PRoTECT Webinar: Technology Evaluation Framework

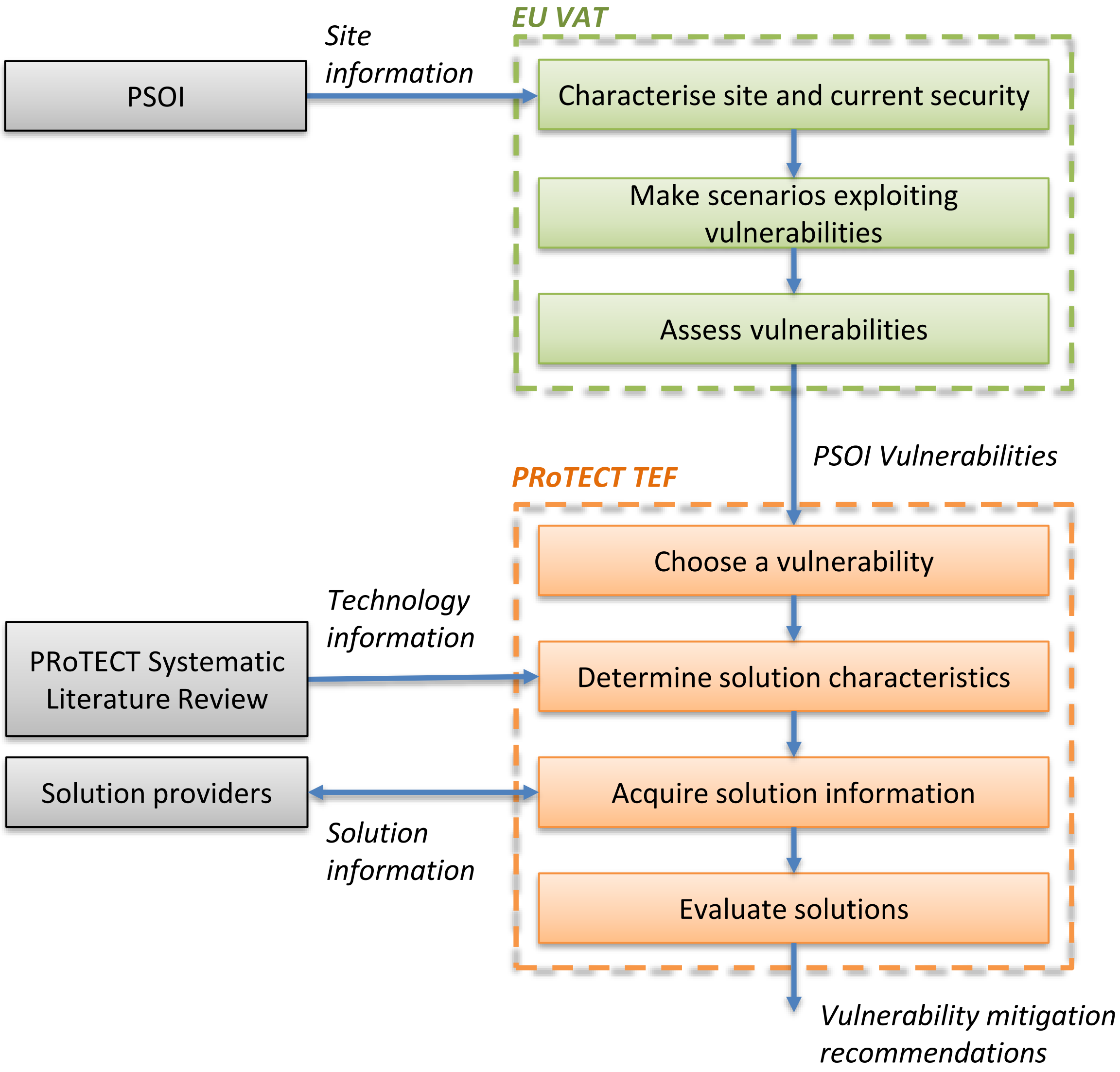
Graeme van Voorthuijsen | Puck van den Brink

PRoTECT is funded by the European Union's ISF-Police Action Grant, under grant agreement no 815356

