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

D3.2 – Technology Evaluation Framework

WP number and title	WP3 – Technology Evaluation Framework
Lead Beneficiary	TNO
Contributor(s)	KEMEA, EINDHOVEN, MALAGA, LARISSA, VILNIUS, BRASOV
Deliverable type	Report
Planned delivery date	20/12/2019
Last Update	23/12/2019
Dissemination level	PU

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	15/09/2019	Draft	TNO	First draft outline
V0.2	22/10/2019	Draft	TNO / KEMEA	Second draft
V0.3	27/11/2019	Draft	TNO/ KEMEA	Version ready for peer review
V0.4	23/12/2019	Draft	TNO/ KEMEA	Reviewed by EFUS, KEMEA, TNO & Municipality of Eindhoven
V0.5	16/12/2019	Draft	TNO/ KEMEA	Reviewed by DITSS & JADS
V0.6	18/12/2019	Draft	TNO/ KEMEA	Submitted for final review
V0.7	23/12/2019	Draft	DITSS	Final review and Quality assurance
V1.0	24/12/2019	Final Draft	DITSS	Final approval and submission

Definitions, Acronyms and Abbreviations

TERM	DEFINITION
(Evaluation) Criteria	Characteristics of a solution which can be measured, either quantitively or qualitatively. Criteria can be used to compare solutions.
Demonstration	An event, organised by a municipality, and usually involving a solution's provider, whereby specific functions of the solution are proven in a relevant operational environment, using scenarios.
Evaluation	An event, organised by a municipality, whereby the degree in which solutions meet certain criteria, set by the municipality, are determined. In the context of PRoTECT, there are three types of evaluation: an evaluation of information given by providers, an evaluation of the operational use of a solution (a table-top exercise), an evaluation of the demonstration of a solution.
Managing body	The managing body is an individual, organisation or group of organisations that takes up the responsibility to identify and work on counter terrorism regarding *PSOI's*. This can be a law enforcement agency, a municipality or possibly also the owner of the *Main site*. In the case of the PRoTECT project, the managing bodies are the 5 municipalities who will identify their *vulnerabilities* against various terrorist attacks and identify their *soft targets*.
Multi-criteria Analysis (MCA)	An MCA is a method to compare optional solutions based on selected criteria.
Public Space of Interest (PSOI)	A PSOI, consists of a *Main Site*, where a public event takes place, and several associated *Surrounding Sites*, which provide access to the *Main Site*. A vulnerability assessment is made for a PSOI.
Request for Information (RfI)	An RfI is a process whereby solution information is solicited from providers based on a list of solution requirements. In the context of PRoTECT, an RfI announcement is made public by a municipality, requesting providers to offer information on a solution which will mitigate a PSOI security vulnerability.
Requirement	In the context of PRoTECT, a requirement is a demand, pertaining to a solution or a solution provider, which must be satisfied by the provider.
Soft target	A site that is insufficiently protected against a terrorist attack and when attacked by a terrorist organization, will help terrorists obtain their goals.
Solution	In the context of PRoTECT, a solution is a commercially available device, software, service or combination of the aforementioned.
Table Top exercise	A type of exercise amongst stakeholders (seated around a table) to determine a solution's performance by running various operational scenarios for an event at a PSOI.
Vulnerability	In the context of PRoTECT, a weakness in or an absence of a security or safety measure, such as the absence of a vehicle barrier or a measure to prevent over-crowding.

ACRONYM / ABBREVIATION	DESCRIPTION
EFUS	European Forum for Urban Security
ENLETS	Network for Law Enforcement Technology Services
EU	European Union
GDPR	General Data Protection Regulation
IED	Improvised explosive devices
ISFP	Internal Security Fund Police
MCA	Multi-Criteria Analysis
MTTR	Mean time to repair
PBIED	Person-Borne Improvised Explosive Device
PRoTECT	Public Resilience using Technology to Counter Terrorism
PSOI	Public Space of Interest
RfI	Request for Information
SLR	Systematic Literature Review
TCA	Total cost of acquisition
TCO	Total cost of ownership
TEF	Technology Evaluation Framework
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle-Drone
UAVIED	UAV Borne Improvised Explosive Device
VAT	Vulnerability Assessment Tool
VBIED	Vehicle Borne Improvised Explosive Device
WP	Work Package

Table of Contents

List of Figures

List of Tables

Executive Summary

For decades, terrorism has been a reality in many European countries and a continuous threat to a great number of European cities. It seriously threatens the safety, rights and liberties of citizens and values of democratic states. Acts of terrorism bring about long-term negative effects for cities and high social costs. There is an increased feeling of insecurity among locals and visitors (EFUS, 2005).

In this context, the PRoTECT project (funded by the European Union's ISFP, from November 2018 until December 2020) aims to strengthen local authorities' capability in protecting public space against terrorist attacks by offering an overarching concept where tools, technology, training and field demonstrations.

Five European cities of the PRoTECT consortium, namely Eindhoven (Netherlands), Brasov (Romania), Vilnius (Lithuania), Malaga (Spain) and Larissa (Greece) implemented and tested the EU Vulnerability Assessment Tool (EU VAT) provided by DG Home and the manual that was developed in Work Package 2 of the PRoTECT project. Workshops were organised in which each municipality assessed vulnerabilities of actual public space events (generally cultural and social events).

One of the next tasks in the PRoTECT project was the development of a framework to assist a municipality in finding and evaluating technologies and best practices for mitigating a vulnerability. The European Technology Evaluation Framework (EU TEF) was developed in PRoTECT project for this purpose and is explained in this document. The framework offers eight (8) steps in which a municipality is guided through various processes of soliciting information on solutions from multiple providers, evaluating the solutions based on the acquired information, carrying out operational exercises in table-top sessions, and conducting live demonstrations of the solutions. The EU TEF can be used to evaluate any form of technology (e.g. technological and social innovative solutions).

The EU TEF was developed to suit the needs of the five PRoTECT municipalities but can be used by any city that wants to gather information on and evaluate technologies for protecting public space. It is however, important to have completed a vulnerability assessment before using the EU TEF (for instance, by using the EU VAT).

1 Introduction

1.1 Background

For decades, terrorism has been a reality in many European countries and a continuous threat to a great number of European cities. It seriously threatens the safety, rights and liberties of citizens and values of democratic states. Acts of terrorism bring about long-term negative effects for cities, and high social costs. There is an increased feeling of insecurity among locals and visitors (EFUS, 2005). The goal of terrorists is (by definition) to achieve political or administrative change in society by raising fear. Applying effective counter terror measures must not only effectively counter the attacks (objective security) but also instil confidence in the capability of the (local) government to protect its citizens against terrorism (subjective feeling of security) while respecting human rights and civil liberties.

Over the years, strategies to protect public space against terrorism have strengthened and evolved, mainly focusing on protecting critical infrastructure. However, terrorist attacks are evolving as well. Increasingly, attackers are exploiting newly discovered opportunities, whereby targets in public space have become attractive. To illustrate, the latest terrorist attacks in European cities such as London, Paris, Manchester, Stockholm, Berlin, Brussels and Barcelona have occurred in public areas. Crowded public places, including the metro, shopping centres, sports stadiums, bars, restaurants, clubs and commercial sidewalks, are easily accessible for terrorists, where they can do great harm. These areas are called **soft targets** as they are insufficiently hardened against terrorist attacks.

1.2 PRoTECT framework objectives

As stated by the European Commission in the Action Plan to support the protection of public spaces, besides Member States, “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.

In this context, PRoTECT – being a project funded by the European Union’s ISFP with a duration of two years (November 2018 through December 2020) – aims to strengthen local authorities’ capability in the protection of areas in public space by applying an overarching concept where tools, technology, training and field demonstrations will lead to enhanced situational awareness and improvement of a direct response before, during and after a terrorist attack.

For this purpose, the five European cities of the PRoTECT consortium, namely Eindhoven (Netherlands), Brasov (Romania), Vilnius (Lithuania), Malaga (Spain) and Larissa (Greece) implemented and tested the EU Vulnerability Assessment Tool (EU VAT), provided by DG Home, using the manual that was developed in WP 2 of this project. The tool assisted the municipalities in identifying vulnerabilities concerning a public space of interest (PSOI) which is characterized by a high concentration of people during a cultural or social event. The vulnerabilities were identified and assessed in workshops, for specific use-cases. The results of the vulnerability assessments provided a record of the most critical threats against the security of the PSOI, based on the feasibility, probability of occurrence and the impact of the threats. It is these vulnerabilities against which selected (technological and social) solutions[1] will be requested from providers. The performance of the solutions will be judged through and evaluation of information, table-top exercises and demonstrations.

[1] These technological and social solutions should be ideas, solutions, innovations or processes at TRL 4 or higher.

As such, upon assessment, security vulnerabilities and future threats which were derived from the EU VAT results will be addressed through the identification of applicable (technological and potential social) security solutions for the purpose of enhancing the situational awareness and response of the law enforcement agencies, the local municipalities and the other local stakeholders responsible for the security of the aforementioned cities. The technological and/or social solutions will be demonstrated at the 5 cities (potentially accompanied by training sessions).

1.3 PRoTECT Work Package 3

In light of the above, local authorities responsible for the safety and security of their citizens must be aware of the vulnerabilities of their public spaces in order to be able to adopt appropriate measures to prevent and mitigate terrorist attacks and their consequences (European Commission, 2017). While some municipalities across Europe have made great progress in counterterrorism and have adopted measures to prevent and be prepared for a terrorist attack in public space, some do not consider terrorism as a specific threat in public space or do not know how to assess the threat properly.

The consortium will make extensive usage of previous efforts in the protection of public spaces and previous work from the ENLETS network and EFUS members. Research results from previous H2020 projects and with high Technology Readiness Level (TRL) level (6 and above) will be assessed as part of our technology evaluation framework; promising research solutions will be selected for a demonstration set up in each of the five city partners. To do so, the evaluation framework will be defined systematically by the entire consortium and communicated and assessed by the five target cities. At the end, PRoTECT will provide a technology roadmap to be used as a handbook by an extended numbers of EU municipalities via the EFUS Association.

Continuing from the results of the first activities of PRoTECT (i.e. the EU VAT usage), this work consists of multiple tasks (Ts) and interactions with tasks of other WPs:

- First, the creation of a Systematic Literature Review (SLR)[2] on existing technologies and best practices
- Second, the development of the EU TEF
- Third, setting up and executing the Request for Information, using criteria from the EU TEF and via an online publication aimed at solution providers
- Fourth, evaluating the information offered by solution providers using the evaluation method specified in EU TEF
- Fifth, evaluation of the operational use during workshops, based on scenarios from EU TEF
- Sixth, setting up and performing demonstrations of the solutions in each of the five PRoTECT cities based on scenarios from EU TEF

1.4 The Technology Evaluation Framework

A **technology evaluation framework** (EU 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. The EU 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.

[2] Systematic reviews are a type of literature review that uses systematic methods to collect secondary data, critically appraise research studies, and synthesize findings qualitatively or quantitively. (source: Wikipedia). In the PRoTECT project next to the SLR, there has been a review of best practices, solutions and results from EU projects.

The EU TEF is meant for municipal staff who are responsible for safety and security in public space and their stakeholders, such as municipal police, urban planners, security departement or crime prevention unit, event organisers, tourism and transport operators etc. The EU TEF aids municipalities in the whole process of gathering information on potential technologies for mitigating specific vulnerabilities and evaluating them.

