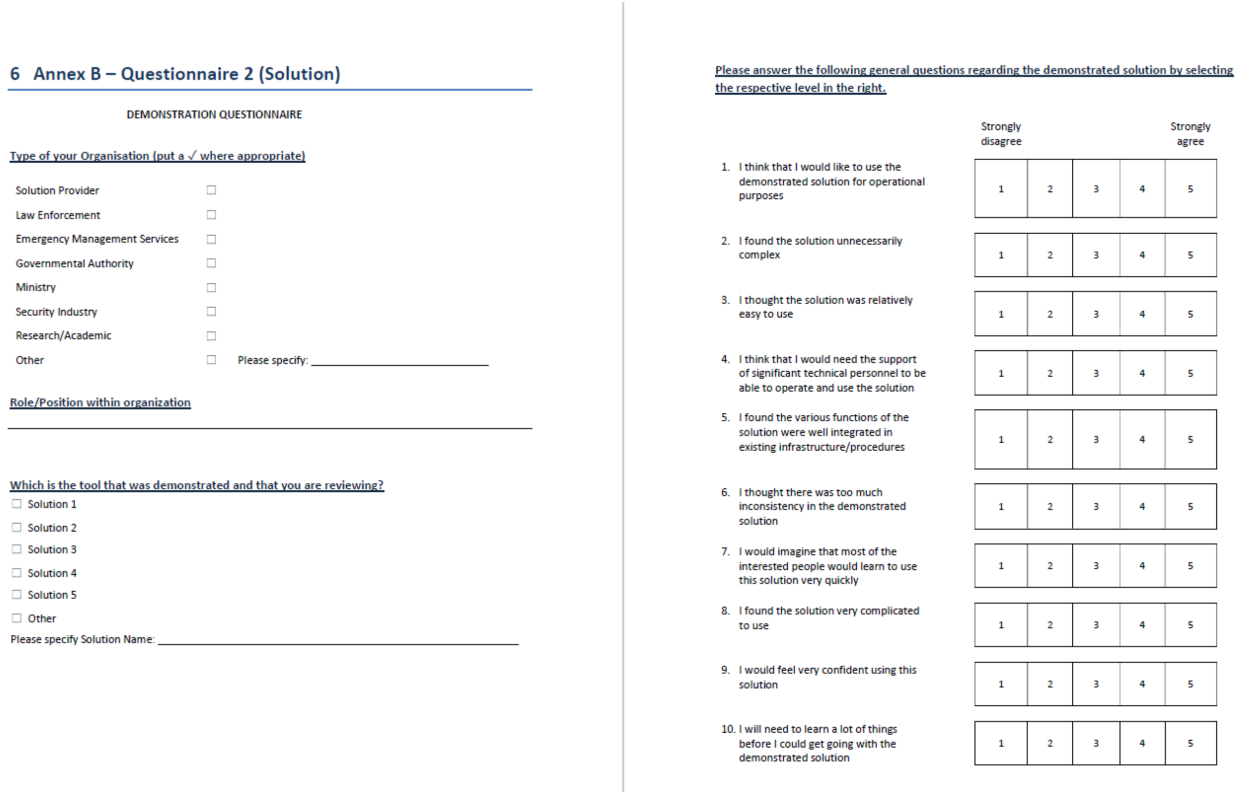
13. Which of the above expectations were not met and based on your expectations/ goals from your participation, what kind of changes would you suggest for improving?

14. The demonstration evaluation form is:
Excellent □
Satisfactory □
Good □
Insufficient □

23

Figure 11 Generic Evaluation Questionnaire

The second questionnaire, focused on assessing specific aspects of the presented solution, targeted towards the various organization types (e.g. solution provides, LEAs, Emergency Response Services, Government Institutions and Authorities, Researchers etc.) participating at the demonstrations. It included questions about the participant's willingness to adopt the solution, complexity of the solution, its practicality and ease of use, and required knowledge of individual for use.



