



PRoTECT 2nd seminar: Technology Evaluation Framework

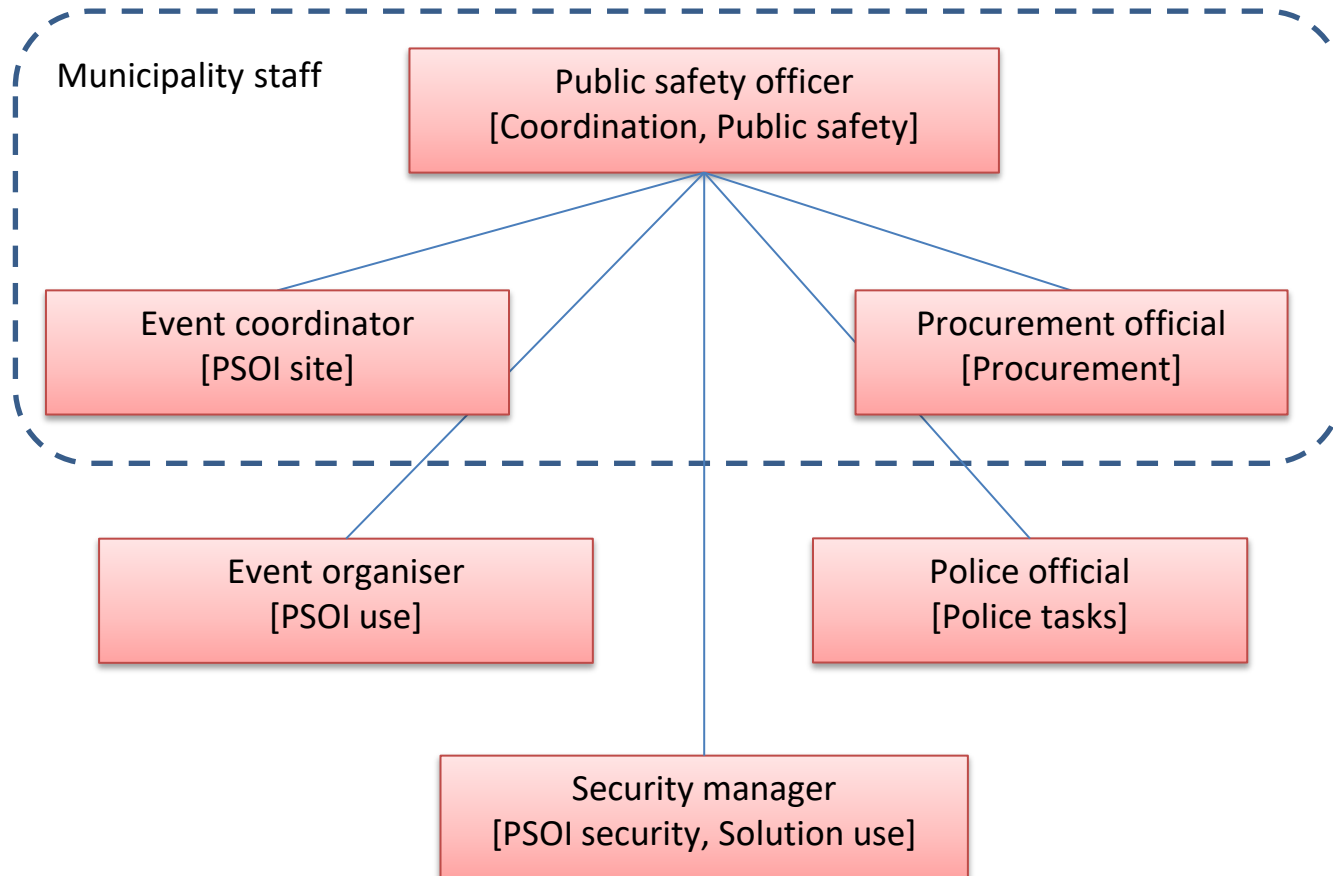
Graeme van Voorthuysen | Puck van den Brink