The framework consists of eight steps which aid a municipality in finding a solution for a vulnerability. The framework steps involve deciding on relevant evaluation criteria, setting up the RfI, evaluating the RfI-yield and, performing table-top sessions and demonstrations. The EU TEF does not explain how to set up an RfI completely nor specifically state how to conduct table-top sessions or demonstrations. However, it does provide the context for these steps. The EU TEF provides an overview of how to go from one prioritized vulnerability to asking the commercial market for solutions to protect a PSOI against a terrorist attack.

The EU TEF describes an evaluation process for one prioritized vulnerability. If a municipality wishes to address multiple vulnerabilities, multiple instances of the framework should be executed. These multiple instances can however be executed simultaneously, possibly by the same team, possibly using some common knowledge, and possibly combing some activities such as carrying out a demonstration.

A final note: detailed information on the five cities' vulnerabilities should be considered confidential information. In executing the EU TEF – a municipality should carefully consider which (generalised) information is made available either online or to third parties.

1.5 Contributions to Technology Evaluation Framework

The framework that lies before you, has been created by TNO and KEMEA, with input from the whole PRoTECT consortium. This framework aids local authorities, in charge of the security in crowded public places, to identify solutions for mitigating vulnerabilities regarding terrorist attacks.

One of the missions of TNO is to help advance innovations leading to a more secure society. TNO has the capability to apply theoretical risk management knowledge and technology expertise for solutions in complex and practical situations.

The Centre for Security Studies (KEMEA) is a thinktank on homeland security policies and an established research centre, within the Hellenic Republic's Ministry of Citizen Protection, aiming to support security policy implementations at a strategic level. A main objective of KEMEA is to bring together all national Law Enforcement Agencies (Police, Fire Service, Civil Protection, etc.) and to enable them to collaborate, interconnecting them with corresponding agencies, research institutions and the industry from around Europe.

1.6 Reader's guide

Chapter 2 describes how to prepare before executing the framework. In Chapter 3 each of the eight steps are described in detail. Chapter 4 briefly mentions what steps can be undertaken after completing the framework. And finally, Chapter 5 concludes this document.

2 Getting started

2.1 Overview

This chapter explains how to evaluate solutions which are being considered to mitigate a vulnerability (i.e. a weakness in or an absence of a security measure, such as the absence or vehicle barriers or measures to prevent overcrowding) concerning a municipality's Public Space of Interest (PSOI). The existence of such a vulnerability could contribute to a (partially) successful execution of a terrorist attack.

The five PRoTECT municipalities identified vulnerabilities in their PSOIs using the EU Vulnerability Assessment Tool (EU VAT) as explained in the EU VAT manual [13]. With the EU Technology Evaluation Framework (EU TEF), a municipality can determine to what degree existing solutions could mitigate a vulnerability. The framework is executed for just one vulnerability at a time. The outcome consists of recommendations concerning the use of the evaluated solution(s) to mitigate the vulnerability.

The general functions of the EU VAT, the EU TEF and their relation are given in Figure 1.

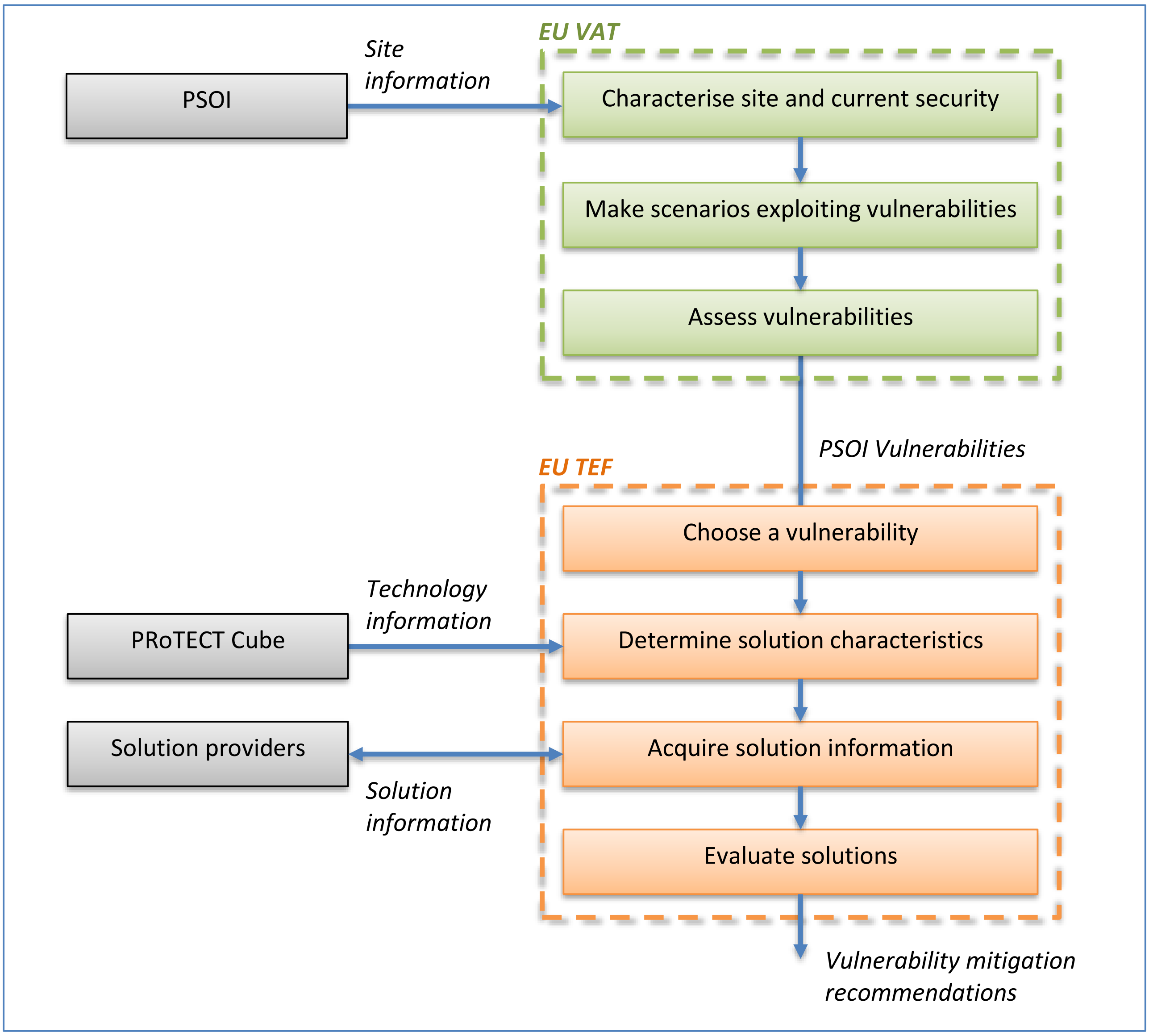


Figure 1 Vulnerability assessment and technology evaluation processes

The framework focusses on selecting and evaluating solutions for vulnerabilities. Solutions using different types of technology can be compared as the evaluation criteria used in the framework are not designed to be technology specific. Solutions are evaluated and compared using results from solution information analyses, results from operational exercises and results from demonstrations.

The framework is intended to be executed by a team, under the leadership of a municipality and possibly involving external partners. During the execution of the framework various team members, each with their own expertise, will need to meet a few times to discuss goals and requirements for the various forms of solution evaluation (i.e. an evaluation of solution information, of solution operational use, and of solution demonstration results). Together with the fact that there are multiple interactions with solution providers means that executing the framework could take a few months.

An important function of this framework is making the team aware of the fact that they should record the argumentation of their decisions along the way. This will facilitate any successive auditing processes or adaptation due to changed circumstances.

This framework should be seen as a guideline to perform the various evaluation activities. It may not be necessary to carry out all the activities mentioned here or all the parts of each activity. It will be up to the municipality to decide to what extent the framework will be used.

The framework uses an example to illustrate some of the steps. The example is the case where a venue might become too crowded and form a risk in the case of a terrorist attack. A need for a solution to count people, either on a square or at entrances to a square, was established.

2.2 Managing body

The framework assumes that the PSOI's managing body (within PRoTECT, this is one of the five municipalities), with its relevant stakeholders, have some existing security strategy pertaining to the main site, the surrounding sites and/or the activity taking place at the PSOI, and that the main site needs to be secured either for a new event, lasting for a predetermined limited period of time (e.g. for a concert or a fair), or continuously from now on (e.g. a city square or train station). There could be a need for updating the existing security plan or making a security plan from scratch.

In the context of PRoTECT, The PSOI's managing body has previously led a team of experts to ascertain the vulnerabilities of a PSOI, using the EU VAT. The managing body can now initiate the process of finding, evaluating and selecting solutions to address the vulnerabilities. The managing body cannot perform this task by itself and will need the cooperation of various professionals, as was the case for the vulnerability assessment. This asks for time from different experts as well as the managing body itself. The EU TEF is a guideline and the managing body should decide who is needed and in what way they want to perform the steps. Please consider that this might take up quite a lot of time and every managing body should decide on a plan that is workable and actionable to them.

The framework can guide the managing body through the process of finding and evaluating solutions for mitigating a vulnerability. Once the managing body has found a viable solution, it can be incorporated into the security plan. This however, is outside the scope of the PRoTECT project duration.

Before using the framework, the actions detailed in the following sections need to have been addressed by the managing body.

2.3 The vulnerability

A **vulnerability assessment** regarding the PSOI needs to have been completed. Though not mandatory, it is assumed in this document that the EU VAT was used to derive the PSOI's vulnerabilities, whereby several

Vulnerability Assessment Records would have been completed (i.e. the template in Appendix A of the EU VAT manual). In doing so, the team of experts assigned to carry out the assessment would have already performed various tasks which are also relevant for conducting a solution assessment (such as establishing the organisation responsible for defining, managing and securing the PSOI, establishing stakeholders, event plan and timelines, budgets, etc).

2.4 Procurement

The framework is not intended for use in the context of a procurement process. However, there are at least the following two important reasons why the managing body should involve a member of municipality's procurement staff in some parts of the framework execution:

- **Fairness towards solution providers**. A procurement officer has the knowledge to determine whether the evaluation process involving solution providers (i.e. companies) and the information exchanged with them does not mislead or bias any particular provider or group of providers.
- **Diminish chance of legal issues**. The procurement officer can make sure it is sufficiently clear for providers that the evaluation is not a procurement and that communications to providers can never be interpreted as being part of a procurement or cause legal issues. In the case that a municipality does decide – after an evaluation – to initiate a procurement based on the results of the evaluation, a procurement officer can best insure that no legal troubles for the municipality will come from the earlier selection and evaluation of solutions (i.e. involving commercially available products).

In general, the procurement officer will only need to be informed and possibly review some activities and communications of the team executing the framework.

2.5 Team of experts

To execute the framework, **a team of experts** should be established by the managing body. The team could possibly consist of the same members of the team involved in carrying out the vulnerability assessment.

One of the team members should be assigned the position of evaluation **coordinator** – someone monitoring the correct execution of the framework, planning meetings, documenting the outcome of each step mentioned in the framework, etc. Before starting each step, the coordinator should verify that all required information is available (e.g. results from the previous session, etc) and that the relevant experts are involved for each step.