6 Annex B – Questionnaire 2 (Solution)

DEMONSTRATION QUESTIONNAIRE

Type of your Organisation (put a ✓ where appropriate)

Solution Provider □
Law Enforcement □
Emergency Management Services □
Governmental Authority □
Ministry □
Security Industry □
Research/Academic □
Other □ Please specify: ______________________

Role/Position within organization

____

Which is the tool that was demonstrated and that you are reviewing?

□ Solution 1
□ Solution 2
□ Solution 3
□ Solution 4
□ Solution 5
□ Other
Please specify Solution Name: ______________________

Please answer the following general questions regarding the demonstrated solution by selecting the respective level in the right.

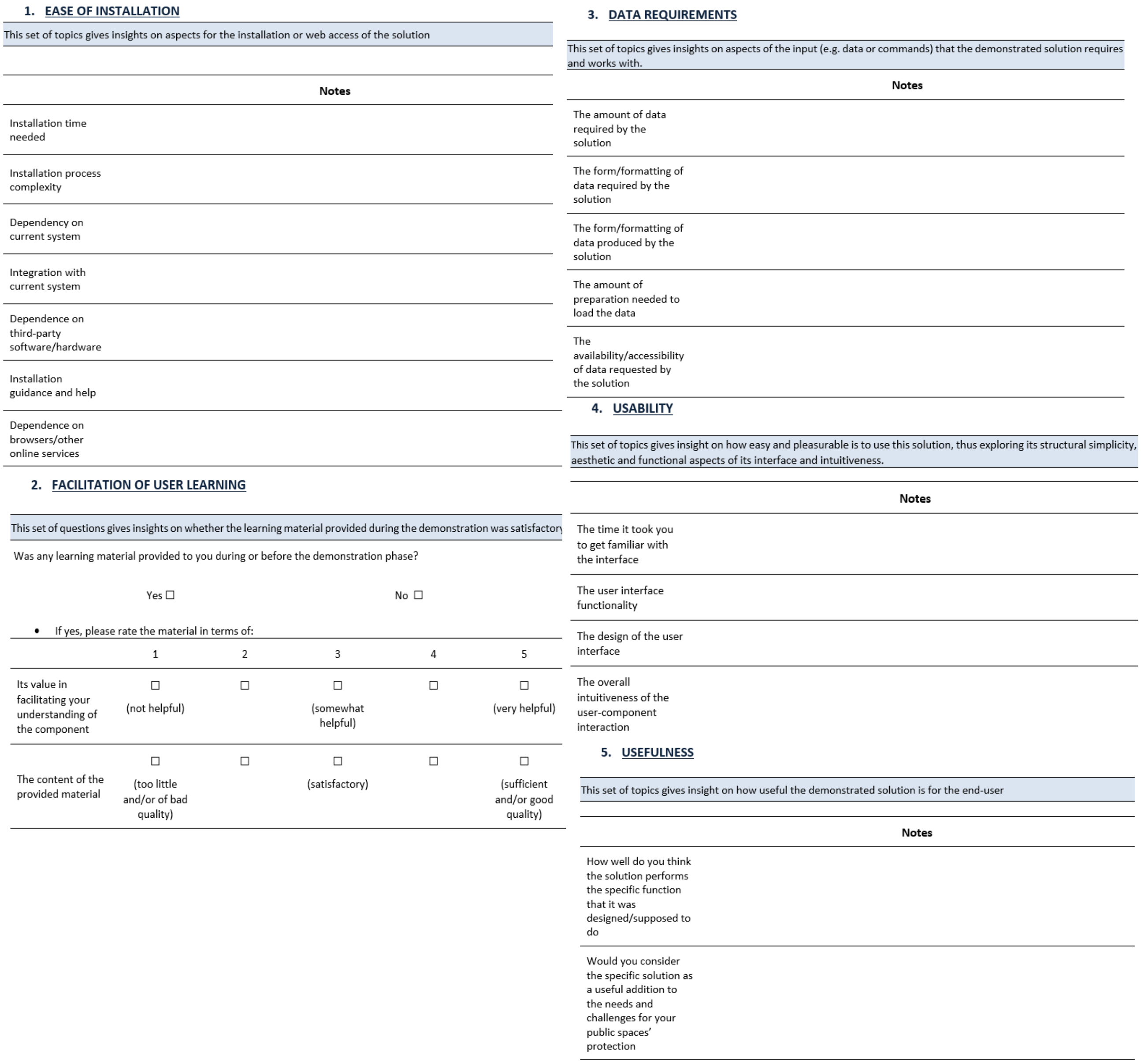
	Strongly disagree				Strongly agree
1. I think that I would like to use the demonstrated solution for operational purposes	1	2	3	4	5
2. I found the solution unnecessarily complex	1	2	3	4	5
3. I thought the solution was relatively easy to use	1	2	3	4	5
4. I think that I would need the support of significant technical personnel to be able to operate and use the solution	1	2	3	4	5
5. I found the various functions of the solution were well integrated in existing infrastructure/procedures	1	2	3	4	5
6. I thought there was too much inconsistency in the demonstrated solution	1	2	3	4	5
7. I would imagine that most of the interested people would learn to use this solution very quickly	1	2	3	4	5
8. I found the solution very complicated to use	1	2	3	4	5
9. I would feel very confident using this solution	1	2	3	4	5
10. I will need to learn a lot of things before I could get going with the demonstrated solution	1	2	3	4	5