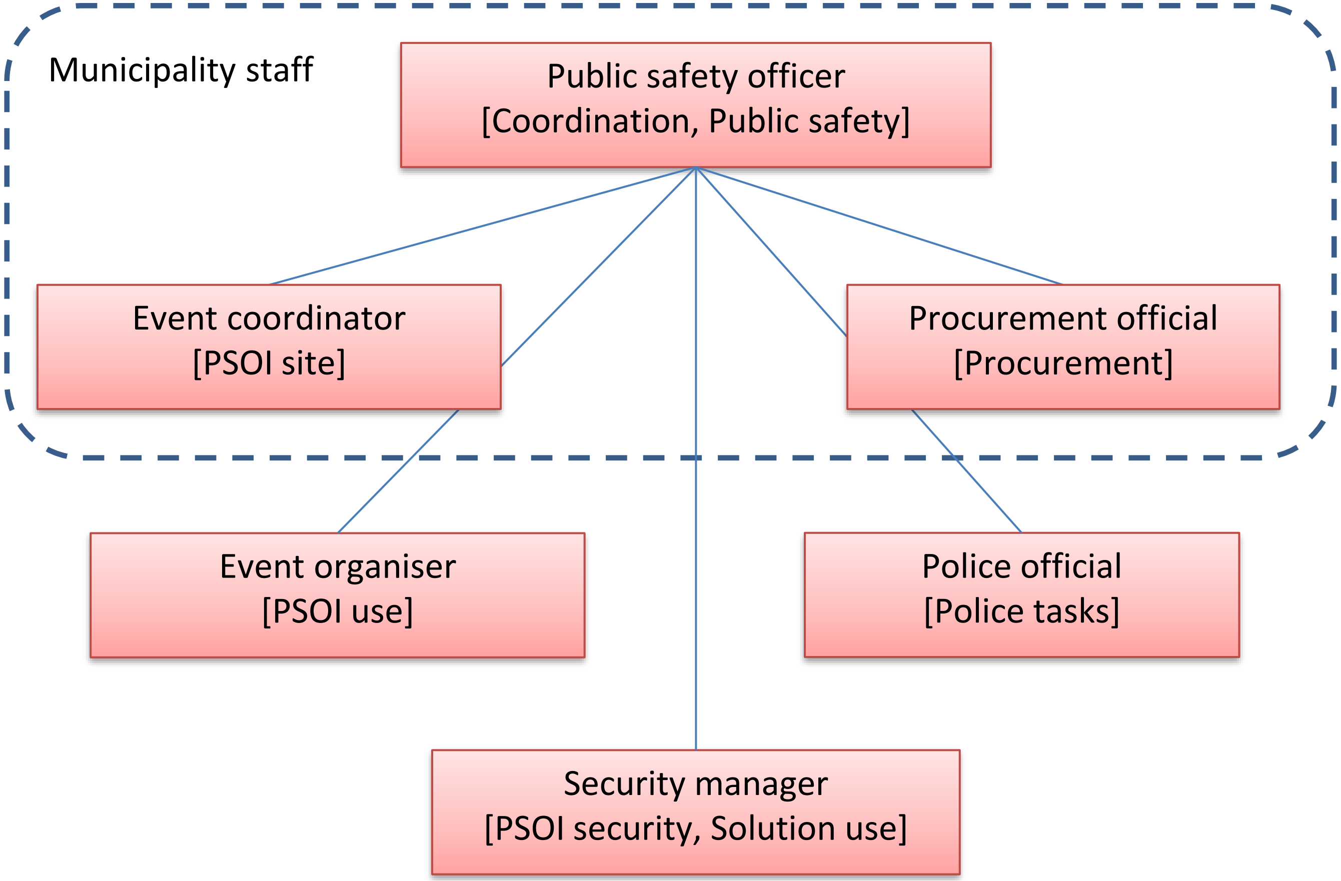
Introduction

- PRoTECT TEF was developed to **evaluate potential technological** solutions for the improvement of public space security regarding the terrorist threat.
- PRoTECT TEF was developed for **municipal staff who are responsible for safety and security in public space** and their stakeholders, such as municipal police, urban planners, security department or crime prevention unit, event organisers, tourism, transport operators, etc.
- PRoTECT TEF addresses one **vulnerability** at a time, requiring a vulnerability study to have been carried out beforehand for a specific Public Space of Interest (PSOI) for instance using the EU VAT (Vulnerability Assessment Tool).
- PRoTECT TEF requires the **formation of a Team of Experts**, including municipality staff, representatives from the police and the event organiser, who in various compositions execute the steps in PRoTECT TEF.
- PRoTECT TEF consists of **8 steps** but it is not necessary to execute all steps for an evaluation (e.g., an evaluation can be based on results from a request for information, a table-top exercise and/or a demonstration).
- **Consider PRoTECT TEF as a toolbox – pick what you need.**