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

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

- **Police tasks**: tactical and operational tasks and requirements of the police involved in protecting the PSOI
- **Evaluation coordination**: mandate from the municipality to organise the evaluation, coordination skills

Not all the above-mentioned skills may be relevant considering the solutions to be evaluated, and it is possible that a team member could possess multiple skills. Furthermore, these skills will not be required for every step in the framework.

It is important that the organisation of the team and stakeholders is clear. Summarizing the organisation in a diagram is recommended. An example of such a diagram is given in Figure 2.

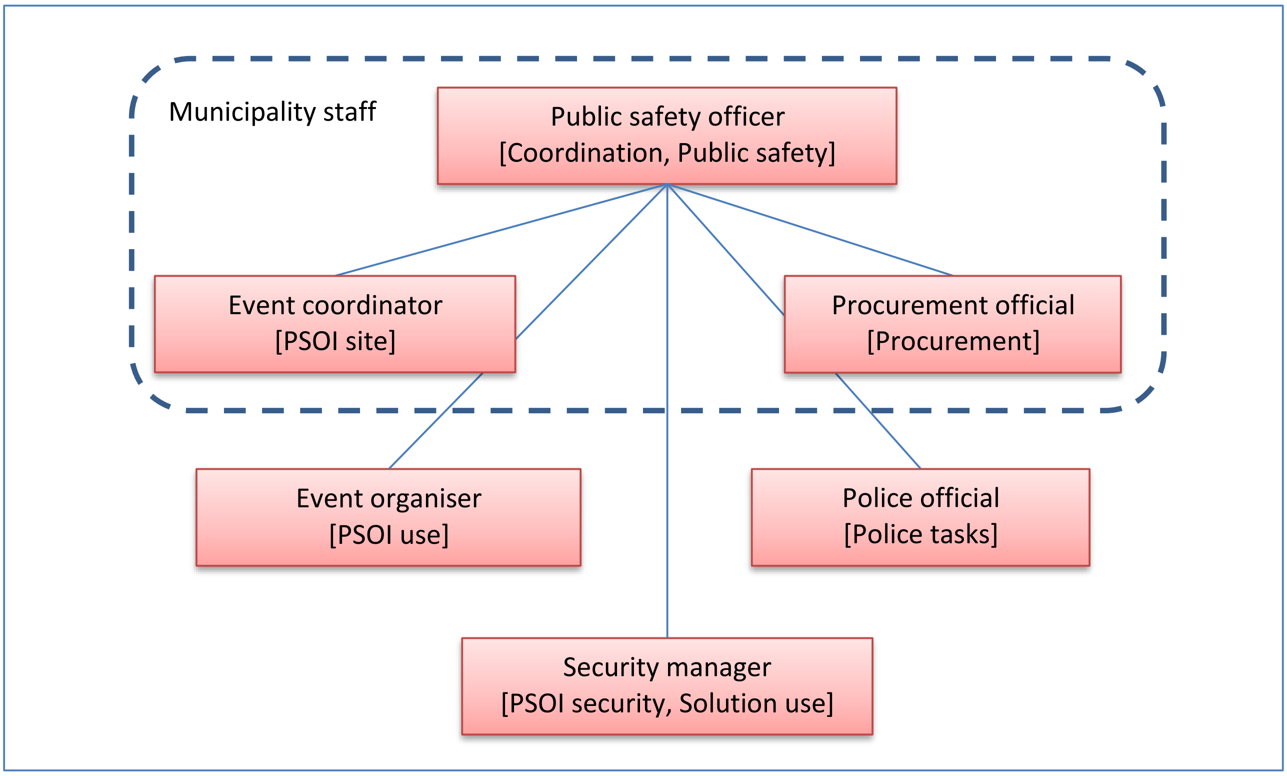

Municipality staff
Public safety officer [Coordination, Public safety]
Event coordinator [PSOI site]
Procurement official [Procurement]
Event organiser [PSOI use]
Police official [Police tasks]
Security manager [PSOI security, Solution use]

Figure 2 Example of a team organisational structure for the framework execution

2.6 Work method

A **work method** should be decided upon by the managing body. Decide and plan how the team of experts will conduct the solution evaluation. There are many ways to do this, but it is assumed that at some time the framework will be used during team sessions. At least for the actual evaluation it is important to have all the relevant experts together and organise a local meeting / workshop (this could be done quite similar to the EU VAT workshops).

The framework will require a great deal of interactivity by all members of the team during the evaluation. It is estimated that different members of the team will need to meet several times while using the framework. The number of meetings required depends on the expertise required at the meeting, how many (different) solutions need to be evaluated, the degree to which information is available (type and quality of information from solution providers), the number of stakeholders involved (and their preconditions and requirements), degree of repetitiveness, the experience of the team and other factors. The number of meetings required, plus the proposed interactions with solution providers, means that executing the framework could take between 3 and 6 months to complete.

A kick-off session could be held before commencing the framework, in which among others the steps and timeline are explained to the team of experts. If the team members are familiar with the process of the EU VAT execution, the kick-off could be combined with the first step of the framework.

Not all the steps, or all the tasks described in each step, are mandatory. The choice of steps and tasks within the steps to be executed, depends on the vulnerability to be mitigated, the nature of the solution and constraints such as time or budget.

Either or both evaluation steps concerning the operational use and the demonstration may not be necessary depending on the nature of the solution (e.g. software may not need to be demonstrated if its functioning has already been proven). These two steps may be done in parallel if there are no dependencies between them. Executing these steps sequentially can provide go/no-go moments in the framework.

The next chapter holds the steps of the EU TEF.

3 Evaluation framework steps

The steps to be taken by a PRoTECT municipality to find and evaluate solutions suitable for mitigating a vulnerability, and the information shared between the steps, are summarized in Figure 3.

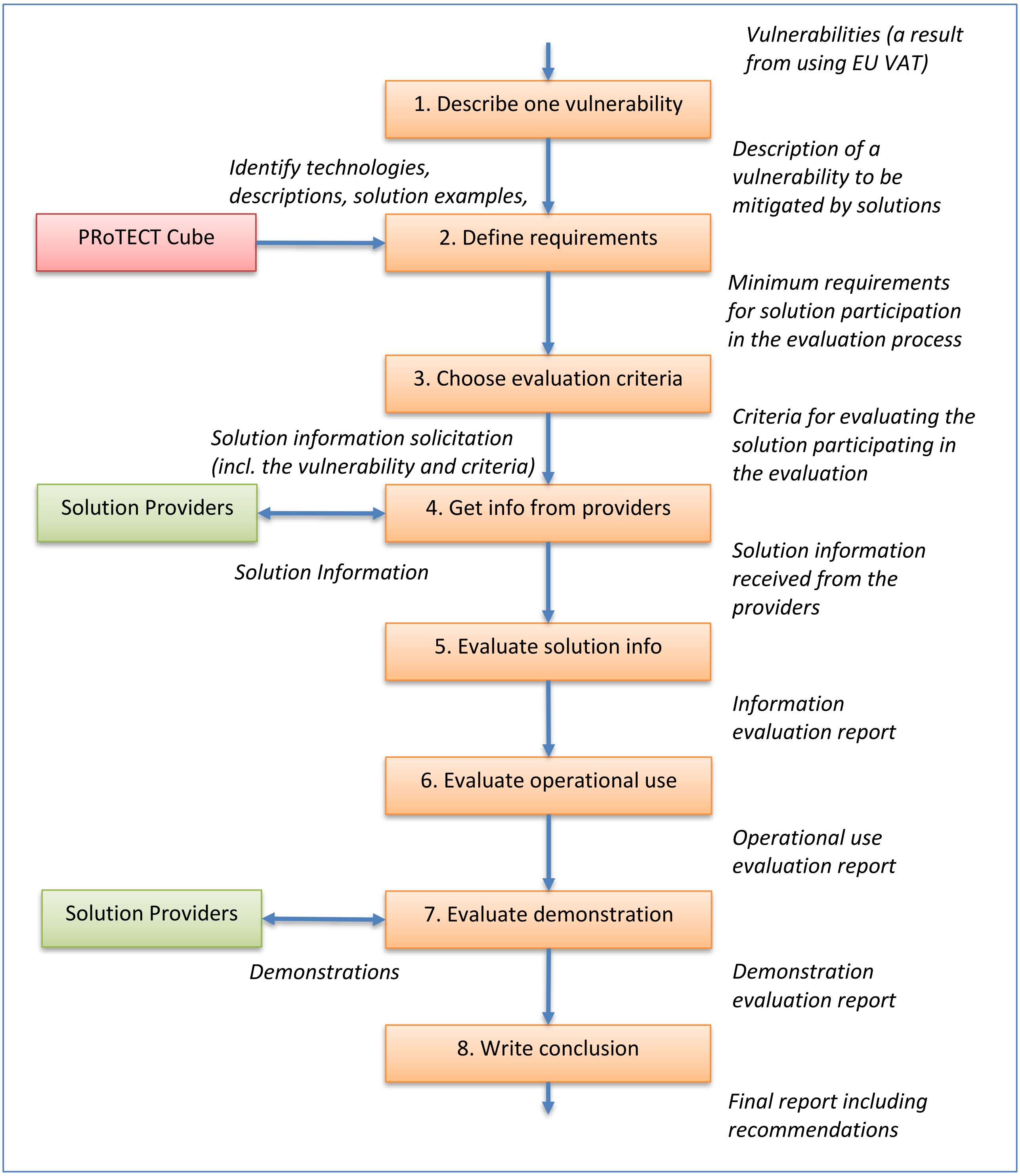
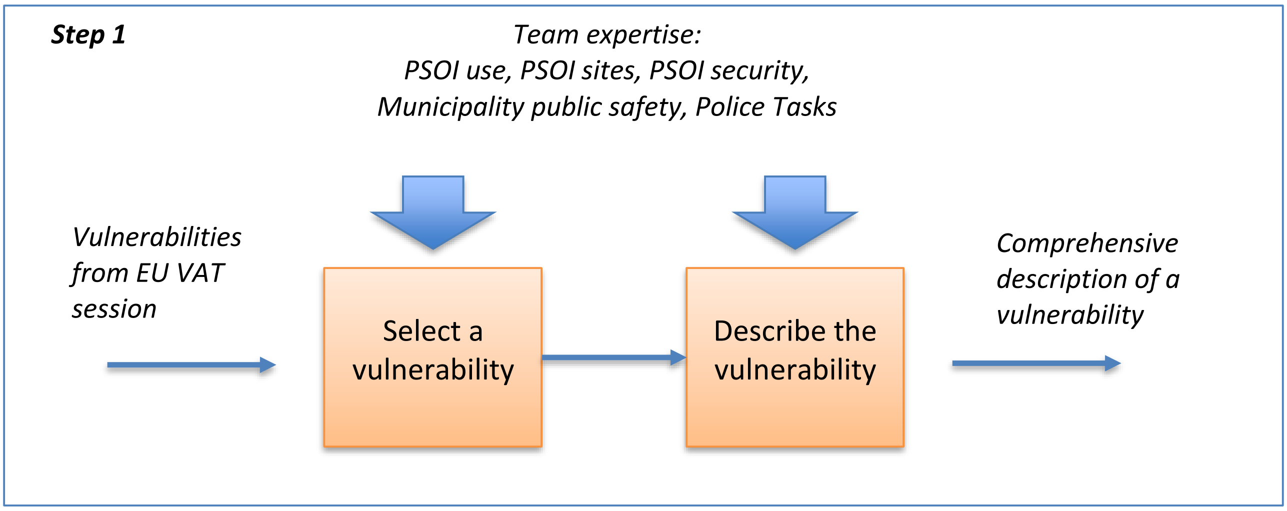

Vulnerabilities (a result from using EU VAT)
1. Describe one vulnerability
Description of a vulnerability to be mitigated by solutions
Identify technologies, descriptions, solution examples,
PRoTECT Cube
2. Define requirements
Minimum requirements for solution participation in the evaluation process
3. Choose evaluation criteria
Criteria for evaluating the solution participating in the evaluation
Solution information solicitation (incl. the vulnerability and criteria)
Solution Providers
4. Get info from providers
Solution Information
Solution information received from the providers
5. Evaluate solution info
Information evaluation report
6. Evaluate operational use
Operational use evaluation report
Solution Providers
7. Evaluate demonstration
Demonstrations
Demonstration evaluation report
8. Write conclusion
Final report including recommendations

Figure 3 Framework steps

Each of the following sections describes a step of the evaluation framework.