Figure 12 End - User Specific Questionnaire

It should be highlighted that the individuals who answer the questionnaires and participate in the interviews, must possess a good grasp of the concept of security in public spaces and related operational aspects. Ideally, they will have participated in a previous VA of the PSOI for which the demonstration takes places, and will be knowledgeable about its security risks, vulnerabilities, security measures and policies in place and protection needs, as well as technical constraints regarding applicability and integration of proposed solutions. Provided that, they will be able to evaluate the demonstration and the solution presented more effectively and will contribute to more accurate evaluations results.

Supplementary to the questionnaire, interviews with participants/stakeholders, may be used as an additional feedback-collecting channel that beyond the aforementioned questionnaires, may contribute to the conclusions drawing process in a semi-structured approach. In this context, organizers can address stakeholders/participants on aspects that refer to the demos/solutions themselves during both group sessions and or individual interviews (as per case). In any case, for having a homogenous base of information, the discussion is proposed to follow a similar structure as outlined by the relevant questionnaires.

In order to facilitate the collection of additional information, and to enable stakeholders to reach a decision, a set of potential topics to be discussed can be listed. Figure 12 provides an example of interview topics as designed for the purposes of PRoTECT, which can be utilized to gather information from the end-users and the demonstrators (technical solutions providers). Similar templates can be created per case study and specified needs.



1. EASE OF INSTALLATION

This set of topics gives insights on aspects for the installation or web access of the solution

	Notes
Installation time needed	
Installation process complexity	
Dependency on current system	
Integration with current system	
Dependence on third-party software/hardware	
Installation guidance and help	
Dependence on browsers/other online services	

2. FACILITATION OF USER LEARNING

This set of questions gives insights on whether the learning material provided during the demonstration was satisfactory

Was any learning material provided to you during or before the demonstration phase?

Yes ☐ No ☐

- If yes, please rate the material in terms of:

	1	2	3	4	5
Its value in facilitating your understanding of the component	☐ (not helpful)	☐	☐ (somewhat helpful)	☐	☐ (very helpful)
The content of the provided material	☐ (too little and/or of bad quality)	☐	☐ (satisfactory)	☐	☐ (sufficient and/or good quality)

3. DATA REQUIREMENTS

This set of topics gives insights on aspects of the input (e.g. data or commands) that the demonstrated solution requires and works with.