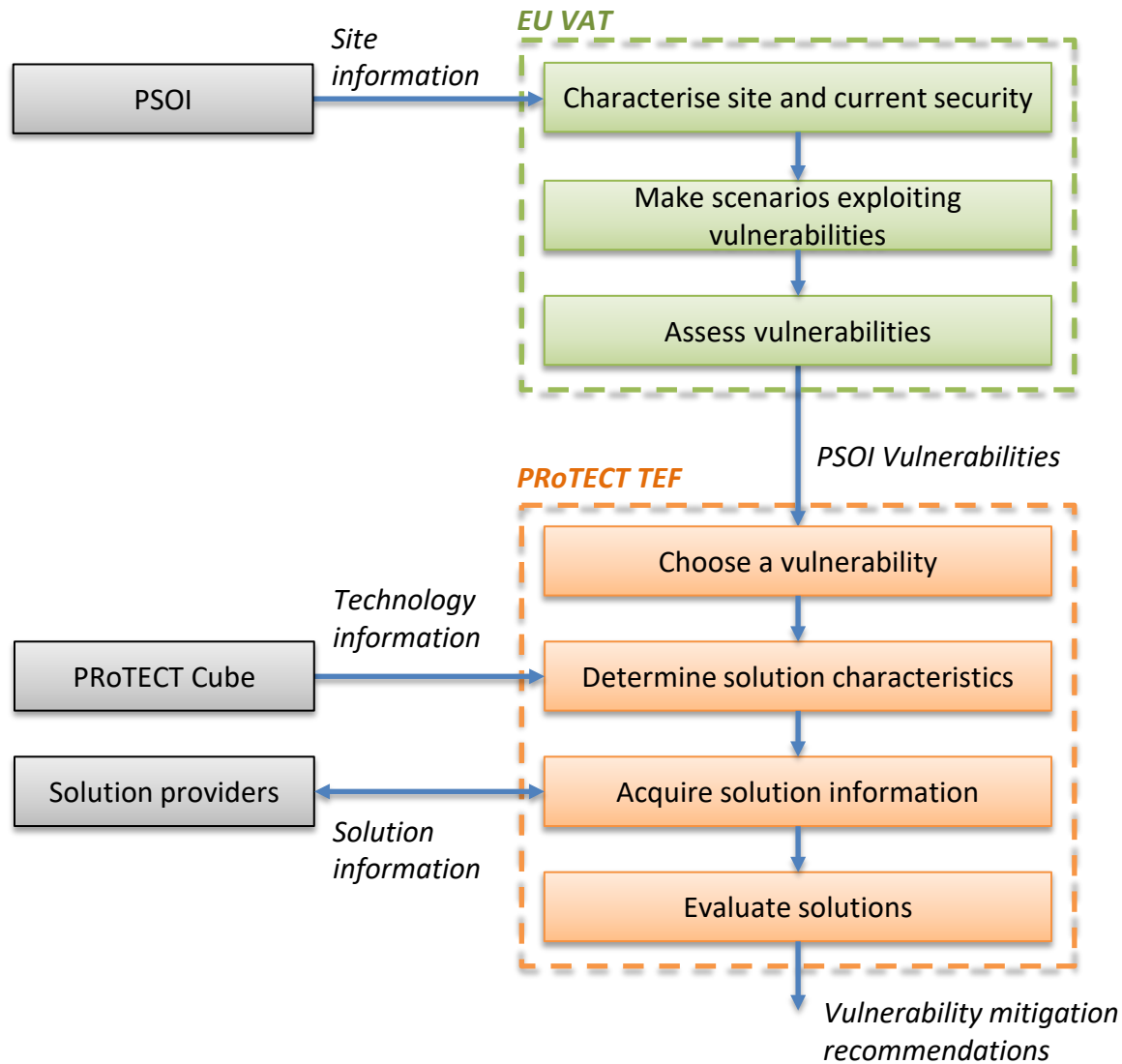
Introduction

- PRoTECT TEF was developed to evaluate potential technological solutions for the improvement of public space security.
- 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.
- PProTECT TEF requires the formation of Team of Experts, who in various compositions execute the steps.
- PRoTECT TEF requires a vulnerability study to have been carried out beforehand, for instance using the EU VAT (Vulnerability Assessment Tool), and considers the evaluated solution in the light of one specific vulnerability.
- PRoTECT TEF consists of 8 steps, some of which are optional.