3.1 Step 1: Describe the vulnerability


Step 1
Team expertise:
PSOI use, PSOI sites, PSOI security,
Municipality public safety, Police Tasks
Vulnerabilities from EU VAT session
Select a vulnerability
Describe the vulnerability
Comprehensive description of a vulnerability

The first step, to be carried out by the team of experts, consists of selecting and describing a vulnerability in such a way that it is suitable to be issued to solution providers and possibly also to other external entities involved in the evaluation process.

All the information gathered in this step, is based on the EU VAT outcome – the vulnerability does not have to be re-assessed. The purpose of this step is to elaborate on the selected vulnerability in such a way that there is enough information for a provider to offer an appropriate solution (during the RfI, described in Step 4) [3].

3.1.1 Select a vulnerability

The municipality would have produced a number of Vulnerability Assessment Records for a PSOI (using the template in Appendix A of the EU VAT manual). Each record has a section "Scenarios per threat type" in which scenarios exploiting a vulnerability in the PSOI's security are described, supplemented with the results of a risk assessment per scenario. The municipality should decide for which of the scenarios a solution evaluation is necessary. This could for instance be based on a prioritisation of the results of the risk assessments (i.e. over all the Vulnerability Assessment Records for the PSOI), for instance focussing on one of the identified high-risk threat types.

The chosen vulnerability scenario will be specific for a certain event and a certain site (the PSOI venue). It will generally not be desirable to make this information known outside the team of experts as this kind of information is usually considered confidential, and may already have been labelled with a classification during the execution of EU VAT. The managing body will generally be responsible for determining the classification of information during the executing the EU TEF too (possibly advised by the team) and should review any information before it is sent to solution providers (or anyone else outside the team of experts). A signed non-disclosure agreement between the solution provider and the PRoTECT consortium (represented by the respective city) could be requested to handle the confidential information to be provided.

[3] This vulnerability description should be used in PRoTECT WP 4.1 for the test case scenarios.

3.1.2 Describe the vulnerability

The purpose of creating a more detailed vulnerability description is to:

- Provide sufficient context for the solution providers (while maintaining the desired degree of confidentiality)
- Provide a basis for operational scenarios used in the table-top exercises (see Step 6)
- Provide a basis for the demonstration scenarios (see Step 7)
- Ensure consistency amongst the various activities within the framework

The vulnerability can be described in more abstract terms (possibly partly fictitious but representative), allowing it to be shared with solution providers, among others, without disclosing sensitive information. Thus, the work done by the team of experts during the EU VAT workshops needs to be translated so it can be made public.

It is strongly advised to be aware of the consequences of placing information on publicly accessible sources (see Step 4). Even though the information itself might not be sensitive, an adversary might be able to create valuable information from a combination of the public announcement and other information, either from Internet or from other sources, revealed either accidentally or on purpose. When choosing what vulnerability to focus on, it is important to discuss what information to provide and what information to leave out.

The vulnerability should be described by the team using the following attributes:

- Short description (as mentioned in the Vulnerability Assessment Record, anonymised if necessary)
- Venue description, as applicable at the time of attack, including:
  - Type and duration of event (e.g. a 3-day festival)
  - Location characterisation (indication of size, surroundings, etc, e.g. a large park in the city, with food stalls and a stage)
  - Visitor characterisation (types, numbers, etc, e.g. thousands of families)
  - Anything else about the venue that might be relevant for the solution evaluation
- Capabilities in which the vulnerability manifests itself (and for which a solution is desired):
  - Planning and management (event organisation and operation, security planning, etc)
  - Intelligence gathering (from social media, etc)
  - Access control (access for persons, vehicles, goods, etc)
  - Threat deterrence (deterring or hindering a terrorist in planning or carrying out an attack)
  - Threat detection (detection of a suspected (imminent) attack; weapons, drones, etc)
  - Threat response (counter measures before an attack occurs, threat elimination)
  - Attack detection (rapid crowd dispersal, screaming, shooting, explosion, etc)
  - Attack response (response during/after an incident, alerting, damage control, emergency response, evacuation, etc)
- Attack scenario, which is a description of events, including:
  - Attack profile (type, motivation, goal, weapons, equipment, etc; e.g. terrorist attempting to drive a truck with explosives onto the venue grounds)
  - Attacker actions (actions undertaken to achieve the goal, e.g. drive through an existing fence)
  - Undesired event (action which is successful for the attacker, e.g. able to breech the fence)
  - Reason for measure failure (why was the attacker (partially) successful; absence or shortcoming of a measure, e.g. fence is too weak to stop a truck)

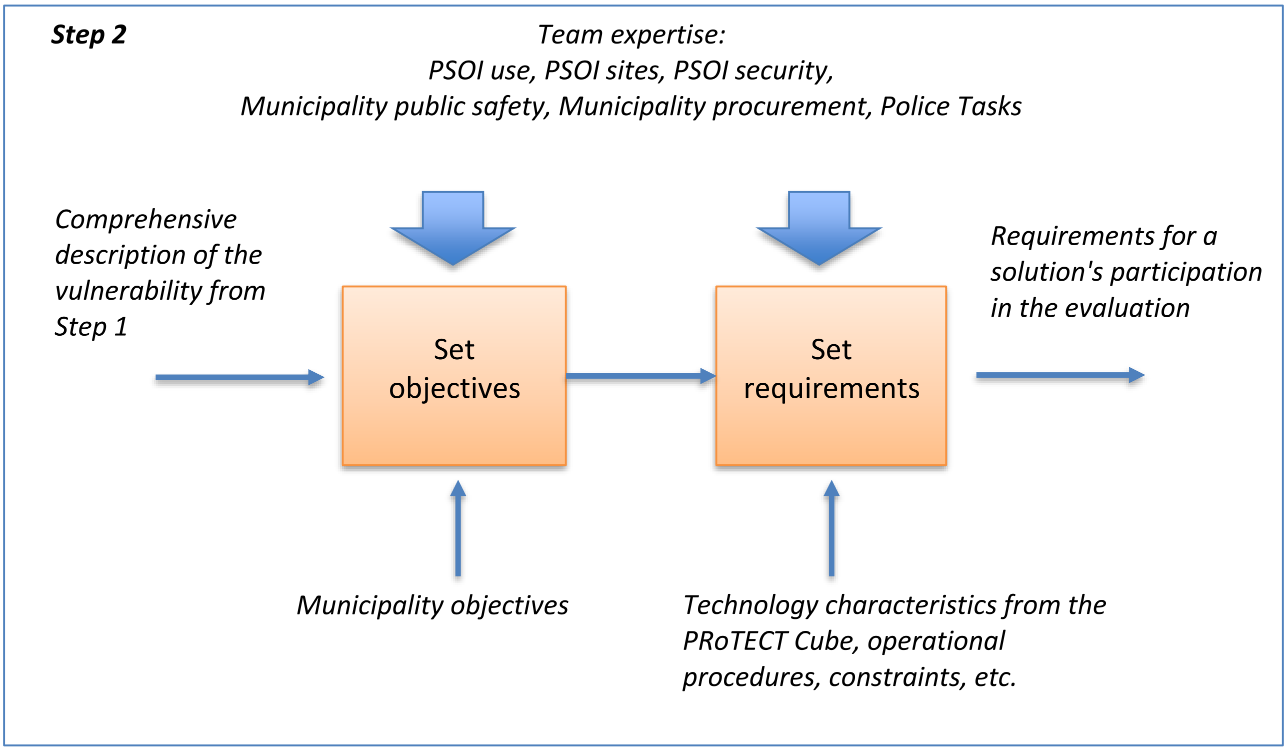
  - Result of undesired event (what happens if the attack is successful, e.g. the explosives if detonated on the ground will cause many deaths)
- Desired scenario, including:
  - Desired event (how should the attack have been stopped, e.g. a more resistant barrier or multiple barriers should replace the fence)
  - Alternatives (other options, if any, to stop the attack from being successful, e.g. placing barriers at other locations further away from the venue with armed guards)
- Dependencies (other influences on the attack or response outcome), including:
  - Other measures present at the PSOI which directly affect (the severity of) the vulnerability (e.g. presence of armed guards who could respond to a breeching of the fence)
  - Public interaction with the measure (e.g. a barrier to stop vehicles might have gaps to allow pedestrians and wheelchairs to pass)
  - Public response to the attack (e.g. the public might need flee through the fence line)
  - Exceptional environmental conditions that need to be considered (e.g. often misty limiting visual verification of an attack)

3.1.3 Result of step 1

This step should result in a document including the following information:

- A vulnerability description, to be used in the solution information solicitation process (Step 4)

3.2 Step 2: Define objectives and requirements


Step 2
Team expertise:
PSOI use, PSOI sites, PSOI security,
Municipality public safety, Municipality procurement, Police Tasks
Comprehensive description of the vulnerability from Step 1
Set objectives
Set requirements
Requirements for a solution's participation in the evaluation
Municipality objectives
Technology characteristics from the PRoTECT Cube, operational procedures, constraints, etc.

In this step, the objectives for the evaluation will be formulated, and requirements will be composed which have to be met by the solution providers to be able to submit solution information for the evaluation (i.e. conditions for participation). The process of acquiring solution information from providers is described in Step 4. This step is aimed at reducing the number of "unusable" responses from providers.

The requirements will generally concern aspects such as timeliness of providing information, conditions concerning confidentiality, conditions for providing a demonstration, minimum solution functionality, etc.

It is assumed that the solutions are commercially available or at least available as a prototype (i.e. to be commercially available soon). This step helps the municipality verify that solutions do exist which could mitigate the chosen vulnerability.

It is also assumed that the team wishes to compare at least two solutions but also no more than a certain maximum. Thus, conditions can be included to limit the number of solutions accepted for evaluation, for instance limiting the number according to order of response, timeliness of response, adequate level of detail of response, etc. Though the framework does not include a procurement process, it is advisable to implement decent procurement ethics. In this light, the method chosen to limit the responses considered, should be clear and communicated to the solution providers during the RfI process (see Step 4).