	Notes
The amount of data required by the solution	
The form/formatting of data required by the solution	
The form/formatting of data produced by the solution	
The amount of preparation needed to load the data	
The availability/accessibility of data requested by the solution	

4. USABILITY

This set of topics gives insight on how easy and pleasurable is to use this solution, thus exploring its structural simplicity, aesthetic and functional aspects of its interface and intuitiveness.

	Notes
The time it took you to get familiar with the interface	
The user interface functionality	
The design of the user interface	
The overall intuitiveness of the user-component interaction	

5. USEFULNESS

This set of topics gives insight on how useful the demonstrated solution is for the end-user

	Notes
How well do you think the solution performs the specific function that it was designed/supposed to do	
Would you consider the specific solution as a useful addition to the needs and challenges for your public spaces' protection	

Figure 13 Discussion topics for Interviews

8.2 Field tests/ Demonstration results assessment

The assessment of demonstration results takes into consideration observations made (by the respectively designated team/individuals) during the demonstration, the results of the questionnaires handed after the demonstrations (see 8.1), the information gathered from interviews (if applied) and finally, any other feedback and recommendations provided at any given time by the participants of the demonstration.

A structured and logical approach for assessing a demonstration's results can be implemented by following the logic of Plan- Do- Check- Act (PDCA or Deming Cycle) cycle for the purpose of quality control and continuous improvement of individual processes or quality management as whole (British Standards Institution, 2015) integrated into the FTGM cycle. The demonstration results assessment focuses on the

"Check" and "Act" steps of the PDCA cycle. "Check" entails the observation and review of on-going processes against set objectives, the report of the results for review and respective actions for improvements. "Act" includes the implementation of corrective- improvement actions based on the results of a process and the set objectives (British Standards Institution, 2015).

Considering the PDCA cycle this step of FTGM's phase 3, focuses on the overall assessment of the demonstration's results regarding two main aspects. The **first aspect** consists of the assessment of the solutions which participated in the Demonstration process and were presented to the end-users.

The assessment of the participating solutions can be based on different aspects, such as **a)** the answers of questionnaires handed to the demonstrations end-users/participants (presented in the previous step) which will allow to sort the solutions demonstrated based on their relevance, **b)** observations made during the demonstration and most importantly **c)** certain Key Performance Indicators (KPIs) set according to the objectives and performance of a solution per an identified vulnerability, as a response to previously recorded needs and end- user requirements for the more effective protection of a PSOI, and last but not least current industry standards.

A method for designing questionnaires for assessing solutions is the System Usability Scale (SUS), introduced by John Brookes in 1986 (U.S. General Services Administration, n.d.). In general, SUS constitutes a quick and reliable tool which can be used to measure the usability of tested systems, via the design of easily comprehensible (by anyone) 10-item questionnaires. The assessment is based on the participant's answers to the 10 questions included, with each question given one of five possible answers to choose from, ranging from "Strongly Agree" to "Strongly Disagree". Questions or statements (to be precise) could include e.g. "I thought that the presented solution was easy to use", or "I found the solution (technically) unnecessarily complex". SUS offers an easy scale to administer to participants, an easy application on small sample sizes with reliable results and required validity since its can effectively differentiate between usable and unusable systems (see also PRoTECT WP4- "Demonstration Plan", 2020).

KPIs on the other hand, are typically specific (e.g., ease of installation, maintenance cost) and are formulated (among other factors) based on the nature of the subject under examination (e.g., type of technological solution), the end-user requirements and the operational environment where a solution is meant to be applied. KPIs can be categorized under different Key Performance Areas (KPAs) such as economic, operational, legal- ethics compliance and others (depended on the case) for a more elaborate analysis of solution's performance and a transparent projection of the aspects that need special attention or further improvement to increase legibility.