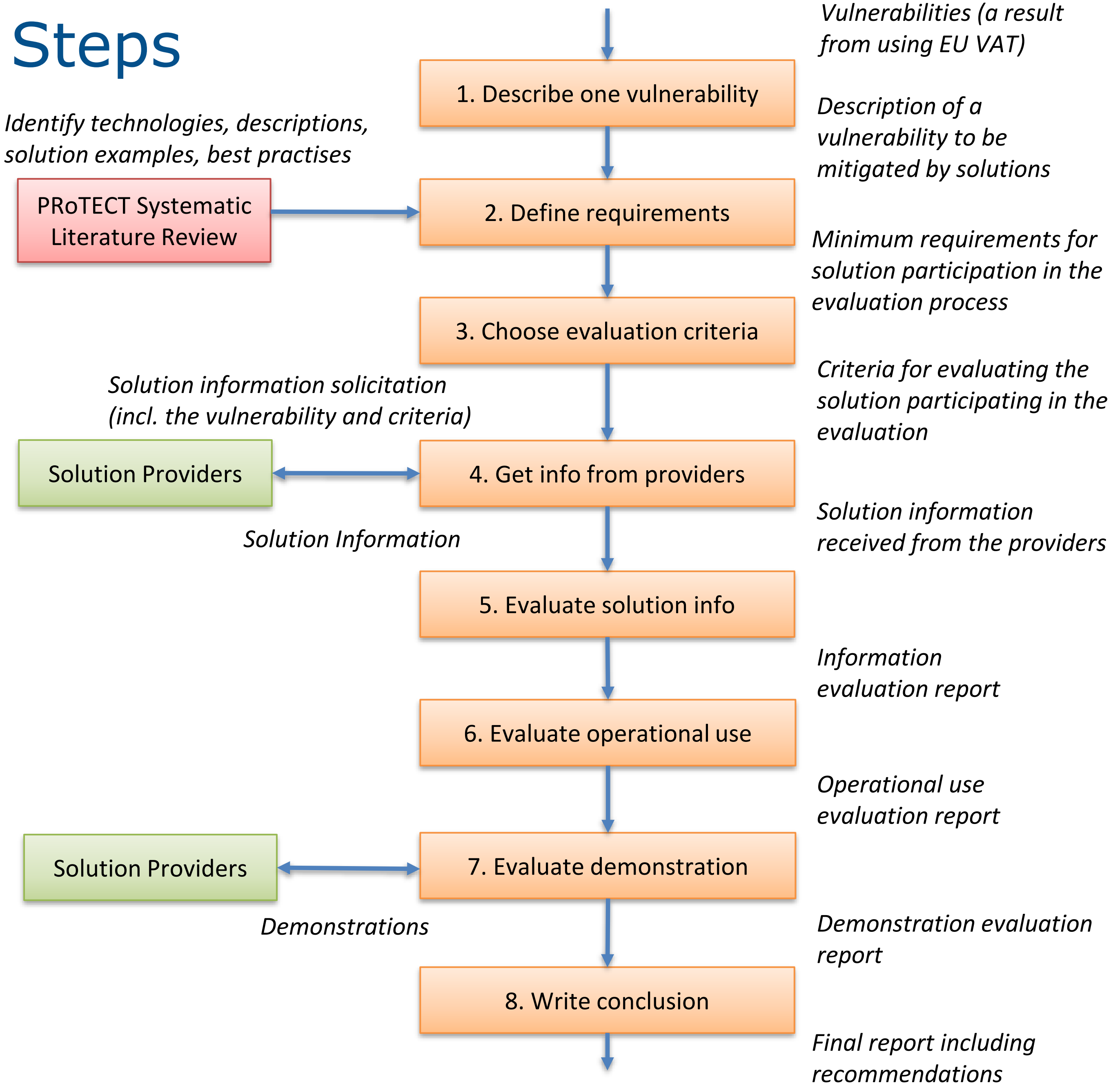
Overview


PSOI
Site information
EU VAT
Characterise site and current security
Make scenarios exploiting vulnerabilities
Assess vulnerabilities
PSOI Vulnerabilities
PRoTECT TEF
Choose a vulnerability
Technology information
PRoTECT Systematic Literature Review
Determine solution characteristics
Solution providers
Acquire solution information
Solution information
Evaluate solutions
Vulnerability mitigation recommendations

Team of Experts



Steps



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, best practises

PRoTECT Systematic Literature Review

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

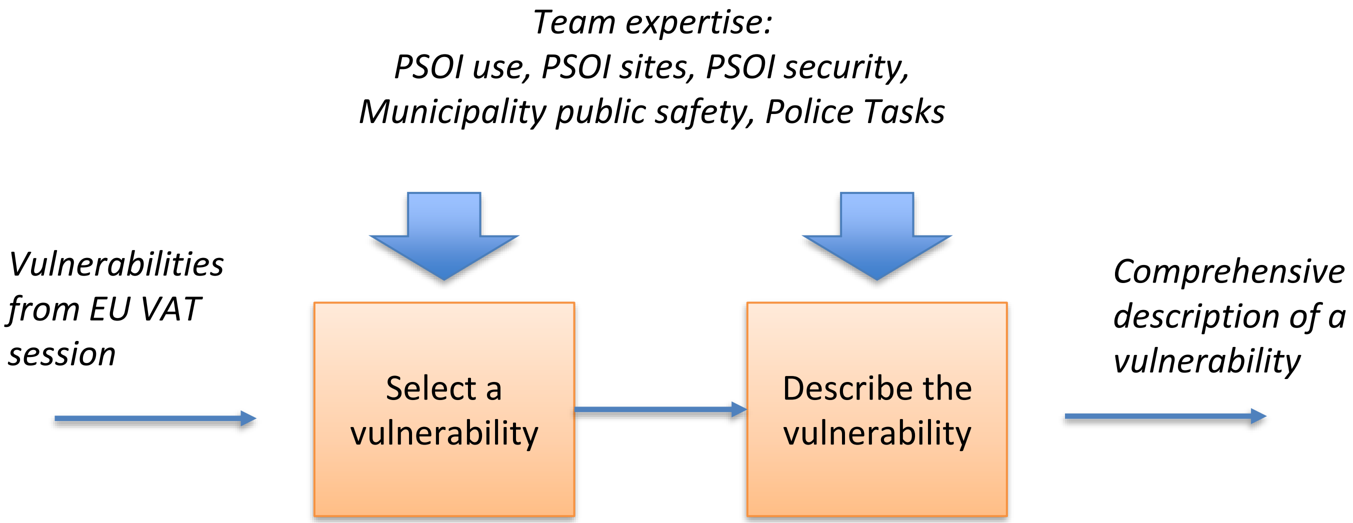
Demonstrations

Demonstration evaluation report

8. Write conclusion

Final report including recommendations

Step 1: Describe the vulnerability



Team expertise:
PSOI use, PSOI sites, PSOI security,
Municipality public safety, Police Tasks