Team of Experts



Overview



Steps

Identify technologies, descriptions, solution examples, best practises

PRoTECT Cube

Solution information solicitation
(incl. the vulnerability and criteria)

Solution Providers

Solution Information

Solution Providers

Demonstrations

1. Describe one vulnerability

2. Define requirements

3. Choose evaluation criteria

4. Get info from providers

5. Evaluate solution info

6. Evaluate operational use

7. Evaluate demonstration

8. Write conclusion

Vulnerabilities (a result from using EU VAT)

Description of a vulnerability to be mitigated by solutions

Minimum requirements for solution participation in the evaluation process

Criteria for evaluating the solution participating in the evaluation

Solution information received from the providers

Information evaluation report

Operational use evaluation report

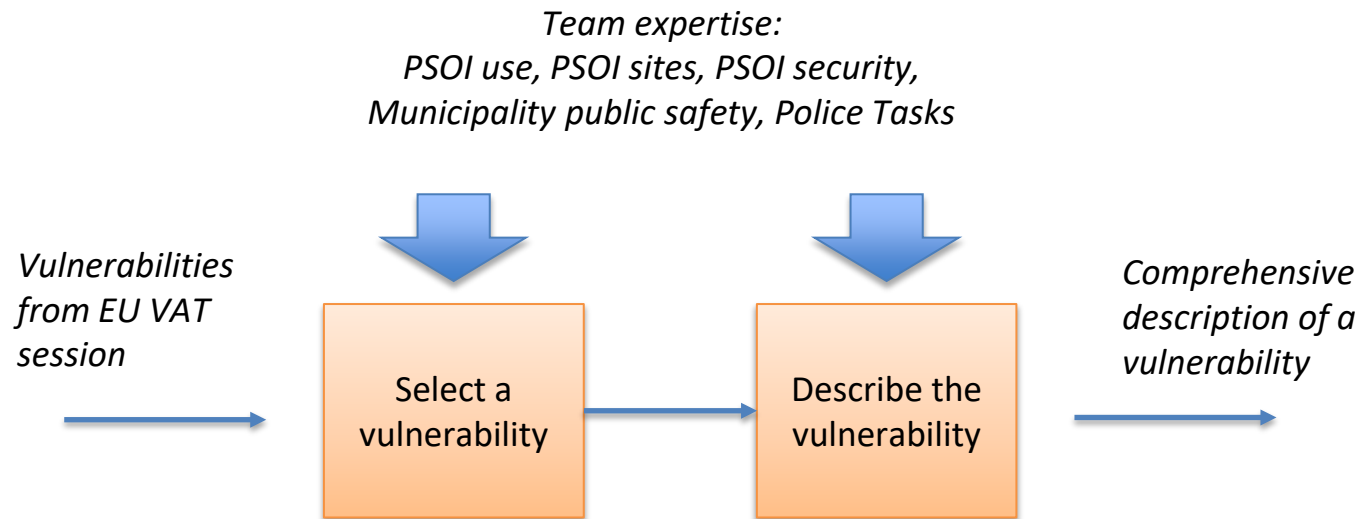
Demonstration evaluation report