The **second aspect** of the assessment of the demonstration results refers to organization of the demonstrations and their further improvement. Similarly to the assessment of the solutions, the evaluation of the demonstration results will be based on the answers of the -end-users/participants to the questionnaire (see section 8.1), field observations, combined with certain KPIs which will provide a clear picture of the strong attributes of the current effort, and the weak attributes which need further improvement for future implementation. Here the KPIs are based on the purpose of the demonstration (e.g., instructional, or informative only) and can refer to the instructional material provided per the effectiveness of its content, the amenities of the invited participants, the methodological approach applied and others performance aspects which define the quality and effectiveness of the demonstration event. The included KPIs can be formulated and adjusted depending on the case, the end-user's needs, widely general accepted criteria of performance and most importantly the objectives of the demonstration. The results of the assessment will be integrated and reported during the next step 8.3 and in accordance with the PDCA cycle as part of FTGM, for identification of needs for further improvement.

8.3 Reporting

Reporting is done through a documented report with the description of the whole demonstration process, the participants and their roles, and the results and conclusion of the evaluation process. Important aspects to be considered are the description of successful actions and positive outcomes produced during the organization and realization of the demonstration, the limitations which may have restricted the quality of the potential outcome of the demonstration, and findings deriving from the evaluation of the demonstration and recommendations for future demonstrations and improvements in the whole process. It is particularly important to clearly document the conclusions drawn from the feedback provided by all participants/ stakeholders with significant expertise on the subject, regarding the success of the demo in solving the given problem statement. This will contribute towards generating further knowledge for the organizers, relevant stakeholders, and other interested entities outside the project, but may also improve quality control for future demonstrations. Recommendations should be communicated to the stakeholders as soon as possible after the demonstration and should be based on the initial objectives of the demonstration and the related evaluation criteria.

9 Conclusion & Lessons Learnt

The conclusion encapsulates a summary of all the main observations and findings during the processes that that took place in phase 1 (preparation), phase 2 (execution) and phase 3 (evaluation). These are related to the effectiveness of the approach for the overall planning, the general way that the event was carried out, its level of success (based on the original scope of the demonstration), how it was received by the participants and its added value for the end-users.

Lessons learned derive from all the documented shortcomings, misses, issues related to the plan design, the organization and execution of a demonstration, as well as the evaluation method used, which should be dealt with in a future demonstration, and processes that should be improved in order to gain all the possible benefits that a demonstration can offer.

The content of the conclusion and lessons learnt will greatly benefit from the efficient documentation of observations during the demonstration, the user evaluation (see section 8.1), the demonstration results assessment (see section 8.2), and a thorough and efficient report (see section 8.3) which will provide valuable input for this section.

Provided the above, experience gained through the implementation of the PRoTECT project has indicated that the high-level methodological approach which has been detailed in previous sections of this deliverable, refers to a highly flexible/adaptive process. In this regard, the context of the proposed methodology considers the diverse particularities, legislative/regulatory framework and administrative mechanism that is applicable throughout the European ecosystem regarding public spaces. Having said that, the sensitive nature of protecting public spaces (soft targets) against terrorist attacks encompasses a wide range of parameters relevant the different steps of this manual.

As such, the initial step concerning the Vulnerability Assessment (VA) has (Step 1) has highlighted the need for identifying and consulting with all stakeholders being responsible for the administration and delivery of security/safety for a selected Public Space of Interest. In order to create a solid picture of the vulnerabilities that are applicable for each case., the range of stakeholders that could participate in a VA should encompass all phases of crisis management (i.e. preparedness, response, recovery). This practice provides additional assurance as to the identification of vulnerabilities that is not directly obvious and may be realized at a later stage of a crisis onset.

Furthermore, the phase of mapping the mitigation of the identified vulnerabilities to the capacity of the relevant market, needs to be characterized by a careful balance between the level of detail publicly provided to the market and the feedback received by the economic operators. A fair approach to addressing this challenge, is the elaboration of a hypothetical scenario to be used as an accurate problem statement that encompasses all those characteristics that need to be examined however in a concealable manner that safeguards security issues without revealing sensitive information.