Vulnerabilities from EU VAT session

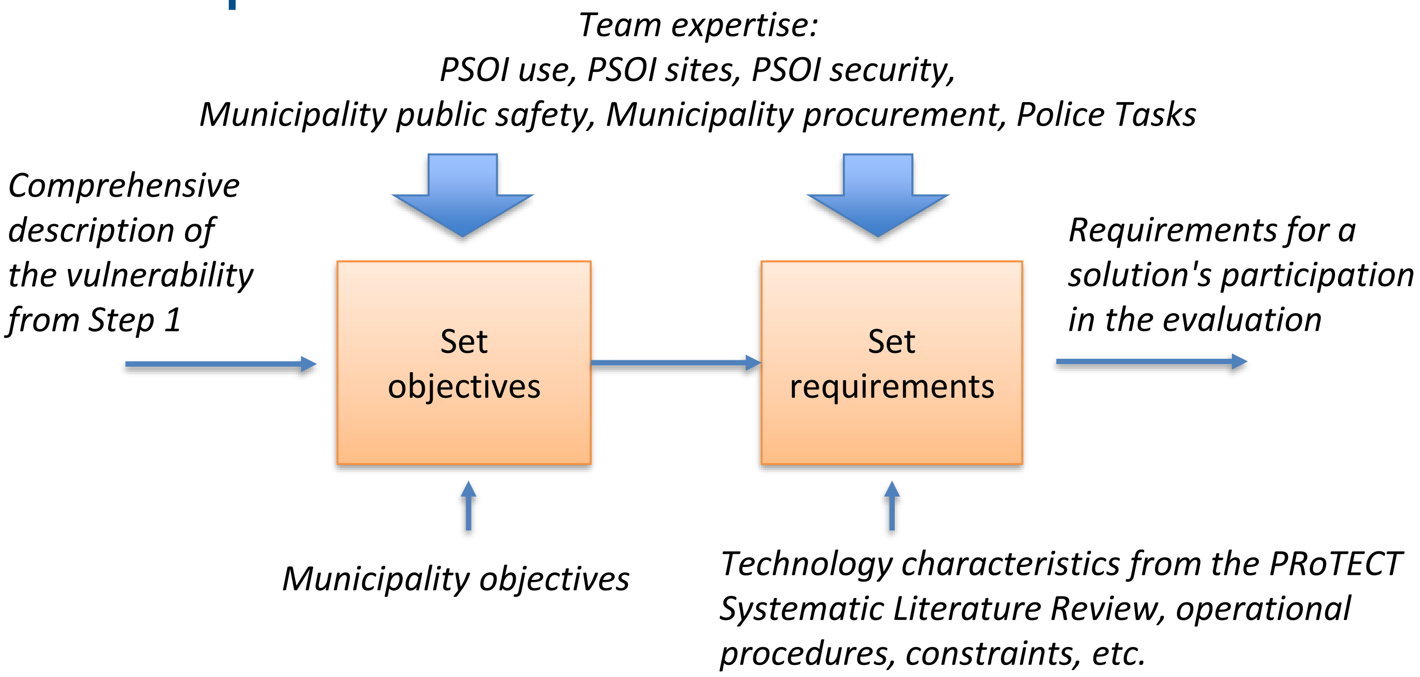
Select a vulnerability

Describe the vulnerability

Comprehensive description of a vulnerability

- Purpose: to choose a vulnerability for which a solution is required, and to describe the vulnerability in such a way that apt solutions can be found.
- The choice for a particular vulnerability could be based on the level of risk involved, uncertainties concerning available solutions, etc.
- The description includes the following parts: venue description (location, event type, visitor characterisation, etc), affected capabilities (e.g., event management, access control, attack detection, etc), attack scenario, desired response scenario, dependencies (influences on attack or response outcome).

Step 2: Define objectives and requirements



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

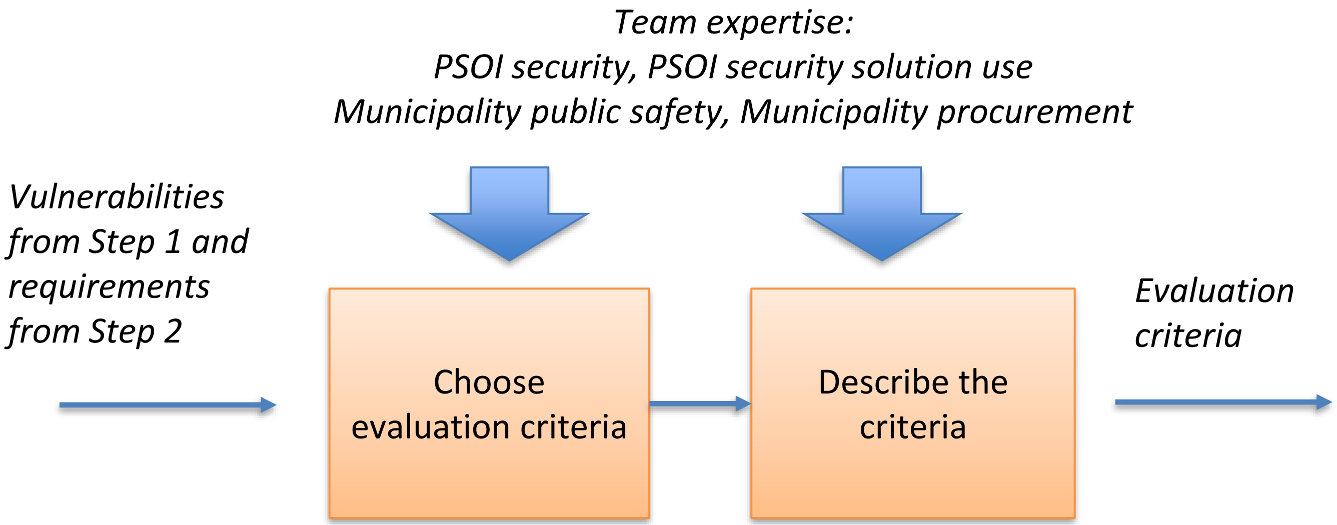
Requirements for a solution's participation in the evaluation