Final report including recommendations

TEF Results

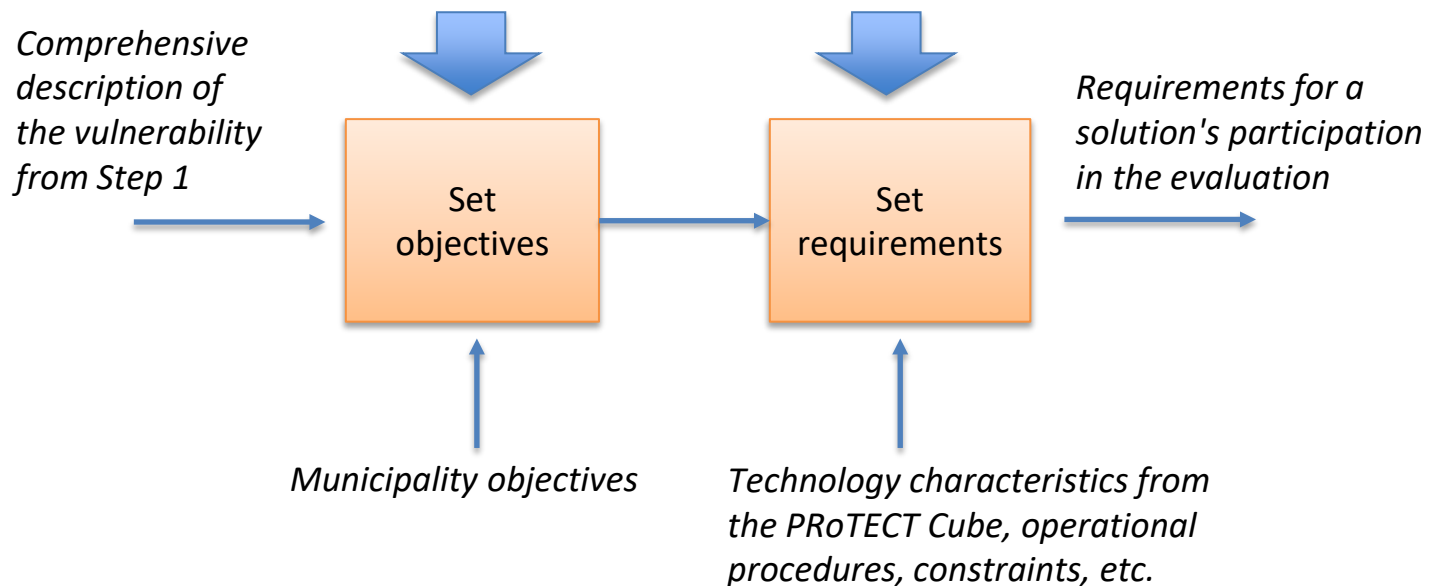
- TEF leads to evaluation reports:
 - The solution information evaluation (Step 5) – evaluation of printed matter on the solution (RfI results)
 - The operational use evaluation, if executed (Step 6) – evaluation of enacting hypothetical operational scenarios based on the use of the solution (tabletop 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, criteria, analysis, conclusion and recommendations.
- TEF leads to a final report which discusses the results of all evaluation reports, the final conclusion regarding the degree to which the objectives concerning the mitigation of the vulnerability have been met (set in Step 2) and any recommendations concerning the acquisition or future use of the solution for the municipality.

Step 1: Describe the vulnerability



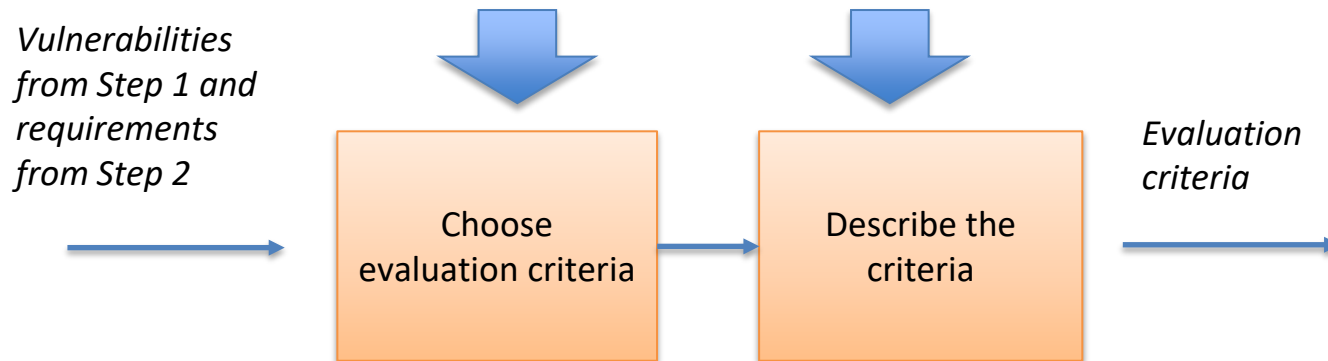
Step 2: Define objectives and requirements