Finally, the delivery of field tests of technologically mature solutions of high TRL (8, 9) will allow the drawing of solid conclusions as to the enhancement of the achievable security levels of a specific public space. These field tests, will shall exploit the expertise of all responsible field stakeholders in order to assess and reach a valid conclusion. The covid-19 pandemic and the limitations imposed by this situation, dictated the need for exploiting alternative approaches for delivering such filed tests. In this context it became apparent that demonstrations can be approached in a hybrid manner encompassing the engagement a remote installation to be used for a demo adapted to a specific site. This approach has proved to be a successful alternative also allowing for a remote consultation with stakeholders on a wider national and/or EU scale. Finally, the elaboration of a solid assessment mechanism, encompassing both qualitative and quantitative dimension will also allow for a concrete outcome.

This Manual, although made for the case of PRoTECT project, is also a frame of reference for EU municipalities and security stakeholders in general responsible for the protection of public spaces against terrorist attacks as well as the mitigation of the impact of such attacks if realized. In this regard, this document aims to provide a general procedural context, in the form of a concise manual, proposed as a solid methodology for investigating/exploiting appropriate solution(s) towards addressing identified security risks, issues and increasing the sense of security.

10 References

Alqahtani, N. D., Al- Jewair, T., Albarakati, S. F., & ALkodife, E. A. (2015). Live demonstration versus procedural video: a comparison of two methods for teaching an orthodontic laboratory procedure. *BCM Medical Education* *15*(199). Retrieved from https://bmcmededuc.biomedcentral.com/articles/10.1186/s12909-015-0479-y#citeas

Anderson, C. (2017, August 19). Fatal Knife Attack in Finland Is Investigated as Terrorism. The New York Times. Retrieved from https://www.nytimes.com/2017/08/19/world/europe/turku-finland-attack.html

BBC. (2016c, August 19). Nice attack: What we know about the Bastille Day killings. BBC News. Retrieved from https://www.bbc.com/news/world-europe-36801671

BBC News. (2015, December 9). Paris attacks: What happened on the night. BBC News. Retrieved from https://www.bbc.com/news/world-europe-34818994

BBC News. (2015, December 9). Paris attacks: What happened on the night. BBC News. Retrieved from https://www.bbc.com/news/world-europe-34818994

BBC News. (2016a, December 26). Berlin lorry attack: What we know. BBC News. Retrieved from https://www.bbc.com/news/world-europe-38377428

BBC News. (2016b, April 9). Brussels explosions: What we know about airport and metro attacks. Retrieved from https://www.bbc.com/news/world-europe-35869985

BBC News. (2017, August 27). Barcelona and Cambrils attacks: What we know so far. Retrieved from https://www.bbc.com/news/world-europe-40964242

BBC News. (2017b, July 28). Hamburg supermarket attack leaves one dead. BBC News. Retrieved from https://www.bbc.com/news/world-europe-40757119

BBC News. (2018, June 7). Stockholm truck attack: Who is Rakhmat Akilov? BBC News. Retrieved from https://www.bbc.com/news/world-europe-39552691

British Standards Institution. (2015). *BS EN ISO 9001:2015- Quality management systems.* BSI Standards Publication. Retrieved from https://shop.bsigroup.com/ProductDetail?pid=000000000030273524

Christodoulou, H. (2018). *DEADLY MASSACRE How many Las Vegas shooting victims are there, have they been named and what is the current death toll?* the Sun. Retrieved from https://www.thesun.co.uk/news/4593987/las-vegas-shooting-victims-names-death-toll/

CyberSecurity & Infrastructure Security Agency. (2020, March 24). Retrieved from https://www.cisa.gov/critical-infrastructure-sectors

Dehbi, C. (2019). *Community- Oriented Policing in the European Union Today- Tool Box Series No14.* Brussels: European Crime Prevention Network (EUCPN). Retrieved from https://eucpn.org/sites/default/files/document/files/Toolbox%2014_EN_LR.pdf