Municipality objectives

Technology characteristics from the PRoTECT Systematic Literature Review, operational procedures, constraints, etc.

- Purpose: determine the general objectives concerning the evaluation (e.g., detect threats earlier, lower response time, etc.) and specify general technology requirements (e.g., regarding operational functionality, interoperability, user operability, compliancy, maintenance, etc) and requirements which must be met by the solution providers (e.g., experience, clearance, capability of giving a demonstration, etc).

Step 3: Choose evaluation criteria



Team expertise:
PSOI security, PSOI security solution use
Municipality public safety, Municipality procurement

Vulnerabilities from Step 1 and requirements from Step 2

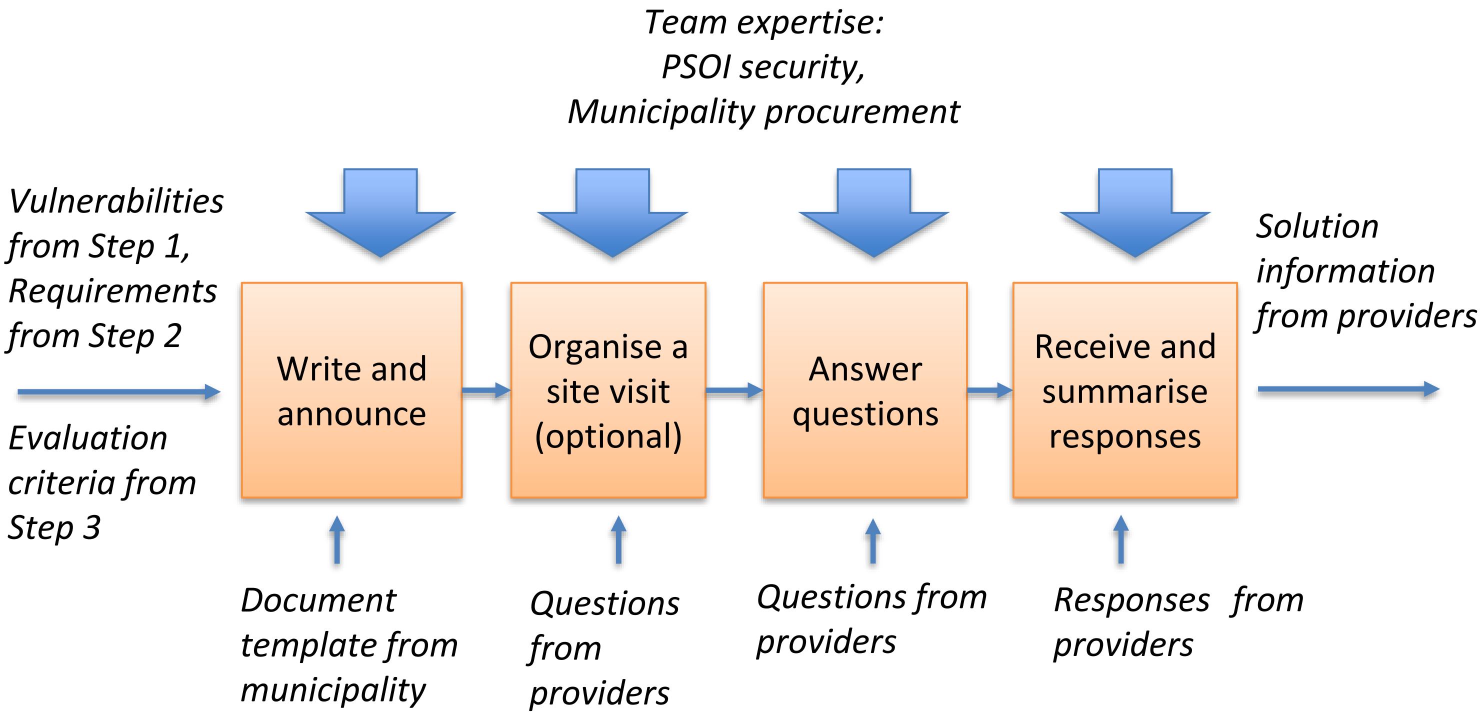
Choose evaluation criteria

Describe the criteria

Evaluation criteria

- Purpose: to determine specific criteria for assessing the suitability of a solution in addressing the vulnerability.
- Criteria may concern costs, physical characteristics, compliancy, performance, operability, interfacing, training, maturity, etc.
- Attention must be paid to criteria quality (e.g., non-redundant, suitable for all solutions considered, clear, measurable) and applicability (e.g., relevant to the vulnerability, in line with the goals and requirements).
- Generally, choosing 5 to 10 criteria should suffice.