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

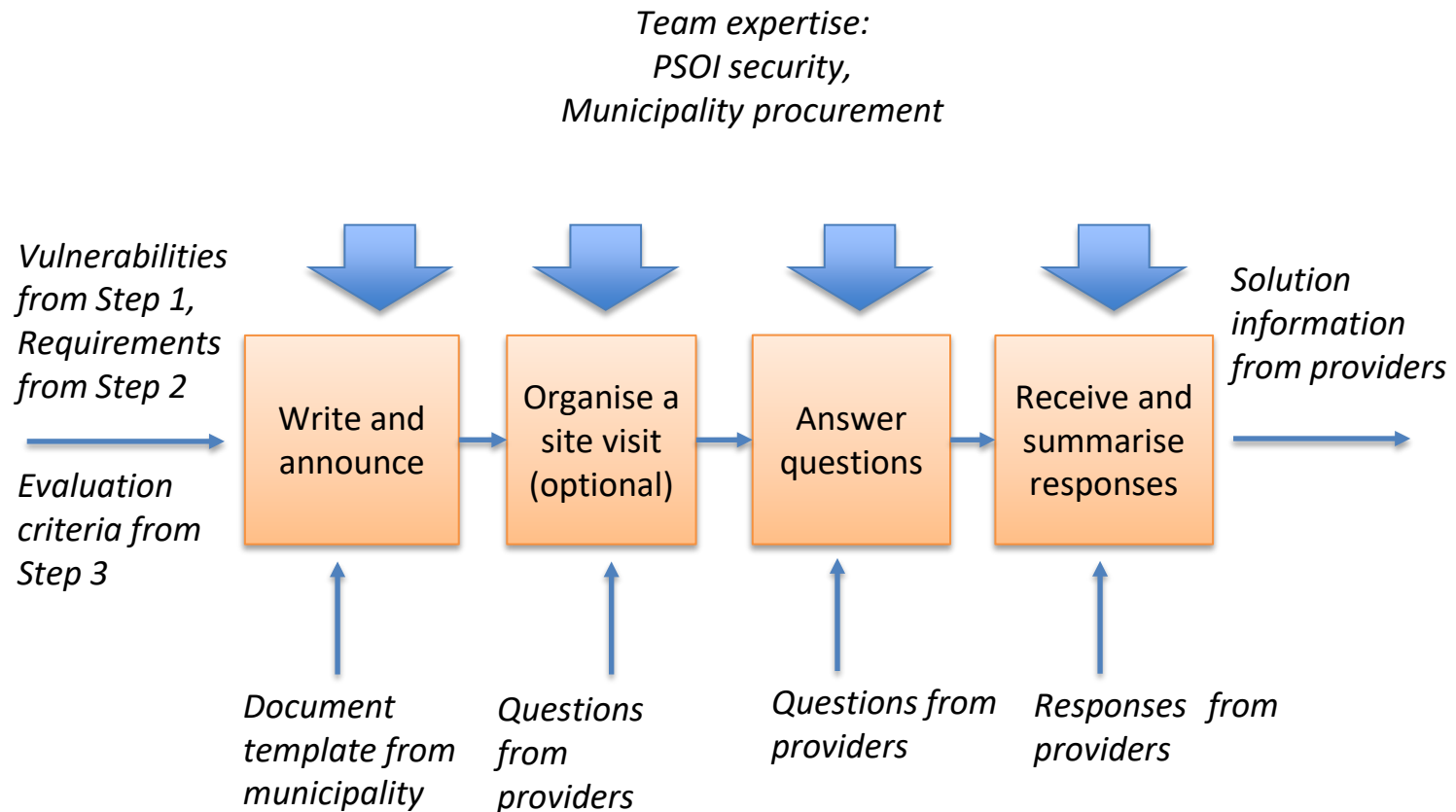


Step 3: Choose evaluation criteria