The PRoTECT cube [14] can be a reference to identify existing solutions and offers various best practices concerning the use of security solutions[4]. These best practices could also guide the team in deciding on solution or provider-related requirements. The Cube also offers some guidance in selecting technologies. The team should be somewhat familiar with the characteristics and availability of the solutions they seek – the Internet is a powerful tool for this.

[4] The PRoTECT cube is a result from PRoTECT deliverable 3.1.

In summary, this step involves:

- Setting objectives for the evaluation
- Optionally limiting technology types
- Setting solution requirements
- Setting solution provider related requirements

This step requires some research work, workgroup sessions, possibly in part combined with the team activity required in Step 1 (describing one vulnerability) or in Step 3 (choosing evaluation criteria). The team coordinator can decide on who should be involved in this step.

3.2.1 Set objectives

The objectives of the evaluation, in a broader context, should be described by the team. The objectives will be communicated to the solution providers when solution information is requested (in Step 4).

There may be various goals the municipality wishes to achieve with this evaluation. It is recommended to mention the higher goals such as ensuring the safety of the public, a desire to increase cost-effectiveness of security measures or improve the emergency service response to an attack, etc.

The lower level goals of the evaluation should also be clear. For instance, stating the immediate necessity to solve a specific security problem (i.e. the vulnerability), or the desire to select the best three solutions for demonstration, or to conduct a proof-of-concept trial, or to ascertain if there are any solutions at all for the given vulnerability, etc. The degree to which these objectives have been met will be assessed at the end of the solution information evaluation (in Step 5).

The solutions that providers offer must satisfy these objectives.

3.2.2 Set requirements

Technology principle requirements

The team could decide to limit the solutions to a specific (type of) technology. Though not necessary, this low-level, technical choice would enable the team to use more technology-specific criteria in the evaluation. If the team chooses to limit solutions, basing them on one or more specific technology types, the following technology types could be considered:

- ICT (for communicating, storing, analysing and protecting information)
  Examples: WiFi, IoT, Encryption, VPN
- Sensors (for detection, identification, localisation, tracking)
  Examples: cameras, facial recognition, acoustic sniper localisation
- Actuators (for warning, intercepting, eliminating)
  Examples: sirens, anti-drone drones, HPM vehicle stopping, guards
- Physical (for controlling access, impeding an attack, protective materials)
  Examples: tourniquets, portable rising steps, bomb blast window film
- Methods (procedures, practices, standards, etc)
  Example: ISO 31000 Risk Management standard

A decision to limit technology types depends on a careful consideration of the vulnerability details as produced in Step 1, such as PSOI site characteristics, current security measures, etc. A Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis could be carried out by the team to compare technology types. The team should document any choices made for future reference.

Solution-related functional and technical requirements

There could also be some general, technology type independent, operational circumstances concerning the solutions which need to be stated as requirements for participation. These will generally be knock-out criteria if not met, the solution provider's response to the RfI will not be considered in the evaluation process.

The following general solution requirements could be considered:

- Required functionality (e.g. must produce a certain output)
- Required interfacing, interoperability with other solutions, or standards
- Required type of user
- Required level of organisational and operational impact
- Required level of maintenance
- Required compliancy to (national) ethical and legal codes
- Etc.

Solution provider-related requirements

Possibly, requirements might be placed on the (type of) solution providers responding to the notice. The providers might have to meet certain pre-conditions which are for instance required by a municipality regulation or required to be able to complete the framework (on time).

The following general solution provider-related requirements could be considered:

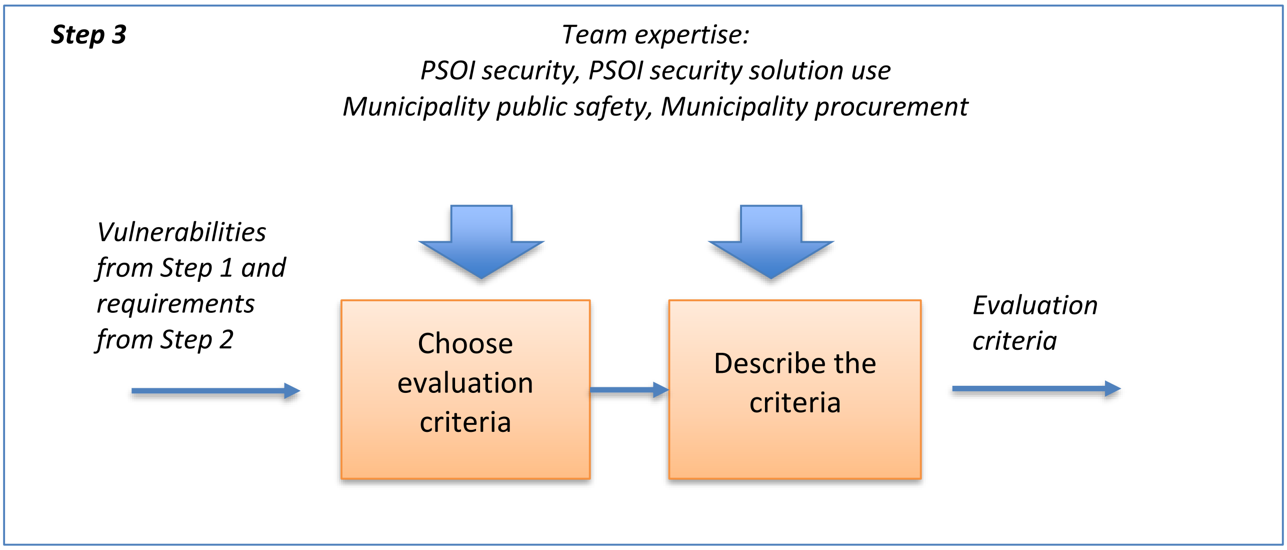
- Minimum provider experience, service organisation, etc
- Minimum security clearance, confidentiality requirements, need for a non-disclosure agreement, etc
- Latest delivery date
- Requirements concerning carrying out a demonstration and costs involved
- Required maximum solution costs (e.g. total cost of ownership)
- Etc.

3.2.3 Result of step 2

This step should be wrapped up with a report on requirements, including the following information:

- The objectives of this evaluation
- The vulnerability description (i.e. a reference to the result of Step 1)
- The requirements for solution information solicitation (Step 4)
- Justification of the choices concerning the requirements (and sources)

3.3 Step 3: Choose evaluation criteria


Step 3
Team expertise:
PSOI security, PSOI security solution use
Municipality public safety, Municipality procurement
Vulnerabilities from Step 1 and requirements from Step 2
Choose evaluation criteria
Describe the criteria
Evaluation criteria

In this step, the team of experts will decide on the criteria for assessing the suitability of a solution in addressing the vulnerability and describe on the basis of which solution information the degree to which the criteria are met will be determined. The selection of criteria depends on the characteristics of the PSOI and of the vulnerability (Step 1) and the requirements for solution participation (Step 2).

The assessment will be based on solution information offered by the providers. The criteria will be communicated to the providers during the solution information gathering process (in Step 4) and used in the solution evaluation process (in Step 5).

3.3.1 Choose evaluation criteria

The team of experts will need to select the most suitable criteria for comparing solutions. Any number of criteria can be selected, but it is important to keep a balance between striving to be efficient (i.e. using a minimum number of criteria, requiring less time but with the risk of ending up with an inadequate comparison) and being thorough (i.e. providing (too) many criteria, requiring more time to process). Generally, choosing roughly 5 to 10 criteria should suffice.

One approach is to have the team brainstorm on all possible criteria and then reduce the list while considering the following aspects:

- Quality:
    - Check that the most important criteria are included
    - The criteria should not be redundant (even partial overlap can influence the evaluation score)
    - Scores assigned to a solution under one criterion may not be affected by the scores assigned under another criterion
    - The criteria must be suitable for evaluating all solutions (i.e. not specific to only some of the solutions)
    - The criteria must have the same meaning for each of the solutions
    - The criteria must be clear and if possible measurable
    - The criteria must be suitable for distinguishing between good and bad solutions

- Applicability:
  - The criteria must be relevant to the vulnerability scenario determined in Step 1
  - The criteria must be in line with the objectives noted in Step 2
  - The criteria must be in line with any minimum requirements set Step 2

Often, when comparing solutions, cost criteria are considered separately from benefit criteria (e.g. performance, operability, etc). In most cases, the real costs of a solution are either quite complicated to calculate (e.g. consider the calculation of costs of civil servant time for implementing a solution) or simply not relevant at this stage of comparing solutions. Also, there can be some dependency between costs and benefits (e.g. a more expensive solution will probably cost more) which could negatively impact the comparison (see the criteria quality aspects mentioned earlier). For PRoTECT it is recommended to exclude cost criteria for the evaluation, but the choice is up to the team. Alternatively, the cost could either be stated as a pre-requisite for participation (i.e. state a maximum cost or factors leading to unacceptably high costs, revisiting Step 2) or costs could be (briefly) considered at the end of the evaluation (either in Step 5 or Step 8).

The following non-exhaustive list of criteria, divided into cost criteria and benefit criteria, could be applicable for the security solutions foreseen in the context of PRoTECT:

- Costs:
  - Total cost of acquisition (TCA)
  - Total cost of ownership (TCO)
- Benefits:
  - Physical (e.g. the team might consider it important that the presence of solution in the PSOI is not too obvious):
    - Volume
    - Weight
    - Dimensions (e.g. height, length, etc.)
    - Robustness (vandal resistance)
    - Visual prominence
  - Compliance (e.g. the team might consider it important that the solution is compliant with privacy legislation):
    - Privacy (e.g. EU GDPR legislation)
    - Security (e.g. antisabotage)
    - Safety (e.g. specific national legislation)
    - Ethics (e.g. municipality policy)
  - Performance (e.g. the team might consider it important that the solution functions reliably):
    - Reliability (e.g. a high detection rate, small chance of malfunction, redundant)
    - Accuracy (e.g. able to count people accurately)
    - Timeliness (e.g. processing time)
    - Capacity (e.g. processing throughput)
  - Environmental (e.g. the team might consider it important that implementing the solution will have no negative impact on the environment):
    - Protection (e.g. against rain, dust, wind, etc.)
    - Emission (e.g. CO_2)

- Operability (e.g. the team might consider it important that the solution is highly user friendly):
    - Usability (e.g. can be operated easily)
    - Staffing (e.g. number of operators required)
    - Deployment (e.g. time necessary to deploy the solution)
- Interoperability (e.g. the team might consider it important that the solution can deliver information which can be used by another system protecting the PSOI):
    - Information (e.g. required by another system or party)
    - Interfacing (e.g. a specific IT-communications protocol)
- Maintainability (e.g. the team might consider it important that the solution can easily be repaired if damaged):
    - Availability (e.g. mean time to repair)
    - Support (e.g. 24-hour service)
- Training (e.g. the team might consider it important that the operators can be trained quickly):
    - Education (e.g. level, duration, course availability, location, etc)
    - Experience (e.g. duration)
- Maturity (e.g. the team might consider it important that the solution is to some degree field proven):
    - Technology Readiness Level (e.g. high TRL)
    - Availability (e.g. development time, time to production)
    - Roadmap (e.g. expected short-term improvements)
- Other (e.g. the team might decide to also consider some general aspects of the solutions):
    - Miscellaneous advantages
    - Miscellaneous disadvantages

The abovementioned list is not complete and is primarily intended as an aid to identify criteria.