Step 4: Gather solution information



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

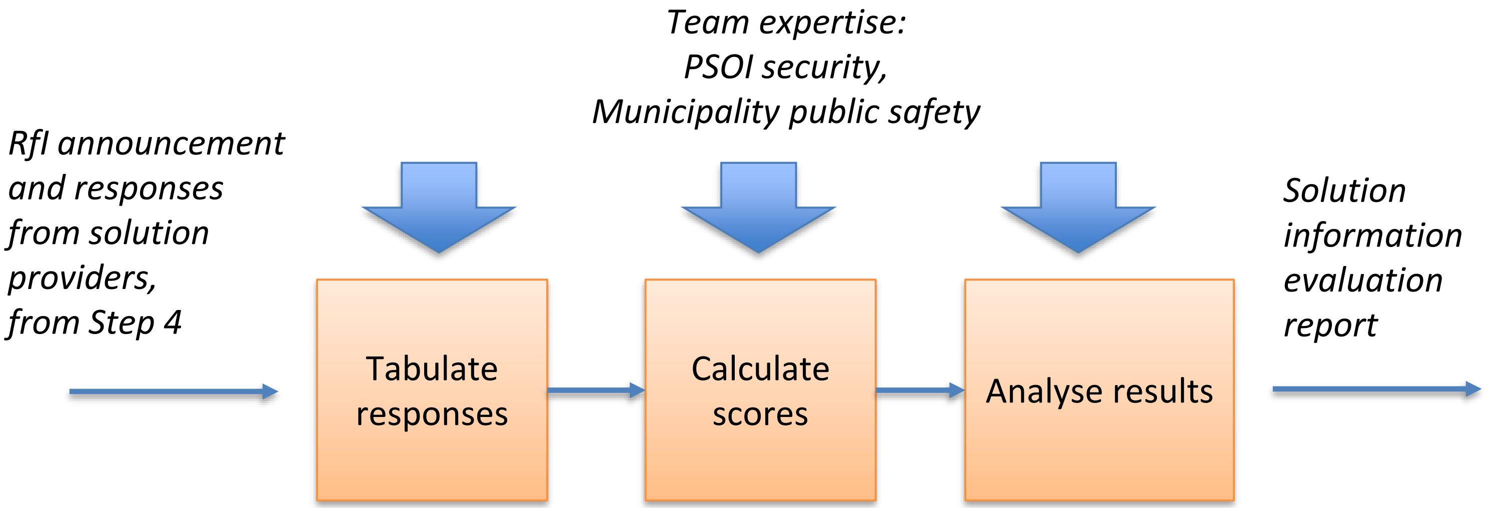
Questions from providers

Questions from providers

Responses from providers

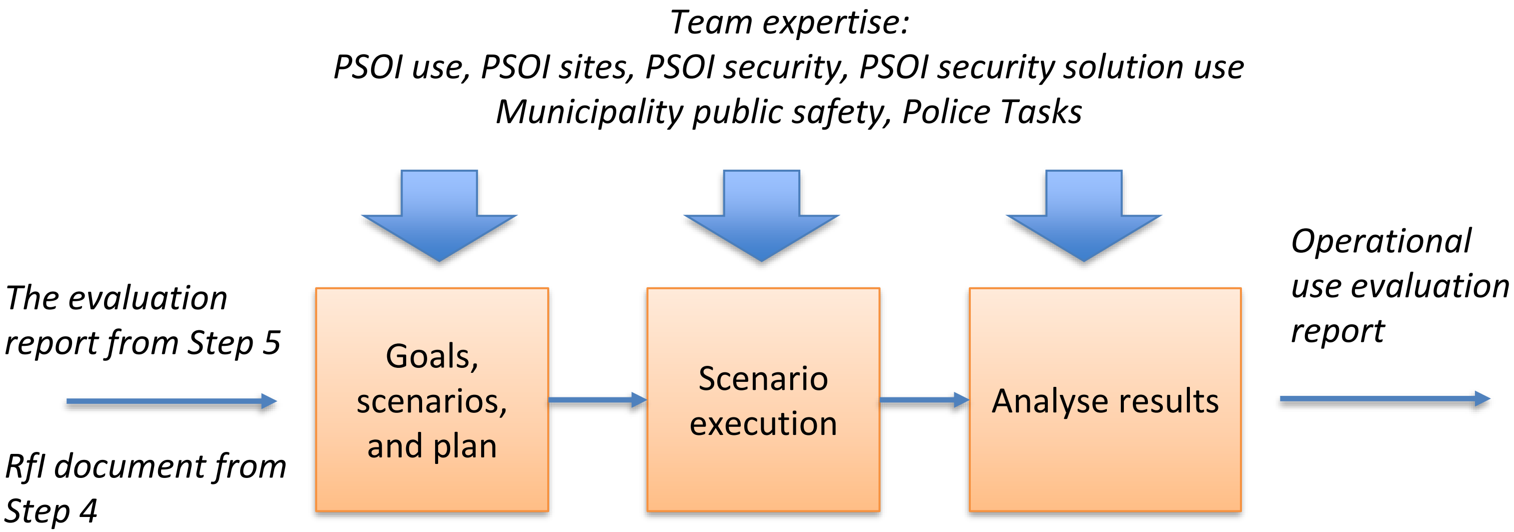
- Purpose: to conduct a Request for Information (RfI) for gathering information on solutions from solution providers.
- The RfI process includes tasks such as writing an RfI announcement, conducting a site visit (optional), answering questions from providers, and summarizing the responses.