Donnelly, D. (2013). *Municipal Policing in the European Union.* Palgrave Macmillan. Retrieved from https://www.palgrave.com/gp/book/9780230232037

DRIVER+. (2020). Trial Guidance Methodology Handbook . DRIVER+ GA No #607798. Retrieved from https://www.driver-project.eu/wp-content/uploads/200619-d_plus-leaflets-EN-spreads-tgm.pdf

EFUS. (2005, February 19). Secucities: Cities against Terrorism- Training Local Representatives in Facing Terrorism. Retrieved from https://issuu.com/efus/docs/cities_against_terrorism

European Center for Disease Prevention and Control. (2014). *Technical Document- Handbook on simulation exercises in EU public settings.* Stockholm. Retrieved from https://www.ecdc.europa.eu/sites/default/files/documents/simulation-exercise-manual.pdf

European Commission. (2018). Public Procurement Guidance for Practitioners on avoiding the most common errors in projects funded by the European Structural and Investment Funds. Retrieved from https://ec.europa.eu/regional_policy/sources/docgener/guides/public_procurement/2018/guidance_public_procurement_2018_en.pdf

European Commission. (2019a). *Commission Staff working Document- Good practices to support the Protection of Public Spaces, SWD (2019) 140 Final.* Brussels: European Commission. Retrieved March 20, 2019, from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190320_swd-2019-140-security-union-update-18_en.pdf

European Commission. (2019b). *Security by design for the Protection of Public Spaces*. Retrieved from https://ec.europa.eu/newsroom/pps/item-detail.cfm?item_id=653933&utm_source=pps_newsroom&utm_medium=Website&utm_campaign=pps&utm_content=Defining%20the%20Concept&lang=en

European Commission. (2020, September 10). Protection of Public Spaces - Use of Digital Technologies for the Protection of Public Spaces. Retrieved from https://ec.europa.eu/newsroom/pps/item-detail.cfm?item_id=686830&newsletter_id=1410&utm_source=pps_newsletter&utm_medium=email&utm_campaign=Protection%20of%20Public%20Spaces&utm_content=Use%20of%20Digital%20Technologies%20for%20the%20Protection%20of%20Pub

European Commission. (n.d.). *Official web site of the EU Commission- Critical Infrastructure definition*. Retrieved from https://ec.europa.eu/home-affairs/tags/critical-infrastructure_en

European Parliament, Council of the EU. (2016b). *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

European Parliemant, European Council. (2016a). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Hayden, M. E. (2017). *Terror in the UK: A timeline of recent attacks.* ABC NEWS. Retrieved from https://abcnews.go.com/International/terror-uk-timeline-recent-attacks/story?id=47579860

International CPTED Association. (n.d.). Retrieved from https://www.cpted.net/

ISO. (2018). *International Standard, Risk Management- Guidelines (ISO 31000).* Geneva, Switzerland: BSI Standards Publication.

Karlos, V., Larcher, M., & Solomos, G. (2018). *JRC Science for Policy Report - Review on Soft target/Public space protection guidance.* European Commission. Retrieved from https://publications.jrc.ec.europa.eu/repository/handle/JRC110885

KEMEA. (2020). *PRoTECT WP4- Demonstrations, Demonstration Plan.* PRoTECT GA n° 815356.

Partnership on Security in Public Spaces. (2019). *Urban Agenda for The EU Security in Public Spaces- Orientation Paper.* Retrieved from https://ec.europa.eu/futurium/en/security-public-spaces/security-public-spaces-orientation-paper

TNO & EFUS. (2019, 03 13). *PRoTECT D2.1 - Manual for Vulnerability Assessment (Confidential Document).* PRoTECT GA n° 815356.

TNO. (2019). *PRoTECT D3.2 –Technology Evaluation Framework.* PRoTECT GA n° 815356. Retrieved from https://protect-cities.eu/protect-project/public-deliverables/

U.S. General Services Administration. (n.d.). *usability.gov*. Retrieved from https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html