Assuming that the team will not select any cost-related criteria, the team can select benefit-related criteria from the third level (e.g. 'Volume' and 'Weight') and grouping the criteria according to headings used on the second level (e.g. 'Physical').

If other, more technology-specific criteria are desired, they could also be grouped under the aforementioned criteria headings.

3.3.2 Describe the criteria

Each criterion should be accompanied by a description, including:

- A definition of the criterion, including a scope if necessary (e.g. 'Maintainability' could be defined as the degree to which the system can be repaired, or for instance the effort required to keep the system ready for use, etc)
- An explanation of how the criterion will be evaluated (e.g. for 'Maintainability', the lesser the effort required to maintain the system the higher the score for this criterion)
- Why the criterion is important for the municipality (e.g. for 'Maintainability' is could that the municipality wishes to ensure that the system will always be ready for use')
- Possibly also include an indication of which (type of) information about the solution needs to be provided in order to evaluate the criterion (e.g. Maintainability will be assessed on various aspects

but mainly concerning the effort required by the municipality and the provider to keep the system available for use)

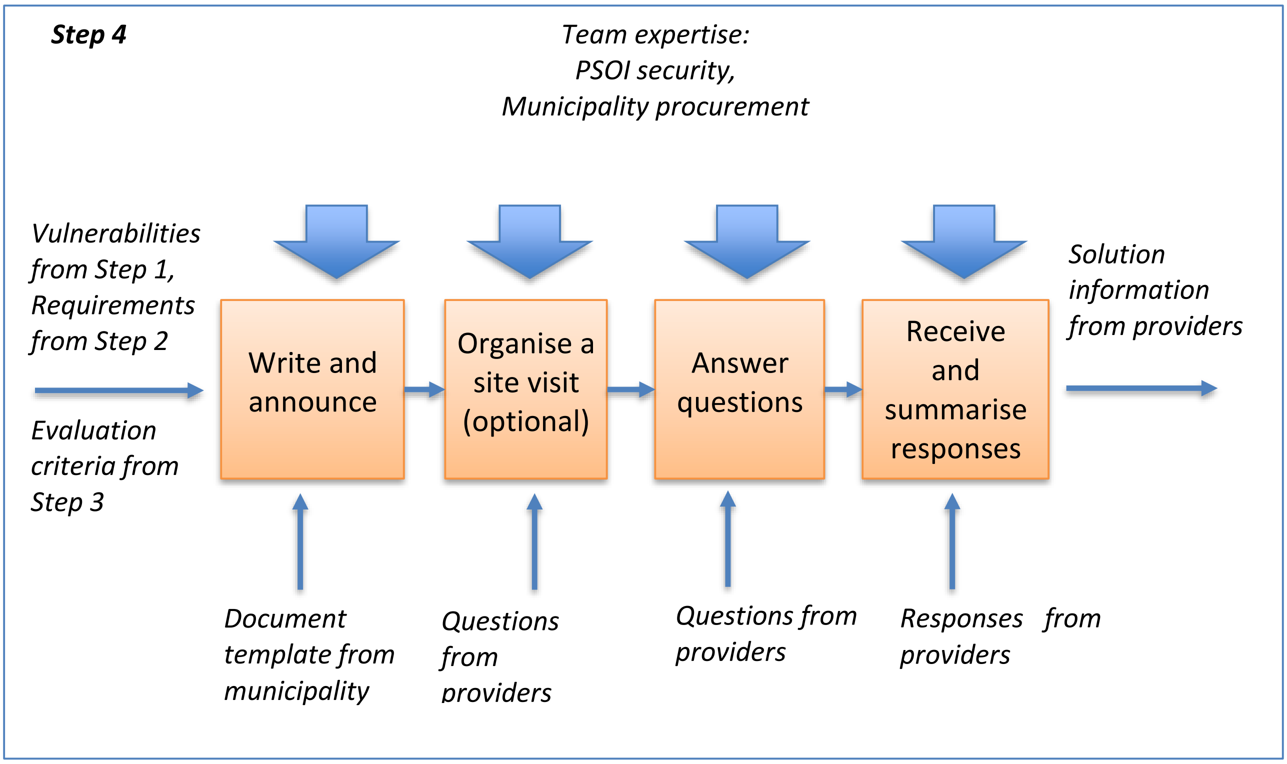
These descriptions are primarily intended as guidance for the solution providers in offering information (in Step 4). These descriptions will also help ensure that each team member judges each criterion correctly during the evaluation (in Step 5).

3.3.3 Result of step 3

This step should be wrapped up with a report on the criteria selection, including the following information:

- A list of evaluation criteria (and their descriptions), for use in Step 4 and Step 5
- How the criteria were selected
- Possibly a summary of important aspects which contributed to the selection of criteria

3.4 Step 4: Gather solution information


Step 4
Team expertise:
PSOI security,
Municipality procurement
Vulnerabilities from Step 1, Requirements from Step 2
Evaluation criteria from Step 3
Write and announce
Organise a site visit (optional)
Answer questions
Receive and summarise responses
Solution information from providers
Document template from municipality
Questions from providers
Questions from providers
Responses from providers

In this step, a Request for Information (RfI)[5] will be carried out to gather information on solutions which might mitigate the selected PSOI vulnerability (selected in Step 1). Certain requirements (from Step 2) should ensure that only useable responses will be received.

A municipality will compose a document and disseminate it to solution providers through a wide range of channels (including, among others, the PRoTECT project website and social media) in order to maximise participation in the process. The responses to the announcement will be summarized for evaluation in the next step (Step 5). If beneficial, the solution providers could be offered an opportunity to visit the site (all providers together). The providers should also be offered an opportunity to ask questions about the request.

3.4.1 Write and post the announcement

The RfI announcement should contain the following information[6]:

- Confidentiality (if not already included in the requirements)
- The objectives of and requirements for the evaluation, including knock-out criteria (from Step 2)
- The vulnerability description (from Step 1)
- The evaluation stages:
    - RfI (e.g. the announcement, possibility of a site visit (if applicable), asking questions, etc)
    - The solution information evaluation (i.e. how the solution information will be evaluated using criteria, etc)

[5] A Request for Information (RfI) is a common process often applied in the context of a procurement.

[6] How to write this down is done in T3.3 of the PRoTECT project.

  - Operational exercise (i.e. evaluating the use of the solution in operational scenarios (if applicable))
  - A demonstration (i.e. demonstrating the solution to stakeholders (if applicable))
- Tasks and deliverables (for each stage, the desired cooperation with the solution provider, etc)
- Time line (including deadlines for written questions and for providing the solution information)
- The evaluation criteria, accompanied with a statement that the solution provider must provide concise information concerning these criteria, and notice that weights will be assigned to the criteria later during the evaluation process
- Clarity that this evaluation is not in the context of a procurement
- Any financial and legal aspects (e.g. if the municipality offers a financial contribution for a demonstration)
- Format of response (i.e. possibly a contents table, format for filling in the criteria, etc)
- Municipality contact information

It is advisable that the PSOI procurement person reviews the announcement before it is sent (even though this is not a procurement process, it will guarantee that the RfI is carried out in a fair way).

The announcement can be posted on the PRoTECT website, the municipality's website, distributed via social media or sent directly to solution providers.

3.4.2 Organise a site visit (optional)

In some cases, it might be more practical to let the solution providers see the site concerned than trying to describe it on paper. This is particularly so, when a vulnerability or the solution required is uncommon. A site visit can be organised to accommodate all interested solution providers at once. Attention needs to be paid how questions from the solution providers are answered. It is important that all solution providers hear/read the same answers.

3.4.3 Answer questions

Solution providers should be offered an opportunity to ask questions about the RfI announcement in writing. These questions should be put to the team and all questions and answers should be distributed to all solution providers taking part. If there was a site visit and questions were asked, these questions and answers could also be provided as well.

3.4.4 Summarise responses

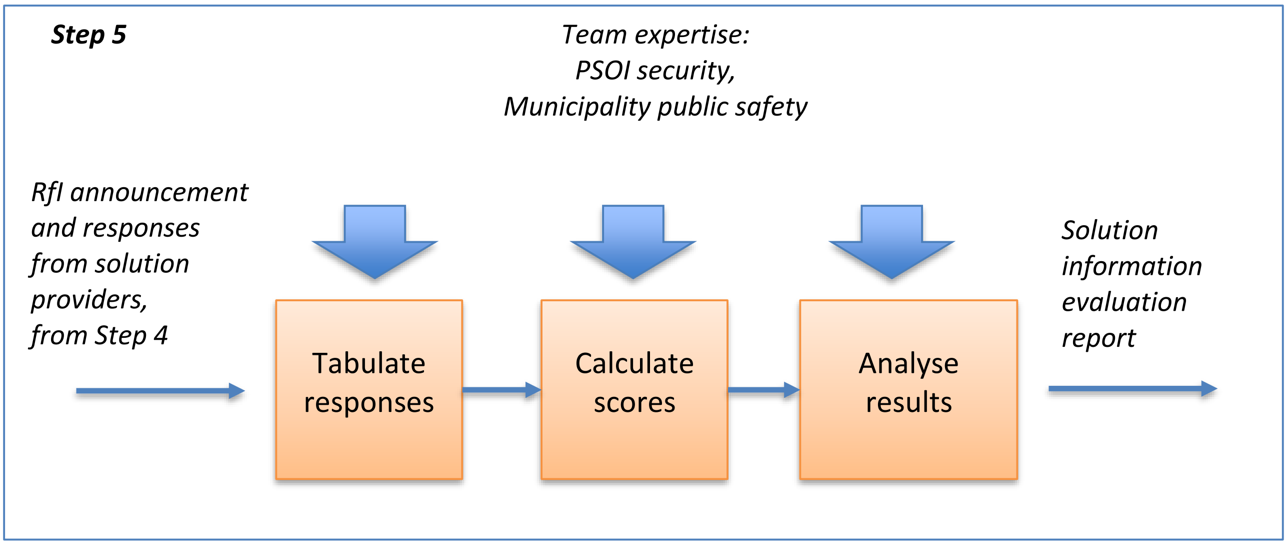
All responses that were received on time, deemed complete and satisfying the requirements (i.e. passing any knock-out criteria), can be bundled for further processing in the next step.

3.4.5 Result of step 4

This step should be wrapped up with a report containing the following information:

- The collected responses from the solution providers, for use in Step 5 (and possibly Step 6 and Step 7)
- A log of questions from the solution providers and the answers given by the team of experts
- A copy of the announcement and amendments made in response to questions from the solution providers

3.5 Step 5: Perform solution information evaluation


Step 5
Team expertise:
PSOI security,
Municipality public safety
RfI announcement and responses from solution providers, from Step 4
Tabulate responses
Calculate scores
Analyse results
Solution information evaluation report

In this step, the solution information received from the providers (in Step 4) will be analysed, and the degree to which each solution meets the criteria (determined in Step 3) will be established. The evaluation method chosen here, a multi-criteria analysis (MCA)[7], will allow solutions to be compared and ranked as options for mitigating the vulnerability. Based on the outcome, the team of experts can decide which solutions qualify for further scrutiny in the remaining steps of the framework (i.e. analysing the operational use and carrying out a demonstration).