Step 5: Perform solution information evaluation


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

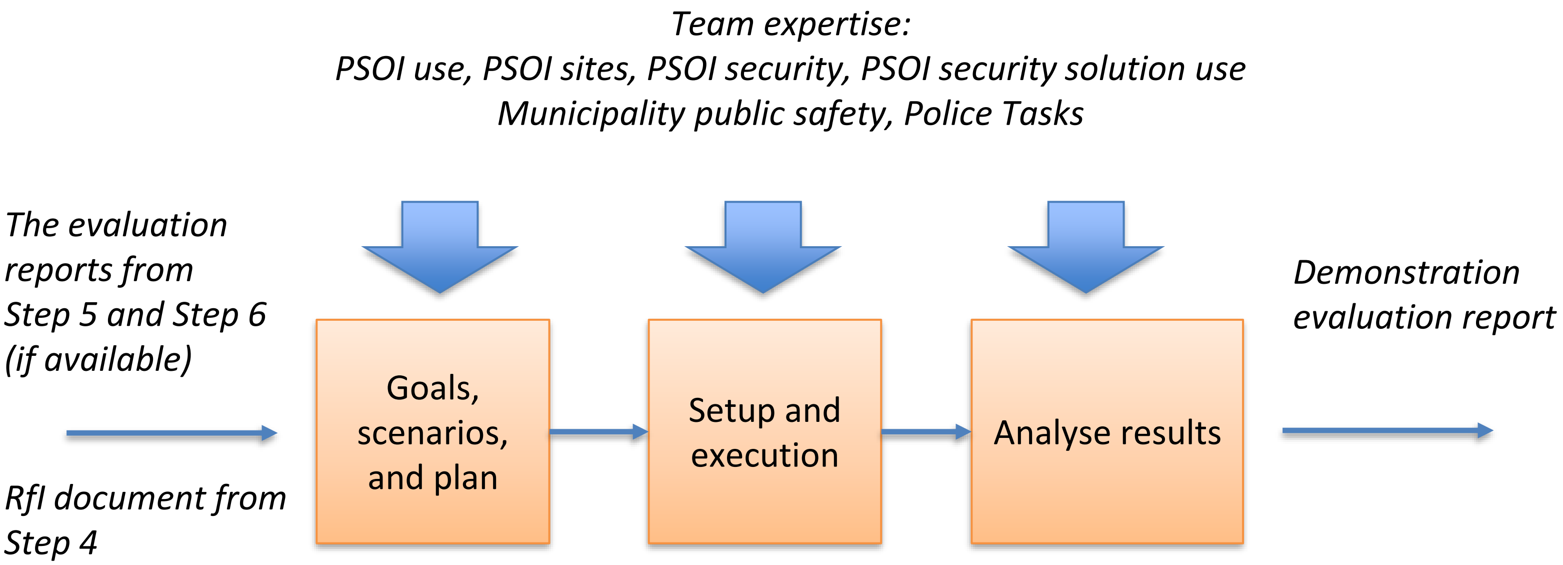
- Purpose: to evaluate the solutions based on information received from the providers.
- The evaluation is carried out using a multi-criteria analysis (MCA) method which includes tasks such as tabulating the information, determining criteria threshold values, assigning weights (optional), calculating scores, analyzing the scores, formulating conclusions.
- This step includes an example.

Step 6: Perform operational use evaluation


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

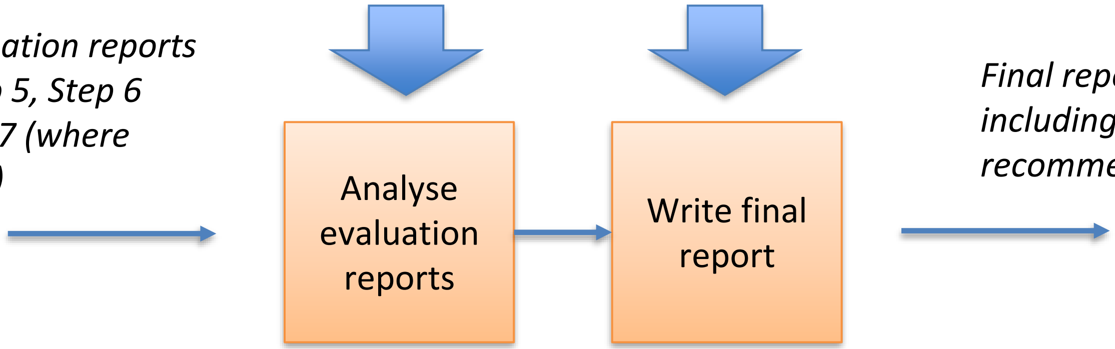
- Purpose: to evaluate the solutions based on an operational table-top exercise.
- The table-top exercise process includes tasks such as setting goals, devising operational scenarios for the exercise, determining the players, planning the exercise, execution of the scenarios by the players, analyzing and documenting the results.