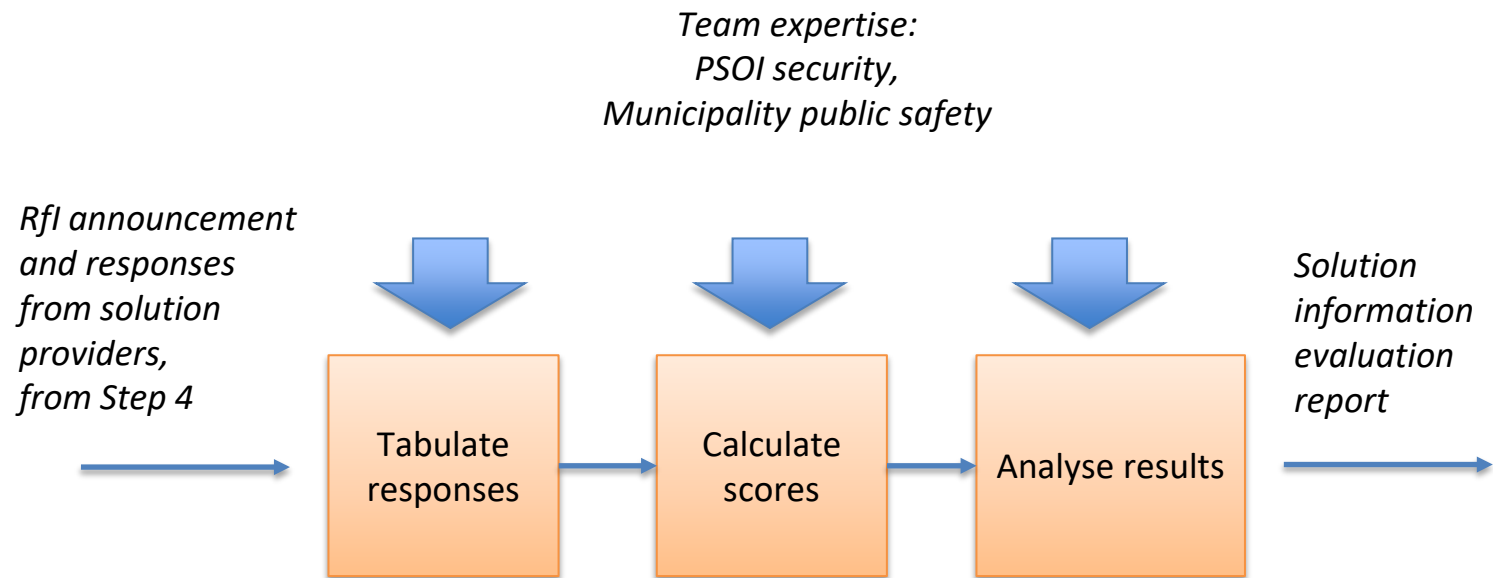
*Team expertise:
PSOI security, PSOI security solution use
Municipality public safety, Municipality procurement*