The solution information evaluation consists of the following steps:

- Tabulate options and criteria, converting the responses from the providers into a numerical scale
- Determine criteria values
- Assign weights (i.e. priorities) to criteria
- Calculate a score per solution, using weights for each criterion
- Analyse results, verifying that the results are sensible, adjusting weights if necessary
- Draw conclusions, determining further actions

Preferably, a software application like Microsoft's Excel is used to tabulate and calculate the scores. This will also make the analysis of the evaluation results easier.

3.5.1 Tabulate responses

The solutions offered by the providers and the criteria can be placed in a table, whereby each solution option is a row and each criterion a column. As an example, some criteria and options have been tabulated in Table 1.

[7] The evaluation method is based on the Multi-Criteria Decision Analysis (MCDA) method, using a linear additive model [14].

Criteria Options	Compliance		Performance	
	Safety	Security	Reliability	Accuracy
Solution A				
Solution B				
Solution C				

Table 1 Example of options and criteria (for a crowd counting system)

3.5.2 Determine criteria values

To be able to compare solutions, it will be necessary to extract information from each response pertaining to each criterion and assigning a numerical value to the criterion. The value represents the degree to which the criterion is satisfied. The scale could for instance be an integer from 0 to 100, whereby 0 could mean a low degree of satisfaction and 100 a high degree of satisfaction. Using discreet steps such as 0, 20, 40, 60, 80 and 100 is possible.

Extract relevant information

The team members can examine all the information received from the providers, looking for statements which might be relevant for a criterion.

An example of relevant information given by providers, regarding one of the criteria mentioned in Table 1 (Safety), is given in Figure 4.

Information from which the degree of safety compliancy of solution A is deduced:

- *Satisfies the European Low Voltage Directive (2006/95/EC)*
- *Each electrical component carries a CE marking*

Figure 4 Example of solution information

Determine scale

The team must now decide on the scaling to be used for the values which will be given for each criterion per solution.

If a scale from 0 to 100 is chosen for the criteria values, information offered by the providers could be mapped as follows:

- 100 could be assigned to the best possible response for the criterion
- 0 could be assigned to the minimum acceptable response for a criterion

Responses lying in-between, will be linearly transformed into numbers between 0 and 100. Having a linear scale is not mandatory – having a non-linear scale might be beneficial for some criteria.

Determine mapping

The team must map the information from the providers onto the scale.

For the example given in Table 1, and based on some arbitrary solution information (partly given in Figure 4), a linear scaling was chosen, and the information was mapped, as depicted in Figure 5.

Safety:	*Relevant EU standards met ⇒ 100*	*...*	*None ⇒ 0*
Security:	*Relevant EU standards met ⇒ 100*	*...*	*None ⇒ 0*
Reliability:	*Highest detection rate & redundant ⇒ 100*	*...*	*Poor ⇒ 0*

Figure 5 Example of scaling criteria values (crowd control system)

Map information onto scale

The team must now decide on the value to be applied for each criterion and for each solution, keeping in mind the descriptions given for each criterion in Step 2.

It is recommended that the team members first determine the values individually and then, in a group discussion, determine the definite values.

An example of the scaled values is given in Table 2.

Criteria	*Compliance*		*Performance*		
Options	***Safety***	***Security***	***Reliability***	***Accuracy***	
Solution A	*50*	*75*	*0*	*50*	
Solution B	*25*	*75*	*75*	*100*	
Solution C	*80*	*50*	*75*	*0*	

Table 2 Example of options and criteria, with scaled values

3.5.3 Assign weights (optional)

The team must now decide if certain criteria are more important than others. If not, this section can be skipped.

If weighting is to be applied, the team could consider carrying out this task as part of Step 2, and making the weights known to the solution providers. This increases transparency towards the solution providers.

A weight can be assigned to a criterion to increase or decrease its importance in relation to the other criteria. Assigning a weight, is carried out in two stages: determine the importance using a grade, then calculate the relative weight.

Determine importance

For each criterion, the team can indicate how important the criterion is. This is done by first choosing the most important criterion and giving it the highest grade. It is suggested to use a simple grading system, for instance 1 to 10, whereby 10 is given to the criterion which is considered the most important. Once the most important criterion has been given a 10, the other criteria can be compared with most important one and given grades accordingly.

It is recommended that the team members first determine the importance individually and then, in a group discussion, determine the definite importance grades.

Convert grades into weights

The weights for the criteria are determined by distributing 100 points over the criteria according to the importance grades. This is done by using the following formula for each criterion:

Criterion weight = 100 x Importance grade / Sum of all grades

An example of converting importance grades into weights, for the criteria in Table 2, is given in Figure 6. In this example, 'Accuracy' was deemed the most important criterion and given 10 points.

Safety:	*Importance grade = 2.5*	⇒	*100 x (2.5/20)*	⇒	*Weight = 12.5*
Security:	*Importance grade = 2.5*	⇒	*100 x (2.5/20)*	⇒	*Weight = 12.5*
Reliability:	*Importance grade = 5*	⇒	*100 x (5/20)*	⇒	*Weight = 25*
Accuracy:	*Importance grade = 10*	⇒	*100 x (10/20)*	⇒	*Weight = 50*

Figure 6 Example of determining a weight from the importance

Subsequently, the weights from Figure 6 have been added to Table 2, giving the result shown in Table 3.

Criteria	*Compliance*		*Performance*		
Options	***Safety***	***Security***	***Reliability***	***Accuracy***	
Solution A	*50*	*75*	*0*	*50*	
Solution B	*25*	*75*	*75*	*100*	
Solution C	*80*	*50*	*75*	*0*	
Weight	***12.5***	***12.5***	***25***	***50***	*= 100*

Table 3 Example of options and criteria, with scaled responses and weights

3.5.4 Calculate scores

Once the weights have been determined, the team can proceed to calculate the score per solution. The score for each solution is the sum of each criterion value for that solution times the criterion weight/100. The highest a solution can score, is 100. For the example given in Table 3, the score for Solution A is calculated as given in Figure 7.

$$\begin{aligned}\text{Score Solution A} &= 50 \times 12.5/100 + 75 \times 12.5/100 + 0 \times 25/100 + 50 \times 50/100 \\ &= 6.25 + 9{,}375 + 0 + 25 \\ &\approx 41\end{aligned}$$

Figure 7 Example of score calculation

In Table 4 the scores for all solution options mentioned in the example of Table 3 are given (truncated to whole numbers).

Criteria	Compliance		Performance		
Options	Safety	Security	Reliability	Accuracy	Score
Solution A	50	75	0	50	41
Solution B	25	75	75	100	81
Solution C	80	50	75	0	35
Weight	12.5	12.5	25	50	

Table 4 Example of options and criteria, with scaled responses, weights and scores

From Table 4 it can be concluded that Solution B has by far the highest score, followed by Solution A and then a little further away, Solution C.

3.5.5 Analyse results

Quick check

The team should briefly check if the score outcome seems logical and intuitive (i.e. can be explained). If not, maybe the scores need to be re-calculated. Looking at the example in Table 4 (considering the values, weights and scores), it can be logically concluded that Solution B is the best option and that Solution C is not.

Sensitivity analysis

Furthermore, the team could discuss if a "sensitivity analysis" needs to be performed. In a sensitivity analysis, the team would determine how sensitive the score outcome is – especially concerning the ranking order of the scores – to changes in the scoring, the scaling or the weighting. This is particularly of interest when the team only wishes to select one solution while the top scores lie very close together.

If the team wishes to perform a sensitivity analysis, it usually involves the following:

- Adjusting weights slightly and observing the effect on the outcome will give insight into the sensitivity of the result to these changes
- If changing weights has an unsatisfactory or unexplainable effect on the outcome, then verify that the chosen scaling is correct or examine the effect of changing the scaling (i.e. consider changing the designation of 0 and 100 or consider using a non-linear scale)
- It is quite possible that after some sensitivity analysis, some solutions can be declared as being equal.

The amount of time spent on a sensitivity analysis – in any – depends on the initial scores, the use of the scores, the importance of the evaluation, and the time available to the team. Some degree of analysis could however be carried out as an extra check.

Further analysis of the sensitivity of the outcome to variations in the scoring, if necessary, can be carried using sensitivity analysis methods described in [14].

Grouping

If a large number of solutions are compared, it might be advantageous to group the solutions, based on their scores, into categories, like "Low", "Medium" and "High". This might be useful if a limited number of solutions needs to be selected for a demonstration.

Recommendations

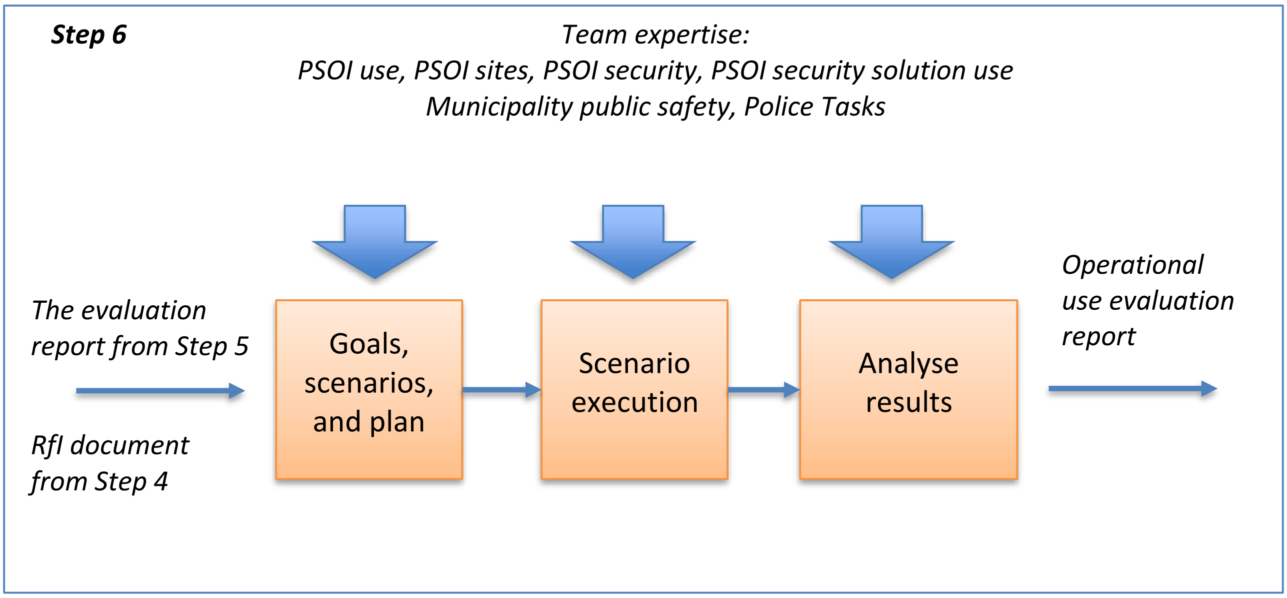
Team can discuss which recommendations need to be made for further evaluation or use of the solution (i.e. in the evaluation of operational use or in the demonstration). The recommendations could concern suggested improvements to the solution (e.g. regarding the example in Table 4, it could be suggested that the safety of the system needs to be improved before further use) or for instance that further information is needed on a particular aspect.

