# HOUSES OF WORSHIP VULNERABILITY ASSESSMENT CHECK LIST

This vulnerability assessment process is based on the Vulnerability Assessment Check list (VAC) of the DG Home but has been modified and simplified. The completed document must be submitted to the Task Leader by the 7th of August. Task Leaders are available to carry out specific training on how to compile the document until the 20th of July.

Instructions for filling the document:

1. Identify the team that will carry out the assessment reducing to the minimum necessary number of people involved, to respect the principle of "need to know".
2. Contact by phone (do not use other means, for example, email or Whatsapp) the Task Leader and verbally communicate the name of the religious building that you intend to analyze to allow the Task Leader verify that two partners are not analyzing the same place of worship. Please also inform the Task Leader of the name of the assessment team to allow him to verify if the principle of the “need to know” has been respected.
3. Contact the person in charge of the place of worship where you will make the assessment and ask for his permission by signing the appropriate form.
4. Read carefully and try to mentally find an answer to the questions that are inserted in Annex 1 – Questions, before starting to fill the document, and remember that the Annex 2 - PROTECT Instructions gives more detailed information about how to use the VAC (from which this table is created). If you decide to read that document, please keep in mind that Steps 4 (Consequence and probability, page 27) and 5 (analysis and results page 28) of Annex 2 - PROTECT Instructions shall not be carried out and the relevant items shall not be included in the table below.
5. Do the assessment.
6. When the assessment is done, please send the form to the Task Leader. If photos were taken during the assessment, they should not be submitted (to keep the document anonymous). When you send the email, do not save it. If saved automatically, delete it.
7. After having read your document, the Task Leader will organize a videoconference with you through Microsoft Teams (or another tool considered reliable from the point of view of cyber security). In this conference the results of the analysis will be discussed, and the photos taken will be shown by screen sharing.
8. After the meeting and after having received the consensus by the Task leader, destroy all the material related to the analysis.

**This table should be compiled avoiding any reference that would allow vulnerability to be associated with a specific place (for example, name of the religious building or streets or names of municipalities). Sensitive information (e.g., photos of the areas / building or names of the buildings or location, even the country) must not be shared here (both in the physical and non-physical criticalities).**

Physical criticalities

|  |  |
| --- | --- |
| Main site | Existing security measures (natural or emplaced) (4) |
| Church / mosque / synagogue (please do not write the name or the address of the House Of Worship, but only write their type,for example; church, mosque, synagogue. Nothing else) | Alert: |
|  |  |
| Activity (1): | Surveillance: |
|  |  |
| Date and time~~s~~ of the Activity: | Respond: |
|  |  |
|  | Protect: |
| Site being assessed (2) |  |
| Please do not write the name or the address, but only describe the area | Detect: |
|  |  |
| Phase (3): | Overcome: |
|  |  |
| Expected crowd density | Improvise: |
|  |  |
|  | Restrict: |
| Vulnerability assessment |  |
| Date of assessment: | Adapt: |
|  |  |
| Other: |
|  |
| Scenario per threat type (5) |
| Physical attacks (without any weapon or tool): |
|  |
| Hate crimes (racist behave or racism based vandalism): |
|  |
| Fire arms attack (e.g., small calibre pistol or semi / full – automatic rifle – AK47): |
|  |
| Sharp object attack (e.g., knifes, machete, other sharp and blunt objects): |
|  |
| Vehicle attack (e.g., use of vehicle as a weapon by ramming large crowds): |
|  |
| IED – Explosives (e.g., left / concealed in objects or goods): |
|  |
| PBIED – Explosives (e.g., explosives concealed on a person (suicide or carrier): |
|  |
| UAVIED – drone (e.g., remote controlled device – explosive or CBR threats carried and |
|  |
| VBIED – explosives (e.g. explosives concealed inside a vehicle (or its cargo): |
|  |
| Chemical attack (e.g., threat object concealed in goods or carried items – ex. Teargas canister): |
|  |
| Biological attack (e.g., threat object concealed in goods or carried items): |
|  |
| Radiological attack (e.g., threat object concealed in goods or carried items): |
|  |

**Footnotes accompanying the record template:**

1) Please describe if there are specific activities happening (like festival, market, or something else), and when this activity occurs. The date and time is important to be aware if an activity is occurring regularly or is incidental.

2) You should specify if you are evaluating the main site (that corresponds to phases 5 and 6) or the surrounding (that corresponds to phase 1, 2, 3 and 4). For more information about what is intended by a phase, please read the footnote below.

3) The type of area (as given in the EU VAT, e.g., Phase 1 - Access roads to venue, Phase 2- parking and transport, Phase 3 – Approach to Venue, Phase 4 – Arrival at Venue, Phase 5: Venue Security – No Access Control, Phase 6 – Venue Security – With Access Control). **Note that Phases 1 to 4 correspond to the surrounding sites. Phase 5 or phase 6 are to be used for the main site. Therefore, you must compile as many tables as there are phases in which the building of worship is divided.**

4) A description of the exiting measures on the site (natural or emplaced)

5) A description and examples of the threat types are given on the Phase tab and a scenario description based on ~~(a)~~ vulnerability (lacking or insufficient existing measure); if not applicable, describe why; if applicable, describe what the threat does to what/whom and how this is achieved (name the exploited weakness); if more than one viable scenario is imaginable for a threat type, add extra lines under the threat type. Before completing this part, try to mentally answer the questions you find in Annex 1.

Non-physical criticalities

COMMUNICATION:

|  |  |
| --- | --- |
| Question | Answer (please describe precisely) |
| Is the holy place of worship perceived divisive, part of the conflict or an instigator of conflict?  |  |
| Cyber-attack (e.g., identity theft of the site and related pages on social networks; theft of sensitive data); |  |
| Crisis management communication (e.g., The impact of the community immediate responsive reaction; spontaneous individual reaction, outcry language. Are they a stimulus that triggers uncalled-for conflict and instability?) |  |

INTERACTION WITH THE CONTEXT

|  |  |
| --- | --- |
| Question | Answer (please describe precisely) |
| Use of the contexts (e.g., are there visits to the place of worship? How often?) |  |
| Level of interaction and participation in public spaces? (Such as participation in civil public events by community stakeholders. What interaction with law enforcement?) |  |
| Level of interaction with other HOW (e.g., Is there any networking group with other religious leaders in your community to share best practices and intelligence information regarding safety and security. Is there any monitoring open-source intelligence information related to threats against the HOW~~s~~ for criminal, cybercrime, and terrorist activities?). |  |

AWARENESS OF THE RISK

|  |  |
| --- | --- |
| Question | Answer (please describe precisely) |
| Security plan (e.g., Is there a security manager? Do you have a list of the major vulnerabilities of the HOW? Is a safety & security plan prepared for demonstrations in public spaces? |  |
| Security guards Training (e.g., volunteers security guards, HOW’s members or even a dedicated professional security staff); |  |