Step 4: Gather solution information

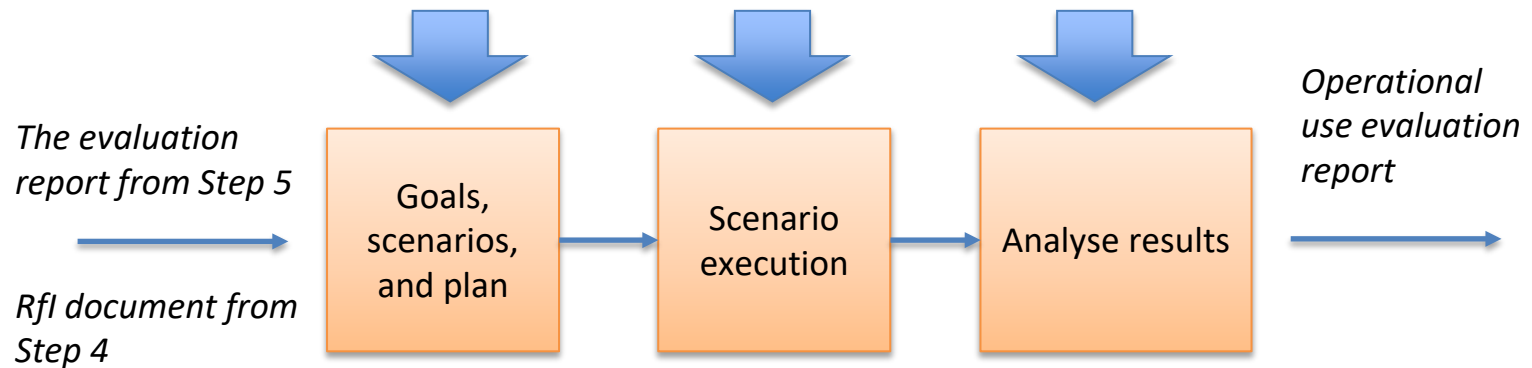


Step 5: Perform solution information evaluation

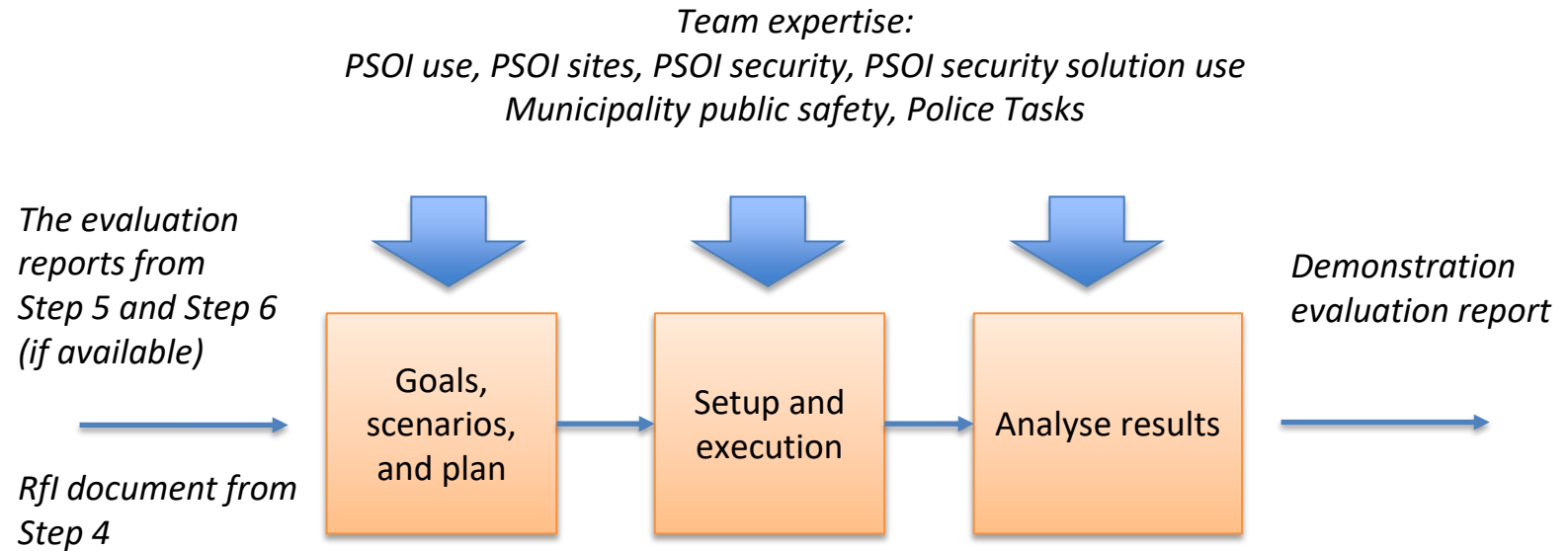


Step 6: Perform operational use evaluation

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

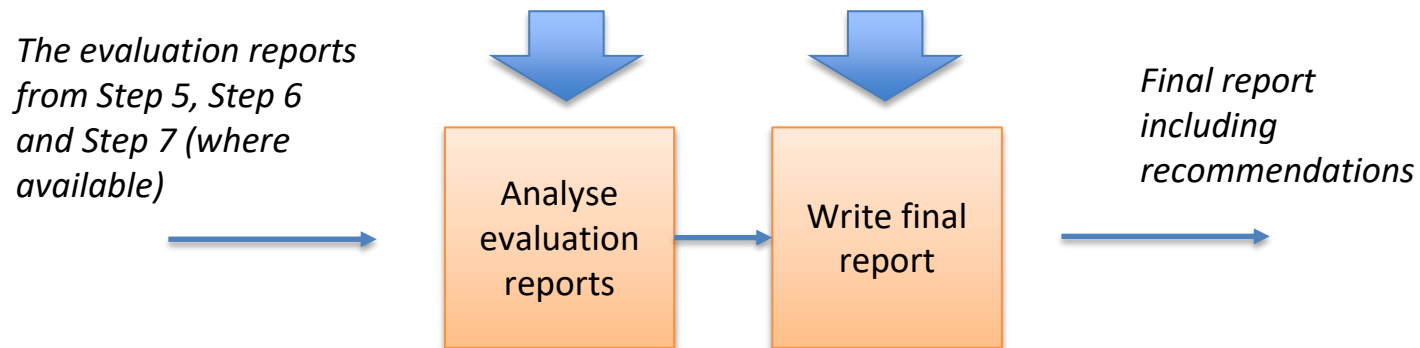


Step 7: Perform demonstration



Step 8: Analyse results and write report

*Team expertise:
Municipality public safety*



End of presentation