Step 7: Perform demonstration


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

- Purpose: to evaluate the solutions based on a demonstration.
- The demonstration process includes tasks such as setting goals, devising operational scenarios for the demonstration, planning the demonstration with the solution provider, execution of the scenarios in the demonstration by the provider, analyzing and documenting the results.

Step 8: Analyse results and write report



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

- Purpose: to form a conclusion regarding the suitability of a solution based on the results of the evaluations carried out.
- This step produces a final report in which the following subjects are covered: a description of the vulnerability, documentation of each of the TEF steps carried out (those involved, actions taken, etc), analysis considerations, assumptions, etc., degree to which goals were met, conclusions and recommendations, next steps (e.g., a procurement process).

PRoTECT TEF Results

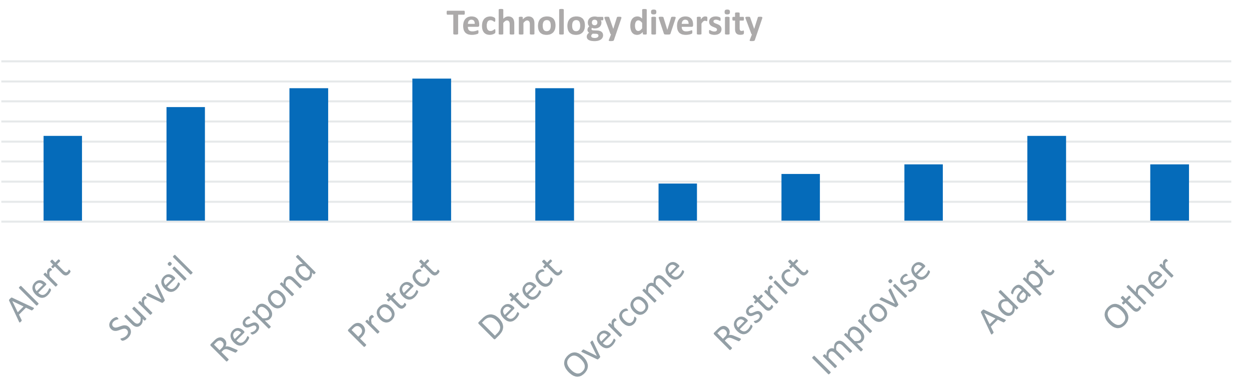
- PRoTECT TEF can lead to these evaluation reports:
  - The solution information evaluation (Step 5) – evaluation of printed matter on the solution (RfI results)
  - The operational use evaluation, if executed (Step 6) – evaluation of enacting hypothetical operational scenarios based on the use of the solution (tabletop session results)
  - The demonstration evaluation, if executed (Step 7) – evaluation of a live demonstration of the solution (demonstration results)

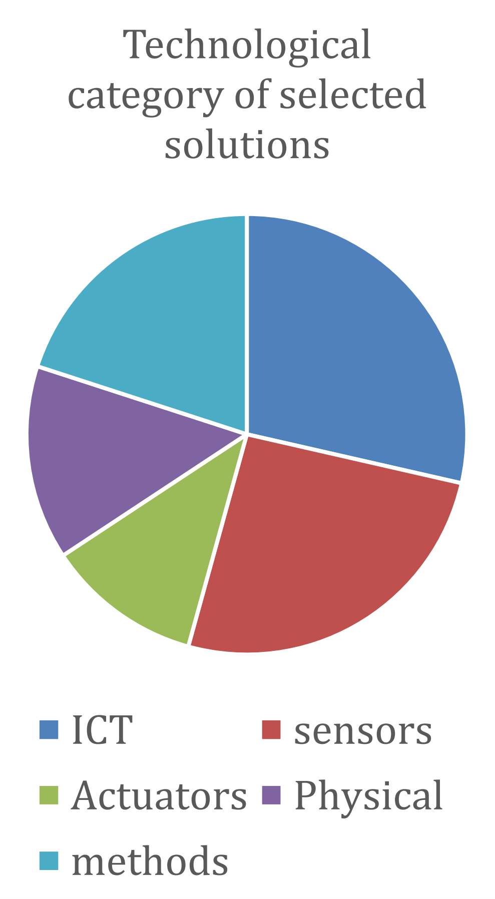
- Each evaluation report generally describes evaluation goals, evaluation criteria, analysis results, conclusions and recommendations.

- PRoTECT TEF leads to a final report which discusses the results of the evaluation reports produced, including the degree to which the objectives (set in Step 2) concerning vulnerability mitigation have been met, and any recommendations concerning the acquisition or future use of the solution(s) for the municipality.

PRoTECT TEF use summary

- For practical reasons, one RfI process was organised for all 5 municipalities involved in PRoTECT. Each municipality contributed vulnerabilities for which solutions were solicited from providers.
- In total, the RfI process resulted in 32 unique solutions being offered for mitigating various vulnerabilities of the municipalities' PSOIs.
- The solutions were evaluated using a method derived from the ProTECT TEF, which resulted in 23 candidates being selected for technology demonstrations organised by each of the 5 municipalities.





Thank you!

There is an opportunity to ask questions after the last presentation in this webinar.

Contact information:

Puck van den Brink
puck.vandenbrink@tno.nl

Graeme van Voorthuijsen
graeme.vanvoorthuijsen@tno.nl

End of presentation

PRoTECT is funded by the European Union's ISF-Police Action Grant, under grant agreement no 815356