3.5.6 Result of step 5

This step should be wrapped up with a report containing the following information:

- The vulnerability details from Step 1 (as context)
- The table containing the scores
- A log of any changes in criteria, scaling or weights and why the changes were made
- The conclusion of the solution information evaluation, including recommendations

3.6 Step 6: Perform operational use evaluation


Step 6
Team expertise:
PSOI use, PSOI sites, PSOI security, PSOI security solution use
Municipality public safety, Police Tasks
The evaluation report from Step 5
RfI document from Step 4
Goals, scenarios, and plan
Scenario execution
Analyse results
Operational use evaluation report

This step involves the planning and execution of a workshop in which the solutions offered by the providers with be evaluated in a table-top exercise.

Generally, this could be seen as an optional step, depending on the necessity or practicality of carrying out this type of evaluation and the results from the RfI. In the context of PRoTECT however, this step will be carried out.

A team session may be carried out to evaluate the functioning of the solution in an operational setting, whereby operational scenarios are used, based on the vulnerability scenario described in Step 1. The operational scenarios are played out, for instance in a table-top session[8] or a workshop[9], with the relevant stakeholders taking part (outside the team of experts). The operational use will also be evaluated (for which goals will be defined).

3.6.1 Activities of Step 6

In general, the following activities are carried out by the team to complete this step:

- Set goals, write operational scenarios, make a plan (who does what, where, when, etc)
- Execute the scenarios with team members and possibly some stakeholders
- Analyse the results in a discussion with the team members

Only an outline of what this step entails is provided here – a detailed description of this process will be devised by the appropriate PRoTECT Work Package team (WP 4) and provided to the municipalities in the form of a separate PRoTECT document.

[8] Tabletop exercises are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator guides participants through a discussion of one or more scenarios.
(Source: https://www.ready.gov/business/testing/exercises)

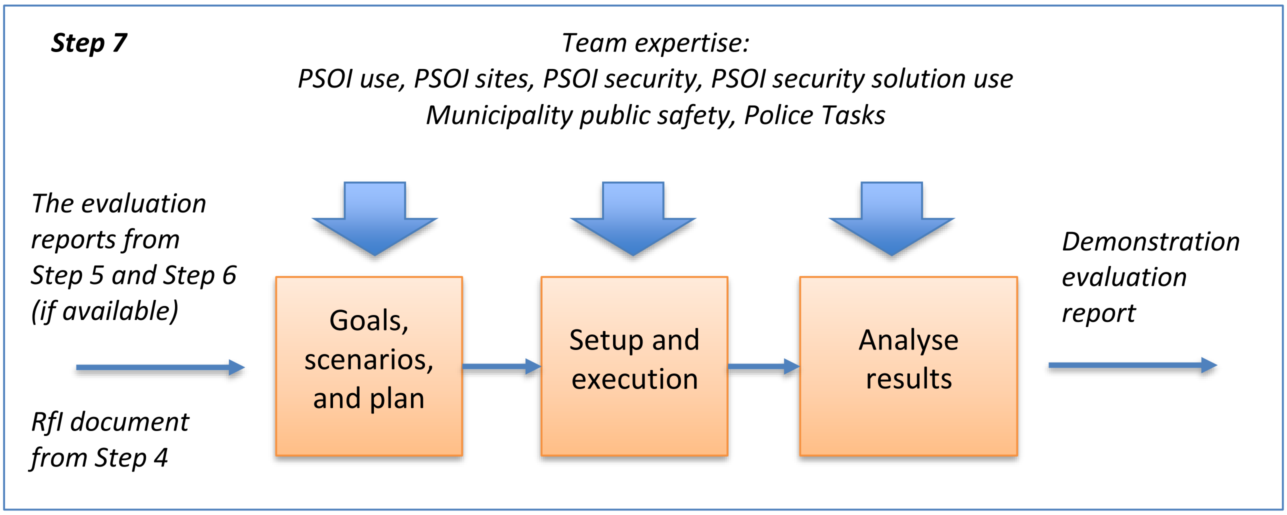
[9] In the PRoTECT project, a municipality can decide whether to perform a table-top session choose another work method for evaluating the operational use.

3.6.2 Result of Step 6

This step should be wrapped up with a report containing the following information:

- The vulnerability details from Step 1 (as context)
- The goals of and scenarios for the operational use evaluation
- The result of the operational use evaluation
- A log of any changes made to the scenarios and why
- The conclusion of the solution operational use evaluation, including recommendations

3.7 Step 7: Perform demonstration


Step 7
Team expertise:
PSOI use, PSOI sites, PSOI security, PSOI security solution use
Municipality public safety, Police Tasks
The evaluation reports from Step 5 and Step 6 (if available)
RfI document from Step 4
Goals, scenarios, and plan
Setup and execution
Analyse results
Demonstration evaluation report

This step involves the planning and execution of a demonstration of the solutions offered by the providers.

Generally, this could be seen as an optional step, depending on the necessity or practicality of carrying out this type of evaluation and the results from the RfI. In the context of PRoTECT however, this step will be carried out.

A demonstration will be arranged together with the solution provider. There could be more than one demonstration if more solutions are to be demonstrated (based on the result from the solution information evaluation (Step 5). The goals for a demonstration must be clear, and a demonstration is executed following one or more scenarios, which might have been derived from the operational use workshop (Step 6) or from the vulnerability scenario (Step 1). A solution provider should be granted the opportunity to setup and configure their solution. The demonstration should be attended by the stakeholders. Feedback on the demonstration is gathered, analysed and documented.

3.7.1 Activities of Step 7

In general, the following activities are carried out by the team to complete this step:

- Set goals, write demonstration scenarios, make a plan (who does what, where, when, etc)
- Prepare for the demonstration and execute the scenarios
- Analyse the results in a discussion with the team members

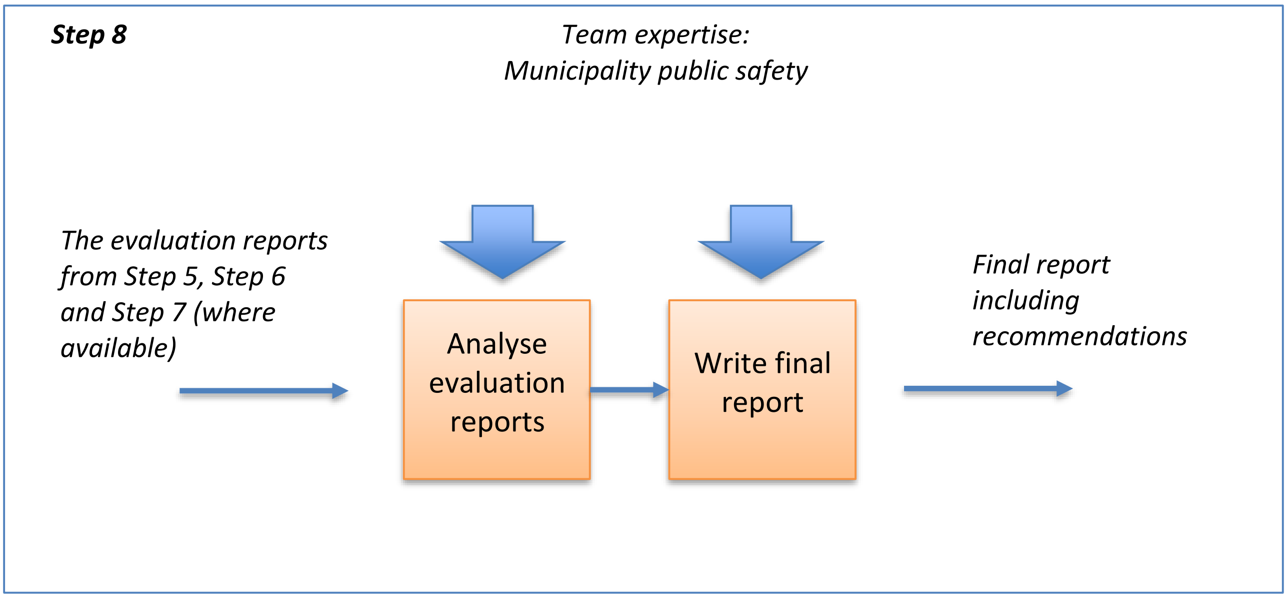
Only an outline of what this step entails is provided here – a detailed description of this process will be devised by the appropriate PRoTECT Work Package team and provided to the municipalities in the form of a separate PROTECT document.

3.7.2 Result of Step 7

This step should be wrapped up with a report containing the following information:

- The vulnerability details from Step 1 (as context)
- The goals of and scenarios for the demonstration
- The result of the demonstration
- A log of any changes made to the scenarios and why
- The conclusion of the demonstration evaluation, including recommendations

3.8 Step 8: Analyse results and write report


Step 8
Team expertise:
Municipality public safety
The evaluation reports from Step 5, Step 6 and Step 7 (where available)
Analyse evaluation reports
Write final report
Final report including recommendations

In this final step of the framework, all evaluation reports, i.e. from the solution information evaluation (Step 5), the operational use evaluation, if available (Step 6) and the demonstration evaluation, if available (Step 7) are discussed by the team. The results are weighed, and the findings are established. Conclusion and recommendations are written in a final report.

3.8.1 Analyse evaluation reports

The team should determine for each result of the evaluation reports from step 5, step 6 and/or step 7, to what degree the goals were met, the consequences of any shortcomings found in the solutions, identifying any lessons learned from executing the framework, etc.

The team should discuss the results from all the reports and form an opinion on the solution's suitability to mitigate the vulnerability and draw conclusions. Recommendations should also be discussed on further implementation of the solution, including more research if necessary.

3.8.2 Write final report

The findings from the solution information evaluation, the operational use evaluation and the demonstration evaluation should be summarised in a final report, including the conclusions and recommendations.

3.8.3 Result of Step 8

This step should be wrapped up with a report containing the following information:

- The vulnerability details from Step 1 (as context)
- Documentation of, or references to, all steps taken in the framework
- The considerations in the analysis of the evaluation reports
- To what degree the goals have been met, which were set in Step 2
- The conclusion including recommendations

4 What's next

The municipality should decide who will receive the final report within the municipality or potential stakeholders, and what further actions are to be taken in response to the conclusions and recommendations stated in final report (produced in Step 8 of EU TEF). The municipality may for instance decide that a procurement process is to be started for the acquisition of a such solution. Much of the knowledge gained during the execution of the framework will come in use for this process.

5 Conclusion

This document provides each EU PRoTECT municipality with a framework to set up, execute and document an evaluation of solutions for a vulnerability in a PSOI. The evaluation consists of an RfI based on the identified vulnerability, an assessment of viable solutions based on the information submitted by providers, an assessment of the operational use of a solution based on scenarios, and a demonstration of a solution. The evaluation relies on the identification and selection of PSOI vulnerabilities found by the five PRoTECT municipalities during the use of the EU Vulnerability Assessment Tool [13].

This document constitutes a starting point for the PRoTECT partners to organise the RfI, evaluate operational use of solutions and perform solution demonstrations in each city.

It is recommended that the practical use of the framework, for other municipalities outside the context of PRoTECT, be determined, for instance on the basis of feedback from the five PRoTECT municipalities and partners who will be using the framework.

References

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

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

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

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

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

[6] ISO standard 31000:2018 series.

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

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

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

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

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

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

[13] PRoTECT Deliverable D2.1 "Manual for vulnerability assessment". March 2019

[14] PRoTECT Deliverable D3.1 “Best Practices and Technologies report”. December 2019

[15] Department for Communities and Local Government UK, Multi-criteria analysis: a manual, January 2009